CANADIAN FORCES COLLEGE/COLLÉGE DES FORCES CANADIENNES
NATIONAL SECURITY PROGRAMME 2

AN ASSESSMENT OF THE APPLICABILITY OF NETWORK CENTRIC WARFARE CONCEPTS TO THE CONTEMPORARY SECURITY ENVIRONMENT AND THE VIABILITY OF THE CANADIAN FORCES' CURRENT NCW CONSTRUCT

By/par Colonel R.G. Mazzolin
NSP 2

June 2010

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

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

CONTENTS

Abstract

The Canadian Forces have pursued a strategy of transformation to position the organization to prosecute operations in the future environment. Central to this transformation is the requirement to invest in a network enabled capability to increase operational effectiveness and provide a force multiplier to conventional forces. Both objectives defined in the Canada First Defence Strategy (CFDS) and tenets of Canadian Forces (CF) transformation advocate the importance of a network enabled capability empowered by a robust Communications, Command, Control, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) infrastructure. CF institutional focus and planned investment however, do not support this representation and the question that arises is whether NCW concepts hold credibility with current CF/DND leadership or whether the current CF organization is adequately postured to effectively deal with NCW concepts.

Proponents of network centric capabilities argue that such an approach contributes to the efficiency and effectiveness of modern military operations. Initial network centric capabilities were originally envisioned in the context of traditional cold war threats and conventional conflict. In light of the evolving doctrine and policies aimed at positioning conventional militaries to fight counterinsurgencies, terrorist networks and other non traditional threats, often in urban environments, some observers question the relevance of the effectiveness of network centric concepts to such an environment. Others also assert that an excessive emphasis on technology may be inappropriately driving the nature of military operations, and that modern Western militaries' high reliance on technology creates potential vulnerabilities that adversaries may be in an increasing position to exploit. This paper addresses this fundamental concern as a vehicle to identify the critical issues that must be considered in the transformational development of a military construct designed to deliver such effects and subsequently assesses the DND/CF posture in this area.

The paper asserts that the application of network centric capabilities to the contemporary operational environment remains relevant and serves as a key enabler to transformation however, CF development in this area remains slow and the CF capability

development strategy defined in the CFDS along with associated funding and acquisition activities, remains focused on the development of a traditional, kinetically based force structure. Capital funding allocated to the C4ISR capability area is disproportionally low relative to that of traditional environmental activities. Although the respective environments independently pursue C4ISR capabilities, it is done in the absence of a departmental champion and associated mature overarching operational construct and technical architecture. Progress has been made over recent years toward implementing a systems development methodology, however, there is a requirement for it to mature in order to be effective. In the absence of a coherent operational and doctrinal construct, integration with platforms planned for procurement and interoperability between the respective environments and strategic systems will be difficult to achieve.

There are also institutional challenges in terms of systems development, engineering, sustainment, acquisition, human resources and training that must be considered. In order for DND to address these issues, it requires an organization and associated processes postured to manage these responsibilities. In addition, existing government processes in the area of acquisition and human resource management are not suited to the management dynamic of such a rapidly evolving discipline.

In summary, the paper will demonstrate that C4ISR capability, as a key operational enabler, has not been adequately developed to ensure CF Transformation success and in light of the recognized benefits that the NCW concepts provide to contemporary operations, the CF requires an enhanced institutional resource commitment and revised organizational structure focused on the provision of a robust C4ISR development capability in order to actualize NCW enablement, a major component of CF transformation. This paper will address this thesis in three parts. First, it will assess the value of the contribution of NCW capability to the contemporary operating environment by considering the breadth of potential operational roles that CF elements would engage in; namely Air to Air, Land based Maneouvre, Special Operations, Theatre Air Missile Defence, Split Based Operations and Strike related activities. The paper will demonstrate the transformative value of NCW concepts enabled by a robust C4ISR infrastructure as a force multiplier for a military of modest means to maximize military effect. Next, in light of the central focus that Afghanistan has had in the recent Canadian military culture, the paper will identify and address concerns regarding the continued applicability of NCW in the contemporary operational environment and confirm that notwithstanding some potential concerns associated with their implementation in complex operating environments such as that faced in Afghanistan, such challenges, if handled with care do not diminish the tremendous potential value of such contributions. The paper will highlight that the identification of such concerns however, form critical elements of a revised management construct that must be invoked in order to effectively manage the institutional implementation of C4ISR as a unique capability in the CF. Finally, the paper will consider the existing CF NCW related development and management structure and associated C4ISR funding and acquisition activities and confirm that it is not yet postured to profit from the potential transformational benefits afforded by its implementation.

Part 1 - Introduction

A significant volume of literature highlights the inter-related concepts of Network Centric Warfare (NCW), Network Enabled Capabilities (NEC), Network Enabled Operations (NEO) and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and these concepts have been identified as key components supporting the transformation of modern militaries.[1] Transformational concepts centre on the implementation of technologies that have the potential for large scale disruptive or dislocational effects on military weapon systems, organizations and operational concepts. Much of this evolution is the product of tremendous developments in the advancement of technologies and operational concepts brought about through the evolving international security environment[2]. In order for military forces to effectively operate in the modern battlespace, combat effectiveness of existing forces must be maximized by establishing a position of advantage through decision superiority. This is enabled through the development of a primarily joint, distributed, network centric force structure capable of rapidly collecting, synthesizing and processing information through the application of sophisticated technologies and related doctrine, training and acquisition. To that end, various CF transformational initiatives being developed include activities designed to develop such capabilities.

Current Canadian NCW concepts represent in large part, derivatives of US based concepts adapted to specific CF circumstances. This position is qualitatively articulated and not based on extensive research regarding potential benefits and challenges.[3] A more fulsome development of the Canadian concept of NCW must be based on what Canadian authorities deem to represent the CF's role in the future security environment. Such developing concepts as JIMP (Joint, Interagency, Multinational and Public) and 3D

[1] Alberts, David S. and John J. Gartska, and Frederick Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd (Revised), Washington, D.C.: CCRP, 2000.

[2] US Government CRS Report RL32238, Defense Transformation: Background and Oversight Issues for Congress, Ronald O'Rourke.

[3] Michael Thomson and Barbara Adams, Network Enabled Operations: A Canadian Perspective, DRDC Toronto No. CR-2005-162, 13 May 2005.

(Defence, Diplomacy, Development) are topical and continue to contribute to the maturation of NCW related capability development within the CF.[4]

The challenge associated with capability development in this complex discipline relates to the development of a comprehensive conceptual framework. Much related terminology is used interchangeably by various nations, environmental elements and organizations thereby creating confusion. To that end, prior to engaging in further development of the subject, the various definitions used in this paper will be clarified.

Network Centric Warfare

The concept of Network Centric Warfare (NCW), which promotes the application of innovative information age capabilities in the execution of warfare, is central to progressive warfighting concepts by modern nations.[5] The institutional embracement of this approach has been categorized in contemporary military writing as a Revolution in Military Affairs (RMA), representing a fundamental change in the conduct of military related activities and whose implication has the implicit effect of rendering obsolete conventional concepts and approaches to warfare.[6]

The first articulation of the term was offered in 1997 by Admiral Jay Johnson (USN), the Chief of Naval Operations (CNO) where he amplified this emerging conceptual construct when he stated that the “US military was undergoing a fundamental shift from platform-centric warfare to that of network-centric warfare”.[7] The contention being that the traditional “platform-centric” approach to warfare whereby military entities

[4] Ibid.

[5] The US DoD defines NCW as “An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.” David S. Alberts, John J. Gartska, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd (Revised), Washington, D.C.:CCRP, 2000),2.

[6] Vice Admiral Arthur K. Cebrowski, (USN), a principal proponent of NCW theory and development reinforced this view by stating: “For nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war.” Arthur K. Cebrowski and John J. Gartska, “Network-Centric Warfare: Its Origin and Future”, Naval Institute Proceedings, January 1998; http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; Internet.

[7] Admiral Jay Johnson. Address at the US Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD, 23 April 1997, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=Get RDoc.pdf&AD=ADA420277.

via soldiers, armoured fighting vehicles, aircraft and ships ostensibly function as independent elements in the traditional physical battle-space, and as a result are not in a position to efficiently collaborate, share information and consequently coordinate and synchronize activities so as to effectively execute mission objectives. Admiral Johnson had articulated the view that the character of the military and its employment of technology had both evolved to the extent that the focus of military operations should shift from a platform-centric type of warfare to a network-centric type of warfare. In such a construct, the various physical elements comprising the military force are linked together through the use of networking technologies to more rapidly and effectively share information, coordinate and synchronize respective effects to act in unison and provide a combat effect that is greater than the simple sum of the respective entities; in effect, serving as a "combat multiplier".

Networking in itself is not a new concept as military organizations have employed various means of communications throughout history. However, this reinforced emphasis of the impact of networking technologies on military operations is largely a result of increased conceptual and programmatic development of cooperative engagement capabilities whereby sensors, decision support systems and shooters were increasingly linked together to share real-time data and collectively see the same image and engage the enemy collaboratively. Recognition of parallel developments in the increased application of technology in society, industry and business has had an analogous impact on the military. To that end, Vice Admiral Cebrowski emphasised this point by stating that "Here at the end of a millennium we are driven to a new era in warfare. Society has changed. The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not".[8]

This position was predicated on the view that the impact of advances of information technology had on the commercial sector during the 1990's would logically follow in the military environment. It was offered that the conceptual structure of such a revised network centric environment would comprise three components: sensor grids,

[8] Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origin and Future", Naval Institute Proceedings, January 1998; http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; Internet.

transaction or engagement grids; and a high quality information backplane. These components would then be supported by automated command and control processes to increase the speed with which decisions could be taken.[9] It must be reinforced however, that notwithstanding the increased emphasis on technology, the human element is a key element of the network centric concept and arguably the most important element of any military organization, networked or not.

Initial US interest in the NCW vision has been the "promise to bring operations to a successful conclusion more rapidly at a lower cost" in addition to shifting the nature of operations away from attrition to a war-fighting style that is characterized by speed of command and self synchronization.[10] The Department of Defence C4ISR (Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance) Cooperative Research Program (CCRP) further developed the vision of NCW toward the implementation and operational realization of an NCW enabled force. In doing so, the CCRP articulated four tenets of NCW:

a. A robustly networked force improves information sharing.

b. Information sharing enhances the quality of information and shared situational awareness.

c. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.

d. These in turn, dramatically increase mission effectiveness.[11]

The CCRP further developed nine governing principles of NCW: information superiority, shared awareness, speed of command, self-synchronization, dispersed forces, de-massing of resources, deep sensor reach, ability to alter initial conditions, and compressed operations.[12]

[9] Ibid.

[10] David S. Alberts, John J. Gartska, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd (Revised), Washington, D.C.:CCRP, 2000),2.

[11] Department of Defense, Network Centric Warfare Report to Congress, 27 July 2001, 4-1. Internet, http://cio-nii.defense.gov/docs/pt2_ncw_main.pdf.

[12] Department of Defense. Office of Force Transformation, 8.

C4ISR

Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) may be viewed as an integrated set of functional components enabling a comprehensive approach to operations, and thus represents the "enabling component" of the NCW capability.[13] As indicated in the reference, this definition supports the higher level collection of C4ISR capabilities, as identified in the C4ISR Capability Development Strategy that encompasses the concepts, the people, the connectivity, the information systems, the sensors, and the tools in support of and required to achieve effective C2 and awareness across the entire spectrum of CF operations through the timely attainment, generation and distribution of trusted and relevant information.

[13] Within this context, the Canadian Forces definition is: "C4ISR is a concept for guiding integrated capability development as applied to the elements of Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance". Canadian Forces "C4ISR Capability Development Plan" distributed under 1180-1 (D Mil CM), 31 August 2009.

Part 2 - Benefits of a NCW Enabled Force

Introduction

This chapter identifies and addresses the benefits of NCW capabilities. Although the asymmetric nature of recent operations in Afghanistan and Iraq have leveraged the employment of NCW related capabilities significantly, the scope of these operations represent only a portion of the broad spectrum of military mission areas. To that end to more fully identify the benefits that NCW concepts bring to the modern battlespace, a number of issues will be considered in this chapter. First, a number of cognitive/social enhancements will be identified. These include issues involving multi-echelon C2, the impact of sensors upon the development and execution of commander's intent and the effect of improved shared situational awareness on logistics and support activities as key enablers to combat functions. These provide the basis for the broader consideration of NCW contributions across the range of operations that the CF may prosecute, which include Air to Air, Land based Maneouvre, Counter SOF, Theatre Air and Missile Defence, Strike and Split Based Operations. The chapter concludes by emphasizing that the growing evidence supporting NCW contributions to operations manifests itself in increased information sharing and shared situational awareness, the relationship between shared situational awareness and synchronization/collaboration, and the relationship between collaboration/synchronization and mission effectiveness.

Cognitive and Social Enhancements

The provision of national security in the "Information Age" speaks to a complex environment whereby the very nature of military operations have become increasingly complex as modern military forces face immediate and real time media coverage, terrorists, regional instability, insurgencies, asymmetric warfare and adversaries who have access to and make effective use of sophisticated high technology equipment. Largely, Canadian conceptual development of NCW represents an extension of US based concepts to particular CF circumstances.

In order to assess the benefits of NCW concepts in supporting contemporary and future CF operations ranging from war-fighting to peacekeeping, humanitarian and nation building operations, it is critical to understand the cognitive and socialization processes that underpin them.[14] The management and conduct of highly complex activities are much less suited to traditional industrial-age approaches of de-constructing activities into smaller manageable, deterministic, predictable pieces. To that end, C2 activities carried out by NCW enabled forces closely align with many characteristics of complex activities; non-linear interaction, decentralization, and self-organization.[15]

Combat power effectiveness is increasingly a function of the ability to access and share information at high speed. Recent military operations have demonstrated that truly joint forces with capabilities that are comprehensively integrated can better exploit the path dependency characteristics[16] of NCW operations. Additional advantages that can be expected from the employment of C4ISR systems in support of NCW operations include the flexibility to employ smaller sized units that are lighter and can move faster requiring less logistical support and have the possibility of carrying out missions using innovative tactics more effectively at lower costs. As an example, the employment of such capabilities led to the development by US forces of "swarm tactics" whereby networked troops in a widespread, highly mobile battlefield environment could maintain mutual situational awareness even when out of sight of one another and could spread out into smaller more dispersed elements, move quickly and avoid the need to dedicate resources to protect the rear. In the event that one unit got into trouble, the accompanying elements could be quickly rallied to "swarm the enemy" from many directions at the same time.[17] In that light, the benefits of the implementation of C4ISR systems in the conduct of NCW

[14] Michael Thomson and Barbara Adams, Network Enabled Operations: A Canadian Perspective, DRDC Toronto No. CR-2005-162, 13 May 2005.

[15] Murray Gell-Mann, "What is Complexity?" Complexity, John Wiley and Sons, 1995, Vol.1, No. 1.

[16] Path dependency represents a characteristic that minor deviations in initial operational conditions will manifest themselves in disproportionately different outcomes. In that light, military forces need to establish initial conditions favourable to their objectives, with the objective of establishing a tempo of operations and associated change the adversary cannot match. Dan Cateriniccia and Mathew French, "Network Centric Warfare: Not There Yet," Federal Computer Week, 9 June 2003, http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp.

[17] Arquilla, John and David Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND 2001.

operations include a number of considerations; greater difficulty for the enemy to attack a widely dispersed formation; knowledge of friendly force locations reduces fratricide; and swarming permits attacks to be oriented directly into the core of an enemy formations' command and control structure, undermining the ability to effectively act in its own defence by operating from within as opposed to fighting on the periphery of the formation. These characteristics apply in a broader context beyond the physical domain, into the cognitive and cyber domains and are scalable in implementation from deployed small units to larger formations.

To that end, additional changes present themselves in terms of how individual soldiers and staffs interact on the battlefield. For example, when a unit encounters difficulties in battlefield operations, they can contact the formation command post where staff input the problem into an on-line chat forum where it can be addressed or "swarmed" by experts located geographically about, distant from one another, such as distant "expert" headquarters linked through cyberspace in the home nation. Aside from reducing sensor-to-shooter times, the use of such of systems enables troops and staffs in deployed units to carry out local intelligence analysis of raw data from sensor systems. This alleviates the need to process information in the home nation and associated turn around time for the analysis to arrive back in theatre.

Benefit of Multi-Echelon C2 (Collaborative OODA)

A shared operational picture enables the Formation level Command Posts to assist in performing C2 (Collaborative OODA). Formation Command Posts are able to use the common operational picture to rapidly identify a situation where elements of friendly forces may be out of position and provide guidance to reposition them. Such rapid collaborative C2 enables forces to relocate themselves to support the Commander's operational plan.[18]

Shared Knowledge of Commander's Intent

[18] Ibid.

Digitization and networking has enabled staffs to share information regarding commanders' intent to the lowest levels, resulting in the ability of sub-units to develop better shared knowledge of commander's intent (in the cognitive domain). Subordinate troops monitoring the battle are able to understand the big picture and develop a better understanding of what is happening on the battlefield.[19]

Sensors (UAV, JSTARS) contributions to Increased SSA

The ability to employ organic sensors and exploit sensors such as JSTARS and additional networked sensor systems enables commanders to visualize the enemy and terrain and see and strike quickly before the enemy is prepared or when he does not expect to be attacked. Canadian Forces Experimentation Centre experiments conducted as part of ROBUST RAM in Alberta during April 2002 and OP GRIZZLY, the G8 summit conducted at Kananaskis in June 2002, assessed the paired capability of Medium Altitude Long Endurance (MALE) UAVs, Vertical Take-Off UAV (VTUAV), Mini UAVs, integrated into the Canadian Forces Command and Control System working in association with the Coyote armoured fighting vehicle EO/IR imagery reconnaissance platform. This arrangement demonstrated a significantly enhanced range, resolution and consequent situational awareness for the grouping, enabling greater situational awareness and ability to gain vital operational information.[20] Further exercises such as the Pacific Littoral ISR Experiment (PLIX) conducted July 2003, and the Atlantic Littoral ISR Experiment (ALIX) in August 2004, further confirmed the qualitative results highlighted earlier.[21]

Improved SSA to Logistics and Support

Greater SSA plays a key role in increasing the effectiveness of logistics and support units and creating a force multiplier. For example, increased SSA available to

[19] Ibid.

[20] Lieutenant Colonel S.J. Newton et al, Canadian Forces Experimentation Centre Experiment Report IICDE-001/2002 (Interim), Uninhabited Aerial Vehicle Concept Development and Experimentation, 1 August 2003, p.vi.

[21] Ibid.

logistics and support units improves their ability to find and fix broken and disabled platforms and increase timeliness of repair resulting in increased combat effectiveness. An additional benefit is total asset visibility and anticipatory logistics which provide the ability to employ modular and tailored sustainment approaches resulting in smaller logistic footprints and reduced lift requirements.[22]

More broadly however, is the growing body of evidence[23] that is developing in terms of three major impact areas of NCW:

a. degree of networking contributing to increased information sharing and shared situational awareness,

b. relationship between shared situational awareness and synchronization/collaboration,

c. relationship between collaboration/synchronization and mission effectiveness.

Although an extensive body of quantitative analysis of the impact of NCW/C4ISR enabled forces does not exist, the most compelling evidence presents itself in the form of qualitative results provided through anecdotes arising from high intensity, tactical conflict operations as well as results from various Service and Combined/Joint capability development, experimentation and interoperability exercises.[24] To that end, most of the results reinforced the impact areas cited above. When considering US based activity areas where the CF may be called upon to operate, the strongest evidence acquired was associated with operational activities and environments associated with Air-to-Air, Land Based Maneouvre, Counter Special Operations Forces, Theatre Air Missile Defence, Strike related activities and Split Based Operations. These specific scenarios will be investigated in greater detail in the following pages.

[22] NCW—Emerging Lessons Learned from the First Digital Division, Presentation by COL (Ret) Fred Stein at conference on “Network Centric Warfare: Missions, Needs, Opportunities, and Challenges, ” Washington, D.C.; Oct 21-22, 1999.

[23] Alberts, David et al. Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd (Revised), Washington, D.C.:CCRP.

[24] Ibid.

Air to Air

The implementation of the E-3 AWACS, and in the case of Naval operations, the E-2 Hawkeye in conjunction with Link 16 capability has contributed significantly to the progress that has been made in permitting pilots to self-synchronize efforts, via the ability to talk with one another and controllers positioned on C2 platforms. Pilots have the capability to increase their awareness of the battlespace and, in theory, greatly improve their shared situational awareness (SSA) since they all see the additional information. The operational benefit of employing F15-C aircraft equipped with Link-16 was explored in an Operational Special Project (OSP) undertaken by the U.S. Air Force during the mid-1990s. The JTIDS OSP compared mission effectiveness for voice only versus voice plus Link-16 in a wide range of tactical situations (1 vs. 1 to 8 vs. 16) in day and night operations. Data was collected during more than 12,000 sorties and 19,000 flying hours. In daylight operations, the average kill ratio increased from 3.10:1 to 8.11:1, a 2.61 fold improvement. During night operations the average kill ratio increased from 3.62:1 to 9.40:1, a 2.59 fold improvement.[25]

Land Based Maneouvre

The results from US based exercises, experiments, and analyses that have dealt explicitly with maneouvre highlight both the challenges and benefits of NCW enabled forces. In early experiments, U.S. Army units were challenged to field high performance tactical networks or develop and employ mature Tactics Techniques and Procedures to enable them to fully exploit high quality Shared Situational Awareness. However, advances over the past 15 years have demonstrated through exercises and operations the increased combat power that maneouvre forces employing more mature NCW capabilities can achieve. The discussion that follows clearly highlights the progress the Army has made in understanding both the challenges and the opportunities faced by maneouvre forces in leveraging the power of the network.

[25] Mission Area Director for Information Dominance, Office of the Secretary of the Air Force for Acquisition, JTIDS Operational Special Project (OSP) Report to Congress, December 1997, Headquarters U.S. Air Force, Washington, D.C.

The U.S. Army's Advanced Warfighting Experiments (AWEs) along with development work conducted by Army Battle Laboratories and the Army Research and Development Centers have been instrumental in integrating C4ISR technologies into battlefield operations. These activities have enabled the US Army to gain insight into the feasibility of NCW technologies and the related doctrinal and organizational implications and analytical basis to support the theory of NCW as a combat multiplier.

Among the most significant exercises where quantitative data was captured was the Experimental Force (EXFOR) for the Task Force XXI Army Experimental Exercise.[26]

The Exercise Force prepared for the experiment at Fort Hood by conducting platoon, company, and battalion collective training, as well as a culminating brigade exercise. This training focused significant effort to mastering the hardware and software digitizing the force. A challenge posed by this requirement to dedicate effort to new hardware and software was a reduction in the available time for unit level training.[27] Despite challenges relating to software interoperability problems and the need for adequate training on new C2 systems, the following improvements, relative to previous warfighter experiments were observed:

a. Operational tempo: plan development time at the division-level was reduced from 72 hours to 12 hours, producing a potential 6 times increase in operational tempo.

b. Speed of calls for fire: time required for processing calls for fire was reduced from 3 minutes to 0.5 minutes, again a six times increase in the ability to bring fire support to bear with greater lethality in addition to added potential to save the lives of friendly forces and increasing the pace of battle or friendly operational tempo.

[26] This experiment consisted of an armoured battalion, a mechanized infantry battalion, a light infantry battalion, and various support units. Within the EXFOR's two heavy maneouvre battalions there were 873 digitized and networked platforms, consisting of M1A1 tanks and M2A2 Bradley fighting vehicles equipped with digitized terminals. The EXFOR's light infantry battalion contained 186 dismounted soldier systems, and was equipped with the Javelin anti-tank missile system. A battalion of M109A6 Paladins provided field artillery support, and the Aviation Task Force consisted of eight AH-4A Apaches, two AH-64D Apache Longbows, and eight OH-58 Kiowa Warriors. Robert C. Holcomb, "Some Lessons Learned While Digitizing the Battlefield," Proceedings of the Battlefield Systems International Conference, London, 1998.

[27] Ibid.

c. Planning time for deliberate attacks at the company level was reduced from 40 to 20 minutes. Substantial improvements in operational tempo and the ability to operate within the adversary's OODA loop were therefore demonstrated.[28]

A number of factors were identified that influenced the divergence between potential performance and observed performance. These factors formed the basis for insights and lessons learned that paved the way for future success. These insights included:

a. The importance of a high performance communications network,

b. The need for adequate training with new digital capabilities,

c. The importance of unit collective training time with digital capabilities,

d. The importance of limiting the number of capabilities introduced prior to a given experiment, and

e. The need to screen digital capabilities for maturity[29]

Numerous training exercises conducted with digitized U.S. Army units provided insight into the validity of individual aspects of the Network Centric Warfare hypotheses. Among the most significant and relevant to the Canadian Forces is a case study on the Network Centric Operations capabilities of the US Army Stryker Brigade; a new US Army medium weight infantry brigade.[30] This organization possesses a unique combination of organic reconnaissance, surveillance, intelligence and target acquisition capabilities in addition to digital battle command, control and communications systems. Of greater significance is the employment of a new

[28] BG William L. Bond, USA, Army Digitization Overview, Briefing to Dr. Jacques Gansler, USD (A&T), at the Pentagon, Washington, D.C., on May 20, 1998.

[29] Robert C. Holcomb, "Some Lessons Learned While Digitizing the Battlefield," Proceedings of the Battlefield Systems International Conference, London, 1998.

[30] Department of Defense, Network Centric Warfare Report to Congress, 27 July 2001, 4-1. Internet, accessed 15 October 2009 from http://cio-nii.defense.gov/docs/pt2_ncw_main.pdf.

organizational structure and information centric concept of operations.[31] The relevance to the CF is that the underlying network infrastructure, operating concepts and ISR assets are already embraced by the Canadian Land Force Command Support System (LFCS) and related Land Force Intelligence, Surveillance, Target Acquisition and Reconnaissance System (LF ISTAR) capability currently fielded with the Canadian land forces deployed in Afghanistan.[32]

The US Stryker Brigade NCW analysis was based upon a comparison with the US Light Infantry Brigade as the baseline during Certification Exercises (CERTEX) conducted at the Joint Readiness Training Centre (JRTC) in 2002. A number of key results were identified and analysis revealed that a number of key NCW factors identified earlier in this paper contributed an order of magnitude increase in the Stryker brigade's force effectiveness at the JRTC CERTEX. The most notable improvements were significant improvement in situational awareness for troops in the Stryker Brigade combat team versus the baseline light infantry brigade. To that end, the "quality of situational awareness information" defined to be the percentage of actual enemy, neutral, and friendly forces correctly identified and accurately located by commanders and soldiers or by their sensor and information systems in each unit increased from approximately 10% in the case of the baseline light infantry brigade to approximately 80% in the case of the Stryker Brigade. A further key enhancement was the acceleration in the speed of command; the time taken by brigade commanders to make key decisions. This metric decreased from 48 hours for the light infantry brigade to 3 hours for the Stryker Brigade. The combination of these factors improved the Blue to Red casualty ratio of 10:1 in the case of the baseline light infantry brigade to 1:1 in the case of the Stryker Brigade.[33]

Upon review of the results arising from the many different exercises and observations a number of common themes can be identified:

[31] Ibid.
[32] Mazzolin, Colonel Robert. Presentation to 2008 NATO Battlespace Information Conference: Defining the Land Force Perspective for C4ISR Development. Brussels, Belgium. 16 April 2008.
[33] Stryker Brigade Study

a. Value of Increased Shared Situational Awareness at the Unit Level. Increased SSA, facilitated by greater sharing of information across the network enables subunits to dedicate greater mental effort to prosecuting the battle against the enemy and less on tracking their own location and that of the remainder of their associated formation. The noted increased SSA presents the potential, (although as of yet rigorously un-quantified) to provide increased survivability and lethality in a number of areas.[34]

b. Value of Increased SSA in Increasing Operational Tempo. Increased SSA has enabled subunits within battalions/battlegroups to retain tactical march formations longer, capitalizing upon the speed of such formations to accelerate combat tempo. There were repeated instances during combat operations and exercises that greater operational tempo enabled units to surprise adversaries and achieve tactical advantage. Prior to this increased shared situational awareness facilitated by information sharing, units were required to deploy into attack formation sooner in order to avoid surprise contact with adversaries and conserve combat power.[35]

c. Value of Increased SSA in Maintaining Force Ratio. At division and brigade levels, increased shared situational awareness permits commanders to maintain forces in contact longer with adversaries. Increased SSA of both blue and red forces permits commanders to develop greater real time awareness and understanding of status and disposition of their own and enemy forces as well as force ratios. Such higher level battlespace awareness provides commanders with the confidence to permit units to remain in contact longer with adversaries, thereby resulting in higher combat power.[36]

d. Value of Increased SSA in Reducing Risk. Company and battalion level units have been able to conduct more complex tactical maneouvres with less risk as a result of increased situational awareness enabled by the network. For example, the complex double-envelopment maneouvre, during which the central part of a ground force retreats or stays in place while the flanks hold their ground or advance to gain superior position and then advance simultaneously to envelop, surround, and cut off an advancing enemy

[34] NCW—Emerging Lessons Learned from the First Digital Division, Presentation by COL (Ret) Fred Stein at conference on “Network Centric Warfare: Missions, Needs, Opportunities, and Challenges, ” Washington, D.C.; Oct 21-22, 1999.
[35] Ibid.
[36] Ibid

force, has proven easier to execute, with less risk. Similarly, passage of lines, in which a major new force passes through a blocking force to occupy a key position, has been executed more successfully at the National Training Centre.[37]

e. Value of Increased SSA to Battle Command. Finally, networking the force has reportedly assisted division commanders by providing increased SSA needed to maneouvre against adversaries. In this case, commanders were able to monitor an enemy column on the periphery that was moving. Rather than being forced to deploy forces and alter the scheme of maneouvre to engage the force, they were able to monitor its progress as it moved into an area not vital to the commander. Knowing its location, they were able to first complete the primary mission by executing the original plan, then maneouvre forces to defeat the now-isolated enemy force.[38]

Counter Special Operation Forces Missions (CSOF)

Among the most significant examples of the power of Network Centric Operations to date were demonstrated when Force Bilateral Exercise (FBE) Delta was conducted by the U.S. Navy in conjunction with Combined Forces Command Korea. This command faces major warfighting challenges in three mission areas: Counter Fire, Counter Special Operations Force, and Theatre Air and Missile Defense. In this experiment, the results with the greatest operational significance were generated in the CSOF mission area, where the especially difficult problem of countering hundreds of North Korean special operations boats (a CSOF mission) was dealt with on a timeline previously not thought possible.[39]

The use of networked C4ISR assets and applications enabled all elements to share information and develop a common operational picture, resulting in improved

[37] Ibid

[38] Ibid.

[39] Maritime Battle Center, Naval Warfare Development Command, "Fleet Battle Experiment Delta Quick Look Report," 2 November 1998, Newport, R.I.

coordination between Naval, Air, and Ground Component Commanders.[40] The ability of networked forces to develop a COP enabled them to simultaneously achieve a very high level of SSA that, when combined with revised TTPs, permitted them to synchronize efforts from the bottom up to achieve dramatically increased combat power and accomplish their mission in half the time required with traditional platform-centric operations.[41]

The empirical results from FBE-Delta and subsequent modeling and simulation are as follows:[42],[43]

a. Average Decision Cycle Time was reduced from 43 to 23 minutes,

b. Average Mission Timeline (C2 time plus operational time) was cut in half,

c. Shooter effectiveness (kills per shot) was increased 50 percent,

d. Assets "scrambled" or deployed on short notice in response to unanticipated or undetected incursions was decreased by 15 percent, and

e. Leakers (special operations elements that passed through the engagement zone to their operational destinations) were decreased by a factor of 10.

Qualitative results of this type are very compelling. C4ISR enablement increases SSA to the point that units involved can self-synchronize, increasing operational tempo and

[40] Ibid.

[41] VADM A.K. Cebrowki, Written testimony to hearing on Defense Information Superiority and Information Assurance—Entering the 21st Century, held by the House Armed Services Committee, Subcommittee on Military Procurement.23 February 1999.

[42] Maritime Battle Center, Naval Warfare Development Command, "Fleet Battle Experiment Delta Quick Look Report," 2 November 1998, Newport, R.I.

[43] An Assessment of IT-21 Warfighting Value-Added, 1 March 1999.

shooter effectiveness, which in turn, saves assets. Consequences of an order of magnitude decrease in the number of special operations vessels reaching their intended destination is also of significance in that it would greatly simplify the defensive operations in an operational theatre. NCW enablement via the implementation of C4ISR capabilities has the resultant effect of facilitating the potential combat power latent in a Joint task force, but has been wasted due to segmentation of the battlespace driven by the traditional inclination of respective environmental (land, air, sea) commanders to exercise independent authority as opposed to the exercise of a holistic joint command construct.[44]

Theatre Air and Missile Defense (TAMD)

The TAMD mission holds great promise for networking to enable a force to significantly improve its warfighting capability. Sensors play a pivotal role in generating battlespace awareness in this environment. Stand-alone radar sensors, and sensors on weapons platforms detect and track objects ranging from aircraft to cruise and ballistic missiles. When such sensors are employed in a stand-alone mode such as those typically associated with platform-centric operations, radio frequency related propagation effects and environmental factors combine and interact to degrade both detection and tracking quality. Such issues are most pronounced against targets, characterized by high speed and/or low observables. This typically results in poor or non-existant track coverage against certain types of targets with the resultant poor SSA in the cognitive domain and consequently have a significant impact on mission performance.[45] Operational performance can be significantly increased through employment of the NCW concepts of Sensor and Engagement Grids which provide a Cooperative Engagement Capability (CEC).

The CEC capability networks the many respective sensors to enable forces to share and improve their information position by overcoming the limits of individual sensors. Such a sensor netting system comprises cooperative engagement processors, data

[44] ADM Dennis Blair, CINCPAC, Remarks during Keynote Address at WEST 2001, January 23rd, San Diego, Ca.

[45] "The Cooperative Engagement Capability," Johns Hopkins APL Technical Digest 16, 4 (1995): p. 377-396.

distribution systems and highly advanced data processing techniques on all cooperating maritime, air and land platforms. This enables the integration of respective air defence, radar, target acquisition and IFF sensors into a single composite network that distributes the measurement data to all cooperating units, providing each with an identical, real time picture. Such increased information richness provides better accuracy, better identification, lower uncertainty, and decreased time to achieve a given level of track accuracy to provide commanders higher quality information to work with and generating "fire control quality" information.[46]

Of equal importance, detection ranges are extended, allowing further time compression and more rapid achievement of engagement quality battlespace awareness, the ability to extend the range at which platforms can engage hostile targets to well beyond the radar horizon and the ability to significantly improve area, local, and self-defense capabilities. Tactical decision making is improved directly by facilitating key decisions: which target to engage, when to engage it, and which platform and weapon should be used to maximize the probability of a kill.[47] New TTPs are emerging to allow commanders to exploit the significantly improved battlespace awareness that can be achieved in this mission area through the employment of NCW techniques. For example, "Fire of Remote Data", in which a platform engages a target it never acquires directly, but rather uses information provided by an external sensor, holds considerable promise for improving battle force asset utilization and TAMD mission effectiveness.[48]

Strike

Network-centric concepts are also enabling new war-fighting capabilities in the realm of strike operations. During the Kosovo air campaign, U.S. and coalition air crews carried out over 36,000 sorties in support of a wide range of missions. A number of precedents were established, including the first combat deployment of the B-2 Spirit stealth bomber and at the time, the largest use of Unmanned Aerial Vehicles (UAV) in history. The

[46] Ibid.
[47] Ibid.
[48] "The Cooperative Engagement Capability," Johns Hopkins APL Technical Digest 16, 4 (1995): p. 377-396.

UAVs were employed not solely as stand-alone platforms, but also in conjunction with a wide range of other ISR assets, including JSTARS, RIVET JOINT, AWACS, U-2, and other joint and coalition sensors.[49] Among the major challenges faced by Allied Air Forces was finding, fixing, targeting, and engaging mobile ground targets. JSTARS operators, which had been extremely successful during Operation Desert Shield/Desert Storm at detecting and tracking moving ground targets in the desert, found that weather, terrain, and other factors made it very difficult to identify and classify possible targets in Kosovo. Moreover, Forward Air Controllers (FAC) and strike aircraft found it difficult to identify small, mobile targets from 15,000 feet (the approximate altitude needed to reduce vulnerability to surface-to-air missiles in the theatre) with their onboard sensors.[50] In order to overcome some of these obstacles, the engagement or "kill" chain was networked to link sensors, analysts, decision makers, and shooters.[51]

Split-Based Operations

A final scenario highlights the power of collaboration and synchronization. Employing networks to increase combat power is central to facilitating rapid deployment into theatres of operation. A central theme of this development is that of distributed operations. Typically, forward headquarters, such as CAOCs consist of approximately 300 people. The ability to connect deployed, modestly resourced

[49] Earl H. Tilford, "Operation Allied Force and the Role of Air Power," Parameters, Vol. 29, Issue 4, Winter 1999/2000, p. 24-38. Jacques de Lestapis, DRONES, UAVs Widely Used in Kosovo Operations, http://www.periscope.ucg.com/docs/special/archive/special-199907011327.shtml.

[50] David A. Fulghum, "DARPA Tackles Kosovo Problems," Aviation Week and Space Technology August 2, 1999, p. 55-56. John A. Tirpik, "Short's View of the Air Campaign," Air Force Magazine, September 1999, p. 43-47.

[51] Ibid. The Predator (UAV) was deployed forward in Bosnia and the associated imagery was transmitted via SATCOM to a ground station in the UK. Fibre optic cable then linked the UK ground station to a processing facility in the United States and the processed information was then transmitted to the Washington, D.C. area, where it was up-linked to a Global Broadcast Service (GBS) satellite and transmitted back into the operational theatre to the Combined Air Operations Centre (CAOC). Targeting information was then communicated to controllers aboard an airborne command and control aircraft, which then provided it to the FAC. The FAC, in turn, provided the information to strike aircraft in accordance with established TTPs.

headquarters back to national based organizations enables them to be supported from a much larger, nationally based operation support centres.[52] The operational benefits of such an arrangement are significant. Historically, forward-deployed organizations have employed as many as 1,500 to 2,000 people which needed to be transported into theatre along with the equipment they required to complete their missions. Such a forward organization makes major demands on transportation, that when translated into terms of lift, potentially require in the order of 10 C-17 loads, during the early phases of an operation, which in turn, reduces lift available to move combat troops and essential logistics required to support them into the theatre. All mission personnel and materiel must compete for this valuable and limited lift. The ability to network the force at such a level and operate with an effective and efficient "split-based" or distributed command structure, where the workload is apportioned across a larger pool of staff located in geographically dispersed areas enabled by a sufficient degree of connectivity and interoperability, would clearly pay major dividends in leveraging combat power at not only early stages of operations but throughout a campaign.

Part 2 Summary Comments

The contemporary military operational environment is fundamentally complex given that modern militaries face many unique and emerging challenges related to media, terrorists, regional instability, insurgencies, asymmetric warfare and adversaries who have access to and make effective use of sophisticated technology. Therefore, in order to effectively exploit the benefits of NCW concepts in the command of contemporary operations, ranging from warfighting, to peacekeeping, humanitarian and nation building operations one must understand the cognitive and socialization processes that underpin them.

The command and control of highly complex military operations are increasingly less suited to traditional industrial-age approaches of de-constructing activities into smaller manageable, deterministic, predictable pieces. To that end, the command and control activities carried out by NCW enabled forces are closely aligned with many characteristics of complex activities; non-linear interaction, decentralization, and self-

[52] JEFX 99 Final Report, http://jefxlink.langley.af.mil/milfinal99/main.htm.

organization. Consequently, there is benefit to extending beyond traditional forms of conflict to explore the full range of command and control concepts enabled by NCW technologies. As such, the scenarios outlined in the preceding pages demonstrate that command effectiveness is increasingly a function of the ability to access and share information and the tempo of applicable exercises and operations have demonstrated that joint forces possessing comprehensively integrated capabilities better exploit the path dependency characteristic of NCW operations.

Additional advantages include the flexibility to employ smaller, lighter units that move faster, require less logistic support and can conduct operations using innovative tactics more effectively at lower costs, characteristics that would be highly instrumental to the realization of truly transformed CF operations. Such capabilities have led to the innovative development of new techniques such as “swarm tactics” that apply in a broad context and are scalable in their implementation from small sub-units to large formations, and in the physical, cognitive and cyber domains. The growing evidence supporting network centric contributions to operations manifests itself in the major areas involving increased information sharing and shared situational awareness, the relationship between shared situational awareness and synchronization/collaboration, and the relationship between collaboration/synchronization and mission effectiveness.

Part 3 - Concerns Related to C4ISR and Network Centric Warfare Capability

Introduction

The nature of conflict has evolved significantly. The nature of operations in Afghanistan and Iraq have demonstrated the increased emphasis on irregular, asymmetric and unconventional conflicts as opposed to confrontations between large standing armies. Many of the NCW benefits identified by proponents have been offered in the context of traditional, symmetric, force-on-force warfare environments. Some observers question the utility of Network Centric Warfare concepts in certain urban and counterinsurgency operations and question whether too much emphasis is placed on technology.[53] Although in Afghanistan and Iraq the implementation of NCW capabilities has had the result of mitigating casualties among coalition forces in light of innovative approaches to warfare carried out by insurgents such as the use of Improvised Explosive Devices (IEDs), some question as to whether revised tactics on the part of the militants, such as mixing with the local population to mask their operations, in fact serves to counter some of these benefits.[54]

In an effort to provide a balanced perspective, this chapter highlights a number of concerns cited above related to NCW that must be considered as key themes to be addressed by organizations managing NCW capabilities. The analysis begins with the scientific basis for assessing the validity of the benefits of NCW concepts and related sociological impacts. Next, social issues related to perceptions related to data-centricity in decision making, reliance on NCW and information management issues are considered. Finally, key organizational challenges related to the complexity of C4ISR technologies such as interoperability, hardware and software vulnerabilities are addressed. The chapter concludes by recognizing that although the nature of conflict along with the socialization of information technologies has significantly evolved, the

[53] Jim Garamone, No Silver Bullet to Counter Explosive Devices, Head of Anti-IED Office Says, American Forces Information Services DefenseLink, 7 September 2006, http://www.defenselink.mil/News/NewsArticle.aspx?ID=743.
[54]Ibid.

fundamental benefits as a transformational force multiplier still hold if NCW reliant organizations recognize and handle them with care.

Scientific Basis of NCW Theory

Supporters of NCW capabilities offer that the strong technological underpinning provides for increased information and cognitive advantage for commanders and combatants with the resultant increase in precision strike, lethality and combat effectiveness. However, there is little in the form of comprehensive Canadian empirical analysis in this domain and thus one must rely primarily on US based experimentation and operations and supporting analysis. While one might extrapolate them against Canadian based situations and capabilities, it may be argued that more detailed comprehensive testing is required in order to develop a more empirical scientific basis on NCW's impact on combat effectiveness. In the absence of such analysis, NCW theories have the potential of perpetuating critically flawed concepts. Two of the most often quoted theorems are Moore's and Metcalfe's Laws.[55] Moore's Law states that semiconductor based processing power doubles every 18 months; Metcalfe's Law being that the value of a communications network increases in proportion to the number of nodes that are connected to the network. The weakness with these laws is that communications network value does not scale indefinitely as in practical terms from a military perspective, its value saturates at sufficiently high numbers of nodes in light of bandwidth deficiencies, information overload and increased costs in terms of data fusion processing and system sustainment. To that end, opponents assert that progressive NCW theory overstates the capability for information and communications technology to deliver.[56] In the absence of a rigorously defined conceptual framework for NCW that can be universally and consistently applied and assessed via a consistent, disciplined scientific protocol, it may be argued that the qualitative nature of results to date, at best, only serve to refute the notion that networks cannot provide improvements to the conduct of operations.

[55] CF C4ISR Capability Development Strategy, issued under 1180-1(D Mil CM), 31 Aug 2009.
[56] Darryn Reid et al., All that Glitters: Is Network Centric Warfare Really Scientific?, Defense and Security Analysis, vol. 21, No. 4, p.359 and p.360.

Over-reliance on NCW

As proponents of NCW capability assert that it enhances situational awareness, collaboration and synchronization, critics assert that dangerous assumptions are being made. Primary concerns relate to the number of troops required to plan, prosecute and support operations in light of an over reliance on networked technologies and the significant information overload burden placed on troops as a result of increased tempo of operations. The net result is that the human capacity to synthesize and assess the volume of information, and coherently respond is unable to keep pace. Information richness itself has the potential to skew combatants' perception of what is happening on the battlefield. Depending on the relative placement and capability of various sensors in the battlespace, differing representations of the operational reality may be conveyed.[57] Consequently, it could be contended that such an over-reliance on NCW concepts may limit the influence of commanders in shaping the scope and nature of operations.

NCW Technology Suitability to rapidly Evolving Battlefield Environment

Given the rapidly evolving nature of Urban and Counter Insurgency operations, and the physical characteristics of the battlefield environment, significant technical challenges are posed regarding the employment of C4ISR systems.[58] A system that relies upon the rapid synthesis of inputs captured and communicated from a number of different sensor systems in such a hostile radio frequency propagation environment must contend with varying degrees of efficiency and uncertainty. Understanding this, an enemy will electronically conceal themselves.[59] Thus it is still necessary to physically engage them on the ground in addition to solely relying on ISR sensor inputs. Adversaries in both Afghanistan and Iraq upon having become aware of the capabilities of progressive C4ISR

[57] Giles Ebbutt, Flaws in the System: Modern Operations Test Theory of Network Centricity, Jane's International Defence Review, July 2006, Vol 39.

[58] Notwithstanding the technical sophistication of modern communication and sensor systems in the ISR realm, physical limitations exist in their ability to function fully effectively in complex urban environments where electronic propogation and imagery may be obscured by concrete and metal as well as revised enemy TTPs such as deployment in sewers, behind buildings and walls.

[59] Giles Ebbutt, Flaws in the System: Modern Operations Test Theory of Network Centricity, Jane's International Defence Review, July 2006, Vol 39.

technologies have developed sophisticated means to avoid detection.[60] Thus, a force that is heavily dependent upon NCW techniques and related technologies, will paradoxically have its situational awareness compromised. To that end, it is critical that such network based technologies be complemented with strong Human Intelligence (HUMINT) based capabilities in order to provide a comprehensive view of the battlespace in all dimensions.

Many examples exist of the extent and associated techniques that adversaries have undertaken in order to deceive and mitigate the effectiveness of advanced NCW techniques and technologies. These include the use of irregular fighters, close range snipers and mortar teams who intermingle with the civilian population and operate in close proximity to sensitive facilities such as Mosques, schools and hospitals, using them as shields. They swarm to attack and then quickly disperse back into the population. The use of Improvised Explosive Devices (IEDs) and suicide bombings have risen to become the primary threat to coalition forces. These examples cite techniques that comparatively unsophisticated adversaries may use to compromise the effectiveness of advanced C4ISR technologies. When considering the more sophisticated capability possessed by state based actors, greater threats are posed to operational C2 and networked weapon and fire control systems. This results from the intertwined nature of strategic and tactical systems which in many instances rely upon commercial bearer systems to carry operational data and consequently, may be more readily exploited by unauthorized personnel and organizations. Further, additional research with deployment potential is being conducted in the area of directed energy devices that may be used to either “burn out” sensitive microprocessor devices used in a wide range of C4ISR applications or interfere with satellite and space based systems.[61]

There is a further implication in terms of risk to the heavy institutional capital and doctrinal development investment associated with high technology C4ISR systems on the part of modern military forces. The increasing sophistication level of potential adversaries and more ready access to advanced technologies creates a scenario whereby

[60] John Matsumura, et al., Preparing for Future War with Advanced Technologies, RAND, Arroyo Center, 2002.

[61] Amy Butler, Heavy DoD Reliance on Commercial SATCOM Prompts Questions of Protection, Defense Daily, 13 April 2004.

such forces can more readily develop technologies and tactics to conceal themselves and counter modern systems increases the possibility of negating the value of this extensive investment.

Information Management

The increasing deployment of sensor systems on the modern battlefield with the consequent increase in data outputs creates the issue of information overload where the collation, management and synthesis of many high volume real-time data streams becomes a significant factor in the integrity of any associated decision processes. A number of data fusion concepts and capabilities are being studied that would enable the filtering and sorting of raw sensor as well as developed battle command and control application data into more user friendly, manageable portions.[62]

Significant Information Assurance challenges present themselves from the perspective of integrating various networks of various classification levels and from various coalition nations and functional groupings, which further compound the problems of information completeness, context and availability[63]. When one considers the increased reliance upon the wireless spectrum environment, frequency and spectrum management issues present themselves in terms of deconflicting spectrum allocation of various sensor and wireless bearer systems.[64]

Another information management concern is the risk of institutional over reliance upon information systems as a decision making asset. As a corollary of the richness of

[62] Canadian Forces C4ISR Capability Development Plan 1180-1(DMilCM) dated 31 August 2009 issued under authority of CFD and CF J6/COS IM.

[63] Such issues relate to interoperability considerations related to ensuring overall system confidentiality, integrity and availability in light of as well as that of one's own system in light of the various standards that may be applied by various organizations, some of whom may or may not be trusted. Given the increased emphasis of Joint, Interagency, Multinational and Public operations where military operations are increasingly being conducted in coalition environments, the issue of interoperability i.e. the requirement for common protocols in order to provide seamless connectivity and ensure the confidentiality, integrity and availability of network connectivity from many nations, federal and public organizations whose networks may not have the same level of assurance as host networks and whose capabilities and intentions may not be known.

[64] US Air Force, US Forces in Iraq Face Obstacles in Getting Intelligence They Need, Inside the Pentagon, 5 May 2005, Vol. 21, No.18 and Ted McKenna, Orchestrating Tactical Communications, Journal of Electronic Defense, August 2005, No. 8.

information sources, there exists a tendency to focus solely on data in order to make decisions. As such, potential undesirable consequences would include an organizational overconfidence in the results of data upon which to project decisions.[65] This issue presents itself in the form of a qualitative change in organizational behaviour as a function of quantitative changes in data. For example, multiple sensor "hits" arising from a target rich environment that are not correctly correlated and deconflicted produce the undesired result of unnecessary sorties or missions being launched, unwarranted expenditures of ammunition and commitment of logistic and support resources. Further, inadequate sensor placement in an information rich environment has the potential to skew the data captured and presented. This potentially results in a consequent reorientation of focus, intent and direction of mission planning and objectives.[66]

Complexity of Military Systems and Technology and Interoperability

Virtually every aspect of military capability is now automated and is reliant upon the networked environment. Networked microprocessor and wireless technologies enabled by complex software based applications perform a spectrum of tasks ranging from collecting and processing sensor data, detecting projectiles and combatant activity, setting targets, coordinating actions between and issuing direction to land, air and sea forces. The trend is now to network together previously unconnected stand alone surveillance, target acquisition and fire control systems in order to more fully automate the decision making and kill chain in order to increase the tempo of operations.

In light of such interoperability requirements being driven by unanticipated coalition partners that arise as a result of the fluid nature operations, most modern systems that are currently being developed are considered as "unbounded" given that no single element of the overall system holds the entire breadth of information and knowledge required to function. Therefore, many individual components of such

[65] Michael Schrage, Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003.

[66] Kimberly Holloman, Evidence Based Research Inc., The Network Centric Operations Conceptual Framework, Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., 20 January 2004.

networks must be connected together in ways that may not have been originally intended or anticipated. Recent operations in Afghanistan and Iraq have mandated the interconnection of systems supporting land and strategic level command and control systems, UAVs, helicopters, artillery systems, long and medium range weapon locating sensors, and allied systems whose original designs were not intended or planned for such interconnectivity.

Such a configuration results in a "system of systems" whereby sensor and command and control data from a variety of sources must be transferred securely across boundaries and fused together. The consequent challenge that is created is that in connecting such disparate networks together, system design assumptions that were logical and correct for individual components, when aggregated with other such systems, become the source of errors and potential malfunction within the system of systems as a whole. This in turn creates both vulnerabilities and the potential source of mission critical failures which may be generated through the normal operation by users or otherwise exploited by knowledgeable adversaries.[67]

Vulnerabilities of Military Hardware and Software

Military networks have historically been a principal target of hackers, from basement amateurs to state sponsored entities. Many of these attacks are prosecuted simply using applications that are readily available off the web. An example of the facility with which some hackers may operate is that of Gary McKinnon, a British hacker who through the use of such software through the Internet, was able to penetrate approximately 100 US DoD networks during 2001 and 2002, installing back doors, Trojan horses, appropriating military passwords, and shutting down network infrastructure at Fort Myers, Fort McNair and the Pentagon in addition to other DoD networks causing significant damage.[68]

[67] Fisher, David and Dennis Smith, Emergent Issues in Interoperability, Carnegie Mellon Software Engineering Institute, No. 3, 2004, http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/eye-on-integration-2004-3.htm.

[68] Brooke Masters, Briton Indicted as Hacker, Washington Post, 13 November 2003, http://www.washingtonpost.com/wp-dyn/articles/A45963-2002Nov12.html.

Such incidents open the debate as to whether military forces should rely extensively on readily available “Commercial Off-the-Shelf” (COTS) or “Open Source” application software for the basis of military command and control systems. Open source software such as Linux, (which is often argued to be freer of bugs than Microsoft products) is openly and freely available to anyone who wishes to contribute to its development; all that is required is simple registration, and consequently there is a significant attraction in terms of minimizing cost associated with purchase and development.

The global application developer community collaboratively contributes to the enhancement of the application environment by building upon each others code development. Consequently, quality assurance and undisclosed functionality covertly built into applications represents a concern for mission critical applications requiring precise performance in support of operations and system functionality. Although proprietary software, which is often based on commercially based applications is frequently developed using higher industry based quality assurance standards, is represented to be more secure by industry representatives, there is an active debate as whether this is actually true. Some would concede that precisely because such software is so widely reviewed by the global development community, this would serve as the best environment within which to identify and prevent the insertion of covert malicious code by a foreign agency.[69]

It is alternatively argued by federally based security authorities that software free of such vulnerabilities may only be achieved through the use of “high assurance” software.[70] The challenge posed therefore, is that such an environment would be significantly more costly in terms of money, time and subsequent development flexibility given that once software has been “sealed”, any further enhancements undermine the very integrity of a certified product. It is also argued that notwithstanding the rigorous testing to which such software is subjected, it has been asserted that with increasing

[69] Eydt, Bernard, Software Assurance is Critical to SDR Success, COTS Journal Online, February 2006, http://www.cotsjournalonline.com/articles/view/100463.

[70] Software that has been subjected to extremely rigorous testing as a result of the highly disciplined development and testing environment so as to ensure that it is free of malicious code that may be used to compromise its integrity.

system complexity, additional testing does not necessarily result in decreased vulnerabilities that may remain embedded in the software and remain undetected.[71]

Although less sophisticated but equally important, threats also manifest themselves in terms of more mundane inadequate physical security processes. For example, in 2006, stolen computer hard drives containing classified US military information were found for sale in local bazaars in Bagram, Afghanistan. In an effort to remediate the problem, in addition to launching an investigation, US officials were forced to direct the purchase of all computer drives from local bazaars in an effort to mitigate potential damage.[72]

An additional hardware based vulnerability that poses a significant risk is that of Electromagnetic Pulse (EMP). This phenomena relates to the significant intense and extremely short duration electromagnetic radiation that is emitted during a nuclear explosion which can harm and disable electronic systems that are dependent on microcircuits and microchips. Given the ever increasing micro-miniaturization of products that are designed to function using ever lower current and voltage levels in order to reduce form factors and power consumption and increasing reliance on commercial based hardware products to rapidly provide this capability, this threat poses increasing relevance given their high susceptibility to power surges. A scenario of this type may be generated via a limited low level nuclear explosion in proximity of a battlefield which would generate no human casualties as a result of blast or radiation. However, this would create widespread damage and disruption to electronic equipment.

Similarly, more focused results are certainly possible on a more limited scale through the deployment of a high power microwave device triggered by a conventional explosive.[73] A significant portion of modern military forces command, logistics and sustainment traffic both within theatre as well as from theatre back to North America is routed over both commercial satellite and internet. In such an attack, many commercial

[71] Simson Garfinkel, Battling Bugs: A Digital Quagmire, Wired News, 9 November 2005, http://www.wired.com/news/technology/bugs/0,2924,6939,00.html.

[72] Carlotta Gall, At Afghan Bazaar, Military Offers Dollars for Stolen Data, The New York Times, Asia Pacific, 15 April 2006, http://www.nytimes.com/2006/04/15/world/asia/15afghanistan.html?ex=1145332800&en=e12bbb6b87a5b3fb&ei=5087%)A.

[73] CRS Report 32544, Clay Wilson, High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave Devices (HPM): Threat Assessments, 14 April 2006.

satellites would be particularly vulnerable and could cease to function after such an attack. Aside from the widespread disruption that would be created on internal networks, the resulting demand by remaining functional networks would compromise operations for a significant period of time. Special "hardening" techniques such as shielding and resilient network design would mitigate such a risk in future equipment development efforts, however, this would be at a significant financial cost. This vulnerability could potentially serve as motivation for some adversaries to acquire such capabilities.

Part 3 Summary Comments

It is clear that modern militaries are increasingly benefitting from enhanced SSA to support command and control and further refining this capability through the innovative conduct of missions that increase speed of command and operational tempo. Although the scope of these scenarios is extensive, available evidence is primarily qualitative and from limited portions of the overall operational spectrum. Notwithstanding, these results emphasize the significant progress that has been made and confirms the potential that NCW concepts hold as a force multiplier in support of contemporary operations and future military transformation. Further, care must be exercised in its application given the limitations related to social dynamics, cognitive considerations, limits related to the laws of physics and the competitive exploitation of technology by an increasingly sophisticated adversary. It is important to minimize fixation on the technological scope of potential contribution to operations and as such, it is critical that military forces fully embrace the nature of transformation in its broadest institutional sense and the associated conceptual shift in the military contribution. To that end, militaries need to better consider and understand the impacts that information management issues have on personnel, culture and organizational constructs. Given the importance of social and cognitive factors that contribute to organizational development, a better understanding of these considerations must be gained to provide a basis for organizational changes within the CF supporting command supported by NCW concepts. From a technical perspective, the complexity of military technology poses significant interoperability issues in light of the increasing number of systems and partners. Further, the increasing military reliance on commercially based hardware and softwaresubjects it to a host of vulnerabilities,

Part 4 – Key Issues Related to C4ISR Technologies and Viability of CF Organizational Structure to Manage NCW Capabilities

The C4ISR domain within the CF/DND represents a new operational domain that differs in fundamental ways from the traditional air, land and maritime domains. As such, the management of such a capability is subject to a number of specific considerations that do not receive central focus within the traditional domains. The respective components of C4ISR within the context of the CF/DND has not coalesced into a holistic capability in light of the fact that the various components, namely in the areas of C4 and ISR are located in different organizations. In the absence of a single organization that can exercise oversight over a consolidated capability, the supporting financial, programmatic and organizational structures are not effectively coordinated to produce integrated effects. To that end, when considering C4, given the significant technical focus of this domain, many rapidly evolving technology developments greatly impact the institutional development of this capability. Issues such as Internet Protocol version 6 (IPv6) migration, Bandwidth, Infrastructure and Software/Hardware development represent foundational issues that require significant technical expertise, programmatic capacity and organizational focus to address.

Further, the increased emphasis on space based systems, sensors, networked weapon systems and UAVs pose significant development and integration issues and represent new capability areas that as of yet have not been developed in terms of organizational focus and development. In light of the tremendously increased scope of complexity in a rapidly evolving technology environment, traditional processes related to research, development and acquisition require modification in order to remain relevant and adequately support capability development activities. The subject of ISR, as a result of both the evolving nature of armed conflict and the significant impact of technology has significantly increased in scope and consequently the related management of this discipline. This manifests itself in the areas of evolving analysis techniques and processes, the enhanced interoperability arrangements that must be made with JIMP partners. Such increased scope of complexity and responsibility mandates greater institutional focus and specialization and as such, the requirement for a specialist professional stream and associated leadership.

Finally, the absence of Level 1 representation within the CF/DND responsible for oversight and management of this emerging functional domain inhibits senior departmental visibility into a key transformational capability and related critical issues. This translates into insufficient representation from an organizational structure and capacity perspective as well as it regards access to funding in competition with other Level 1 organizations.

The implementation of a NCW enabled force involves the management of a variety of specific areas and as such, a number of key technology and management aspects that are used to provide NCW capability for the Canadian Forces are considered in this part of the paper. DND conducted a capability review in July 2002 and five capability gaps were articulated in the areas of intelligence and information for command and control, the absence of joint doctrine, concepts, and training, requirement for integration of C4ISR initiatives so as to support interoperability.[74] The priorities that were articulated were as follows:

a. the development of a truly CF wide joint command system;

b. a comprehensive plan for joint policy, concepts, and doctrine development;

c. the development of a comprehensive strategic-operational joint command structure;

d. the procurement of a coherent and fully integrated suite of intelligence, surveillance, and reconnaissance assets; and

e. the establishment of intelligence and information fusion centres.

[74] Auditor General of Canada, Report of the Auditor General of Canada to the House of Commons - Chapter 4 National Defence – C4ISR Initiative in Support of Command and Control; April 2005.

Additional areas of improvement that were identified included the following areas:

a. underutilization of existing network capabilities,

b. no common goals or standards,

c. lack of integration between projects,

d. lack of a management system,

e. need for cultural and organizational change,

f. need for more personnel and training,

g. bandwidth constraints, and

h. funding constraints.

This analysis will consider the issues cited above in greater depth via discussion related to three main subject themes; the first is Communications, Command, Control and Computing (C4) transformation requirements, the second relates to Intelligence, Surveillance and Reconnaissance (ISR) transformation requirements and finally financial and organizational issues. The motivation to separate C4ISR into the respective functional components; C4 and ISR, is related to the respective issues that arise given their alignment within the DND/CF organizational structure. Currently, the ADM(IM) Group is responsible for C4 capability management within DND. The management of ISR however is spread about various organizations within the VCDS Group, the respective Environmental Chiefs and CDI. The issues of financial and organizational resources involve broader departmental level considerations that transcend the respective organizations involved in C4ISR.

Communications Command Control Computing (C4)

The C4 network and associated processing environment represents the nervous system for military command and operations. Historically, military organizations have functioned on the basis of “pushing” information whereby information owners would select information and transmit it to those that they had designated as being authorized users having a “need to know”. As a result of the volume and widespread availability of information provided by web enabled services on both classified and unclassified military networking environments, the policy environment has evolved to one of “pulling” information. Here authenticated users on a network may access information they deem necessary in the execution of their responsibilities notwithstanding the owner of the data. Such a policy shift has been invoked with the anticipation that collaboration and information sharing would improve the prosecution of military operations. The implementation of a seemingly simple concept however, creates a number of significant technical challenges for an organization. These issues will be addressed in the subsequent pages.

Internet Protocol 6 (IPv6) Migration and Indigenous Military Technical Capability

The implementation of such a broad based information environment is dependent upon a high bandwidth backbone network that comprises a mix of terrestrial wired, fibre optic, radio based as well as satellite based systems all using Internet Protocol (IP). The common protocol environment that has matured and served as the basis for internet communication since the inception of the Internet is IPv4 (version 4). In light of the advances required to accommodate projected internet growth and capability requirements, modern organizations (including militaries) reliant upon the internet will require to migrate to IPv6 in order to increase network flexibility in terms of mobility, enable the creation and allocation of more internet addresses and alleviate current system management challenges.

All commercial carriers (over which most military based networks currently make use) will eventually transition to IPv6. Given that IPv4 is currently embedded so deeply in North American and European civilian and military network infrastructures, a number of challenges will present themselves to modern western military nations. Given this solid entrenchment, the business case for both commercial and military network infrastructure to transition will not be straightforward. However, many developing nations such as India, China, North Korea, Pakistan, Iraq and Iran, currently without an extensive network environment will be in a position to embrace IPv6 immediately as the foundation for their emerging networked commerce environment. To that end much of the knowledge associated with the implementation and management of this next generation network environment could well end up outside of developed western nations.[75] The result of such a situation could potentially be the creation of a digital divide between western and emerging nations that would effectively isolate them during the period of time required for transition and further make them dependent upon manufacturers and providers of IPv6 equipment from these countries.

This creates a vulnerability for countries such as Canada. Given the almost exclusive reliance on the commercial network environment for the transmittal of data between operational theatres and Canada, the future operational network environment would be heavily dependent upon manufacturers and service providers from the countries cited above, some of whom western nations may not have positive relations with. Consequently, as a result of their advanced standing in this technology environment, such countries would be in a position to identify and exploit vulnerabilities in the network and thereby put western military nations' critical command and control information at risk.

Notwithstanding the global advancement and development in this area, the DND/CF have moved more slowly to develop NCW capabilities. This is largely as a result of budgetary limitations and an operational tempo which precluded institutional focus being placed on this capability area resulting in the degradation of a C4ISR engineering and programmatic development capability within the DND/CF during the 1990's and 2000's.[76]

[75] Christian Le Bas and Frederic Miribel, Is the Death of Distance Argument Relevant: The Agglomeration Economies Associated with Information Technology Activities, http://www.ish-lyon.cnrs.fr/labo/walras/Objets/Membres/Miribelebas_paper.pdf.

[76] Sandy Babcock, Canadian Network Enabled Operations Initiatives, Defence Research and Development Canada, undated (post 2004).

Interoperability

NCW capabilities supporting the modern concepts of JIMP coalitions in both a purely national or international environment depend heavily on the ability to interconnect a wide array of communications equipment, wireless, wireline and satellite bearer systems, sensors, data, software and people both rapidly and seamlessly. Such systems must be able to enable secure communications between personnel and systems in all these various organizations as well as commercial entities providing contractual support and research organizations providing development support. Further, the dissemination of data from the various sensors to support mission critical fire control systems and the ability for the network to autonomously adapt to changes and breaks in the network environment in order to ensure an extremely high level of Quality of Service must be assured.

In light of the impressive range of military systems expected to reside on this communications infrastructure and the highly dynamic nature of system development, it will be very difficult to achieve full network interoperability and integration among the many organizations. To that end, any capability delivery organization (i.e. Level 1's and ECS's) within the Canadian Forces and DND will be required to devote significant attention and care to the issue of interoperability. Particular attention will need to be devoted to standards and development methodologies associated with architectural integration as well as identifying capability and associated funding incongruence's between programs.

The requirement for physical interconnection of networks to facilitate the exchange of information between CF elements, allies, other government departments and first responder organizations reinforces the need for institutional focus on standardization and architectural development. In essence, the DND/CF needs to mature its internal analogue of the US based Global Information Grid (GIG) that would operate along with requisite standards and systems that may be applied across such a domain and with other government departments and allied nations to enable interoperability. The large number of organizations with which potential connectivity needs to be effected, most of whom have different connectivity standards based on varying functional requirements, necessitates the practical approach of developing a prioritized listing of networks to be connected along with a plan to address the policy issues of information protection and sharing across the expanding environment.

A further requirement exists for the development of common "content management systems" among the various networks so as to facilitate the sharing of information resident on the various networks in a consistent way all the while ensuring the integrity of the applicable security policies.[77]

Space Based Capability Development

Given the expeditionary nature of Canadian and other modern western military nations, satellite systems are critical to the enablement of deployed operations around the globe. In addition, satellite based capabilities provide the basis for the provision of navigation, imagery, weather, and missile warning information. A further key capability is that of providing deployed forces with the ability to reach back to Canada for support and sustainment activities. Unlike the US, which currently operates a number of space based networks including the Global Positioning System (GPS), six additional orbital constellations for intelligence, surveillance and reconnaissance, and an additional Army Coalition Military Network intended to enhance bandwidth support to coalition forces, Canada does not possess its own indigenous military satellite based capability and is required to rely upon a complicated environment of contractual arrangements for access to the space segment to support operational missions.

Further challenges are posed to Canada from the perspective of access to the space segment in a competitive environment when one considers that notwithstanding the access to a number of military designated satellite networks, the US has had to rely upon commercial satellite service providers for the majority of its communications bearer support during Operation Iraqi Freedom.[78] This heavy reliance upon commercial providers which makes the US military one of the biggest customers for commercial satellite services does not necessarily ensure adequate quality of service. For example,

[77] Canadian Forces C4ISR Campaign Plan, Interim Report, Director Joint Force Capabilities, 27 June 2003.
[78] "DISA Chief Outlines Wartime Successes", Federal Computer Week, 6 June 2003.

US military traffic on the Iridium system overwhelmed the network, which was consequently required to suspend service in order to affect updates. As well, the Inmarsat system which has become increasingly relied upon to carry military traffic was unable to satisfactorily support encrypted data services, which required the US Army to work with a degraded data rate capability which ultimately did not satisfy operational requirements.[79]

The US Air Force will be deploying additional advanced extremely high frequency communications satellites during the 2014-2018 timeframe in order to put in place a space based system to complement the US Global Infrastructure Grid (GIG) network to provide high speed broad band datalink capacity network support to US warfighters deployed worldwide.[80] Such an indigenous military capability will become increasingly necessary for nations to flexibly respond to future operational exigencies overseas. There is a further requirement for a progressive development program to not only provide “bandwidth on demand”, but also do so in a secure fashion. In order to support expeditionary and to a lesser extent domestic operations, the CF, in the absence of dedicated space segment competes for access to the same commercial based infrastructure as the US and consequently, given the requirement to rely on awkward contracting processes to secure access, places it at a disadvantage when planning for deployed operations.

In light of the elevated reliance on commercial capabilities to provide space based capabilities to support operations, two further relevant issues present themselves. The first is the comparative advantage that western nations such as Canada enjoy by virtue of access to space based capability will increasingly diminish as developing nations and non-state actors begin to exploit access to commercial systems by purchasing bandwidth from service providers or purchasing high resolution imagery from countries such as Russia and China who own space assets. The second issue is one of protecting space assets from both non-state actors and technologically advanced foreign state based entities. A range of threats are present to existing military and non military based space

[79] Warren Ferster, Military Bandwidth Demand Energizes Market, Space News, 2 September 2003, http://www.space.com/spacenews/archive03/militaryarch_090203.html.
[80] Rebecca Christie, DoD Space Program’s Costs Rise as New Plan Takes Shape, Wall Street Journal, 21 February 2006.

assets. It has been demonstrated that jamming of commercial satellites may be done relatively simply and Chinese ground based lasers have been directed at US optical surveillance satellites in an effort to blind them.[81]

To date, a coherent indigenous Canadian program to provide a secure space based capability to support bandwidth requirements for expeditionary operations and space based ISR capability is in the initial stages of taking form after virtual elimination as a result of financial cuts during the 1990's. Current CF Space policy and strategy development mandates the delivery of three objectives and associated tasks to deliver upon its vision:

a. Assure access to space and its unhampered exploitation to deliver and sustain space effects,

b. Effectively integrate space effects, and

c. Assure the freedom of space operations by protecting national space systems and those allied systems critical to National Defence from threats.

The draft guidance that has been promulgated emphasizes that the delivery of these objectives is dependent upon the development of a National Defence Space Plan and a Joint Space Doctrine. It goes on to recognize that although specific core activities are entirely within the purview of DND/CF, it is clear that the development of a comprehensive space capability is beyond the resources of the CF and Canada alone and as a consequence, there is a critical requirement for close collaboration with the Canadian Space Agency (CSA), other federal departments, agencies and key allies to effect the delivery of the necessary space effects.[82]

Sensor and Networked Weapon Systems

[81] Vago Muradian, China Tried to Blind US Sats with Laser, Defense News, 25 September 2006.
[82] DND - Directorate of Space Development, Canadian National Defence Space Strategy (Undated Draft) produced fall 2009.

The next step in weapon system integration into Network Centric Operations involves the remote operation of weapon systems on a variety of air, land and sea platforms via data link over command networks. Currently, from a Canadian perspective, a limited range of operational weapon locating sensors and artillery systems have been integrated into the Land Force Command System. Other work is being conducted to more fully integrate sensor data from UAV and weapon locating systems.[83]

From an international perspective, US based testing through the Weapons Data Link Network Advanced Concept Technology Demonstration has shown that standard networking techniques may be used to report weapon status upon release and impact from air platforms. The potential exists for weapon controllers to provide command guidance during weapon flight to correct direction prior to impact in order to engage an alternate target or abort the mission if necessary. The key consideration in the case of many networked weapon systems, is that of high Quality of Service broad bandwidth availability in order to ensure positive control throughout the mission. This reinforces the need to develop a consolidated and robust information grid to support military operations.

This represents another emerging field whereby sophisticated sensor systems in the realm of electro-optical, thermal, imagery, signals intelligence, measurement and signature intelligence, which have historically been in the realm of purely strategic based capabilities are now being integrated onto platforms that are deployable at a tactical level and linked into a broader national infrastructure so as to be able to coalesce a far more comprehensive picture of the battlespace and provide more detailed intelligence information to the warfighter. The challenge that exists in such a dynamic and rapidly evolving sphere of technology is that technically sophisticated adversaries are in a position to counter such technologies with countermeasures thereby potentially negating the operational relevance of a significant programmatic investment on the part of a nation. Once again, this is an emerging capability area that from a Canadian Forces

[83] The Canadian Army Land Force Command System integrates sensor information from the Land Force Intelligence Surveillance Target Acquisition and Reconnaissance Program which integrates data input from the Lighweight Counter Mortar Radar Locating System, Acoustic weapon locating systems, infrared and electro-optic systems located on the "Coyote" armoured fighting vehicle, M777 artillery gun fire control system, RCIED systems on armoured fighting vehicle platforms, as well as the ScanEagle and Heron UAV systems currently operating in Afghanistan.

perspective, has not witnessed a broad based CF institutional investment in terms of programmatic focus and doctrinal development.

Bandwidth and Related Infrastructure Issues

Since the inception of active internet protocol and related digital application use on military networks, there has been an explosive increase in the military requirement for bandwidth. When considering the expansion of warfighter networks, inter theatre connectivity between tactical and strategic command and control systems, greater integration of data intensive intelligence, surveillance and reconnaissance products on these networks and greater emphasis on coalition interoperability, the question arises as to whether sufficient bandwidth exists through indigenous military networking systems and whether such capacity will be able to keep up pace with the demand in the future.

Given the heavy reliance of warfighter units and formations on networked systems, the impact of insufficient bandwidth poses grave consequences on situational awareness and coordination of combat actions during battlefield operations.[84] To that end, there is significant research and development being undertaken in industry to identify innovative data transmission protocols, storage and networking technologies in order to more efficiently handle the throughput required to support modern NCW systems.[85]

This highlights one of the key aspects of C4ISR support; specifically, the data link and associated information management aspects of the fielded capability. A key priority for DND is to deal with the issue of data management in the first instance, and subsequently, address the challenging data link issues that are specific to the military environment.[86] The need however, is for the CF to be able to maintain a robust and flexible engineering development and acquisition capability in order to readily adapt

[84] For example, US units in Iraq during the first Gulf War were surprised by Iraqi tank units that appeared without notice given that their computer screens displaying intelligence information had not been updated for some hours given the reduced data flow in light of other high priority applications.

[85] Mazzolin, Robert and Asad Madni, A Recommended Scenario for the Future Wireless Network Environment, Proceedings of the 2003 Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference, Big Sky, Montana.

[86] Department of National Defence, Defence Science Advisory Board Report 0912, Conceptual Framework for DND's National ISR System, Ottawa, November 2009.

existing tactical and strategic networking infrastructure to emerging networking capabilities.

Unmanned Remotely Controlled Vehicles

An area of capability that has evolved tremendously from a nascent cottage industry to a vital mainstream military capability is in the area of Unmanned Remotely Controlled Vehicles. Such systems comprise Unmanned Aerial Vehicles (UAVs), Ground Vehicles (UGVs) and Underwater Vehicles (UUVs). Although such systems have been primarily used in a purely surveillance role, they are increasingly taking on an active combat role using on board weapon systems. Such systems are heavily reliant on advanced networking techniques requiring significant bandwidth in order to transmit surveillance data from theatre back to command centres at home thousands of kilometers away and in return, receive control and steerage information to direct its actions toward intended targets. To date, Canadian fielding of such capability has been done through the "double hatting" of existing program resources in response to urgent operational requirements as opposed to a well developed capability development methodology. The CF/DND do not have dedicated staff focused on the programmatic delivery, fielding and doctrine development associated with this discipline.[87]

Software and Hardware Development

As the core of many military technologies increasingly become software based, the discipline of software development increases in importance as a means of rapidly enhancing, tailoring and delivering weapon system capabilities to meeting a rapidly evolving operational threat. Although a significant portion of military requirements require tailored software development thereby demanding a need for a strong in house software engineering and development capability, the CF and other militaries have faced

[87] Mazzolin, Colonel R.G. Director Land Command Systems Program Management, Presentation to COS ADM(Mat) 8 Feb 2008 in support of DLCSPM Development.

challenges in schedule delays and cost overruns. This has caused significant challenges for programs that are reliant upon the development of dedicated sophisticated software.

To that end, in the case of the DoD, the US Government Accountability Office (GAO) has recommended that it follows private sector best practices to avoid such issues.[88] The challenge presented in adhering to such guidance is that many software development firms involved in military development outsource programming activities to sub contractors overseas. Consequently, configuration control, espionage and the risk of insertion of malicious code and back doors becomes a significant concern.

The issue of what balance must be struck between in-house versus contracted software development and associated costs is significant and much effort has been devoted to identifying processes whereby government and industry develop security methodologies to promote software integrity and reliability. The DND currently relies on the Land Software Engineering Centre (LSEC) for much in-house development. Although this organization supports in limited fashion projects in the Joint as well as Air and Maritime environment, it is by exception only as this organization is an Army materiel management resource and funded only to that end. Consequently, a comprehensive overarching software development capability that embraces Joint as well as respective environmental specialization does not exist for DND, consequently coordinated effort towards the achievement of a fully integrated command and control capability will be difficult.

An additional challenge in the realm of rapid technology advancement presents itself in the ever increasing micro-miniaturization of hardware in modern military capabilities. The conventional application of the often quoted "Moore's Law" whereby microprocessor computer devices double in density and speed while maintaining the same cost over an eighteen month cycle is well recognized. Both government and industry forecasts for capability delivery and procurement costs have respected this convention since the early 1990's, however, the predictability of this law is increasingly being challenged in light of disruptive advances in microminiaturization of new technologies to the order of nanometres. New microcircuit designs are reaching physical

[88] US General Accounting Office, Defence Acquisitions: Stronger Management Practices Are Needed to Improve DoD's Software Intensive Weapon Acquisitions, GAO-04-393, March 2004.

limits in terms of low level currents associated with the transmission of digital signals leaking across microscopic insulators which pose significant information assurance implications as well as increasingly expensive associated manufacturing costs.

Photonic switching which relies on laser technology as opposed to electricity offers the advantage of being faster by factors of thousands over conventional electronic based circuitry and more inexpensive to fabricate. Notwithstanding, to date, critical key elements associated with realizing this capability, namely the production of inexpensive non-linear crystals to quickly switch light beams at reasonable power levels have proven infeasible to manufacture at commercially viable levels.[89]

An additional consideration however relates to government inclination toward the acquisition of COTS based products which poses the potential challenge of creating significant technology assurance risks in light of micro-miniaturization or the rapid lowering of the cost associated with acquiring such devices. Given such technology advancement, adversaries or terrorist entities also benefit by gaining easier access to increasingly sophisticated and advanced commercial technologies.

To that end, in considering the many technology development considerations cited above that relate to the development, exploitation and protection of key technologies employed in support of C4ISR capabilities, the ability for government, in particular Defence, to be able to track and manage such technology development and successfully influence industry becomes increasingly difficult. Given the current DND capability development and acquisition construct whereby solid engineering development and programme management is de-emphasized, this poses an increasing challenge to the CF's ability to develop, acquire and field effective systems.

Technology Transfer Threat to Canadian NCW Capability Development

The capability of modern military weapon systems is heavily dependent on advanced technology, and consequently, the ability for a nation to maintain superiority in this very competitive field, is dependent on its ability to innovate and field advanced technical capabilities ahead of adversaries. Given the desire to minimize costs associated

[89] The CoolScience Center, http://www.rmrc.org/photonics/photon1.htm.

with technology development, modern western militaries have increasingly relied on procurement of COTS systems which are openly available commercially to potential adversaries. The critical design and manufacturing associated with the development of these systems is increasingly reliant on off shore capability in nations that may not be sympathetic to the west. The potential implication of such a trend is that the technological advantage over potential adversaries that modern military nations rely upon may in fact disappear over time.[90] A number of reasons present themselves; these include the de-emphasis of technical education within North America as witnessed by the fact that a majority and increasing percentage of advanced degrees in electrical engineering and computer science are being awarded to foreign nationals.[91]

Additional issues arise in the areas of export controls associated with the off shore transfer of high technology development and manufacturing, particularly in the areas of integrated circuit design and fabrication techniques. Foreign acquisition by non-aligned nations of North American companies involved in such fields demonstrates a potential for an erosion of the North American defence industrial base.[92] Further, in the case of the US, a significant proportion of semiconductor manufacturing capability is increasingly moving internationally. The US government once had dedicated microprocessor manufacturing facilities and selected suppliers to support the specialized classified needs of selected US agencies and allies such as Canada. However, the costs associated with customized low production volume microchips has risen significantly in light of technological advancement and manufacturing techniques associated with high production volumes. Consequently, in light of an inadequate economic model to serve as an incentive for such fabricators to remain active, the manufacturing base to support DND manufacturing needs has fallen dramatically.[93]

[90] US Defense Science Board, UK Defence Scientific Advisory Council Task Force on Defense Critical Technologies Report, March 2006.

[91] Eric Chabrow and Marianne McGee, Immmigration and Innovation, Information Week, 23 Feb 2004.

[92]Countries such as China have increasingly bought up advanced military technology production capacity internationally and subsequently seek export licences from US companies for advanced microprocessor fabrication equipment in order to make up for deficiencies in its own defence technology development capability. John Tkacik, China's Military Power, House Committee on Armed Services, 27 July 2005.

[93] Defense Science Board Task Force on High Performance Microchip Supply, US Department of Defense, February 2005, http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.

Consistent with the off-shore migration of the design, development and manufacturing base is the practice on the part of major North American companies to transfer high end research and development activities to overseas partners. Companies such as Microsoft and Intel have opened research and development facilities in China and other Asian countries. In order to support this development base, a large number of Ph.D. graduates and associated researchers (approximately 350 in the case of Microsoft) are employed in these locations. As well, corporate spending on information technology services has increased approximately tenfold over five years from $2B in 2003 with fifty percent going to places in Asia such as China and India. Among the most significantly outsourced government activities is that of defence.[94]

Research and Development

The impressive evolution in C4ISR technologies supporting the warfighter has been the product of a dynamic research and development environment over the past four decades into innovative technologies and material sciences that have enabled the fabrication and fielding of ground breaking advancements. In order to continue to maintain this competitive advantage, research into critical fields of science such as nanotechnology must be pursued in order to achieve the major innovations in material science and associated fabrication techniques that will enable the development of future generation C4ISR networks. Such research contributing to the development of radically new technologies is increasingly beyond the scope of but an exceptionally few nations. Consequently, the associated high risk investments increasingly require international collaboration, and as such, in order to maintain relative influence in such multi-lateral engagement, nations such as Canada may need to develop stronger policies to foster domestic education in engineering, science and technology and develop an enduring culture of research within the defence community which comprises government labs, private industry and universities.

As it regards capability development within the CF/DND, the requirement for rapid high technology capability insertion imparts an increased focus on activities related

[94] Paul McDougall, Optimizing Through Outsourcing, Information Week, 1 Mar 2004.

to research and development. Traditionally, pure research and development has been focused on extended timelines, such as ten or more years and concentrating on future generational technology steps. Given the fragmented adoption of many technologies in light of evolving industry standards alignment, commercial business cases and integration into existing fielded capability evolution paths, a tension is created between pure research and development organizations and in-service support organizations responsible for the development, procurement, engineering and maintenance of fielded systems that must work within much tighter timelines. To that end, an iterative or spiral development process is appropriate to C4ISR capability implementation given that overall system requirements can at best, only be broadly defined and the final detailed end product is not known.[95]

Such a methodology accommodates the evolution and refinement required during development however, associated federal government procurement processes are not postured to exercise the necessary flexibility in project approvals and expenditure authority to facilitate such a dynamic development environment. The consequent limited resources devoted to pure research conducted by DND organizations tends to be oriented at extended time frames which although appropriate in terms of investigating potential future generation technology trends, does not assure their linkage to the existing in-service capability base from technical, programmatic and financial approval perspective.

The current DND C4ISR capability development plan[96] specifies that Departmental C4ISR plans are to be developed centrally, and as such, would increase the participation from across DND by the organizations involved in the definition and development of C4ISR requirements and implementation. Regrettably, in light of limited resources, the necessary level of user involvement has not been fully realized, thereby compromising the capture of clear user requirements and the full institutional backing for supporting development, acquisition and fielding activities. Further, the spiral objectives developed as part of the Departmental plan were developed without the benefit of an

[95] Canadian Forces C4ISR Command Guidance and Campaign Plan, December 2003 sourced from web archives DND Departmental Wide Area Network.
[96] Ibid.

enterprise architecture, and of the spiral objectives, many were very broadly defined and consequently would be subject to interpretation.[97]

Acquisition of C4ISR Technologies

Although the identification and development of independent technologies is considered to be research and development, the delivery and fielding of an integrated C4ISR capability is not within the responsibility of a research and development organization. Such activities require the involvement of a number of actors that include various government departments such as DND, Industry Canada, Public Works, agencies such as the Communications Research Centre and private industry. Given current personnel and financial resource limitations as a result of a DND/CF de-emphasis of engineering and project management capability, DND/CF organizations responsible for these disciplines are pressed to deliver and manage such activities. To that end, there is a critical need to recruit and develop the best possible personnel to carry out these responsibilities.[98]

The rapidly advancing nature of technology and the continually evolving nature of user expectations, raises the question as to whether existing federal government procurement practices are suitable to the contemporary operational environment. Current Canadian procurement practices are postured to support procurement and sustainment of discreet platforms whose associated technology remains stable over an extended period of time, requiring only replacement of identified sub components and assemblies. Procurement budgets and processes are predicated on extended requirements definition and approval processes that lead to the acquisition of a discreet platform that is expected to have a life-cycle in the order of tens of years with planned operations and maintenance sustainment activities limited to replacement of well defined subcomponents throughout the lifespan without incremental enhancements in capability.

[97] Office of the Auditor General, Report of the Auditor General of Canada to the House of Commons – Chapter 4 – National Defence – C4ISR Initiative in Support of Command and Control, April 2005.

[98] Department of National Defence, Defence Science Advisory Board Report 0912, Conceptual Framework for DND's National ISR System, Ottawa, November 2009.

C4 capability is now critical to supporting the breadth of operational and sustainment environments within DND, and as such, must be flexible and capable of readily evolving.[99] To that end, procurement practices must permit greater flexibility in accommodating rapid focused procurement in support of iterative system development. One approach to achieving this is having the acquisition community more directly engaged with the warfighter and system engineering development community so as to tailor or revise current procurement protocols in order to be more agile and adaptable in supporting evolving network enhancements. In that spirit, the traditional DND extended acquisition cycle must be accelerated to maintain currency with commercial high technology development.[100] Consequently, military programme development cycles must be aligned with those of commercial industry, which are typically measured in terms of years and months as opposed to decades.

Intelligence Surveillance and Reconnaissance Transformation Requirements

Analysis

Recent operations in Afghanistan and Iraq have demonstrated the significant transformation that Intelligence, Surveillance and Reconnaissance (ISR) capabilities have made over the past decade given the high standard of precision engagement that have become the expected norm. The military's ability to capture and move data has increased significantly in light of higher bandwidth transmission and higher speed processing technologies. Notwithstanding, the emerging concern is that the analytical capability, largely a function of the human element is now the main impediment to increasing operational tempo. A number of potential innovative approaches present themselves. Examples include the use of contractors producing unclassified products that would compete with traditional classified analysis and reporting; the more aggressive exploitation of artificial intelligence (AI) in support of database analysis; and the potential establishment of even more operational analysis centres. Given the dynamic

[99] Colonel R.G. Mazzolin, Director Land Command Systems Program Management, Presentation to COS ADM(Mat) 8 Feb 2008 in support of DLCSPM Development.
[100] Ibid.

and fluid nature of what constitutes "information" during recent military operations over the past decade, it is argued that traditional analytical models and tools such as databases developed during the cold war are reaching obsolescence and as such, the case may be made for a revised approach to analysis.[101]

Intelligence and Warning (I&W) represents an activity associated with intelligence analysis that warns of impending enemy actions and is dependent upon the ability to anticipate and predict enemy actions or attacks. This has traditionally been based upon knowledge gained from research of adversary's established doctrine, plans, training and exercises. As today's adversaries become increasingly aware of technologies and associated techniques used to gain intelligence on their activities, they constantly evolve the manner by which they conduct their activities in order to avoid observation and detection. Consequently, the utility of traditional templated databases has becoming increasingly limited. The need has evolved to that of very specific information, delivered rapidly so as to concurrently satisfy the exigencies of a specific nation's world-wide strategic interests as well as the accurate delivery of precision guided munitions. The requirement has become even more acute in light of the need to maintain intelligence on the diffuse employment of a wide range of weapon systems by friendly and adversary combatants associated with either traditional cold war entity, and the requirement to maintain a much broader range of information on the civilian population in light of the diminishing distinction between combatants and non-combatants. Clearly, Canadian operations have seen the scope and nature of activity within deployed ASICs in Afghanistan and the associated support from Canada evolve significantly.

Interoperability

The issue of stove-piped intelligence conduits has been the subject of much consideration. The military concept of amalgamating the products from the respective intelligence disciplines to ensure that the most complete and accurate representation of the environment is provided is a tenet that is long-standing in the military intelligence

[101] Bruce D. Berkowitz and Allan E. Goodman, Intelligence in the Information Age, Yale University Press, New Haven, CT, 2000, p.100.

community. Therefore, the issue related to interoperability is that there must be an ability to share products freely between the different intelligence producers. New concepts that have been developed include the Canadian All Source Intelligence Cell (ASIC) and US Army Reconnaissance, Surveillance Target and Acquisition Squadrons, US Defense Intelligence Agency's Joint Intelligence Virtual Architecture and the rapidly increasing emphasis on the use of Unmanned Vehicles in the various environments. Significant emphasis has been placed on the development of tools to support analysis given the evolution in the sources of intelligence. For example, the primary source of intelligence throughout the cold war was made available only through classified sources, however, an increasing amount of information is now becoming available through open source means such as the internet. To that end, potential constructs could involve a more decentralized, market based approach to intelligence gathering and analysis, possibly soliciting contributions from contractors and civilian blogs.[102] Consequently, the judicious extension of DND classified command and control networks outside the Department to other governmental partners enables the possibility of significant changes in the use of intelligence.

Military Leadership in the Intelligence, Surveillance and Reconnaissance Community

Operations in Afghanistan over the past decade have captured the priority of effort of the CF and Canadian Government. As a consequence, C4ISR activities have been heavily postured with this imperative in mind. However, consistent with the principal that a nation's responsibility is to provide security for its citizens, the requirement for a nation as large as Canada to have appropriate situational awareness of activities across its territory is intuitive. Although it can be argued that airspace surveillance is well defined and largely accomplished via the collaborative partnership with the US under the NORAD agreement, there are additional specific surveillance requirements in support of maritime activities as well as the arctic where focused indigenous CF capabilities must be developed. Although other government departments,

[102] Robert David Steele, On Intelligence: Spies and Secrecy in an Open World, AFCEA International Press, Fairfax, VA, 2000, p.76.

namely Transport Canada and Fisheries and Oceans have surveillance responsibilities, the primary responsibility will remain with DND in light of its global responsibility for security and significant programmatic development capability that would enable only DND to sustain this type of activity in the long term.[103] The challenge that exists however, in terms of establishing priorities and direction for capability development and operational requirements is the absence of a detailed national threat analysis in light of the focus of the existing limited intelligence resources toward the Afghan theatre. Lacking such an analysis, it is impossible for DND to posture a comprehensive cost-effective programme to acquire future ISR capability.[104]

A further consideration is that given the range of potential threats and the vastness of the territorial space to be protected, notwithstanding the DND/CF pre-eminent role in this environment, such an undertaking is not feasible without the involvement and support of other government departments and agencies. It must be understood that any ISR asset being employed by any organization provides only part of the overall picture. Consequently, a mix of assets must be used and the employment of such assets must be driven by operational requirements, not solely a fixation on technology. Certainly, the optimization of programmatic feasibility, efficiency and return on investment is predicated upon the re-use of platforms for multiple uses such as search and rescue, environmental resource assessment, climatic observation etc.[105]

Two additional aspects that must be considered from this perspective include the need for modern military forces such as the CF to maintain an indigenous capability to develop and field ISR equipment and capabilities and the selection of leadership with the requisite background in the discipline. In the first instance, as a result of the demise of the cold war environment, national intelligence agencies such as the NSA and the Canadian Communications Security Establishment (CSE) had re-oriented activities to strategic economic related issues and the significant emerging scope of the strategic commercially based electronic environment. This caused a resultant decrease in support

[103] Government of Canada, The National Security Policy (NSP) dated 2004.
[104] Department of National Defence, Defence Science Advisory Board Report 0912, Conceptual Framework for DND's National ISR System, Ottawa, November 2009.
[105] Ibid.

to the military domain[106]. To that end, military forces have identified measures to mitigate the loss of national agency support. Such measures have included the upgrading of land, maritime and aerial platforms, the fielding of UAVs, the US based PROPHET tactical ground based sensor system and Canadian Land Force Intelligence Surveillance Target Acquisition and Reconnaissance (LF ISTAR) program in addition to SOF enablement. Notwithstanding that re-orientation of national agency activities has taken place throughout the period of operations in Afghanistan and Iraq, there remains a requirement for service driven tailored support to the warfighter. In that light, there is still a requirement for the military to develop indigenous intelligence capabilities as well as receive support from national agencies in the areas of technology and access critical to the advancement of military programs.[107]

The second aspect relates to the issue of selection of senior leadership positions in NCW related disciplines. Most militaries place their greatest emphasis for selection to senior leadership positions on those officers who have been trained and served in organizations whose primary role is the direct engagement of military assets with lethal force. Officers who have served a significant portion of their careers in areas of C4ISR with exceptional rarity are selected to be environmental chiefs. Since the inception of the Chief of Defence Intelligence at National Defence Headquarters, no officer named to the post has pursued a career path predominantly oriented in this domain.[108] In the case of the US military, those chosen are typically those that have been associated with the planning and employment of kinetic effects as opposed to the procurement, planning and employment of C4ISR capabilities.[109] Paradoxically, the increasing replacement of military officers with civilians in positions of leadership within organizations associated with the C4ISR capability area further limits the opportunities for advancement and influence for military officers whose background is oriented toward this discipline. Although empirical data to support such an assertion may not exist, it is probable that the strength with which C4ISR related issues are progressed within the DND leadership

[106] Best, Richard. The National Security Agency: Issues for Congress, CRS Report RL30740, 7.

[107] Discussions with C4ISR Programme staff Sept 09-April 10.

[108] Since the inception of CDI during General Hillier's term as CDS in 2004, the respective CDI's have been 1 Infantry Officer, 2 Combat Engineer Officers, and 1 Armoured Corps Officer.

[109] Vernon Loeb and Thomas Ricks, 1's and 0's Replacing Bullets in US Arsenal, Washington Post, 2 Feb 2002.

would be reduced as well as the potential range of solutions that senior DND leadership would explore to face the challenges posed by new situations and adversaries.

Although it makes sense that those entrusted with the responsibility to direct soldiers into battle be combat officers, there do exist other senior level positions at the senior General rank that do not command combat forces. Therefore, the question that must be considered is that if NCW effects and C4ISR capabilities are becoming increasingly important to modern military forces and national security, is the information and intelligence supporting the weaponry becoming more important than the weaponry itself? Consequently, it may make sense for greater numbers of officers with such a background to be selected for senior positions in the area related to the provision of command support and intelligence.

Financial and Organizational Considerations

Financial

The 2005 Report of the Auditor General of Canada reviewed the planned expenditures for 91 C4ISR related projects associated with the transformation activity. Of the $9.7B total identified spending available, $5.7B was identified as remaining to be spent between 2005-2015. Although it is asserted that this planned amount, which could in some years represent up to 40 percent of the capital equipment budget, the actual approved amount is only $1.7B against a Strategic Capability Investment Plan and approved projects amount of $23B.[110] Spending in support of the Afghan mission and future departmental capital investments have placed significant pressure on anticipated C4ISR related capital spending and if appropriate prioritization of the remaining planned and unfunded projects is not done, the possibility of a coherent C4ISR infrastructure will be placed in jeopardy. Notwithstanding, given the large number of projects which are potentially required to realize the planned comprehensive C4ISR infrastructure, the inability to fund a significant portion of these projects will further place this objective at

[110] Office of the Auditor General of Canada, Report of the Auditor General of Canada to the House of Commons, Chapter 4 National Defence – C4ISR Initiative in Support of Command and Control, April 2005.

risk. Of these projects, it was determined that they were proceeding in the absence of an overall plan in place. In order to mitigate this risk, the planned projects have been prioritized into three categories; enablers – those that are considered key to implementing C4ISR, related projects – those that are part of the C4ISR initiative to address capability deficiencies, and "other" projects – those that are identified as part of C4ISR.[111]

Consideration of the Canada First Defence Strategy released 12 May 2008 identifies potential gaps as it regards C4ISR funding.[112] Although the stated amounts for capabilities such as tactical airlift, battlefield helicopters, main battle tanks, arctic offshore patrol vessels, joint support ships, destroyer/frigate replacement, maritime patrol aircraft, next generation fighters and the new family of land combat vehicles amount to approximately $18B, the amount does not appear to take into consideration critical projects identified in the Departmental Report on Plans and Priorities issued in April 2008, which includes C4ISR related capabilities such as fixed wing search and rescue aircraft, uninhabited aerial vehicles and an integrated command and control system for the CF.[113]

The figures articulated quantify acquisition costs only, and subsequent sustainment costs for the maintenance of newly acquired equipment over a 20 year time period comfortably amount to fifty percent of acquisition costs. Notwithstanding budgetary announcements by Prime Minister Harper which effective FY 2011/2012 invoke an automatic annual budgetary increase of 2 percent out until FY 2027/2028 for a $28B defence budget in that year, not all of this funding can be used in support of capital acquisition.

The Canadian defence budget is effectively divided into three parts; costs associated with personnel, operations and maintenance, and capital acquisition whereas the latter captures costs associated with the full spectrum of platforms from ships, aircraft, armoured fighting vehicles, buildings as well as C4ISR capabilities. On an annual basis, personnel costs account for over 50 per cent of this budget, and given the stated intention to increase CF manning to 70,000 personnel, this relative level of expenditure is not likely to decrease. In light of the increased tempo of operations that

[111] Ibid.
[112] Canada First Defence Strategy, Minister of National Defence, 12 May 2008.
[113] Departmental Report on Plans and Priorities, April 2008.

the CF has undergone over the past twenty years, a significant portion of the defence budget is allocated to cover those expenses with the remainder being allocated to capital activities.

During periods of high operational activity, the capital program becomes the source of funding to sustain the remaining two areas. Although as a general principal NATO nations endeavour to maintain capital investment at a level between 20 – 25 percent of defence budgets, this has not been achieved in Canada as DND has been challenged to maintain a level of 10 percent.

Assuming that this was to continue, DND by extrapolation would receive approximately $42B for capital based activities over the next twenty years. Given the lack of capital investment throughout the 1990's however, this has created a situation whereby a broad range of military platforms from ships, aircraft, armoured fighting vehicles must be replaced during the same period of time between 2012 to 2017. The CF will require $30B over the next 5 years to initiate this process, and subsequently an additional $15B over the following 20 years to maintain it. Consequently, of the $42B theoretically available, the majority of this capital acquisition spending must be skewed earlier in the 20 year timeframe to accommodate these capability pressures. Therefore, the comparatively low level of capital funding relative to other CF activity areas, combined with the requirement to expend the large majority of funding toward major platforms to address obsolescence and the absence of emphasis in the CFDS toward the C4ISR capability area, the prospect for increased emphasis on the area of C4ISR is not positive.[114]

Organizational Considerations

The cost consideration of separate C4ISR capability development by the various environments has highlighted potential inefficiencies. Although the recognition of the requirement for a structured and disciplined approach to C4ISR development has been recognized, the mechanisms by which DND would prioritize projects, develop a comprehensive program underpinned by a joint C4ISR doctrine and concept of

[114] Presentation by MGen S. Beare, CFD, to NSP January 2010.

operations to serve as a blue print had not been in place by 2005.[115] The assignment of overall systems development responsibility to the Assistant Deputy Minister Information Management was seen as a key enabler to this end. However, a clear conceptual construct for the C4ISR capability and associated development supported by goals, success criteria and interoperability does not yet exist.

Among the deficiencies noted was the need for appropriately skilled personnel to develop, operate and sustain these systems. Although it is felt that the human resource deficiency may be mitigated to some extent in the short term through the reliance on in-house senior military personnel with enhanced training, it recognizes that the timelines required to identify, secure and train appropriate people to fill C4ISR positions needs to be accelerated.[116] Recognizing the importance of C4ISR, ADM HR (Mil) and ADM HR (Civ) are represented on the departmental level review and decision boards related to C4ISR programs, and there is indication that it is a stated intention to put in place an HR plan to address C4ISR requirements. Notwithstanding these measures, it is recognized that skill-set shortages will exist consequently requiring the use of civilian resources to mitigate the shortfall of skill-set resources.[117]

It was identified that in 2003, the CF lacked over 700 officers and non-commissioned members with the required competencies to carry out the responsibilities associated with C4ISR. Although it was felt that the initial development of C4ISR capability could be achieved from within CF resources, there are a number of critical skill sets that were identified as being difficult to resource from within the existing and projected military human resource processes. These include:

a. ISR fusion analysts for specific spectral systems,

b. Content managers for information processing and database management,

[115] Sheila Fraser, Auditor General of Canada, Opening Statement to the Standing Committee on National Defence and Veterans Affairs; National Defence – C4ISR Initiative in Support of Command and Control, http://www.oag-bvg.gc.ca/internet/English/osh_20050421_e_23427.html.
[116] Ibid.
[117] Ibid.

c. Web Administrators for Web-based content management and dissemination.[118]

Although not identified in the report, the increasing technical complexity, and distributed industry base from which to source systems being procured mandates the requirement for a very strong systems integration capability within DND in order to rapidly adapt and integrate such systems into an evolving C4ISR technology baseline. To that end, there is the need to engage through various means the necessary engineering expertise in order to carry out this work.[119]

Among the most effective of such techniques is the use of flexible contracting processes with industry in order to secure the appropriate technical skillsets. An innovative approach to this end has been employed by the Director Land Command Systems Program Management as the Army C4ISR Programme Manager, through the development and award of three Long Term Support Contracts; Engineering and Integration, Software Support and Weapon Systems Management. Federal public service hiring practices are insufficiently responsive for ensuring that dynamic C4ISR programs are adequately resourced given that hiring timelines for personnel with specialist skills typically take years, thereby failing to satisfy important requirements and causing the loss of individuals with critical skills to industry. Therefore, the benefit of such an arrangement is that of being able to quickly secure personnel with the necessary technical skill sets so as to be able to accomplish the necessary development, acquisition and fielding work.[120]

As of 2005, it was expected that once conversion training for military personnel within DND from non-technical to technical trades and modification of existing career and training paths was initiated, seven years would be required to address the issue of recruitment and training of personnel with strong information management and technology skills. Initial engagement of these issues did not take place until 2007 where

[118] Office of the Auditor General, Report of the Auditor General of Canada to the House of Commons – Chapter 4 – National Defence – C4ISR Initiative in Support of Command and Control, April 2005.

[119] Colonel R.G. Mazzolin, Director Land Command Systems Program Management, Presentation to COS ADM(Mat) 8 Feb 2008 in support of DLCSPM Development.

[120] Colonel R.G. Mazzolin, Director Land Command Systems Program Management, Presentation to COS ADM(Mat) 8 Feb 2008 in support of DLCSPM Development.

some of these concerns were engaged via the Military Occupational Structure Analysis, Redesign and Tailoring (MOSART) project through its analysis of C4ISR human resource requirements. To that end, concern had been expressed that efforts toward resolving these human resource issues were not advancing at a sufficient pace to remain current with CF Transformation requirements, thereby putting at risk the ability of DND to satisfy its demands.[121]

The Assistant Deputy Minister Information Management Group released an IM Group Campaign Plan in 2009 which outlined in broad terms three key strategic objectives for the provision of corporate information management services; enhancing information management governance, delivering-operating-sustaining, and aligning and developing.[122] Reflective of the departmental focus that has evolved within the IM group after the dissolution of Canadian Forces Communications Command[123] in the early 1990's, the plan maintains the existing organizational structure and places greatest emphasis on its alignment toward the effective management of the corporate IM/IT and Enterprise Resource Management system environment. This organizational emphasis detracts somewhat from the necessary focus on the maturation of an Integrated Command and Control Capability and enhanced connectivity with the Canadian Secure Network Infrastructure (CSNI) via the Integrated Command and Control Capability Strategy[124] that would effectively enhance the departmental backbone over which a broader integrated C4ISR capability could reside. Therefore, the plan does not as yet embrace the broader scope of ISR and related capabilities independently resident with the VCDS group under Chief of Force Development (CFD) such as the Directorate of Space Development, CF Experimentation Centre (CFEC) etc. Consequently, clarity as it regards how the broadly distributed intelligence, surveillance and reconnaissance

[121] Office of the Auditor General, Report of the Auditor General of Canada to the House of Commons – Chapter 4 – National Defence – C4ISR Initiative in Support of Command and Control, April 2005.

[122] Department of National Defence, Information Management Group Campaign Plan, 1000-1 (ADM(IM)) released 2 June 2009.

[123] Canadian Forces Communications Command served as an operationally focused military structure focused toward the provision of military command and control capability to the Canadian Forces. It was restructured over a period of years in the early 1990's into a civilian led service provider organization with institutional focus toward corporate information management services.

[124] Department of National Defence/Canadian Forces, Integrated Command and Control Capability Strategy 1180-1 (DMilCM3) 23 July 2008 issued under joint signature of CFD and COS(IM).

capability base would be embraced in conjunction with the C4 capability as part of a holistic, effects based departmental C4ISR capability does not yet exist. Among the primary challenges is the absence of a consolidated organizational perspective that coalesces the broader institutional doctrinal, operational requirements, infrastructure development, engineering, integration and training considerations across the broader C4ISR environment in the form of an effects based environment.

The Canadian Forces C4ISR Capability Development Strategy issued in 2009 recognizes the need to develop a comprehensive and integrated DND/CF approach to C4ISR capability development. As part of this strategy, a key enabling element is the establishment of the Canadian Forces Experimentation Centre (CFEC) as a centre of excellence, to serve as a vehicle to coalesce the contributions of a number of key stakeholders such as ADM(IM), ADM(S&T) and the various ECS's specific development centres to develop joint doctrine, concepts of operations and serve as the CF's central repository for lessons learned.[125] The document defines a C4ISR framework and identifies the need for the Doctrine, Organization, Training & Education, Materiel and Policy (DOTMP) elements to evolve and develop in unity with technology components in order to exploit and capitalize upon the enhanced C4ISR technological capabilities supporting a broader operational capability. The guidance further recognizes the involvement of a number of other stakeholders including Allies, security partners, OGDs and NGOs. The strength of such a collaborative development environment is recognized as it emulates, in many respects, the iterative laboratory development environments currently in place by the respective ECSs and CANSOFCOM in the formulation of their environment specific C4ISR capabilities.

In order to move this forward however, there is a need for a focused development, engineering and project management structure that will facilitate the material realization of such capabilities. The complementary CF C4ISR Capability Development Plan identifies a range of challenges to the CF in its advancement toward a holistic and integrated C4ISR strategy which is consistent with the institutional challenges cited

[125] Canadian Forces C4ISR Capability Development Strategy issued under signature of VADM J.A.D. Rouleau, VCDS dated 13 July 2009.

earlier in the paper.[126] Notably absent from these is the focused engineering development, project management and acquisition authority that is vitally critical to actualize and integrate many of these concepts. It must be noted however, that the generic capability to provide such a function currently resides in both ADM(IM) and ADM(Mat) groups, however, it is not yet ideally postured. Consequently, the solution may be provided via a rationalized approach whereby an operationally focused, joint C4ISR engineering development and acquisition organization is established in order to serve as the basis upon which to build this critical function. To elaborate, there is currently no organization as of yet focused on joint C4ISR engineering development and acquisition. The existing organizations within the ADM(Mat) group are focused on the respective land, sea and air environments whereas the capability within the ADM(IM) Group, although slowly evolving toward greater involvement within the strategic command and control (C4) environment, does not as of yet embrace the joint ISR environment.

The question therefore arises as to whether the CF in its current construct is ideally suited to enabling NCW operations and fully exploiting the C4ISR capability base currently at its disposal and further enhancing it commensurate with the requirements of an evolving security environment and associated technological developments. Part of the limitation is a result of the current CF institutional focus on "domain" rather than "effects" as the current CF paradigm emphasizes combat effects over combat support effects. Given the increasing emphasis on combat support effects in the form of NCW concepts and capabilities to support combat operations as demonstrated in the earlier parts of this paper, the argument may be posed that greater institutional focus needs to be placed on consolidating and more effectively enabling such effects in support of a joint approach.

A potential approach would be to separate institutional focus between combat effects and combat support effects by creating a separate organization specifically focused on the provision of NCW related combat support effects at the Joint level across the CF. This would serve to consolidate a comprehensive, flexible C4ISR program able

[126] Canadian Forces C4ISR Capability Development Plan 1180-1(DMilCM) dated 31 August 2009 issued under authority of CFD and CF J6/COS IM.

to integrate environmental specific NCW or combat support capabilities with a cohesive joint and strategic capability environment. Such a structure would better take advantage of potential synergies between the various elements that make up the combat support function in each combat environment and joint/strategic level thereby contributing in a vital way to the execution of combat effects. The principal thrust of the concept is the consolidation of the activities and organizations associated with the production of support effects into a unified structure that benefits from the synergies to be gained by organizing, developing, engineering, sustaining and training similar capabilities that would enable the CF to be a more effective military force across the range of operations it is likely to undertake. Organizing along these lines emphasizes common effects as opposed to common domains and would enhance the ability of the CF to assert cross domain dominance in a more flexible, balanced manner across the potential spectrum of CF operations.

Part 4 Summary Comments

The development of an organization intended to manage an emergent transformational capability for a modern military such as the CF, must consider the key issues related to the capability as the foundation upon which to posture the organization. To that end, many of the issues that will require particular consideration involve the development and management of emergent areas of technological capability. The development of a robust C4ISR capability is heavily dependent upon the integrity of the underlying network infrastructure which is required to rapidly evolve in response to user requirements and technological advancements. Fundamental issues relate to bandwidth, network quality of service and associated computer processing considerations. Issues such as IPv6 transition and microminiaturization pose tremendous challenges to integrated network evolution. The problem becomes further compounded when considering the requirement to engineer previously unconnected space based, unmanned remotely controlled vehicles and emergent networked weapon and sensor systems into a comprehensive interoperable capability. The challenge from an interoperability perspective is further exacerbated when the requirement to rapidly interconnect sensors and networks from other countries, agencies and organizations which had not originally been designed to do so. In order to maintain a capability to do so invokes the requirement to maintain an advanced and flexible indigenous technical capability which is dependent upon second order effects arising from technology transfer, research and development, hiring practices, education and associated acquisition approaches. Current CF focus in this area is deficient and would benefit from the creation of a focused joint engineering and development organization.

Similarly, the Intelligence discipline has been profoundly impacted by advancements in NCW concepts and C4ISR technology. This has required the Intelligence community to reassess fundamental approaches relating to the analysis discipline both from the perspective of techniques needed to deal with the emerging security environment as well as processing technologies used to carry out the analysis function. Issues of interoperability pose particular challenges from the perspective of the requirement to rapidly integrate various nations, agencies and organizations in support of operations, and who do not have pre-existing relationships and varying levels of trust. This consideration raises the issue of military leadership in a broader governmental and multi-agency environment in order to secure the necessary sources and analytical capacity to prosecute NCW based operations as well as the need for specialization in the Intelligence discipline at the most senior ranks in the military.

Finally, funding of such capability development remains problematic from a CF perspective in light of the requirement to procure and replace major air, land and maritime platforms that have "rusted out" as a result of the absence of investment during the 1990's and early 2000's. To that end, aside from the heavy near term demand on capital funding by the major environments, the absence of a Joint organizational champion to advocate for resources and develop capabilities in order to progress C4ISR capability development inhibits the ability for the CF to fully benefit from the potential transformational effects of C4ISR enabled NCW concepts. This highlights the requirement to shift the focus of CF organizational alignment from that of a "domain" based focus where air, land and maritime functionality is predominant to one that more greatly emphasizes "effects" such as that provided by the combat support capability afforded by NCW concepts. Consequently, there is significant potential benefit to be derived from the synergy achieved by concentrating the institutional capabilities dealing with C4ISR doctrinal and engineering development, project management, and acquisition into one Joint focused organization.

Part 5 - Conclusions

It has become clear that modern military forces are achieving and relying upon increased shared situational awareness facilitated by progressive NCW concepts and enabled by rapidly evolving C4ISR technologies. Mission effectiveness is being increasingly enhanced via continuing refinements through the innovation of new ways of conducting operations that accelerate speed of command and tempo through increased networking which, in turn, contributes to information sharing, shared situational awareness, synchronization and collaboration.

Although the scope of the scenarios (Air to Air, Land Maneouvre, etc.) cited in Chapter 2 is extensive, it is recognized that evidence presents itself largely in qualitative form from limited portions of the overall mission spectrum, and therefore may be challenged from a rigorous quantitative perspective. Consequently, current efforts to develop empirical evidence of the power of C4ISR enabled NCW constructs remain subjective, rather than focused or systematic. However, the fact that few of the scenarios considered in Chapter 2 actually reach across the full complexity of mission areas, joint task forces, operational level missions, or operations other than war that dominate practical experience today but nonetheless provide tremendous effects, indicates that although much work remains to be done, great potential exists in continuing the maturation of C4ISR capabilities and concepts.

Notwithstanding that much of the analysis serves to emphasize the progress that has been made over the past twenty years and confirms the value in bringing a consolidated C4ISR enabled NCW capability to bear in support of contemporary operations and the potential that it holds as a force multiplier, there is some care required in the implementation of these capabilities in light of limitations related to social dynamics, cognitive considerations, the practical limits of the laws of physics and the manipulation of technology by an increasingly sophisticated adversary.

The absence of a widely recognized conceptual and architectural framework for defining a C4ISR enabled NCW environment and measuring the value and/or maturity of network-centric operations has hindered the evaluation of exercises, experimentation, and operational evidence. Notwithstanding, the value of such results and evidence should not be trivialized. The significant improvements in combat power that have been repeated anecdotally support the quantitative results obtained through the various experimentation activities and operational missions to date lends credence to the assertion that Network Centric Warfare and the ability of maturing C4ISR technologies and capabilities serve a central role in making modern military transformation a reality. Clearly, there is a benefit to going beyond traditional combat to explore the full range of command and control concepts enabled by Information Age technologies and employing a more systematic approach to organizing research, collecting evidence in operations, exercises, experiments, and demonstrations, and in assessing that evidence so as to identify areas of institutional focus required to enhance this capability area.

To that end, from a Canadian perspective of a modern western military of modest means, there is clearly the sense that military organizations should fully exploit technological advancements in order to achieve the information advantage over potential adversaries that is critical to assure success in contemporary operations. Care, however, must be exercised in his regard so as to not be fixated with the technological scope of potential contribution to CF operations. Consequently, in order to achieve success in this environment, it is critical that the CF/DND fully embrace the nature of transformation in its broadest institutional sense and the associated conceptual shift in the nature of combat from that of purely kinetic primacy to that of greater emphasis on NCW related combat support forming the military contribution to the unique roles that Canada undertakes in the international stage.

The next evolutionary step in terms of holistic NCW discipline development involves the greater integration and fusion of information supporting a consolidated military command and control environment from the many different sensor systems resident in both military and non-military organizations increasingly being employed on a wider variety of platforms for different requirements. The challenge is in integrating the many systems that may not have traditionally been considered to be within the strict military ISR domain into a comprehensive, joint communications, command and control environment so as to facilitate even broader situational awareness across the different environments (land, sea and air) and throughout the command hierarchy (tactical to strategic and JIMP).

To that end, a number of institutional issues present themselves. The CF currently faces a challenge in identifying and addressing the many disparate C4ISR related issues in order to develop a truly comprehensive NCW capability. Among these are significant C4ISR infrastructure development and integration issues, considerations related to interoperability with military, nonmilitary and allied organizations and the increasing employment of sensors on an expanding base of platforms such as UAVs, and capability development in the context of emerging battlespace environments such as space and the network. Further, capability development in this discipline, perhaps more so than other military capabilities is dependent upon considerations related to a nation's and respective military's commercial technology development and industrial capacity. This is emphasized by the fact that in light of primarily economic considerations, there is an increasing trend for North American industry to develop relationships with developing nations with whom political alignment may not exist. This factor combined with the emerging technological capacity of a number of developing nations presents a potential risk to the technological superiority that modern western militaries have come to rely upon in order to mitigate numerical disadvantage. In that light, concerns arise as to DND/CF visibility and capacity to effectively engage and adequately address such complex and important issues.

Further, the CF/DND needs to more completely consider and understand the impacts that the embracement of NCW concepts has on personnel, CF culture and organizational constructs. Given the importance of social and cognitive factors that contribute to organizational development, a more detailed understanding of these considerations needs to be achieved in order to provide a basis for organizational changes supporting NCW concepts within the CF/DND. This is particularly true when considering the emphasis on CF integration into broader JIMP/3D contexts that embrace broader governmental activities. In that light, NCW potentially takes on a broader governmental context from a Canadian military perspective, which may serve to be a key differentiation from the US concept.

At the heart of the issue is the current posturing of a CF/DND C4ISR capability in light of the Canada First Defence Strategy which, following from the institutional success enjoyed as a result of the Afghan mission appears to have positioned the CF favourably from a financial perspective, at least in the short term. Regrettably, upon more careful inspection, given the absence of investment in CF capability during the 1990's, many of the CF's principal weapon systems and platforms suffer from "rust out" and require immediate replacement. The large capital investment required in the near term therefore puts at risk critical support for C4ISR development at this critical juncture. Notwithstanding, an emerging institutional appreciation within the CF leadership and institutional culture for the benefit of NCW concepts, a clear conceptual and management construct is only slowly evolving.

The absence of a Departmental champion consequently limits the influence of a C4ISR and NCW combat support domain advocacy to assert itself in the competition for scarce capital, maintenance, personnel funding and resources against the traditional air, land and sea combat domain environments. It may be effectively argued that in light of the increasing importance of net centricity in support of contemporary and future operations, a revised organizational construct emphasizing combat "effects" over the traditional combat "domains" would enable greater synergies between the organizations providing NCW support to operations across the breadth of CF operations. Given that many of the capabilities and organizational functions required to realize a comprehensive C4ISR based organization to support NCW capability within the CF reside in disparate locations within the Department, focused effort toward the development of a clear conceptual and organizational framework would permit the actualization of such a construct in the near future and thereby facilitate a major step toward CF transformation in the most complete sense.

Bibliography

1. Alberts, David et al., Network Centric Warfare, DOD Command and Control Research Program, October 2003.

2. Alberts, David and Richard Hayes. Power to the Edge, Washington, D.C.:CCRP, 2003.

3. Alberts, David S. and John J. Gartska, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd (Revised), Washington, D.C.:CCRP, 2000.

4. Auditor General of Canada, Report of the Auditor General of Canada to the House of Commons - Chapter 4 National Defence – C4ISR Initiative in Support of Command and Control; April 2005.

5. Babcock, Sandy. Canadian Network Enabled Operations Initiatives, Defence Research and Development Canada, undated (post 2004).

6. Bailey, J. Over by Christmas: Campaigning, Delusions and Force Requirements, AUSA Land Warfare Institute, The Land Warfare Papers, No. 51, September 2005, accessed 28 December 2009 from http://www.ausa.org/pdfdocs/LWP_51WBailey.pdf.

7. Berkowitz Bruce D. and Allan E. Goodman, Intelligence in the Information Age, Yale University Press, New Haven, CT, 2000, p.100.

8. Best, Richard. The National Security Agency: Issues for Congress, CRS Report RL30740, 7.

9. Blair, ADM Dennis. CINCPAC, An Assessment of IT-21 Warfighting Value-Added, Remarks during Keynote Address at WEST 2001, January 23rd, San Diego, Ca.
1 March 1999.

10. Bond, BG William L. USA, Army Digitization Overview, Briefing to Dr. Jacques Gansler, USD (A&T), at the Pentagon, Washington, D.C., on May 20, 1998.

11. Butler, Amy. Heavy DoD Reliance on Commercial SATCOM Prompts Questions of Protection, Defense Daily, 13 April 2004.

12. Canadian Forces C4ISR Campaign Plan, Interim Report, Director Joint Force Capabilities, 27 June 2003.

13. Canadian Forces C4ISR Capability Development Strategy issued under signature of VADM J.A.D. Rouleau, VCDS dated 13 July 2009.

14. Canadian Forces C4ISR Capability Development Plan 1180-1(DMilCM) dated 31 August 2009 issued under authority of CFD and CF J6/COS IM.

15. Castonguay, LCol Francis. Evaluating Canada's Cyber Semantic Gap, CFC JCSP 35.

16. Cateriniccia, Dan and Mathew French, "Network Centric Warfare: Not There Yet," Federal Computer Week, 9 June 2003, accessed on 7 January 2010 from http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp.

17. Cebrowki, VADM A.K. Written testimony to hearing on Defense Information Superiority and Information Assurance—Entering the 21st Century, held by the House Armed Services Committee, Subcommittee on Military Procurement.23 February 1999.

18. Cebrowski, Arthur K. and John J. Gartska, "Network-Centric Warfare: Its Origin and Future": Naval Institute Proceedings, January 1998. accessed 3 January 2010 from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm.

19. Center for Defense Information. USAF Transformation Flight Plan Highlights Space Weapons, 19 February 2004.

20. Center for Strategic & International Studies. The Future Combat System – What Future Can the Army Afford?, 5 February 2009.

21. Chabrow, Eric and Marianne McGee, Immmigration and Innovation, Information Week, 23 Feb 2004.

22. Christie, Rebecca. DoD Space Program's Costs Rise as New Plan Takes Shape, Wall Street Journal, 21 February 2006.

23. Congressional Review Service Report for Congress, Air Force Transformation, 25 January 2005.

24. Congressional Review Service. Military Transformation: Intelligence, Surveillance and Reconnaissance, Report for Congress, 31 May 2002.

25. Congressional Review Services. CRS Report for Congress – Network Centric Operations: Background and Oversight Issues for Congress, March 15, 2007.

26. de Lestapis, Jacques. DRONES, UAVs Widely Used in Kosovo Operations, article accessed 28 December 2009 from http://www.periscope.ucg.com/docs/special/archive/special-199907011327.shtml.

27. Department of Defense, Network Centric Warfare Report to Congress, 27 July 2001, 4-1. Internet, accessed 15 October 2009 from http://cio-nii.defense.gov/docs/pt2_ncw_main.pdf.

28. Department of National Defence/Canadian Forces, Integrated Command and Control Capability Strategy 1180-1 (DMilCM3) 23 July 2008 issued under joint signature of CFD and COS(IM).

29. Department of National Defence, Defence Science Advisory Board Report 0912, Conceptual Framework for DND's National ISR System, Ottawa, November 2009.

30. Department of National Defence. Departmental Report on Plans and Priorities, April 2008.

31. Department of National Defence, Directorate of Space Development, Canadian National Defence Space Strategy (Undated Draft) produced fall 2009.

32. Department of National Defence. Information Management Group Campaign Plan, 1000-1 (ADM(IM)) released 2 June 2009.

33. DRDC. Network Enabled Operations: A Canadian Perspective; Toronto No. CR-2005-162.

34. Ebbutt, Giles. Flaws in the System: Modern Operations Test Theory of Network Centricity, Jane's International Defence Review, July 2006, Vol 39.

35. English, Allan et al. Networked Operations and Transformation – Context and Canadian Contributions, 2007.

36. Eydt, Bernard, Software Assurance is Critical to SDR Success, COTS Journal Online, February 2006, http://www.cotsjournalonline.com/articles/view/100463.

37. Fulghum, David A. "DARPA Tackles Kosovo Problems," Aviation Week and Space Technology August 2, 1999, p. 55-56. John A. Tirpik, "Short's View of the Air Campaign," Air Force Magazine, September 1999, p. 43-47.

38. Federal Computer Week. DISA Chief Outlines Wartime Successes, 6 June 2003. Feickert, Andrew. Congressional Research Service. The Army's Future Combat System (FCS): Background and Issues for Congress, 3 August 2009.

39. Ferster,Warren. Military Bandwidth Demand Energizes Market, Space News, 2 September 2003, accessed 15 February 2010 from http://www.space.com/spacenews/archive03/militaryarch_090203.html.

40. Fisher, David and Dennis Smith, Emergent Issues in Interoperability, Carnegie Mellon Software Engineering Institute, No. 3, 2004, http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/eye-on-integration-2004-3.htm.

41. Fraser, Sheila. Auditor General of Canada, Opening Statement to the Standing Committee on National Defence and Veterans Affairs; National Defence – C4ISR Initiative in Support of Command and Control dated 21 April 2005. Accessed 2 February 2010 from http://www.oag-bvg.gc.ca/internet/English/osh_20050421_e_23427.html.

42. Gall,Carlotta. At Afghan Bazaar, Military Offers Dollars for Stolen Data, The New York Times, Asia Pacific, 15 April 2006, accessed 16 November 2009 from http://www.nytimes.com/2006/04/15/world/asia/15afghanistan.html?ex=1145332800&en=e12bbb6b87a5b3fb&ei=5087%)A.

43. Garamone, Jim. No Silver Bullet to Counter Explosive Devices, Head of Anti-IED Office Says, American Forces Information Services DefenseLink, 7 September 2006, accessed 12 February 2010 from http://www.defenselink.mil/News/NewsArticle.aspx?ID=743.

44. Garfinkel, Simson. Battling Bugs: A Digital Quagmire, Wired News, 9 November 2005, http://www.wired.com/news/technology/bugs/0,2924,6939,00.html.

Gell-Mann, Murray. "What is Complexity?" Complexity, John Wiley and Sons, 1995, Vol.1, No. 1.

45. Government Accountability Office. Defense Acquisitions – Decisions Needed to Shape Army's Combat Systems for the Future, March 2009.

46. Government Accountability Office. Defense Acquisitions – The Army's Future Combat Systems' Features, Risks, and Alternatives, GAO Testimony Before the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives, 1 April 2004.

47. Government Accountability Office. Defense Acquisitions – 2009 Review of Future Combat System Is Critical to Program's Direction, GAO Testimony Before the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives, 10 April 2008.

48. Government Accountability Office. Defense Acquisitions – Issues to be Considered for Army's Modernization of Combat Systems, GAO Testimony Before the

Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives, 16 June 2009.

49. Government of Canada, The National Security Policy (NSP) dated 2004.

Harney, Robert. Naval Postgraduate School, Personal Communications, 12 April 2004.

50. Holcomb, Robert C. "Some Lessons Learned While Digitizing the Battlefield," Proceedings of the Battlefield Systems International Conference, London, 1998.

51. Holloman, Kimberly. Evidence Based Research Inc., The Network Centric Operations Conceptual Framework, Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., 20 January 2004.

52. JEFX 99 Final Report, http://jefxlink.langley.af.mil/milfinal99/main.htm.

CF C4ISR Capability Development Strategy, issued under 1180-1(D Mil CM), 31 Aug 2009.

53. Johns Hopkins APL Technical Digest 16, 4 (1995), p. 377-396.: The Cooperative Engagement Capability.

54. Johnson, Admiral Jay. Address at the US Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD, 23 April 1997, accessed 16 December 2009 from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=Get RDoc.pdf&AD=ADA420277.

55. Le Bas, Christian and Frederic Miribel, Is the Death of Distance Argument Relevant: The Agglomeration Economies Associated with Information Technology Activities, http://www.ish-lyon.cnrs.fr/labo/walras/Objets/Membres/Miribelebas_paper.pdf.

56. Levin, Carl. US Senator. Summary of the Weapon Systems Acquisition Reform Act of 2009, 24 February 2009.

57. Loeb, Vernon and Thomas Ricks, 1's and 0's Replacing Bullets in US Arsenal, Washington Post, 2 Feb 2002.

58. Maritime Battle Center, Naval Warfare Development Command, "Fleet Battle Experiment Delta Quick Look Report," 2 November 1998, Newport, R.I.

59. Masters, Brooke. Briton Indicted as Hacker, Washington Post, 13 November 2003, accessed 29 December 2009 from http://www.washingtonpost.com/wp-dyn/articles/A45963-2002Nov12.html.

60. Matsumura, John et al., Preparing for Future War with Advanced Technologies, RAND, Arroyo Center, 2002.

61. McDougall, Paul. Optimizing Through Outsourcing, Information Week, 1 Mar 2004. Canadian Forces C4ISR Command Guidance and Campaign Plan, December 2003 sourced from web archives DND Departmental Wide Area Network.

62. McKenna, Ted. Orchestrating Tactical Communications, Journal of Electronic Defense, August 2005, No. 8.

63. Mazzolin, Colonel R.G. Director Land Command Systems Program Management, Presentation to COS ADM(Mat) 8 Feb 2008 in support of DLCSPM Development.

64. Mazzolin, Robert and Asad Madni. A Recommended Scenario for the Future Wireless Network Environment, Proceedings of the 2003 Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference, Big Sky, Montana.

65. Minister of National Defence. Canada First Defence Strategy, 12 May 2008. Mitchell, Paul, Network Centric Warfare and Coalition Operations – The New Military Operating System, Routledge Group, 2009.

66. Morrisey, Charles. A CF Strategic Capability Planning Process, undated. Network Centric Operations: Background and Oversight Issues for Congress, CRS Report for Congress, 15 March 2007.

67. Muradian, Vago. China Tried to Blind US Sats with Laser, Defense News, 25 September 2006.

68. Newton, Lieutenant Colonel S.J. et al, Canadian Forces Experimentation Centre Experiment Report IICDE-001/2002 (Interim), Uninhabited Aerial Vehicle Concept Development and Experimentation, 1 August 2003, p.vi.

69. Norris, Guy. Major Exercise to Prove Net Warfare, Flight International, December 2004, p.5.

70. NSA Security Enhanced Linux, accessed 13 February 2010 from http://www.nsa.gov/selinux/index.cfm.

71. Office of the Auditor General. 2005 OAG Report National Defence – C4ISR Initiative in Support of Command and Control.

72. O'Rourke, Ronald. US Government CRS Report RL32238, Defense Transformation: Background and Oversight Issues for Congress, Department of Defense. Office of Force Transformation.

73. Reid, Darryn et al., All that Glitters: Is Network Centric Warfare Really Scientific?, Defense and Security Analysis, vol. 21, No. 4, p.359 and p.360.

74. Schrage, Michael. Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003.

75. Steele, Robert David. On Intelligence: Spies and Secrecy in an Open World, AFCEA International Press, Fairfax, VA, 2000, p.76.

76. Senenko, Christopher. Network Centric Warfare and the Principles of War, Joint Forces Staff College Joint Advanced Warfighting School, 5 April 2007.

77. Stein, COL (Ret) Fred. NCW—Emerging Lessons Learned from the First Digital Division, Presentation at conference on "Network Centric Warfare: Missions, Needs, Opportunities, and Challenges", Washington, D.C.; Oct 21-22, 1999.

78. The CoolScience Center. Accessed 27 December 2009 from http://www.rmrc.org/photonics/photon1.htm.

79. The SecDev Group. Bullets & Blogs – New Media and the Warfighter, Center for Strategic Leadership, US Army War College. 2009.

80. Thomson, Michael and Barbara Adams, Network Enabled Operations: A Canadian Perspective, DRDC Toronto No. CR-2005-162, 13 May 2005. accessed 28 December 2009 from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm.

81. Tilford, Earl H. Operation Allied Force and the Role of Air Power, Parameters, Vol. 29, Issue 4, Winter 1999/2000, p. 24-38.

82. Tkacik, John. China's Military Power, House Committee on Armed Services, 27 July 2005.

83. US Air Force, US Forces in Iraq Face Obstacles in Getting Intelligence They Need, Inside the Pentagon, 5 May 2005, Vol. 21, No.18.

84. US Defense Science Board, UK Defence Scientific Advisory Council Task Force on Defense Critical Technologies Report, March 2006.

85. US Department of Defense. Defense Science Board Task Force on High Performance Microchip Supply, February 2005, accessed 27 December 2009 from http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.

86. US General Accounting Office, Defence Acquisitions: Stronger Management Practices Are Needed to Improve DoD's Software Intensive Weapon Acquisitions, GAO-04-393, March 2004.

87. Wilson, Clay. Congressional Review Services Report 32544, High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave Devices (HPM): Threat Assessments, 14 April 2006.