National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NETWORK-ENABLED OPERATIONS AND CANADA'S AIR FORCE: TIME FOR IMMEDIATE ACTION

Lieutenant-Colonel Sean T. Boyle

JCSP 34

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI N° 34

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE — COLLÈGE DES FORCES CANADIENNES

JCSP 34 — PCEMI N° 34

2007-2008

MDS RESEARCH PROJECT — PROJET DE RECHERCHE DE LA MÉD

NETWORK-ENABLED OPERATIONS AND CANADA'S AIR FORCE: TIME FOR IMMEDIATE ACTION

LCol Sean T. Boyle

ABSTRACT

In response to rapid technological advances brought on by the Information Age, the Canadian Forces and many of her Western allies are undergoing a Revolution in Military Affairs. This has led to Transformation initiatives designed to produce more efficient military forces while capitalizing on significant improvements in communications, weaponry and computer technology. Critical to the CF's successful transformation through the Information Age is the concept of Network Enabled Operations (NEOps) which, like its American progenitor – Network Centric Warfare (NCW), will likely determine Canada's force structure and doctrine for the foreseeable future.

This paper contends that significant caution will be required in the implementation of CF NEOps. We must avoid past habits of wholesale adoption of US NCW doctrine and procedures. NEOps must be specifically tailored to Canadian needs and reflect our unique identity, culture, national values, goals and priorities. Specifically, NEOps must continue to give priority to the human as the focal point of any networked operation.

The CF is poised to make the same costly and frustrating errors as other allies in the implementation of networked operations. Notwithstanding limited progress made by the Canadian Navy (via close training and operations with the USN), very little has been done beyond hardware acquisition in the CF since the NCW concept was introduced a decade ago. The CF leadership must take immediate and decisive steps to ensure the full spectrum NEOps implementation, to include: doctrine, organizational revision, military occupation review, networked operations training and equipment acquisition.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

LIST OF FIGURES

FIGURE **PAGE**

LIST OF ACRONYMS

ACRONYM	DEFINITION (& comments, as required)
21AC&W	21 Aerospace Control and Warning Squadron (22 Wing, North Bay, ON)
ABD	Airborne Division (US)
ADF	Australian Defence Force
ADM(IM)	Assistant Deputy Minister (Information Management) (Canada)
ADR	Air Defence Regiment (Canada)
ADSI	Air Defence System Integrator
AEC	Aerospace Controller (CF occupation)
AFB	Air Force Base (US)
AWACS	Airborne Warning And Control System (aircraft)
BFT	Blue Force Tracker
BLOS	Beyond Line Of Sight
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
CAF	Canadian Air Force
CAOC	Combined Air Operations Centre
CELE	Communications Electronics Engineer (CF occupation)
CF	Canadian Forces
CIDA	Canadian International Development Agency
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off The Shelf
DFAIT	Department of Foreign Affairs and International Trade (Canada)
DND	Department of National Defence (Canada)
DoD	Department of Defense (US)
DRDC	Defence Research and Development Canada
EBO	Effects Based Operations
FBCB2/BFT	Force XXI Battle Command Brigade & Below System / Blue Force Tracker
GCI	Ground Controlled Intercept
GIG	Global Information Grid (US)
HALE	High-Altitude, Long-Endurance
HF	High Frequency
HQ	Headquarters
IKC2	Integrated Knowledge-based Command and Control (Singapore)
IT	Information Technology
JCS	Joint Chiefs of Staff (US)
JICO	Joint Interface Control Officer
JTIDS	Joint Tactical Information Distribution System
MHP	Maritime Helicopter Programme (CF)
MOC	Military Occupation Code (Canada)
MOD	Ministry Of Defence (UK)
MOOTW	Military Operations Other Than War
NATO	North Atlantic Treaty Organization
NBD	Network Based Defence (Sweden)
NCO	Network Centric Operations

LIST OF ACRONYMS (continued)

ACRONYM	DEFINITION (& comments, as required)
NCPM	Naval Combat Procedures Manual (Canada)
NCW	Network Centric Warfare (in use by both the US and Australia)
NEC	Network Enabled Capabilities (UK and NATO adaptation of NCW)
NEO	Non-combatant Evacuation Operation (NATO) / Network Enabled Operations (US)
NEOps	Network Enabled Operations (Canadian adaptation of NCW)
NGO	Non-Governmental Organizations
NM	Nautical Mile
NMCI	Navy-Marine Corps Intranet
NORAD	North American Aerospace Defence Command
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OODA	Observe, Orient, Decide, Act (USAF Col John Boyd's "OODA loop" theory)
R&D	Research and Development
RAF	Royal Air Force (UK)
RMA	Revolution in Military Affairs
RN	Royal Navy (UK)
RPDE	Rapid Prototyping, Development and Evaluation (Australia)
SA	Situational Awareness
SACEUR	Supreme Allied Commander Europe
SAGE	Semi-Automatic Ground Environment
SATCOM	Satellite Communication
SHAPE	Supreme Headquarters Allied Powers Europe
SIPERNET	Secret Internet Protocol Routing Network
SOF	Special Operations Forces
TCR	Tactical Control Radar (Canadian mobile deployable TPS-70 radar Sqn's)
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UN	United Nations
US	United States
USAF	United States Air Force
USN	United States Navy
UUV	Unmanned Underwater Vehicle
NCPM	Naval Combat Procedures Manual (Canada)
NCW	Network Centric Warfare (in use by both the US and Australia)
NEC	Network Enabled Capabilities (UK and NATO adaptation of NCW)
NEO	Non-combatant Evacuation Operation (NATO) / Network Enabled Operations (US)
NEOps	Network Enabled Operations (Canadian adaptation of NCW)
NGO	Non-Governmental Organizations
NM	Nautical Mile
NMCI	Navy-Marine Corps Intranet
NORAD	North American Aerospace Defence Command
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OODA	Observe, Orient, Decide, Act (USAF Col John Boyd's "OODA loop" theory)

LIST OF ACRONYMS (continued)

ACRONYM	DEFINITION (& comments, as required)
R&D	Research and Development
RAF	Royal Air Force (UK)
RMA	Revolution in Military Affairs
RN	Royal Navy (UK)
RPDE	Rapid Prototyping, Development and Evaluation (Australia)
SA	Situational Awareness
SACEUR	Supreme Allied Commander Europe
SAGE	Semi-Automatic Ground Environment
SATCOM	Satellite Communication
SHAPE	Supreme Headquarters Allied Powers Europe
SIPERNET	Secret Internet Protocol Routing Network
SOF	Special Operations Forces
TCR	Tactical Control Radar (Canadian mobile deployable TPS-70 radar Sqn's)
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UN	United Nations
US	United States
USAF	United States Air Force
USN	United States Navy
UUV	Unmanned Underwater Vehicle

NETWORK-ENABLED OPERATIONS AND CANADA'S AIR FORCE: TIME FOR IMMEDIATE ACTION

CHAPTER 1

INTRODUCTION

> There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.[1]
>
> Niccolò Machiavelli
> Il Principe, Ch. 6 (c. 1505)

What exactly is Network-Centric Warfare (NCW)? How does it differ from Network-Enabled Operations (NEOps)? Are they truly revolutionary forms of warfare? How do they apply to the Canadian Forces (CF), specifically the Canadian Air Force? This paper sets out to answer these questions. In order to understand Network Centric Warfare[2] and the Canadian variant, Network Enabled Operations it is critical to first establish a baseline of common understanding, particularly in the face of so many widely varying definitions. Specifically we must examine the current Information Age, the Revolution in Military Affairs and the resultant Transformation, in order to fully appreciate the emerging concept of Network Centric Warfare. After an overview of the history and development of NCW in the US and its variants among Canada's allies, the idiosyncrasies of Canadian NEOps will be analyzed in greater detail.

---

[1] Wikiquote. "Niccolo Machiavelli." Available at http://en.wikiquote.org/wiki/Niccol%C3%B2_Machiavelli; Internet; accessed 2 March 2008.

[2] The US NCW was the first networked military operational concept developed among western nations, and to date is also by far the most developed. As such this paper will continue to make reference to NCW throughout. Unless specifically stipulated as "Australian NCW", any use of the term NCW will refer explicitly to the US programme. The Canadian variant (NEOps) and other allies implementation of NCW will be discussed in greater detail in Chapter 4.

Canada's vast geographic size and comparatively small population & tax-base has frequently led to stiff competition for defence funding. This has resulted in the CF operating outdated equipment, asked to do more with less, and awaiting capital equipment expenditure decisions made at the whim of the government in power. Despite these realities, this paper will show that the time for decisive NEOps action is now and that ironically, the most pressing changes required for implementation will come with little or no fiscal cost.

Although other allied Air Forces embraced, integrated and fielded NCW capable forces during the past decade, the Canadian Air Force (hereafter referred to as CAF) is only now coming to grips with the concept of NCW in a real way. The extent of CAF NEOps capability is very limited. Although the CP-140 Aurora has had a Link-11(HF) connectivity since the fleets inception in the mid 1980's,[3] this capability was driven primarily by a need to communicate with the Canadian Navy.[4] Canada's two TPS-70 systems (Tactical Control Radars (TCRs)) are Link-11 equipped and have very recently acquiring Link-16 capability as part the TCR modernization programme. The only remaining operational system is a Beyond Line Of Site (BLOS) Link-11 capability help by 21 Aerospace Control and Warning Squadron (21 AC&W) that manages seven ground entry sites nationwide, accessible via landline dialup. The recently announced Maritime Helicopter Programme (MHP) is expected to include a Link-11 capability, upgradeable to Link-22. The CF-18 modernization program, currently underway, will see the integration of Link-16 Joint Tactical Information

[3] Authors personal experience. The CP-140 fleet had also been planned for upgrade to Link-16 capability as part of AIMP, but this Block IV upgrade was eventually cut for budgetary reasons.

[4] While the Canadian Navy is undoubtedly the most advanced service with regards to NEOps implementation, a significant driving factor behind that capability is a requirement to be interoperable with allied navies (particularly the USN and RN). For more on the Canadian Navy/USN NCW history, see Dr. Paul T. Mitchell, "Small Navies and Network-Centric Warfare: Is there a Role?" *Naval War College Review* 56, no. 2 (Spring 2003).

Distribution System (JTIDS) terminals and thus one of the hardware essentials required for NCW operations.

This paper will demonstrate however that technology is only part of NCW capability, and many experts argue the least complex component. The CAF has far greater challenges to surmount before NEOps can be effectively implemented into the operational CF/CAF concept. NEOps will require a fundamental cultural change in the CAF, development of doctrine and a datalink cell at the Air Division level, ideally with membership on an, as yet non-existent, national level datalink panel.

This paper will argue that in order for the CF to maintain joint and coalition warfare fighting capability it must invest immediately and substantially in NEOps. This must include not only the technology required but substantial doctrinal changes, organizational restructuring and training.

The treatment of this subject will be limited to an examination more specifically of the CAF as an effective analysis of Canada's Army, Navy, Air Force and Special Forces is beyond the scope of this paper. Other branches of the CF will be alluded to when discussing Joint operations and some lessons regarding doctrine and organizational reform will apply equally to other CF branches.

CHAPTER 2

ORIGINS AND THEORY OF NETWORK CENTRIC WARFARE

In many ways, Network Centric Warfare is simply a logical military adaptation of Information Age technology. In order to fully understand the importance of NEOps to the Canadian Forces, we must understand the history and development of NCW and the theories on which this concept is based. CF NEOps will certainly be different from NCW, but the core tenets of three grids, self-synchronization, speed of command and the OODA loop will remain fundamental to any nations networked warfare doctrine.

2.1 - THE INFORMATION AGE

> Each age of warfare required different treasured capabilities. In agrarian-age warfare, strength and cunning were valued. In industrial-age warfare, organization and discipline were valued. In information age warfare, the treasured capabilities are knowledge and creativity.[5]

History has proven futurist Alvin Toffler to have been very accurate in his predictions of some highly disparate historical and contemporary movements. He has a remarkable grasp of the psychohistorical dynamics that inform the economic, political and military realms. As such, Toffler's observations of the Information Age merit our examination. In his 1971 work, Toffler quite remarkably predicted that information would become central to decision making and that we would see a shift to the "electronic office" and that this would trigger an eruption of social, psychological, and economic consequences.

---

[5] Gregory A. Roman, "The Command or Control Dilemma: When Technology and Organizational Orientation Collide" (Department of Defense, Air Force 2025 Paper, 1996), 36.

In the same book he wrote that the most significant feature of modern industrial society was the rate at which it was changing. The pace of this change was bewildering and led to a cultural phenomenon he called "Future Shock."[6] This then led to a depiction of historical epochs that are characterized by revolutionary technological breakthroughs that cause "waves" of socioeconomic change. Toffler considers the agricultural revolution of 10,000 years ago the "First Wave" of transformational change, the industrial revolution of 300 years ago the "Second Wave" of transformational change, and the information revolution currently underway is the "Third Wave" of transformational change.[7] In his latest work, he relates how warfare has adapted and evolved throughout these transformational changes, making insightful proposals regarding warfare in the Information Age.[8]

In practical terms, the technological advances of the Information Age have led to significant increases in computing power, coupled with similarly increasing demands for faster computers and greater communications bandwidth. In 1964, semiconductor engineer Gordon Moore (who co-founded Intel four years later) estimated that the storage capacity of silicone computer chips would roughly double every year (simultaneously bringing down the cost with successive advances). Known now as "Moore's Law", this estimate remained valid until the late 1970's when the doubling period slowed to every 18 months.[9] Similarly, advances in communications technology and increased demands to network brought upon by more capable computers gave rise to Gilder's Law in 1997 (stating that the total bandwidth

---

[6] Alvin Toffler, *Future Shock* (Toronto: Bantam, 1971), 18.

[7] Alvin Toffler, *The Third Wave* (Toronto: Bantam, 1984), 163.

[8] Alvin Toffler and Hedi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 90-117.

[9] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command, Control in the Information Age* (Washington, DC: CCRP Publication Series, 2004), xvii.

of communications systems will triple every year). This combination of cheaper and more powerful computer memory and increasing communications bandwidth significantly facilitated the near exponential growth in computer networking. Metcalfe's Law, frequently quoted by NCW proponents, states that the value of a network is proportional to the number of nodes in the network.[10]

It is the arrival of this Information Age and all the technological implications therein that have led to what is known today as the Revolution in Military Affairs.

2.2 - REVOLUTION IN MILITARY AFFAIRS

Much has been written about the Revolution in Military Affairs (RMA). However there is a wide disparity of opinions as to what this concept really means and, perhaps more importantly, at what stage we currently find ourselves in this "revolution."

Krepinevich argues that military revolutions are characterized by four essential elements: technological change, systems development, operational innovation, and organizational adaptation.[11] He gives strong supporting evidence to this definition by analyzing ten military revolutions since the fourteenth century – from the Infantry Revolution during the Hundred Years' War through the Nuclear Revolution in the mid twentieth century. From this analysis seven key lessons are extracted, the most important of

---

[10] Ibid, xvii. "Metcalfe's Law and Legacy" was first published in Forbes ASAP, 13 September 1993. The frequent quoting and interpretation of Metcalfe's Law by NCW supporters is one of many issues considered misleading by critics. They maintain that Metcalfe was referring to the "value" of "goods and/or services" and that translating that idea into "power" (to mean "computing power") was not Metcalfe's intention, and is therefore inaccurate and misleading. For a detailed explanation of this problem (and others) in associating Metcalfe's law to NCW, see Ralph E. Giffin and Darryn J. Reid, "A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy," 2003.

[11] Andrew F. Krepinevich, "Cavalry to Computer; the Pattern of Military Revolutions," *National Interest* (Fall 1994).

which is that emerging technologies do not define militaries but facilitate their implementation. Krepinevich concludes that "failure to realize a great increase in military effectiveness typically resulted not so much from ignoring technological change as from a failure to create new operational concepts and build new organizations."[12] This observation supports on of the key recommendation of this paper concerning the CF implementation of NEOps.

Edmund Blash also cautions heavily against over-reliance on technological advancements and he claims that many of the characteristics and tenets of the current RMA remain undemonstrated and unproven. Furthermore, he believes that the term "evolution" (vice "revolution") is both more appropriate and succinct.[13] Other authors note that past RMAs have frequently not "revolutionized" warfare as much as initial supporters believed. For example, Krepinevich classifies the nuclear age as a revolution but despite the enormous power of nuclear weapons, that period failed to discredit traditional notions of strategy.[14] Despite numerous arguments to the contrary, it seems safe to conclude that the current RMA is indeed a revolution, what is critical to understand is that it is far from complete. Because the introduction of new technologies and ideas is still in the infancy stage, the process must

---

[12] Krepinevich, *Cavalry to Computer* ...

[13] Edmund C. Blash, "Network-Centric Warfare Requires a Closer Look," *Signal* (May 2003). [Journal on-line]; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=235&zoneid=62; Internet; accessed 8 December 2007.

[14] Martin C. Libicki, "Information & Nuclear RMAs Compared," *Institute for National Strategic Studies Strategic Forum* no. 82 (July 1996).

continue to evolve and mature before the exact shape and structure of the current RMA becomes clear.[15]

The Canadian Forces (CF) definition of the Revolution in Military Affairs (RMA) is "a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts fundamentally alters the character and conduct of military operations."[16] While there exists many variations on the definition of RMA, this CF definition is particularly careful to define the RMA beyond just technology. The CF sees this revolution as involving a symbiosis of new technology, the doctrine for its use and an organization that can support both.[17] In fact, the assertion and acknowledgement that advancements in technology alone are not a panacea will be a recurring theme throughout this paper. Notwithstanding some of the clear benefits of technological advances in military hardware, the military-industrial base's euphoria and radical expectations of networked operations must be tempered with measured analysis and balanced reality.

A number of academics and military experts alike caution against over-reliance on technology alone. John Gentry warns that the US may be unwittingly creating what historians will one day call "the Maginot Line of the 21st century" in this regard.[18] He cites four fatal flaws to the United States military "Joint Vision 2020" doctrinal publication's

---

[15] Andrew Richter, "The Revolution in Military Affairs and its Impact on Canada: The Challenge and the Consequences," Working Paper, University of British Columbia, March 1999, 6.

[16] Department of National Defence, *Shaping the Future of the Canadian Forces: A Strategy for 2020* (Ottawa: DND Canada, 1999) available from http://www.cds.forces.gc.ca/pubs/strategy2k/intro_e.asp; Internet; accessed 3 January 2008, 1.

[17] Elinor Sloan, "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities," *Canadian Military Journal* 1, no. 3 (Autumn 2000): 7.

[18] John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters* 32, no. 4 (2002): 88.

belief that the RMA will result in dominant US military capabilities, primarily through information superiority. First, is the narrow applicability; the doctrine pays only lip service to full spectrum missions, clearly written with Desert-storm type operations in mind (ignoring, for example, counter-insurgency). Second, he cites the vulnerability of proposed infrastructure. The over-reliance on information technology (IT) and other infrastructures that are incompatible and unreliable (regularly failing in peacetime). The third fatal flaw concerns the existence of effective countermeasures, including adversaries operating beyond the scope of US military capabilities. Finally, Gentry sees strategic resistance to change and other institutional impediments as a key area that must be addressed in the RMA.[19] These cautions are valuable to review here as elements of his four fatal flaws have appeared in discussions and writings about the application of the RMA to the Canadian Forces, albeit on a far smaller scale. Fortunately, more recent writings have applied a uniquely Canadian examination of the RMA and Transformation.[20]

2.3 - TRANSFORMATION

Transformation, in the military sense, is adapting armed forces to capitalize on the RMA and prepare for future warfare. Although the US Department of Defence (DoD) initiated their own Transformation some time ago (the Office of Force Transformation was established in October 2001),[21] DoD is not alone. Many other western militaries are

---

[19] Gentry, *Doomed to Fail* …, 89.

[20] For a thorough overview of US Military Transformation and recommended ways ahead for the CF see Dr. Paul T. Mitchell, "A Transformation Agenda for the Canadian Forces: Full Spectrum Influence," *Canadian Military Journal* 4, no. 4 (Winter 2003-2004): 55-62.

[21] United States, Department of Defence, Office of Force Transformation, *Network Centric Operations*. Available from http://www.oft.osd.mil/initiatives/ncw/ncw.cfm; Internet; accessed 19 November 2007.

pursuing their own transformation initiatives, including the United Kingdom, Australia, New Zealand and Canada. NATO also recognized the importance of Transformation and military and created Allied Command Transformation in 2002[22] (Headquartered in Norfolk, VA) to oversee Transformation efforts of NATO's 26 member Alliance.

Canadian Forces Transformation is seen as "a process of strategic re-orientation in response to anticipated or tangible change to the security environment, designed to shape a nation's armed forces to ensure their continued effectiveness and relevance."[23] One of the four overarching imperatives of CF Transformation is that "the CF must remain abreast of and *selectively align itself with emerging allied (predominantly US)* concept and technological development if the maintenance of interoperability is to remain a mainstay of Canada's operational approach" (emphasis added).[24] Hence, while the CF has a duty and responsibility to implement Transformation that will optimize the military for the benefit of Canada and Canadians, we also have a vested interest in closely observing the transformation based NCW implementation in DoD.

2.4 - NETWORK CENTRIC WARFARE

Admiral Arthur K. Cebrowski, sometimes referred to as the "Godfather of NCW",[25] is credited with coining the term (and concept) of Network-Centric Warfare in his seminal

---

[22] North Atlantic Treaty Organization, *Allied Command Transformation - History*. Available from http://www.act.nato.int/content.asp?pageid=240; Internet; accessed 18 March 2008.

[23] Department of National Defence, *Canadian Forces Integrated Operating Concept* (Ottawa: DND Canada, 2005), 5.

[24] Ibid, 5.

[25] Paul T. Mitchell, "Small Navies and Network-Centric Warfare: Is there a Role?," *Naval War College Review* 56, no. 2 (Spring 2003): 88.

1998 US Naval Institute *Proceedings* article. Cebrowski describes NCW as the "emerging military response to the Information Age."[26] Cebrowski's original article likened NCW to changes in the American business model due to advances in Information Technology (IT). His parallel between retail economic practices and networked warfare drew wide criticism for being militarily irrelevant, perhaps explaining the absence of such references in today's NCW theory.

In terms of NCW, Information Age warfare is seen to be linked by three distinct themes: a shift in focus from platform to network centricity, a shift in viewing actors as independent to being part of a continuously adapting ecosystem, and the importance of making strategic choices.[27] In broad terms, NCW is defined as the combination of strategies, emerging tactics, techniques, procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage.[28]

The NCW concept is framed in terms of four domains of warfare: physical, information, cognitive, and social.[29] The *physical domain* includes the traditional movement of a force through time and space (in land, sea, air and space environments). The *information domain* incorporates sensors and processors, intelligence, communication of C2 and conveyance of the commander's intent. The mind of the warfighter is represented by the *cognitive domain*, which includes the intangible concepts of leadership, morale, unit cohesion and situational awareness. Finally, the *social domain* describes the necessary

---

[26] Arthur K. Cebrowski, "Network-Centric Warfare: An Emerging Military Response to the Information Age," *Military Technology* 27, no. 5 (2003): 6.

[27] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origins and Future," *US Naval Institute Proceedings* 124, no. 1 (January 1998): 29.

[28] United States, Department of Defence, Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, DC: Office of Force Transformation), 3.

[29] Ibid, 19.

elements of any human enterprise. This is where humans interact, exchange information, form shared awareness and understandings, and make collaborative decisions.[30] The figure below provides a useful graphical depiction of the NCW hypothesis and demonstrates the interrelationship between each of the tenets of NCW and how they apply to each of the domains of warfare.

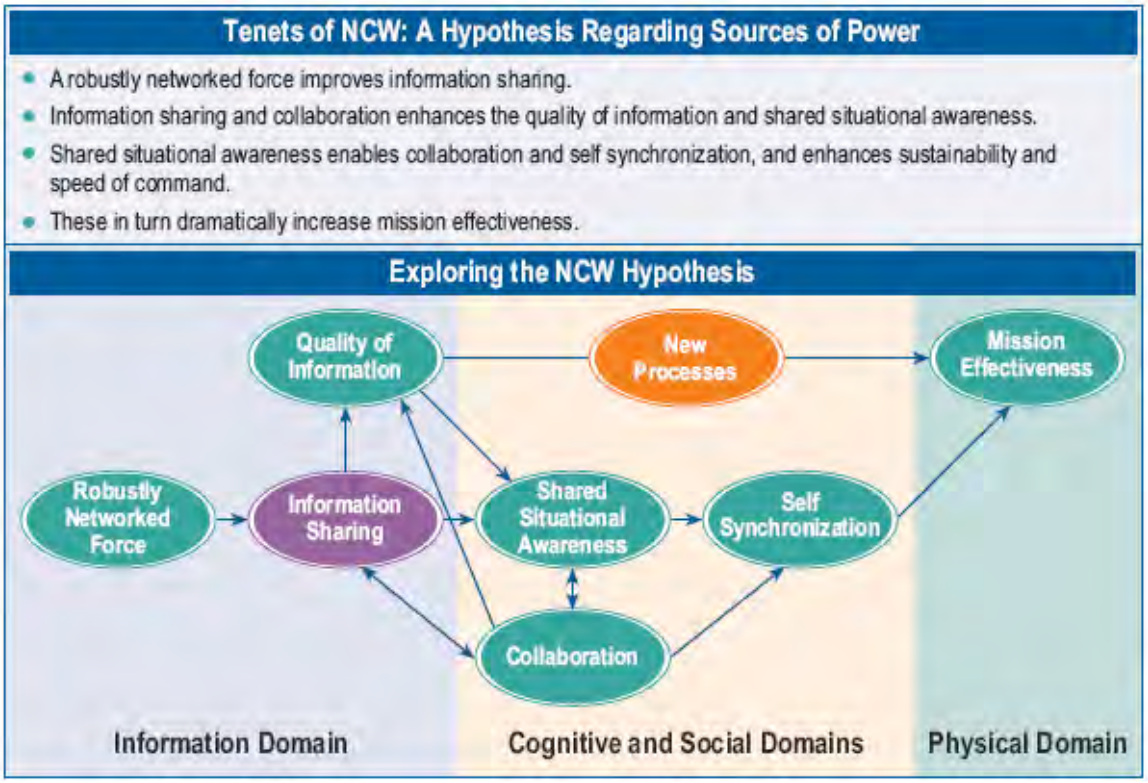

Figure 1: Tenets of NCW - The New Value Chain
Source: United States, Office of Force Transformation, *The Implementation of Network-Centric Warfare*, 19.

Another instructive illustration (Fig. 2 below) demonstrates that these domains of conflict can be described using a Venn diagram to depict the relative relationship of each domain. The intersection of information and cognitive/social domains facilitates shared

---

[30] United States, Office of Force Transformation, *The Implementation …,* 20.

awareness, including the rapid and clear passage of commander's intent. Where the physical domain meets the cognitive/social domain a resultant compression of operations is seen, increasing the speed and efficiency of the plan, organize, deploy, employ and sustain cycle of warfighting. The overlap of the information domain with the physical domain leads to a precision force, enhancing the concepts of speed and access. Finally, NCW finds itself at the intersection of all four domains and thus gleaning the advantages of the three aforementioned synergies.

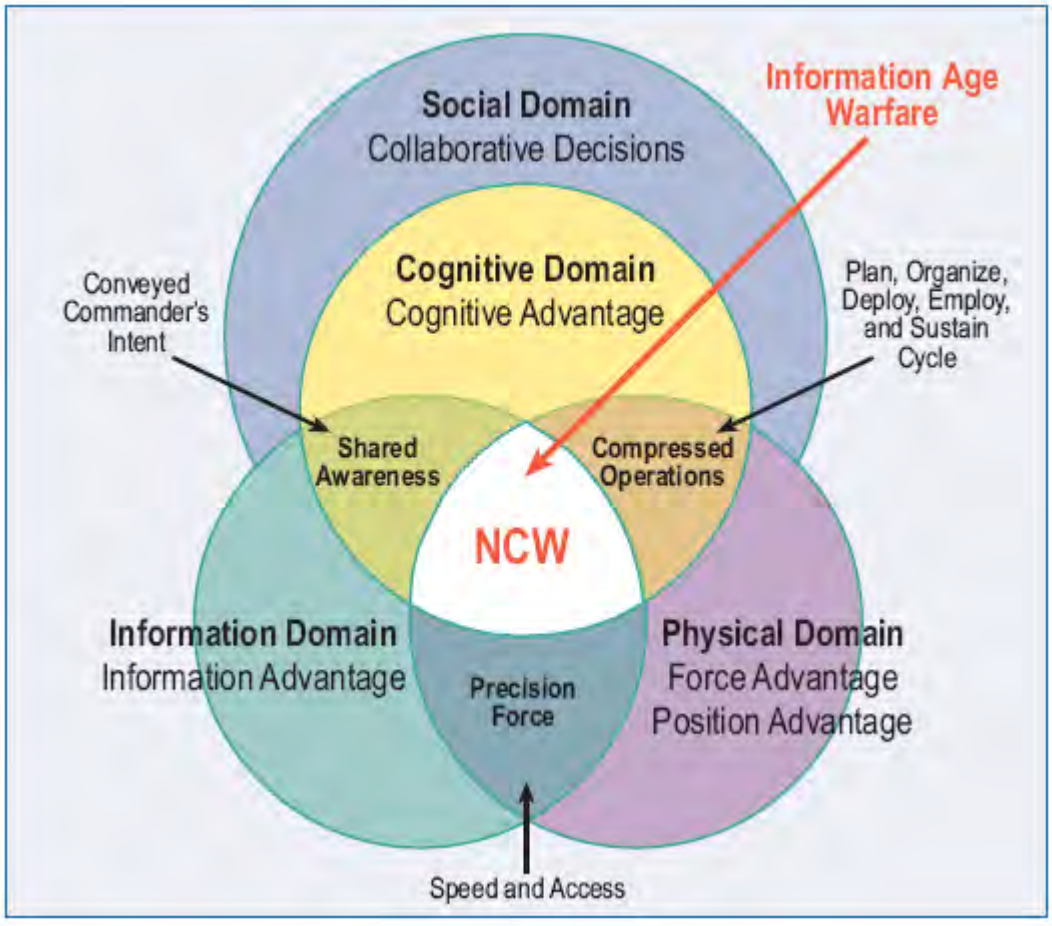

Figure 2: Information Age Warfare - Domains of Conflict
Source: United States, Office of Force Transformation, *The Implementation of Network-Centric Warfare*, 21.

Moving from theoretical to more practical definitions, NCW has been further describe it 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 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 degree of self synchronization."[31] In essence, NCW translates information advantage into combat power by effectively linking friendly forces within the battle space, providing a much improved shared awareness of the situation, enabling more rapid and effective decision making at all levels of military operations, and thus allowing for increased speed of execution. This "network" is underpinned by information technology system, but is exploited by the military personnel that use the network and, at the same time, are part of it.[32]

But what does this all really mean? How will these grandiose objectives be achieved and in what manner will they truly enable military operations (specifically those of the CF)? The concept of NCW has not been without its critics, both academic and military. However, before we examine criticism levied against NCW, we should first understand the theoretical advantages it brings to the warfighter.

---

[31] David S. Alberts, John Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* (Washington, DC: National Defense University Press, 2000), 2. The "Social Domain" did not appear in original US NCW literature and seems to have been added in response to criticism that NCW neglected the critical human component of warfare, command and networks. See the three domains described in : David S Alberts, *Understanding Information Age Warfare,* (Washington, DC: CCRP Publication Series, 2001), 10-34.

[32] United States, Office of Force Transformation, *The Implementation…,* 5.

2.4.1 - Three grid Concept

Cebrowski proposed a structural or logical model of network centric warfare that involved three interdependent and overlapping grids; information, sensor and engagement grids. The information grid is key to this concept and provides a "high performance backplane for computing and communications."[33] The information grid enables the operational architectures of both the sensor and engagement grids (see Fig. 3 below).

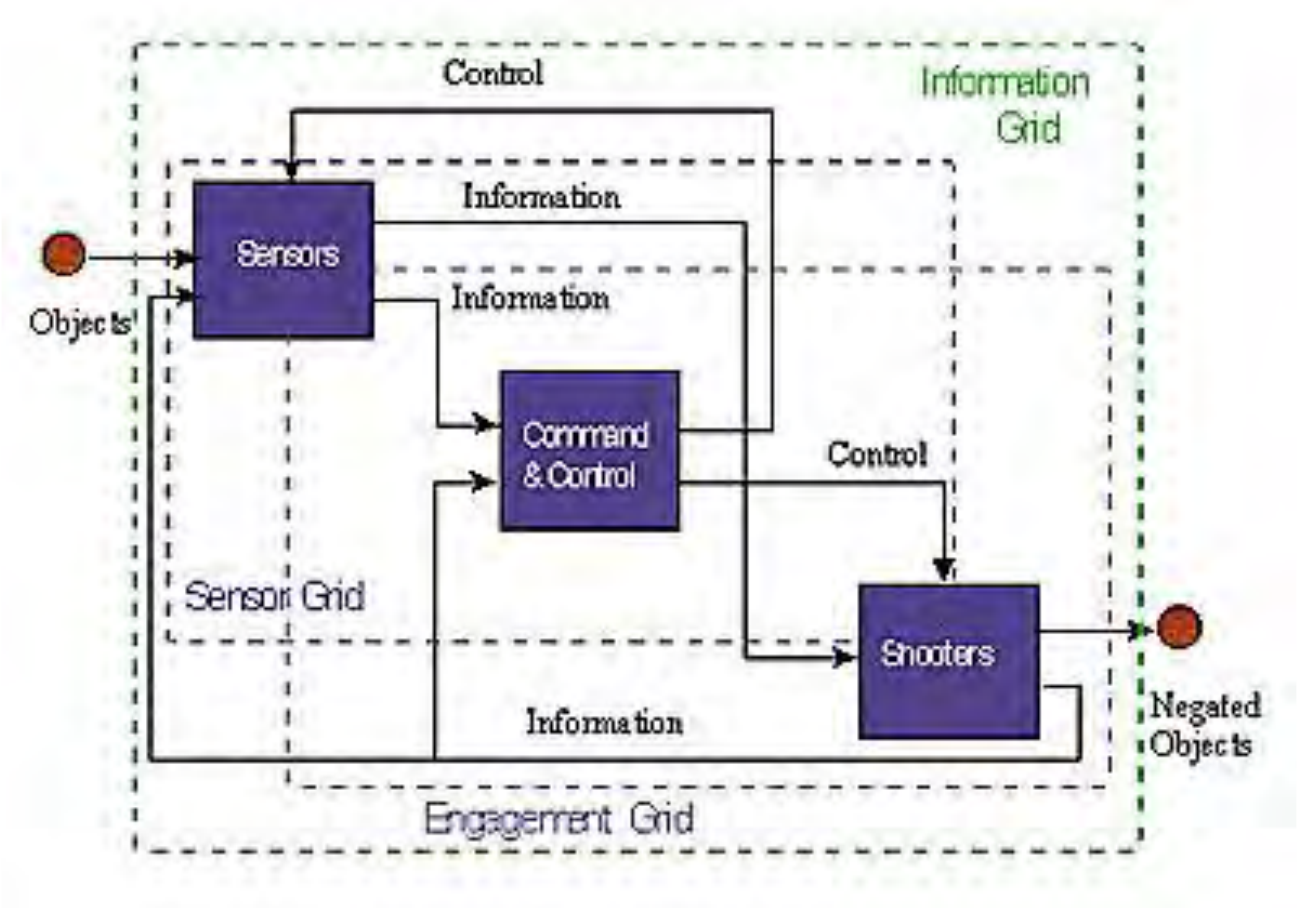

Figure 3: Logical Model for Network Centric Warfare
Source: Cebrowski, Arthur K. and John J. Garstka, Proceedings, January 1998, *Network-Centric Warfare – Its Origin and Future*, 33.

[33] Cebrowski and Garstka, *Network-Centric Warfare* …, 33.

For the US, this *information grid* is proving to be a challenging and expensive endeavour. It is a fundamental component of any NCW implementation, yet also seems to be a critical point of failure. If the information plane is hacked, blocked or otherwise disrupted then the functioning of the other two planes would be jeopardized. Apart from this potential vulnerability, there is also the challenge of technical throughput. As networks amass more and more sensors from sub-surface to space-based, and commanders demand more widespread coverage in real-time, the bandwidth demands become exorbitant. The costs of the Global Information Grid (GIG) are in the tens of billions of dollars. The US Navy-Marine Corps Intranet (NMCI) alone will cost up to US$4.1 billion for the first five years, followed by a three year option worth US$2.8 billion.[34]

The sensor grid is designed to "rapidly generate high levels of battlespace awareness and synchronize awareness with military operations."[35] The US is focusing on unmanned vehicles, both airborne (UAVs) and undersea (UUVs), in addition to the existing constellation of satellite based surveillance assets (electro-optical and synthetic aperture radar). UAVs such as Global Hawk have spawned a new class of sensors know as High-Altitude and Long-Endurance (HALE) UAVs, capable of providing a wide area search of up to 40,000 NM^2 and collecting up to 1,900 spot images per mission.[36] There are two key challenges that come to mind immediately regarding the NCW sensor grid. First will be the standardizing and fusing the data from these multiple sensor types to eliminate "double-

---

[34] David W. Roberts and Joseph A. Smith, "Realising the Promise of Network-Centric Warfare," *Military Technology* 27, no. 7 (2003): 2.

[35] Cebrowski and Garstka, *Network-Centric Warfare* …, 33.

[36] Airforce Technology, "RQ-4A/B Global Hawk High-Altitude, Long-Endurance, Unmanned Reconnaissance Aircraft," http://www.airforce-technology.com/projects/global/; Internet; accessed 17 February 2008.

tracks" and provide an accurate Common Operating Picture (COP). Second, once a usable COP is achieved, establishing a system of filters to reduce information overload will be essential, least the COP become too cluttered to be useful.[37] Like the GIG, a NCW *sensor grid* is an extremely expensive proposition. Each Global Hawk UAV system (including aircraft, ground station and integrated sensor suite) costs up to US$70 million each, Predator UAVs cost approximately US$40 million each.[38]

The *engagement grid* is designed to "exploit this awareness and translate it into increased combat power."[39] The ideal goal of a networked force in theatre is that an appropriate weapon will always be within striking range of any target at any given time. Clearly this is a lofty goal but, in theory, proponents believe that it will contribute to a reduction in manpower required, number of weapons (cost savings), increased accuracy (reduced collateral damage) and a significant reduction in reaction time between threat detection and engagement, potentially providing decisive advantage over an adversary.[40]

A word on cost; we have briefly touched on some of the considerable expenses of embarking on NCW. This has certainly prompted further reflection from scientists, academics and military personnel alike. Firstly there are those who look at the entire cost of a proposed US national NCW architecture to be very expensive, if not cost prohibitive. If this is causing pause for reflection in the nation spending more on defense than the next

---

[37] This observation from the authors personal experience with fused COPs in the CAOC, Vicenza, Italy and during E-3A missions aboard NATO AWACS.

[38] Roberts and Smith, *Realising the Promise* …, 2.

[39] Cebrowski and Garstka, *Network-Centric Warfare* …, 33.

[40] Cebrowski and Garstka, *Network-Centric Warfare* …, 35.

three countries combined,[41] how are middle powers supposed to afford this (and be capable of operating in multinational coalitions in future networked conflicts – see chapter 3 below)? Secondly, there is no doubt that this entire concept represents a significant windfall for the US defence industry. As such, tempering unfounded promises, exaggerated claims and euphoric hyperbole remains important in any analysis of NCW theory and implementation.

A full understanding of the proposed theoretical advantages of NCW is impossible without examining two fundamental concepts. Cebrowski maintains that NCW enables a shift from attrition-style warfare to a more rapid and effective warfighting style characterized by two new concepts: speed of command and self-synchronization.[42]

2.4.2 - Speed of Command

Speed of command is considered a basic measure of one's command and control approach, organization and systems, and is defined as the "time it takes to recognize and understand a situation (or change in the situation), identify and assess options, select an appropriate course of action, and translate it into actionable orders."[43]

Speed of command is frequently voiced as one of the criticisms of NCW; the unchecked quest for speed, it is argued, may result in mission degradation as we outpace not only the adversary but ourselves on the battlefield. Critics suggest that "we may find ourselves acting so rapidly within our enemy's decision loop" [OODA loops are discussed in the next section] "that we largely are prompting and responding to our own signals, which

---

[41] Central Intelligence Agency, "The World Fact Book," https://www.cia.gov/library/publications/the-world-factbook; Internet; accessed 11 March 2008.

[42] Cebrowski and Garstka, *Network-Centric Warfare* …, 32.

[43] David S. Alberts, *Understanding Information Age Warfare* (Washington, DC: CCRP Publication Series, 2001), 163.

our beleaguered target cannot process. In short, we could end up like Pavlov's dog ringing his own bell and wondering why he's salivating so much."[44]

Proponents acknowledge that uncontrolled acceleration in decision cycles could render the situation potentially harmful. However they are quick to affirm superior speed of command will be decisive in many circumstances, and that NCW provides the opportunity to increase speed of command as appropriate (and that commanders are not forced to do so when not required).[45] It follows that having global situational awareness fed to a commander in real time is of little use if there is no net improvement in the decision cycle time. In fact, in the information age, speed of command will frequently be essential.[46]

Speed of command is considered the process by which a superior information position is turned into competitive military advantage. Not unlike the definition of today's counter-insurgency operations, proponents foresee future operations as "non-linear in space time and intensity" and "there may be no lines to organize forces in the battlespace – no forward line of own troops, forward edge of the battle area, or fire support coordination line."[47] Increased speed of command becomes advantageous in these cases because non-linear conflict no longer requires sequential action, operations can be conducted "in parallel, simultaneously, and continuously. Operational pauses will be rare."[48]

Conceptually, effective speed of command requires three fundamental components. First, greater battlespace awareness (not simply more raw data) leads to information

---

[44] Thomas P. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *US Naval Institute Proceedings* 125, no. 1 (January 1999): 38.

[45] Alberts, Garstka, and Stein, *Network Centric Warfare …,* 13.

[46] Alberts, *Understanding Information Age Warfare* …, 194.

[47] Cebrowski, *Network-Centric Warfare: An Emerging* …, 18.

[48] Ibid, 18.

superiority. This will require a precise array of sensors, rapid and powerful networks, display technologies and sophisticated modeling and simulation capabilities. Informed by this superior situational awareness, friendly forces can strike with speed and precision facilitating the massing of effects vice simply massing forces. Finally, the rapid, decisive and accurate application of force, will disrupt, discourage and if required destroy the enemy. Decisive and coordinated effects will negate enemy courses of action and precipitate defeat.[49]

2.4.3 - Self-synchronization

Before we can properly discuss self-synchronization, one must first understand the concept of synchronization, which is defined well by the US Army FM 3-0:

> Synchronization is arranging activities in time, space and purpose to mass maximum relative combat power at a decisive place and time. Without synchronization, there is no massing of effects. Through synchronization, combat power at the chosen place and time to overwhelm an enemy or dominate the situation. Synchronization is a means, not an end. Commanders balance synchronization against agility and initiative; they never surrender the initiative or miss a decisive opportunity for the sake of synchronization. Through separated in time and space, commanders closely synchronize such actions to mass overwhelming effects at the decisive time and place. Synchronization often requires explicit coordination and rehearsals among participants.[50]

Traditional command directed synchronization is applied in a top-down fashion, communicating the commanders intent and directing required level of mass and fires at the point of contact with the enemy. NCW proposes a radical departure from this command

---

[49] Cebrowski and Garstka, *Network-Centric Warfare* …, 32.

[50] United States, Office of Force Transformation, *Network Centric Operations …,* 4-15.

tradition by suggesting a bottom-up organizational framework that permits self-synchronization.[51]

The belief is that with units at all levels in the military organization networked together, they are all able to share the same Common Operating Picture (COP) in addition to receiving the commanders intent and other guidance. This will permit units at the lowest level to act decisively and immediately while still complying with the commanders intent, but without having to incur the traditional delay in waiting for continual command direction.

NCW proponents maintain that networked military units are capable of self-organizing behaviour and thus should be structured in accordance with the premise of complexity theory whereby greater synchronization can be achieved by organizing from the bottom up vice top down (hence "self-synchronization"). In order to prevent chaos however, effective self-synchronization must meet four conditions. These units must have "a clear and consistent understanding of command intent; high quality information and shared situational awareness; competence at all levels of the force; and trust in the information, subordinates, superiors, peers and equipment."[52]

Cebrowski depicted graphically the combined advantages of speed of command and self-synchronization (Fig. 4 below). He contends that in traditional planned synchronization, combat power is applied in "spurts" over time as each operation successively coordinated, force generated and executed.[53] Network enabled shared situational awareness would empower self-synchronization such that friendly forces would

---

[51] Cebrowski and Garstka, *Network-Centric Warfare …*, 33.

[52] Alberts and Hayes, *Power to the Edge …,* 27.

[53] Edward A. Smith, Jr., "Network Centric Warfare: Where's the Beef?," *United States Naval War College Review* (1999), 8.

no longer be required to wait to assess impact of action on the enemy and then decide on further action. The availability of networked information would permit virtually continuous recurring action over short time periods. With the addition of speed of command, the pace of semi-independent actions would accelerate further resulting in more effective combat power being applied in less time.[54]

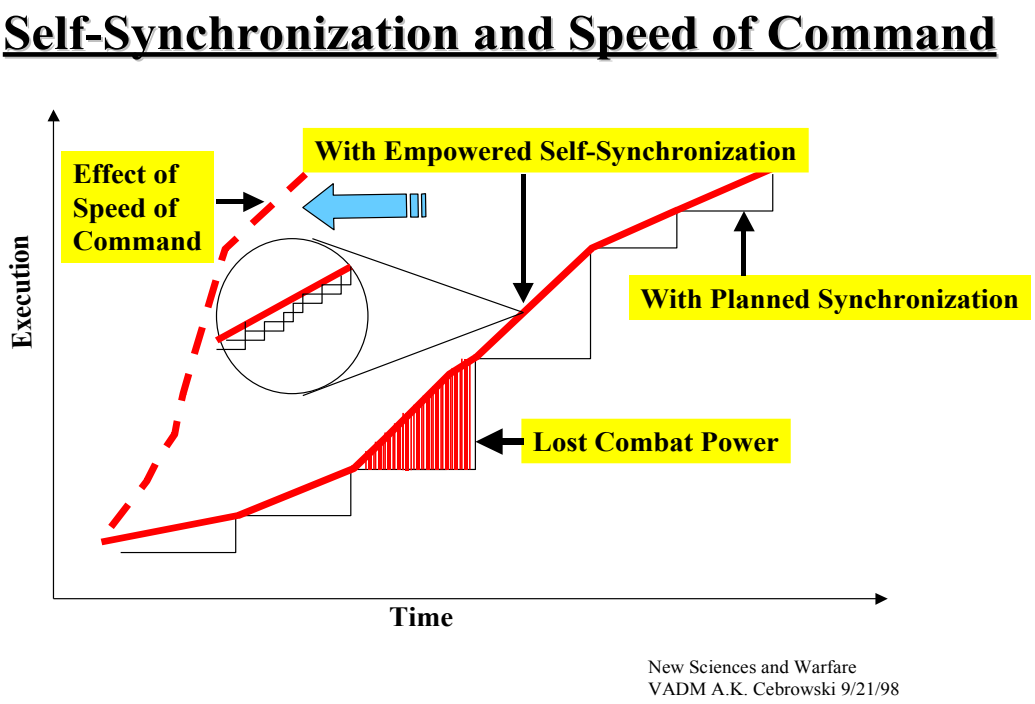

Figure 4: Self Synchronization and Speed of Command
Source: Smith, Edward A., Naval War College Review, *Network Centric Warfare: Where's The Beef?,* 8.

Clearly the application of bottom-up self-synchronization will require a serious revision of the military command structure and the command and control hierarchical process – this challenge will be discussed in the next chapter.

[54] Ibid, 9.

2.4.4 - OODA loop

Col John Boyd, a former USAF fighter pilot, is considered by many as one of the most influential military strategists of the twentieth century. His theories can be found as basis for American, British and other allied defence doctrine manuals.[55] It is not unusual that his theories are key to the foundation of NCW as he was well known for synthesizing ideas from diverse fields of study such as physics, philosophy, mathematics and history.[56]

Influenced heavily by the teachings of Sun Tzu, Boyd studied and analyzed maneuver, attrition and moral warfare types. He gave particular focus to maneuver warfare, developing a unique interpretation that became more temporal and psychological than physical and spatial.[57] Unlike attrition warfare, the key to Boyd's approach was the idea that conflict resides in a time competitive domain. His ideas focused on the effort to disrupt, disorient and overload the enemy's psychological and/or physical capacities and bring about paralysis and eventual defeat.[58]

It was from here that Boyd proposed the concept of his OODA loop, composed of the four iterative stages of Observe, Orient, Decide and Act. All living organisms observe (or sense) the environment, collect data on the surroundings, the self and interactions. The orientation step then conducts analysis and synthesis of the data collected (a highly complex process taking into account previous experiences, culture, training, etc.) and generates a

---

[55] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston: Little, Brown, 2002), 445.

[56] Grant Tedrick Hammond, *The Mind of War: John Boyd and American Security* (Washington: Smithsonian Institution Press, 2001), 194.

[57] David S. Fadok, "John Boyd and John Warden : Air Power's Quest for Strategic Paralysis," (Maxwell AFB: United States Air Force School of Advanced Airpower Studies Paper, 1995), 14.

[58] William S. Lind, *Maneuver Warfare Handbook* (Boulder, CO: Westview Press, 1985), 5.

series of alternative courses of action.[59] The decision stage factors in a any applicable guidance or control and selects the optimum solution for the given time. This decisions implementation in the Act phase, is a transition from cognitive process to physical world, in effect testing the hypothesis formulated during orientation and decision making. The environment reacts and we return to the Observe step (see Fig. 5 on the next page).[60]

[59] Grant Tedrick Hammond, "From Air Power to Err Power: John Boyd and the Opponent's Situational Awareness," in *Air Power Leadership: Theory and Practice*, ed. Peter W. Gray and Sebastian Cox, 107-128 (London: The Stationery Office, 2002), 115.

[60] Fadok, *John Boyd and John Warden* …, 16.

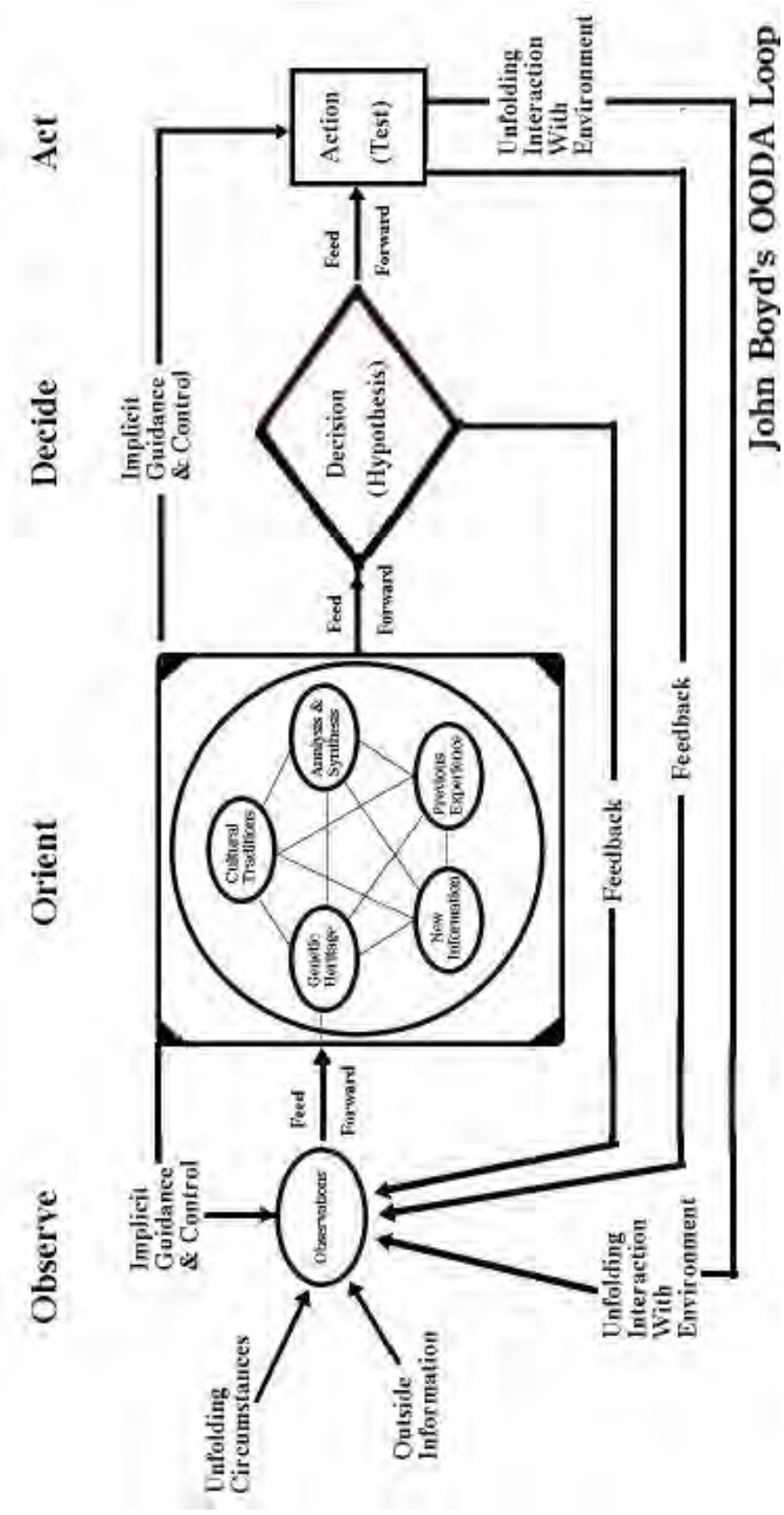

Figure 5: Observe, Orient, Decide, Act (OODA) loop
Source: Defence and the National Interest, http://ww.d-n-i.net, 2008

Warfare in the information age has evolved into an inherently cyclic nature. Military forces monitor the battlespace (friendly & adversary forces, terrain, weather, etc.), extract information from sensor data and fuse with previous reports to generate reliable situational awareness, generate alternative courses of action, select and disseminate to subordinates as orders, and monitor their effect on the battlespace – reinitiating the cycle.[61]

Ironically, Boyd's initial application of the OODA loop was to a platform-centric warfighting environment, where he observed that the speed with which a pilot moves through the OODA process can serve as a source of competitive advantage.[62]

The OODA defined by John Boyd has since been adapted to capture this iterative nature of warfare. It recognizes that the result of our actions is not just the direct effect on the adversary, but it is his adaptations to our actions, and his subsequent actions (or at least our observation of them) become part of the next input. It includes as inputs several feedback loops with which to reorient.[63]

The concept has since been significantly further developed and the popularity of the OODA loop (Observe, Orient, Decide, Act) among western militaries is an indication of their recognition of this cyclic process.[64]

The OODA loop is particularly important to understand with respect to NCW because it allows one to appreciate how the power of Cebrowski's shared situational

---

[61] Alberts and Hayes, *Power to the Edge…,* 49.

[62] Alberts, *Understanding Information Age Warfare*…, 22.

[63] Linda P. Beckerman, "The Non-Linear Dynamics of War," Science Applications International Corporation, 1999. Available from http://www.calresco.org/beckermn/nonlindy.htm; Internet; accessed 4 April 2008, 3.

[64] Keith H. Hammonds, "The Strategy of the Fighter Pilot," *Fast Company* (May 2002) [journal on-line]; available from http://www.fastcompany.com/magazine/59/pilot.html; Internet; accessed 15 February 2008, p 98.

awareness translates into actual increased combat efficiency. First we must expand our application of the OODA loop concept beyond its originally conceived tactical engagement level and apply it also to the operational and strategic levels. Second, we must alter our interpretation of Boyd's concept from a circular repeating loop to a series of repeating linear cycles over time. Smith developed the idea of overlaying linear OODA cycles onto Cebrowski's NCW step functions diagram (at Fig 4 above).[65] Depicted graphically (Fig 6 below) we see Boyd's OODA cycle phases plotted on the X-axis as a function of time, and the NCW cumulative application of military force on the Y-axis. This way the cycles are simply repeated as often as required to achieve the objective, with the cumulative military force augmenting over time.

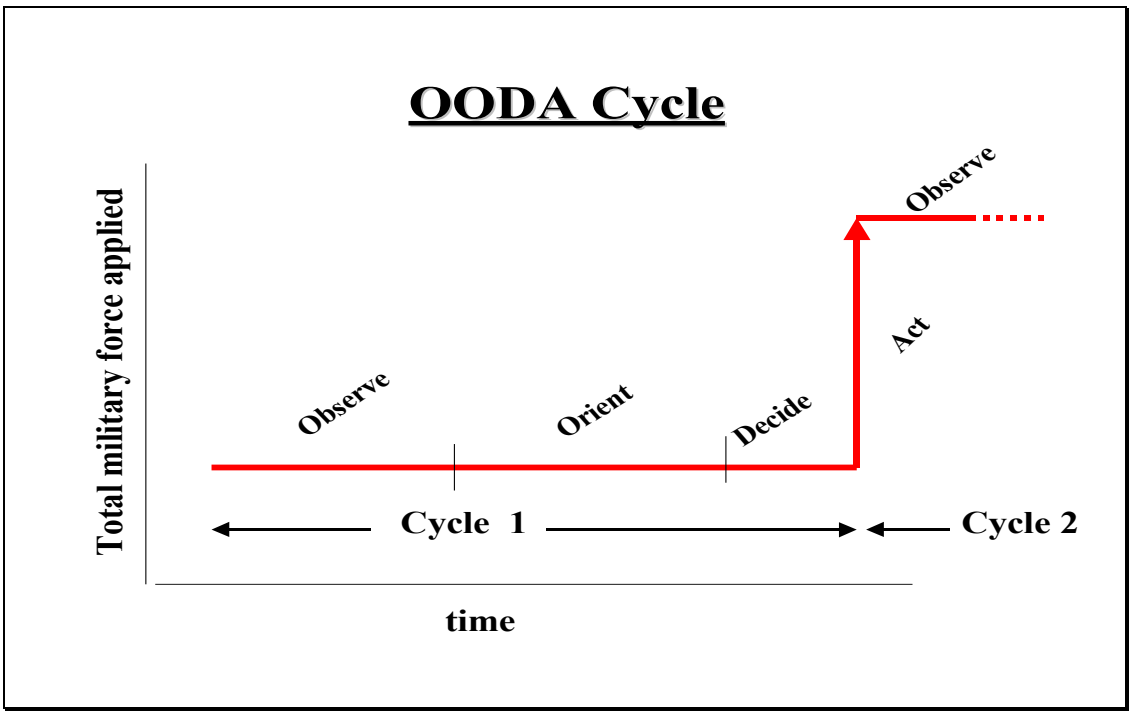

Figure 6: OODA Cycle
Source: Smith, Edward A., Naval War College Review, *Network Centric Warfare: Where's The Beef?,* 11.

[65] Edward A. Smith, Jr., "Network Centric Warfare: Where's the Beef?," *United States Naval War College Review* (1999), 10. Smith also draws a number of detailed insights from Fig. 4 (above) regarding the practical applications of NCW.

Smith goes on to use this graphic to give meaning to the hackneyed term "getting inside the enemy's OODA loop." From purely a question of timing between a friendly decision cycle (depicted in blue) and the enemy cycle (red), it is clear that a friendly "act" (application of massed, effects based, combat power) that is phased to occur during the enemy's "decide" phase as depicted (or, for that matter, during enemy "observe" or "orient" phases) will interrupt the adversary OODA cycle and necessitate a resultant reset in his process. Because the complexities of combat would involve multiple simultaneous force-on-force engagements (at tactical, operational and strategic levels) it is anticipated that a succession of arrested adversary cycles might lead beyond disruption to "an almost catatonic state of 'lock out' in which the enemy can no longer react coherently."[66]

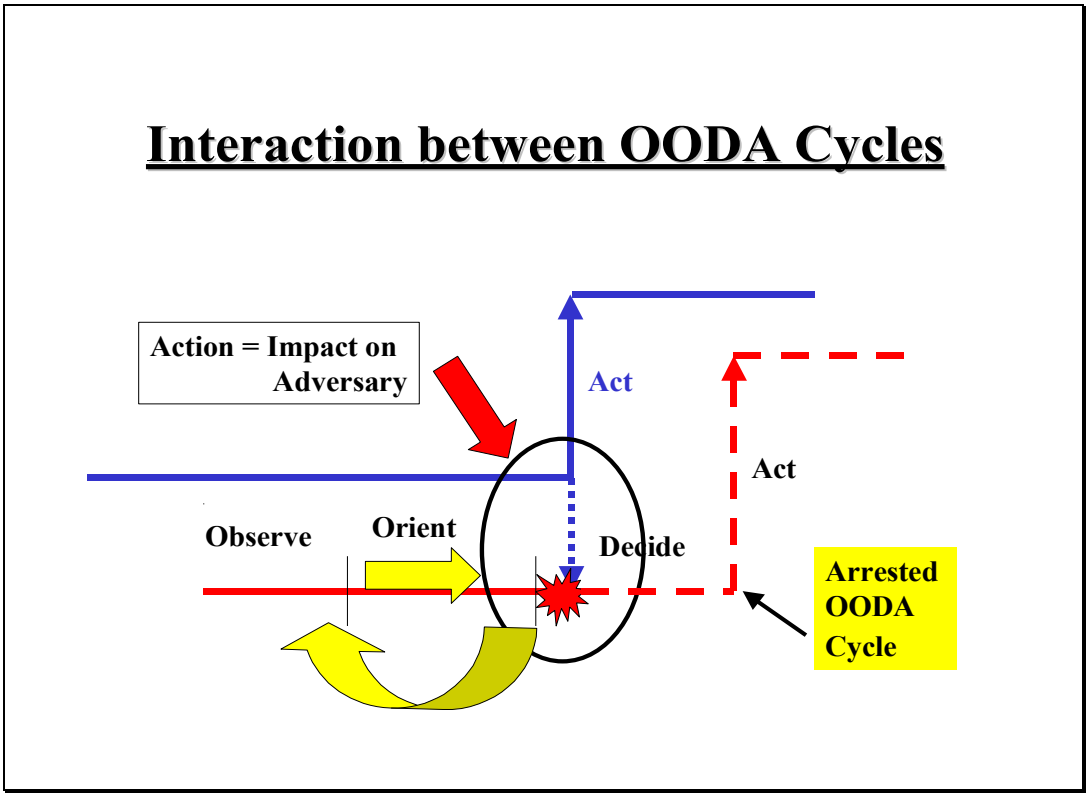

Figure 7: Interaction Between OODA Cycles
Source: Smith, Edward A., Naval War College Review, *Network Centric Warfare: Where's The Beef?,* 19.

[66] Smith, Jr., *Network Centric Warfare: Where's …*, 18.

If one views warfare in terms of the OODA loop, then it is clear that the ability to observe, orient, decide and act faster than your opponent is necessary for success in future warfare. Gen Gordon Sullivan, a former US Army Chief of Staff observes in War in the Information Age that throughout history the tempo of operations caused by the impact of technology has accelerated.[67]

	Revolutionary War	*Civil War*	*World War II*	*Gulf War*	*War of Tomorrow*
Observe	Telescope	Telegraph	Radio/Wire	Near Real Time	Real Time
Orient	Weeks	Days	Hours	Minutes	Continuous
Decide	Months	Weeks	Days	Hours	Immediate
Act	A Season	A Month	A Week	A Day	Less Than An Hour

Figure 8: Tempo and Command
Source: Sullivan, Gordon R. and James M. Dubik, *War in the Information Age*.

Combining this increased tempo of operations with the tenets of NCW we discover the situation illustrated below (Fig. 9). Although both red and blue forces depicted apply the same total amount of combat power, the friendly force (blue) is able to capitalized on information technology, shared awareness and self-synchronization and effectively shorten his OODA cycle times to compress the time required to apply the same combat force. Increased frequency of strikes ("act"s) serves to increase the probability of adversary disruption and potential "lock-out".[68]

[67] Gordon R. Sullivan and James M. Dubik, "War in the Information Age," (Carlisle Barracks, PA: United States Army War College Paper, 1994), 5.

[68] Smith, Jr., "Network Centric Warfare: Where's …, 22.

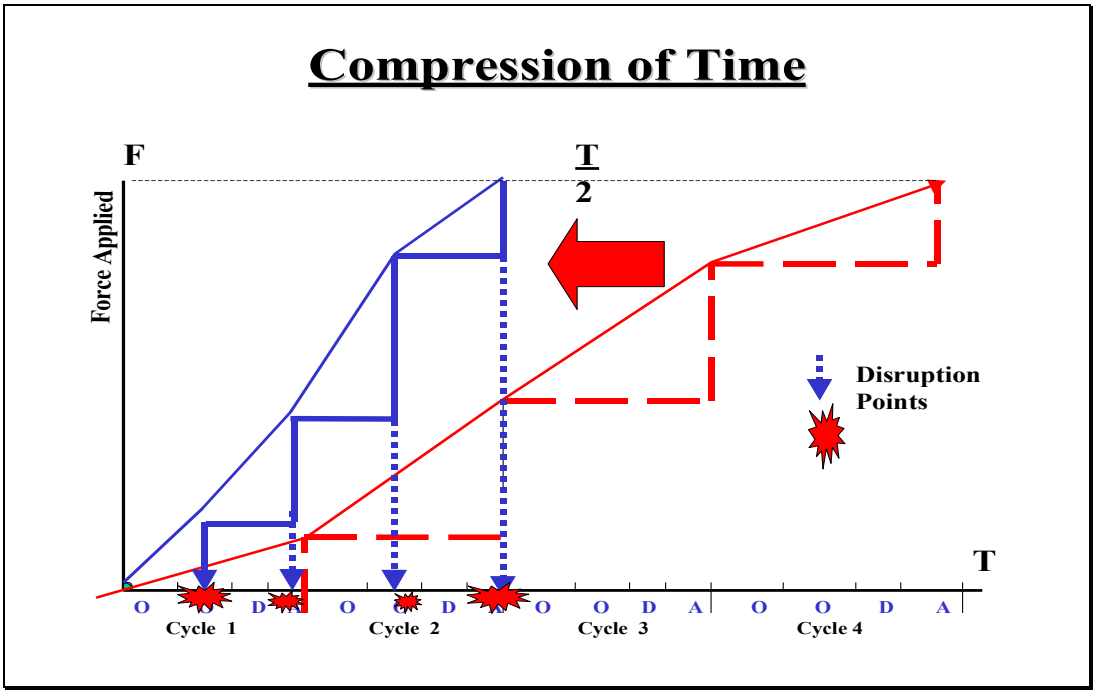

Figure 9: OODA Cycle
Source: Smith, Edward A., Naval War College Review, *Network Centric Warfare: Where's The Beef?,* 22.

While the trends identified in the table at figure 8 (above) seem reasonable, Sullivan goes on to suggest that information technology has decreased the time available for commanders to gather information and make decisions.[69] In reality this is not entirely correct, information technology will provide the means by which commanders will be *able* to make more rapid decisions, but there is no evidence to suggest they are obliged to do so. Under the reasonable assumption that some of our adversaries will also make full use of information technology, it is fair to assume that commanders will want to make operational decisions as quickly as possible. From the table then, we observe that the time differential between orienting (finding out "what is actually happening?) and deciding ("what can I or should I do about it?") has compressed to the point that in information-age warfare, orienting and deciding can no longer be sequential actions but must be simultaneous,

[69] Sullivan and Dubik, *War in the Information …,* 5.

continuous actions. Therefore, organizational orientation and procedures are critical components in determining the tempo of a commander's OODA loop.[70]

2.5 - CHAPTER CONCLUSION

The dawn of the Information Age has precipitated an ongoing international Revolution in Military Affairs (RMA). The US military concept to implement this RMA is Network Centric Warfare. Graphically depicted (Fig. 10 below), NCW provides for the shift from platform centric operations (individual virtually autonomous units) to a system of integrated units with greater cooperation and shared mission accomplishment. The final goal of NCW is however a situation involving overlapping sensor and engagement grids fused by a comprehensive information grid. In theory NCW (and similarly CF NEOps) will allow a potentially smaller force in numbers, technology or position to succeed in battle as any networked strike unit can act on the observation, orientation and decision of any other networked unit.[71]

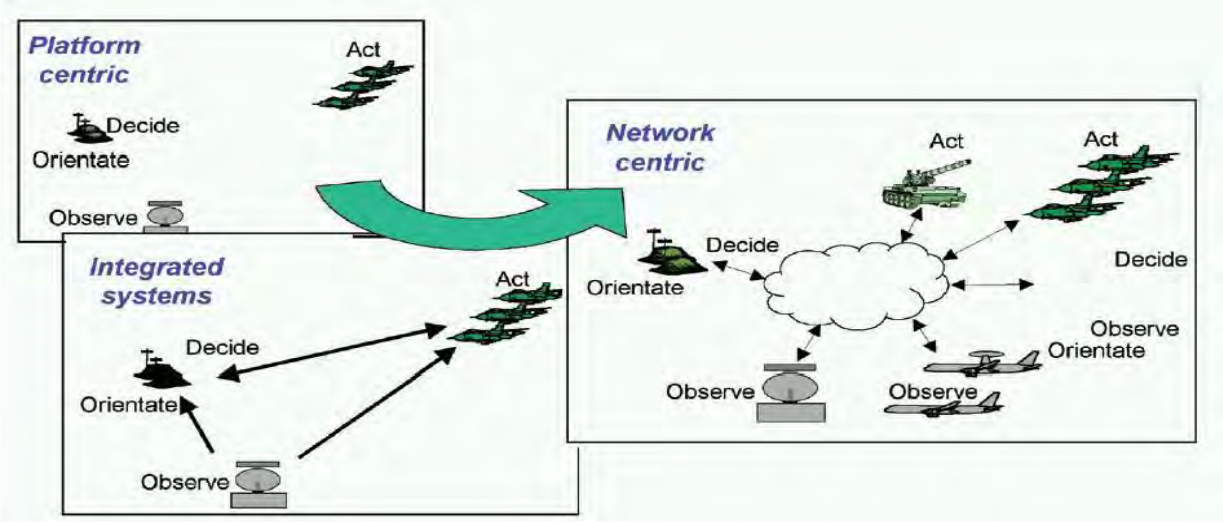

Figure 10: Illustrative Example of Information Age Practices.
Source: Babcock, Sandy, DND/CF Network Enabled Operations Working Paper, 8.

[70] Roman, *The Command or Control Dilemma*…, 16.

[71] Paul Murdock, "Principles of War on the Network-Centric Battlefield: Mass and Economy of Force," *Parameters* (Spring 2002): 91.

CHAPTER 3

NETWORK CENTRIC WARFARE CHALLENGES

> Topology, robustness, and vulnerability cannot be fully separated. All complex systems have their Achilles' heel.[72]

Canadian military research scientists warn us to use serious caution before accepting wholesale the principles of NCW in the CF. They maintain that "NCW 'Theory' is no more than a "series of largely untested hypotheses or assumptions that should be subjected to research and a Clausewitzian dialectic to determine their usefulness."[73] Unfortunately the US Department of Defence (and other western nations) policy documents frequently present NCW not as speculative theory, but as an authoritative doctrine on future warfare.

In the preceding chapter, we examined the origins and background of NCW theory. Before the CF can hope to implement its own NEOps concept, it is imperative to analyze and understand some of the key theoretical and practical challenges already faced by NCW.

3.1 - COMMAND STRUCTURE

> The NCW environment will not determine the essence of command in war. The technology will indeed bring a new set of variables to the command equation that must be solved by commanders. It the words of Martin van Creveld, 'Far from determining the essence of command, then, communication and information processing technology merely constitutes one part of the general environment in which command operates.' The technological component of war can never fully account for the dynamic interaction of human beings and 'war will remain predominantly an art, infused with human will, creativity, and judgment.[74]

---

[72] Albert-Laszlo Barabasi, *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life* (New York: Plume (Penguin Group), 2002), 121-122.

[73] Allan D. English, Carol McCann, Richard Howard Gimblett, and Howard G. Coombs, *Beware of Putting the Cart before the Horse: Network Enabled Operations as a Canadian Approach to Transformation* (Toronto: Defence R&D Canada, 2005), 6.

[74] Pierre Forgues, "Command in a Network-Centric War," *Canadian Military Journal* (Summer 2001): 30.

As we have observed, in theory, NCW will increase speed of command, provide greater amounts battlespace situational awareness information at all levels of warfighting and enable self-synchronization by ensuring rapid and accurate dissemination of the commanders intent. Proponents of NCW suggest that this will also lead to a flattening of the chain of command and a "blurring" of the traditional levels of war (tactical, operational, and strategic).[75] Others have suggested that this "blurring" may lead to the complete elimination of the operational level of war (and associated "operational art") leaving a situation where tactical operators in the field are directed by strategic commanders in distant command and control centres.[76] There is a requirement for significant analysis of the impact of NEOps on the traditional military hierarchical command structure and many have observed that significant trust across the span of military control will be essential in this new command structure.[77]

Recognizing the potentially significant impact NCW could have on command and control (C2) relationships and execution, Australian defence scientists conducted interviews with over 100 ADF personnel (all ranks and occupations) following their return from deployments in Iraq and Afghanistan. The report observed varying degrees of success in devolution of authority of NCW C2, impacted significantly by levels of trust, command support and communications effectiveness. Their chief recommendation was that their must be a greater emphasis on training if the ADF is to ensure effective C2 in an NCW

---

[75] Alberts, Garstka, and Stein, *Network Centric Warfare …,* 84.

[76] Erik J. Dahl, "Network Centric Warfare and the Death of Operational Art," *Defence Studies* 2, no. 1 (2002): 8.

[77] Jennifer Free, "Network-Centric Leadership: Why Trust is Essential," *US Naval Institute Proceedings* 131, no. 6 (June 2005): 58.

environment.[78] Another potential challenge to the military chain of command under NEOps, particularly in an absence of strong levels of trust, is the danger of micromanagement, a situation we will discuss next.

3.2 - MICROMANAGEMENT

> The seductiveness of information technology stimulates military organizational orientation towards greater centralized control and more rigid hierarchical organizations instead of the desired orientation of decentralized control and more flexible organizations. Unless the US military recognizes the danger of succumbing to technological temptation, control functions may take priority over command functions resulting in both a less efficient and less effective military.[79]

NCW promises to flatten military hierarchies, but the serious nature of military operations and an almost unlimited data flow may push too many commanders into becoming control freaks. "In the end, the quest for sharing may prove more disintegrating than integrating."[80]

One of the very benefits of NCW, the Common Operating Picture (and associated networked worldwide communications) has the potential to result in a highly disruptive micro-management. As NCW successively brings about a more robust battlespace picture "the more tempting it is for superiors believing their views are better, their judgments more mature, or their authority more compelling to usurp control and decision making."[81] While

---

[78] Celina Pascoe, *Network Centric Warfare and the New Command and Control: An Australian Perspective,* 11th International Command and Control Research and Technology Symposium (Canberra, Australia, 2006), 11.

[79] Roman, *The Command or Control Dilemma …,* 2-3.

[80] Barnett*, The Seven Deadly Sins …,* p 39.

[81] Chris Johnson, "Net-Centric Fogs Accountability," *Proceedings* 129, no. 5 (2003): 32.

this seductive and compelling temptation to micromanage is both understandable and natural to human nature, it must be recognized and actively avoided.

The Kosovo campaign (Operation Allied Force) in 1999, is widely recognized as one of the first networked conflicts in history and it provided a classic demonstration of overt micromanagement. From his SHAPE, Belgium headquarters, Supreme Allied Commander (SACEUR), General Wesley Clark was provided robust NCW enabled connectivity and a high fidelity COP, complimented by live UAV video feed, Video Teleconferencing (VTC) and access to a considerable volume of data via the SIPERNET (Secret Internet Protocol Routing Network). Unfortunately, the temptation to micromanage proved irresistible and General Clark elected to make many tactical decisions himself, rather than providing subordinate commanders ample latitude and trust to make their own decisions.[82]

Ironically, General Clark seemed to be oblivious to the dangers of these actions, seeing himself as regulating tactical level actions that had potential for strategic impact. His views on the issue were clear when he wrote: "What we discovered increasingly was that the political and strategic levels impinged on the operational and tactical levels …… sometimes evening seemingly insignificant tactical events packed huge political wallop. This is a key characteristic of modern warfare."[83]

In a similar situation years later during Operation Enduring Freedom, the term "3,000 mile screwdriver" was coined to describe the frequent tactical level interference by

---

[82] Benjamin S. Lambeth, *Air Power Against Terror: America's Conduct of Operation Enduring Freedom* (Santa Monica, CA: RAND Corporation, 2001), 210.

[83] Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo, and the Future of Combat* (New York: Public Affairs, 2001), 10-11.

General Franks from his Central Command HQ in Tampa, Florida[84] - illustrating that the temptation to micromanage in NCW remains very strong indeed.

Some experts have suggested that one of the dangers of headquarters having a detailed COP is that it "will lead operational commanders to be increasingly involved in purely tactical decisions, instead of focusing on the operational and strategic aspects of the situation."[85] Given the potentially vast and detailed COP NCW can provide, the temptation to micromanage must be understood, recognized and avoided by commanders at all levels.

3.3 - INFORMATION OVERLOAD

> We are drowning in information but starved for knowledge. This level of information is clearly impossible to be handled by present means. Uncontrolled and unorganized information is no longer a resource in an information society, instead it becomes the enemy.
>
> John Naisbitt, Megatrends, 1982

Frequently cited as one of the growing challenges to implementing a NCW concept is the vast volumes data made available to decision makers. One recent NCW case study found that "senior commanders are inundated with information while maneuver commanders get too little operationally useful information, or they get it too late or not at all."[86] The tremendous quantity of real-time data being collected by an array of sensors results in a double-edged sword. Either the commander can choose to view all the raw feed live, risking being overwhelmed sifting through data to the detriment of other command

---

[84] Milan Vego, "Net-Centric is Not Decisive," *Proceedings* 129, no. 1 (2003): 53.

[85] Ibid, 56.

[86] John Luddy, *The Challenge and Promise of Network-Centric Warfare* (Arlington, VA: Lexington Institute, 2005). Available from http://www.lexingtoninstitute.org/docs/521.pdf; Internet; accessed 1 November 2007, 6.

responsibilities, or he/she can choose to be presented more actionable information post-analysis, the time delay for which however may at best negate the NCW operational advantage or at worst be no longer tactically relevant.[87] Even in the CFs current state, we see signs of information overload; moving to a network-enabled force will risk compounding this problem, particularly with the proliferation and increasing data rates of sensors and increasing bandwidth capable of pushing phenomenal amounts of information across the infostructure. Extracting useful information from this sea of data risks becoming extremely difficult and time consuming.

While the concept of a COP is not new, what has changed is the potential for inundating all participants with an ever-increasing flow of data masquerading as information because it has been slickly packaged within the picture. The danger lies in the COP's "collapsing all participants' perceptions of what is tactical versus operational versus strategic, and by doing so, creating strong incentives for all to engage in information overload in an attempt to maintain their bearings in this overly ambitious big picture."[88]

Cebrowski counters the charge that information overload will be a paralyzing challenge in NCW with his assertion that information superiority will not necessarily lead to larger volumes of data or information. He suggests that information must be evaluated with respect to the discriminants of relevance, accuracy, and timeliness. Once evaluated "and the chaff has been winnowed, the question of overload subsides."[89] Unfortunately, he provides no definitive description of how information overload would be avoided, short of suggesting

---

[87] This dichotomy was observed first hand by the author with respect to live Predator UAV feed in the Vicenza CAOC during the Bosnia crisis.

[88] Barnett, *The Seven Deadly Sins*…, 39.

[89] Cebrowski, Network-Centric Warfare: An Emerging…, 21.

rapid and accurate information evaluation and discrimination "perhaps by automation or organizational adaptability."[90]

3.4 - NETWORKED COALITIONS

> Imbalances are growing within the Alliance, between those countries that are investing more quickly in new technologies and capabilities, and those that are proceeding at a slower pace. This is increasing posing challenges to interoperability, as some Allies move to higher-tech command, control, communications and intelligence equipment …… So we need to ensure that we take advantage of technology to enhance our teamwork, rather than letting technology get between us.[91]
>
> Lord Robertson, NATO Secretary General

True today as it was when articulated in the 1994 Canadian Defence White Paper is Canada's commitment to collective international peace, security and stability through continued participation in the UN, NATO and NORAD.[92] In the history of the Canadian Forces, the nations military has never "gone it alone" in any unilateral and independent military mission. The relatively small size of the CF coupled with certain key capability shortfalls (aircraft carriers, strategic lift, strategic deterrence, theatre ballistic missile defence, etc.) suggest that Canada will continue to participate in Multinational Operations, those involving forces from two or more nations. Nations with much larger and more capable militaries have and will likely continue to seek multinational support for operations

---

[90] Ibid, 21.

[91] Lord George I. Robertson, "Rebalancing NATO for a Strong Future," (Remarks Given at the NATO Defence Week Conference, Brussels, Belgium, 31 January 2000). Available from http://www.nato.int/docu/speech/2000/s000128a.htm; Internet; accessed 16 March 2008.

[92] Department of National Defence, *1994 White Paper on Defence*. Available from http://www.forces.gc.ca/site/Minister/eng/94wpaper/white_paper_94_e.html; Internet; accessed 11 December 2007.

because they "… afford political legitimacy (e.g., through United Nations Resolutions), and can ease domestic objections to military operations."[93] The United States doctrine recognizes that the formation of multinational operations is greatly influenced by "cultural, psychological, economic, technological, informational, and political factors as well as transnational dangers."[94] In the final analysis "nations come together in multinational operations because of their own security interests, although the specific objectives do not necessarily have to coincide."[95]

Given that the end of the Cold War left only one remaining military superpower, many other nations find themselves in similar situations as Canada and thus it is fair to assume that multi-national coalition operations will continue for the foreseeable future. What has not been fully addressed vis-à-vis NCW, and may well be the concepts most significant challenge, is the issue of multinational interoperability. The operability challenge stems from both equipment and procedural compatibility and accessibility concerns. The latter issue presents the greatest long-term combined NCW impediment. This is because technological and procedural compatibility issues can be resolved as a function of a nations will, resource allocation and appropriate training. Shared access to sensitive national classified information (particularly when intelligence based) is an entirely different issue.

In "Small Navies and Network Centric Warfare", Dr. Mitchell points out that despite decades of peacetime training and combat operations between the USN and Canadian Navy,

---

[93] Eric S. Miller, *Interoperability of Rules of Engagement in Multinational Maritime Operations*. Center for Naval Analyses Research (Alexandria, VA, 1995), 11.

[94] United States, Department of Defence, Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations* (Washington, D.C.: U.S. Government Printing Office, 1999), I-2.

[95] Miller, *Interoperability of Rules of Engagement…,* 10.

Canadian ships still experience significant difficulties in integrating into USN carrier battle groups because of accessibility issues.[96]

The US has, understandably, been reluctant to grant full access to its most secure information, even to her closest allies. While there has been some limited success in "working around" these releasability issues, at the end of the day it takes a human in the loop to make the determination of the classification and sensitivity of certain intelligence information – this results in delays to information passage. As NCW becomes the norm in US joint operations, some have suggested that the US may even elect to act unilaterally rather than accept the choice between sharing sensitive information or sacrificing NCW combat speed advantage.[97] The US desire to fight in "coalitions of the willing" (political legitimacy, public support) is set to conflict with the fundamental precepts of NCW (unrestricted information sharing & speed of command). There may soon come a time when "it will be forced to choose between operational efficiency and strategic expediency."[98]

Mitchell's "Small Navies" is a profound and far reaching analysis of the challenges of integrating a middle power navy (in this instance Canada) into an increasingly networked USN. The observations and conclusions made are likely to be useful considerations for *any* nation looking to operate inside the US NCW structure. He concludes that while the technological incompatibilities can be resolved, the chief challenge remains that of trust and information sharing policies and protocols.[99]

---

[96] Mitchell, *Small Navies and Network-Centric Warfare*…, 94.

[97] Ibid, 96.

[98] Paul T. Mitchell, "International Anarchy and Coalition Interoperability in High-Tech Environments," in *Peacekeeping Intelligence : New Players, Extended Boundaries,* edited by David Carment and Martin Rudner (London: Routledge, 2006), 87.

[99] Mitchell, *Small Navies…,* 95.

A similar problem, to a lesser degree, has been seen regarding technical and procedural compatibility *within* the US military forces in joint operations between the four services; this has led to standardization concerns and has hampered interoperability. Cebrowski admits that security concerns and technical and procedural compatibility are indeed significant challenges, but contends that neither warrant abandoning the phenominal potential benefits of NCW.[100]

In reality, the question in coalition operations is not whether or not to share information but how and to what degree multinational forces *must* share information in order to ensure success in future operations.

3.5 - OVER-RELIANCE ON TECHNOLOGY

Another frequent criticism of NCW is the fact that it appears to hold a blind faith in military technology. Gentry observes that the US military Joint Vision 2020 is based on a number of fundamental flaws with regard to NCW. Chief among these are the IT infrastructure challenges. Under the vision of NCW, US military control of land, sea, air and space domains would hinge on the simultaneous, continuous and networked functioning of thousands of IT sub-systems, a challenge never attempted by any nation's military. Managing massive IT networks is a significant technological challenge, "the United States does not do it well in peacetime. There is no good reason to think the US military can achieve it while fighting a competent enemy."[101]

---

[100] Cebrowski, *Network-Centric Warfare: An Emerging…*, 22.

[101] Gentry, *Doomed To Fail…,* 1.

Gentry also warns of the lack of concern for the relatively easy NCW countermeasures that are available. The simplest of which would see "adversaries operate in politico-military arenas beyond the scope of US military capabilities, rendering the technology irrelevant"[102] (a factor in today's counterinsurgency campaigns in both Iraq and Afghanistan). Equipment to jam or disrupt high-tech sensors and weapons is readily available and often simple and inexpensive to construct.[103] As we have discussed, the NCW concept groups sensors, weapons systems, intelligence and COP together via the information grid. There have been numerous reported instances of successful hacker attacks into DoD secure networks; it would be naïve to imagine that a determined and funded enemy cannot replicate the successes of bored American teenage hackers.

Another danger emerging in the midst of the bow-wave of NCW enthusiasm is that many supports seem to understand the broad theoretical concepts but have not examined the practical operational realities. A brilliant example of this lack of understanding is shown in the Mitre Corporation DVD entitled "Network Centric Warfare – Theories, Examples and Challenges."[104] As an NCW case study, the video describes how the Stryker Brigade vehicles employ the Blue Force Tracker system, and how they provide each team "better decision making options" and "enable speed of command."[105] A demonstration takes place at the Joint Readiness Training Center at Ft Poke, Louisiana. Major Hugo Jackson explains that from his Stryker he has just observed a simulated enemy vehicle and dutifully enters the

---

[102] Ibid, 1.

[103] The author was recently involved in CF testing of a Russian made COTS GPS jammer in addition to a laboratory built version (constructed by DND defence scientists).

[104] Roy Modeen, John J. Garstka and Frederick P. Stein. *Network Centric Warfare*. Bedford, Mass.: Mitre Corporation (DVD), 2005

[105] Modeen, Garstka and Stein, *Network Centric Warfare*.

position of the "enemy" vehicle and number of personnel into the BFT COP system. Once he hits "send", Maj Jackson turns to the camera and announces that "everybody has situational awareness", everyone with access to this picture knows that there is an "enemy vehicle with five soldiers at that grid location."[106] The video ends and we are returned to the PowerPoint briefing presented by Mr. Stein. What the audience is *not* told, and is a significant issue with any COP, is that a nanosecond after Maj Jackson updates the BFT COP, it potentially becomes inaccurate, or worse yet, misleading. The second that enemy vehicle moves, unless an individual or sensor is specifically designated to track it, the COP becomes outdated. Many observers, having seen how well the BFT system works for friendly forces, fail to realize that there is no such automated tracking process for enemy combatants. Accuracy of the COP has been a challenge since the first implementation of military datalinks,[107] however under NCW this enemy position data becomes even more critical as it will be used for targeting and weapons guidance. This explains the heavy NCW emphasis on C4ISR, UAVs and satellite imagery. However until such time as our adversaries agree to wear Red Force Trackers, maintaining an accurate COP will remain a significant NCW challenge.

Notwithstanding the potential benefits of NEOps in the battlespace, command remains "a mission-oriented human endeavour, performed within the limits of a commander's personal attributes, and guided by a framework of fundamental principles."[108]

---

[106] Ibid.

[107] During operation Allied Force, senior officers were concerned when the COP showed coalition aircraft operating in "no-fly" areas – in a majority of the cases the author was required to explain that the issue was a COP symbology error and that no actual aircraft was at the indicated position.

[108] Pierre Forgues, "Command in a Network-Centric War," *Canadian Military Journal* (Summer 2001): 22.

NCW proponents frequently suggest that computers will assist commanders with decision-making programs and information sorting, processing and distribution. In reality, computers are not capable of cognitive reasoning, creativity or intuition and have done little more than repetitive administrative data sorting and limited pattern recognition in photo interpretation. No one has developed a "computer program that can differentiate between a feint and a main effort"[109] in combat. As suggested in the section above, humans also play a key role in NEOps between coalition partners where vetting of sensitive, intelligence-based, or classified information is required before being shared over a network.

3.6 - MILITARY OPERATIONS OTHER THAN WAR

Cebrowski admits that the US Navy, for example, does not train organize or equip for the conduct of MOOTW (such as counter-drug operations, non-combatant evacuation operations, foreign humanitarian assistance, peace-keeping, etc.), however he contends that "there is little in the way of requirements for Navy ships or aircraft to participate in MOOTW for which combat training does not suffice"[110] (a statement that strongly debated by CF MOOTW veterans). Cebrowski does grant the fact that, for example, counter-insurgency operations would not realize the full benefit of NCW if complete and thorough information collection was not possible. However, he contends that "even in the case where information is far less perfect, it could be reasonably argued that being able to have a shared understanding of what is known and what is not known would be preferable to a situation in which units operated in isolated ignorance."[111]

---

[109] Alan D. Zimm, "Human-Centric Warfare," *Proceedings* 125, no. 5 (1999): 30.

[110] Cebrowski, *Network-Centric Warfare: An Emerging…*, 22.

[111] Cebrowski, *Network-Centric Warfare: An Emerging…*, 22.

US literature initially referred almost exclusively to NCW; we now see more frequent use of the term Network Centric *Operations* (NCO) to reflect that not all military operations involve war. As will be discussed in more detail later, this idea was also influential in the Canadian coinage of the term NEOps. "Operations" more accurately describes the full spectrum of CF missions, including: aid to civil power, foreign humanitarian assistance, peace-keeping, counter-insurgency and full-scale conventional combat. Furthermore the word "Enabled" vice "Centric" confirms the importance of the human in the military decision loop (a concept that will also be discussed in more detail later). Canada's unique nomenclature decision is widely approved by senior Canadian leaders with command experience of networked forces in operations.[112]

---

[112] Joe Sharpe and Allan D. English, *Network Enabled Operations : The Experiences of Senior Canadian Commanders* (Toronto: Defence R&D Canada, 2006), 4.

3.7 - CHAPTER CONCLUSION

As we have seen, NCW implementation brings with it a number of unique and serious challenges. This is particularly true for some of the more complex, new and untested technologies. Ironically while it is the human in the loop that will be critical to the success of NCW and NEOps, it is also the human that is potentially one of the concepts weaknesses. Imagine the impact of a single human error in a system of thousands of netted IT networks working at lightning speed. For example, what if the incorrect coordinates of an enemy submarine were entered into the network – what would be the impact? Erroneous operational plans? Inaccurate weapons delivery? Fruitless tactical action?

This is not to suggest that these NCW challenges cannot be overcome or at least mitigated, however NEOps proponents in Canada must be aware they exist and be prepared to address each.

CHAPTER 4

ALLIED AND CF NCW IMPLEMENTATION

Thus far this paper has focused on the US military concept, development and implementation of Network Centric Warfare. Logic dictated an initial analysis of US NCW as this concept was born in the US and the US military currently invests more resources to NCW development than any other nation.[113]

One might ask why Canadian and allied NCW programmes should be any different than that of the US. Why not simply apply the results of billions of US R&D in this concept? We have established that future conflicts are likely to involve multi-national coalitions, have we also not concluded that in these cases interoperability is critical to success? The answer seems to stem from two key areas.

Canada does share common values, economic goals, culture and interests in collective defence with our allies. However, our national priorities, political objectives, and national identity have led to the employment of the Canadian Forces in a uniquely Canadian fashion. When fully implemented, NCW will permeate all aspects of the CF (and other government departments), hence it is quite normal that our interpretation and implementation of NCW will have a unique slant.

Our non-US allies have concluded similarly. Prior to addressing the Canadian Forces' unique interpretation and implementation of NCW, and in the interest of balance, it will be useful to examine the NCW interpretation of two of Canada's closest military allies

---

[113] Arthur K. Cebrowski and Thomas P. M. Barnett, "The American Way of War," *Proceedings* 129, no. 1 (2003): 42.

(both of which have older, more robustly and developed programmes). This will serve to broaden our view of NCW implementation among allies.

4.1 - UNITED KINGDOM – NETWORK ENABLED CAPABILITY (NEC)

After the US, the UK armed forces are considered the next most developed networked force. The UK networked operations, Network Enabled Capability (NEC), shares many similarities with the US NCW concept but also incorporates distinct differences. The UK defines NEC as "linking sensors, decision makers and weapon systems so that information can be translated into synchronized and overwhelming military effect at optimum tempo."[114]

A more precise explanation of the structure and primary purpose of NEC comes from the UK Defence Minister, displaying clear similarities to NCW, he stated that NEC "encompasses the elements required to deliver controlled and precise military effect rapidly and reliably. At its heart are three elements: sensors (to gather information); a network (to fuse, communicate and exploit information); and strike assets to deliver military effect. The key is the ability to collect, fuse and disseminate accurate, timely and relevant information with much greater rapidity (sometimes only a matter of minutes or even in "real time") to help provide a common understanding among commanders at all levels."[115]

There are a number of similarities between NEC and NCW, both share the same key tenets. Both concepts aim to establish robust joint military networks facilitating information sharing. Both are predicated on the assumption that information sharing and collaboration

---

[114] United Kingdom, Ministry of Defence, *Network Enabled Capability - Working Definition.* Available at http://www.mod.uk/issues/nec/working_definition.htm; Internet; accessed 15 March 2008.

[115] United Kingdom, Ministry of Defence, *Defence White Paper: Strategic Defence Review New Chapter* (London, UK: HMSO, 2002), 15.

will improve situational awareness which, in turn, will facilitate synchronization and thus enhance mission effectiveness.

A key difference between NEC and NCW (a departure we will see that has been adopted by the CF) is the UK hesitation to seek a predominantly technology driven approach. It has maintained that "NEC does not aim to put the network at the centre of capability in the same doctrinal way as NCW."[116] The UK maintains that both the Maneuverist approach and concept of Mission Command must be preserved. The UK MOD attaches great significance to the human element in warfare and it suggests that integrating the human into NEC may be this concepts biggest challenge. Interestingly, the original US NCW approach as espoused by Cebrowski and Gartska was very heavily technology dependant. Since that time their appears to have been a shift in philosophy towards a greater appreciation of the human element.[117]

Another key difference is that NEC seems to have an evolutionary vice revolutionary outlook. "NEC shares the tenets of NCW but is more limited in scope in that it is not a doctrine or a vision. Nor does it seek to place the network at the centre of capability in the doctrinal way that the term NCW implies. Rather, NEC is much more concerned with evolving capability by providing a coherent framework to link sensors, decision makers and weapon systems to enable emerging UK doctrine on effects-based operations to be achieved".[118]

---

[116] United Kingdom, Ministry of Defence, *Network Enabled Capability - Network Enabled Capability Vs. Network Centric Warfare*. Available at http://www.mod.uk/issues/nec/nec_vs_ncw.htm; Internet; accessed 17 January 2008.

[117] Cite original NCW paper and more recent paper (with references to human in network).

[118] Anthony Alston, "Network Enabled Capability - the Concept," *Journal of Defence Science* 8, no. 3 (2003): 108.

Despite the relative maturity of the NEC concept and the UK's status as second most developed networked military, some serious challenges were noted during Operation Telic (UK Operation in Iraq). A number of these challenges stemmed from the need to interoperate with the heavy bandwidth demands of US NCW C4ISR systems that utilized a large amount of video and imagery.[119] Other UK challenges resulted from existing legacy system problems that were exacerbated by the increased demands of the modern network-centric battleforce. Bandwidth limitations and restricted access from US SIPERNET terminals resulted in large amounts of data having to be moved physically using CD-ROMs. These types of delays proved highly challenging in an operating environment when some targets had to be prosecuted within a 15 minute window of opportunity.[120]

4.2 - AUSTRALIA – NETWORK CENTRIC WARFARE

Interestingly, the Australian interpretation of NCW seemed to initially concur with the UK (and Canada) in moving the nomenclature focus away from the central nature of the network and viewing the concept more as a combat enabler. Hence, initial ADF references in 2002 detailed Australia's ambition towards "Network *Enabled* Warfare."[121] Three years later, Australia decided to adopt the US term Network Centric Warfare, but has adapted its definition to best suite the needs of the Australian Defence Force (ADF). NCW is seen as one of the key enabling concepts underpinning the ADFs Future Joint Operations Concept.

---

[119] For example, the UK HQ in Qatar was receiving 4 MBits of data/sec, while the US equivalent HQ received 300 MBits/sec. Robert K. Ackerman, "British Warfighters Exploit Network Centricity." *Signal* (September 2003). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=147&zoneid=6; Internet; accessed 8 December 2007.

[120] Ibid.

[121] Australia, Department of Defence, *NCW Roadmap* (Canberra: Defence Publishing Service, 2005), 19.

Australia is clear in stating that NCW will not dictate how the ADF will fight, but will facilitate a transition from the current "network aware" force to a seamless network-enabled, information-age force.[122]

Successful NCW implementation in the ADF will be achieved by "effectively linking Command and Control, Sensor and Engagement systems via a network, to facilitate enhanced situational awareness, collaboration and offensive potential."[123] The ADF recognizes the importance of having responsive network connectivity that permit the right information to accessed at the right time by the right force elements. Combat power benefits are expected through rapid, quality shared information, exploitation of new systems and command relationships.[124]

Similar but not identical to the US NCW fundamentals are the ADF's four key interdependent elements that make up the ADF NCW package. Central to the package is the Information Network, feeding into this central network are three grids: Command and Control, Sensors and Engagement. A unique facet of this concept is that the entire package is bound together by the imperative of "personnel enabled."[125] As with our analysis of the UK NEC, the ADF does not consider NCW as a new theory of warfare but more as an

---

[122] Australia, *NCW Roadmap…,* iii. The most recent ADF adoption of the term NCW should not suggest Australia does not recognize the importance of the human in networked operations, nor the fact that networked concepts are applicable outside war. In fact, one report risks significantly confusing matters by proposing, in addition to NCW, that the ADF should also consider "Network Centric Peacekeeping (NCP)", "NC Military Operations Other Than War (NCMOOTW)", and "NC Military Operations in Urban Terrain (NMOUT)"! See Warne, *et al, The Network Centric Warrior: The Human Dimension of Network Centric Warfare*.

[123] Ibid, 4.

[124] Ibid 4-5.

[125] Ibid 5.

enabling tool to support commanders in making faster, more accurate and more effective decisions.

While the ADF is moving ahead on the practical components of NCW; establishing the physical network (linking C2, sensor and engagement grids) and accelerating the process of change and innovation through partnerships with defence industry (via a Rapid Prototyping, Development and Evaluation (RPDE) capability), it remains cognizant of the significant human component. In fact, the ADF sees the ultimate success of NCW as depending upon a thorough understanding of how people think, interact and make decision in a networked environment.[126]

4.3 - OTHER ALLIES

Like the UK, NATO has adopted the term Network Enabled Capabilities (NEC). Although the concept has not seen the same level of development completed by the UK, it appears that NATO shares the same basic UK tenets of primacy of command and networks acting in an enabling capacity.[127]

Sweden's answer to NCW is called Network Based Defence (NBD). While that country is still struggling to define the exact make-up of NBD, certain facts are clear. Sweden plans to make the focus on societal defence, in keeping with it's long-standing commitment to international political neutrality but with strong indigenous self-defence. NBD, like NEC and NEOps will place greater emphasis on human-centricity than the technology driven NCW. The fact that Sweden is a small nation is seen as an advantage by

---

[126] Gerard Fogarty, *Progressing the Human Dimension of NCW in the ADF,* Department of Defence, Human Factors in Network-Centric Warfare Symposium (Canberra: Russell Offices, 2006), 4.

[127] North Atlantic Treaty Organization, *Examining NATO's Transformation*. Available from http://www.nato.int/docu/review/2005/issue1/english/special.html; Internet; accessed 18 March 2008.

defence analyst Staffan Näsström; the armed forces is tightly controlled by government, local defence industry is highly proficient and closely linked to the military, and the country is known for innovators and visionaries. He concedes, however, that a definitive national NBD strategy is still lacking.[128]

Singapore has one of the largest and best trained and equipped military forces among the 10 ASEAN nations.[129] The Singapore Armed Forces (SAF) has adopted a concept know as Integrated Knowledge-based Command and Control (IKC2) as a means to prepare their military for Information Age conflict. The SAF is still largely organized along component service lines, hence one of the chief challenges of IKC2 will be improved joint interoperability among SAF services. Successfully implementation of IKC2 into the SAF will require a transformation in their military culture and changes to existing structure and processes.[130]

4.4 - CANADA – NETWORK ENABLED OPERATIONS

> The only thing harder than getting a new idea into the military mind is getting an old one out.[131]

Canada's adaptation of Network Centric Warfare is referred to as Network Enabled Operations (NEOps). Unlike Australia, the term NCW was not adopted because it fails to

---

[128] Staffan Näsström, "We can definitely become world champions in network-based defence," *Framsyn Magazine*, no. 6 (2003). Available from http://www.foi.se/FOI/templates/Page____3787.aspx#; Internet; accessed 2 April 2008.

[129] Seng Hock Lim, "Myth Or Reality : Network-Centric Warfare and Integrated Command and Control in the Information Age?," (Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2003), 23.

[130] Ibid, 34.

[131] Cebrowski and Garstka, *Network-Centric Warfare…,* 35.

precisely reflect Canada's unique understanding and application of networked concepts, as in the United Kingdoms adoption of Network Enabled Capabilities (NEC).

4.4.1 - Nomenclature

The term NCW was considered problematic for two key reasons. Like the UK, Canada believes very strongly in the central role played by humans in networked operations. NCW suggests that the network is central to the concept (as, in fact, the initial US writings on NCW seemed to suggest); really the network must be seen to facilitate human command. The second issue was the "W" (Warfare) which clearly implies that NCW does not support non-warfare related operations. Canada's vision for networked operations most definitely sees them used across the full spectrum of military activities (humanitarian assistance, peacekeeping, counter-insurgency, and warfighting). Additionally, as we are seeing today in Afghanistan, effective asynchronous warfare requires participation from the Whole of Government (CIDA, DFAIT, DND, NGO's, etc), ideally all government departments would eventually take advantage of networked operations. Network Centric Operations (now seen more frequently in US use[132]) was also considered, while it was not focused on warfare, it still gave central focus to the network. The UK's NEC was strongly considered since it allows for operations other than war and implies the network is an enabler not the central focus. The "C" (Capabilities) however, did not resonate with Canadian experts; the UK defence planning talks about "Lines of Capabilities", but no one else uses this terminology. The group agreed that the most accurate reflection of Canada's networked operational

---

[132] Some more recent US reports use NCO and NCW interchangeably. See Daniel Gonzales, *et al, Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16* (Santa Monica, CA: RAND Corporation, 2005), xvi, note 1.

concept would be Network Enabled Operations. This had to be abbreviated NEOps, as NEO already exists as a NATO acronym (Non-combatant Evacuation Operation).[133]

Another reason why it is important that Canada take ownership of its own unique interpretation and application of networked operations is the fact that despite ten years of evolution, the concept of NCW still involves considerable confusion, as is seen in debates over NCW-driven transformation in the US. Exacerbating this problem is the lack of clear definition of "transformation" in the US, in addition to the lack of clarity regarding NCW specifics in some official publications.[134]

4.4.2 - General

Canadian NEOps is defined as "a concept that has the potential to generate increased combat power by networking sensors, decision makers and combatants to achieve shared battlespace awareness, increased speed of command, higher operational tempo, greater lethality, increased survivability, and greater adaptability through rapid feedback loops."[135]

Recognized that not only will there be unique Canadian application, but that the services will need to tailor NEOps implementation to their unique missions and command styles.

---

[133] The decision was made at a CF Network Operations working group for which Mr. Babcock was co-chair (held prior to the 30 Nov –1 Dec 04 CF NEOps Symposium). The working group included representatives from all NDHQ Level 1 organizations. Following the working group, Mr. Babcock authored a Network Enabled Operations paper which was eventually reviewed and approved by the VCDS, DCDS and ADM (S&T), providing the basis for NEOps becoming the established official DND/CF-wide definition. E-mail from Mr Sandy Babcock to the author, 21 Apr 08.

[134] English, *et al, Beware of Putting the Cart*…, 91.

4.4.3 - Canadian Air Force

Many are unaware that Canada's Air Force was equipped with an albeit rudimentary datalink when the CF-101 "Voodoo" was in service as an Air Defence fighter (1959-1987). SAGE GCI controllers would pass the code words "follow dolly" to Voodoo navigators and then proceed to send heading, speed and altitude commands via datalink.

Effects Based Operations (EBO) was intentionally not discussed in chapter 2 (origins of NCW theory) because, the author believes that it to be little more than the latest buzz-word for what Air Forces have been doing for years. And, unlike other fleetingly popular catch-phrases, there are numerous and varied definitions available for EBO. However, EBO is frequently discussed alongside NCW when describing USAF transformation; given our close military relationship with the US, the "concept" warrants brief explanation here. In essence EBO is about selecting enemy targets, not for what their destruction will represent, but for what reaction they will precipitate. EBO is really about "predicting how physical actions can result in behavioural outcomes."[136] According to Deptula, EBO is applicable in all mediums of warfare, but the aerospace power characteristics of "speed, range, flexibility, precision, perspective, and lethality" are ideal suited for the EBO strategic construct.[137] However his argument becomes suspect when he claims that EBO's "parallel approach changes the basic character of war."[138] Here he is really only referring to coordinated simultaneous attacks, a concept difficult to argue as novel in that it was perfected by Attila

---

[135] Michael H Thomson and Barbara D. Adams, *Network Enabled Operations : A Canadian Perspective* (Toronto: Defence R&D Canada, 2005), 5.

[136] English, *et al*, *Beware of Putting the Cart before the Horse*…, 45.

[137] David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare* (Arlington, VA: Aerospace Education Foundation, 2001), 25.

[138] Ibid, 25.

the Hun in 453 AD. EBO is little more than an exercise in careful targeting[139] and should therefore not be allowed to cloud the issue when discussing implementation of NCW/NEOps by Air Forces.

4.4.4 - Canadian Navy and Army

From a network-enabled perspective, the Canadian Navy is undoubtedly the most experienced and capable element of the CF. Western Navies have been communicating and sharing information via datalinks for decades. The concept of a common shared "picture", communicated at ranges beyond line of sight is ideally suited to the fashion in which Western naives plan, manage and fight at sea. The long continuous periods at sea in both training and live operations, particularly those spent with allies such as the USN and RN have significantly enhanced Canadian Navy experience in networked warfare. As such, the Navy is the only CF element with datalink doctrine and a datalink CONOPS. However, there are challenges ahead with respect to coalition interoperability. As Mitchell observes, the CF Navy may be capable of remaining technologically compatible with her US counterparts, but the issue of sharing classified information in an NCW construct remains a significant hurdle.[140] Notwithstanding these challenges, CF Naval officers have proven they have the aptitude command coalition naval forces in a networked environment with remarkable success.[141]

---

[139] English, *et al*, *Beware of Putting the Cart before the Horse*…, 46.

[140] Mitchell, *Small Navies*…, 95.

[141] Richard H. Gimblett, *Command of Coalition Operations in a Multicultural Environment: A Canadian Naval Niche? the Case Study of Operation Apollo* (CF Leadership Institute, 2006), 1-13.

By contrast, the Canadian Arm has had very little exposure to networked warfare concepts. The only Army units with any extensive background in datalinks is the 4th Air Defence Regiment (ADR) with Air Defence Systems Integrator (ADSI) terminals, allowing Link-11B (via land-line). They unfortunately have no other army units to train with and have cooperated with Canada's TCR's, linking in to the TPS-70 search radar to obtain an early warning picture in their Air Defence role. CF soldiers have also apparently had some experience with Blue Force Tracker in Afghanistan, but as yet no formal feedback has been published regarding successes in that endeavour.

4.5 - CHAPTER CONCLUSION

Clearly we have seen that a number of nations have embarked on network-based military transformation. While it is understandable that each has been developed with the unique requirements and priorities of that nation, a concerted effort should be made to nonetheless ensure a degree of interoperability between networked forces, in the interest of facilitating coalition operations in the future. Perhaps an international monitoring and standardization body should be set up to facilitate national network-based initiatives, in the interest of ensuring a "plug-and-play" capability is retained with international allies?

CHAPTER 5

CASE STUDIES

We have seen that NCW/NEOps offers a potential plethora of theoretical advantages to military forces, across the spectrum of operations. But how does this theory translate into reality? Can new doctrine, command structure, procedures and technology truly mitigate the Clausewitzian "fog and friction" of combat and result in tangible tactical, operational and strategic level military advantage?

Western navies have been employing early forms of network centricity for decades and much has already been written about maritime NCW challenges and successes. But what of the application of the NCW concept and principles to land and air warfare? Particularly when incorporating multinational forces? A number of extensive case studies have been conducted recently that address this very question. Three of these will be reviewed below.

5.1 - AIR-TO-AIR COMBAT & LINK-16

The Office of Force Transformation contracted RAND Corporation to apply the Network Centric Operations Conceptual Framework in an analysis of a USAF Joint Tactical Information Distribution System (JTIDS) Operational Special Project exercise (conducted in the mid-1990s). The exercise comprised over 12,000 F-15 sorties and more than 19,000 flying hours. Friendly (blue) F-15s were equipped with JTIDS Link-16 systems while

adversary (red) F-16s were not; both sides were controlled and cued by Airborne Warning and Control System (AWACS) aircraft.[142]

Simulated engagements were flow during both day and night conditions and involved engagement sizes from 2 blue vs. 2 red up to 8 blue vs. 16 red. On average, Link-16 equipped blue F-15s achieved a two-and-a-half times improvement in kill ratio over the voice-only F-15s during both day and night operations.[143]

While it would seem evident that with Link-16 being the only factored difference between the engaging forces, it must have been a significant contribution in the improved blue kill ratio. However, RAND was tasked to analyze the exercise data in an effort to quantify the increase in combat effectiveness achieved by the NCW employment of Link-16.

RAND concluded by validating the NCW hypothesis for air-to-air combat missions. Despite similar doctrine, tactics, training, pilot experience, airframes and sensors, the Link-16 equipped F-15 pilots were able to more quickly and accurately build SA and exploit this tactical advantage early in most engagements.[144] The case study generated quantitative date concerning the benefits of Link-16 in terms of both information distribution and tactical level SA development. The case study acknowledged that this particular exercise involved relatively simple scenarios, and that the quantitative analysis was done based on sortie outcomes and not by attempting to measure actual NCW based improvements to pilot SA. These and other areas are recommended as the focus for any future such studies.[145]

---

[142] Daniel Gonzales, John Hollywood, Gina Kingston, and David Signori, *Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16* (Santa Monica, CA: RAND Corporation, 2005), xv.

[143] Ibid, xv.

[144] Ibid, 75.

[145] Ibid, 79-80.

Another excellent Air Force example of leveraging the NCW information advantage took place during a Red Flag exercise (also in the mid 1990s) between RAF Tornado aircraft and USAF F-15Cs at Nellis AFB, Nevada. According to the report "historically, the most favourable outcome that the absolute best RAF pilots could manage when flying against the F-15Cs was a draw."[146] In this instance, the Tornados were equipped with Link-16 datalink terminals while the F-15Cs relied on traditional voice-only communications. The results were astounding; the Tornados demonstrated a 4-to-1 kill ratio over the F-15Cs.[147]

5.2 - US/UK OPERATIONS DURING OIF

The Office of Force Transformation released a report in March 2005 detailing their case study of Network Centric Operations (NCO) employed during US & UK combat operations during operating Iraqi Freedom (OIF). The case study examined the degree of improved situational awareness of UK and US forces through the exploitation of the Force XXI Battle Command Brigade & Below System Blue Force Tracker (FBCB2/BFT) and other exiting C4 capabilities (e.g. SATCOM).[148] Data was collected through a detailed series of interviews and questionnaires, initially concentrating at the tactical level of operations. In general, most respondents agreed that the deployment of FBCB2/BFT enhanced operational effectiveness. US personnel were most favourable while many UK

---

[146] John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage," *Signal* (May 2003), 2. Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=234&zoneid=62; Internet; accessed 8 December 2007.

[147] Ibid, 3.

[148] United States, Department of Defence, *US/UK Coalition Combat Operations During Operation Iraqi* Freedom (Washington, DC: Office of Force Transformation, 2005), 3-8.

interviewees concluded that the system had not delivered its full potential benefit.[149] The chief benefits of FBCB2/BFT were summarized as: planning (access to multi-scale digital mapping and imagery), C2 agility (improved by enhanced SA), Tempo (assisted by real-time maneuver deconfliction), enhanced C2 (BLOS communications enabled greater unit dispersal) and Synchronization.[150] Lessons learned from this study related to: lack of adequate training (system was fielded very rapidly), importance of also equipping combat support and combat service support units (giving total blue force SA), and suitable BLOS communications (to facilitate highly mobile and dispersed units).[151]

5.3 - NETWORKED FORCES IN STABILITY OPERATIONS

RAND cooperation was contracted by the OFT to conduct a case study examining the use of networked forces in stability operations, with analysis of the 101st Airborne Division (ABD) and 3/2 and 1/25 Stryker Brigade operations in northern Iraq between 2003 and 2005. The comparative analysis of these three units was considered particularly useful because the 101st ABD was a largely analog unit (having a limited number of advanced battle C2 systems but with most communications via voice-only, they also were limited to line-of-sight analog radios). The 101st ABD was equipped with the FBCB2/BFT system. By contrast, the Stryker units employed networked digital communications with access to high-capacity satellites (giving reliable, secure and BLOS communications).[152]

---

[149] Ibid, 8-1.

[150] Ibid, 8-1.

[151] Ibid, 8-2.

[152] Daniel Gonzales, John Hollywood, Jerry M. Sollinger, James McFadden, John DeJarnette, Sarah Harting, and Donald Temple, *Networked Forces in Stability Operations: 101st Airborne Division, 3/2 and 1/125 Stryker Brigades in Northern Iraq* (Santa Monica, CA: RAND Corporation, 2007), xiii-xiv.

The authors recognized the limitations inherent in this case study methodology; although these units were operating in the same area at the same time, such a real-world study can only yield qualitative comparisons. However, the results of this exhaustive case study did assess the stability operation mission effectiveness to be higher in the Stryker units than the 101st ABD (despite the latter unit having more equipment and a significantly higher reconstruction funding budget).[153] While not without operational challenges, both Stryker units suffered lower US casualty rates and were seen to have greater overall combat SA than the 101st ABD.[154]

5.4 - OTHER

Although not formalized in a case study, another unanticipated warfighting advantage of NCW was observed in combat during operation Enduring Freedom. In this case, improved combat power was not derived from new technology but by networking legacy USAF platforms with special operations forces (SOF). The speed and precision with which ground-based SOF were able to share precision information with C2 aircraft and fighter, bomber and attack aircraft was unprecedented in military operations. Analysts noted that this combat cooperation "represented an order of magnitude increase in information sharing over what had previously been demonstrated anywhere in the world in combat operations."[155]

[153] Ibid, 129-138.

[154] Ibid, 133-139.

[155] Garstka, Network-Centric Warfare Offers…, 2.

5.5 - CHAPTER CONCLUSION

The "take away" from these NCW case studies seems to be that networking forces, depending on the circumstances and employment have seen improvements in operational effectiveness. This understanding must however be tempered with the fact that we are a long way from seeing a robust and fully networked NCW test, involving joint and multi-national forces in a complex environment against a technologically savvy enemy.

CHAPTER 6

WAY AHEAD FOR THE CF

> Without originality, let alone genius, the new technologies will merely by grafted on to existing organizations and doctrines in a way designed to cause the least inconvenienced and least unpleasantness in peacetime. The risks of having operated on this principle in the past are as nothing to the dangers of doing so in the future.[156]
>
> Brigadier J.P. Kiszely

The CF is poised to make the same costly and painful implementation errors as our allies. Senior operators from the US, UK and Australia have all confirmed the same critical error in the fielding of their tactical datalink systems. All these nations, to varying degrees, fielded datalink hardware prior to establishing a management organization, procurement and sustainment process, training, doctrine, CONOPS, and operating procedures.[157] The error is quite understandable as budgeting for and purchasing Commercial Off The Shelf (COTS) datalink and other Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) hardware is relatively simple. What is not readily understood by many senior officials it seems is the phenomenal complexity of NEOps. This is not simply a matter of purchasing a new radio set for the CF. This is a fundamental shift in the way the CF pursues the application of force (and other non-kinetic missions). It will require organizational change, doctrinal adaptation and significant training to implement.

---

[156] Roman, *The Command or Control Dilemma…,* 2.

[157] In accordance with UK, Australian and US military personnel, as discussed with the author during exchange tours and/or operations.

Datalink, for example, is a highly complex system, experience has shown that to produce a competent Joint Interface Control Officer (JICO), operators must be sent on a series of specialized training courses over a period of two years. Dedicated positions are required and analysis must be done to determine which military occupation or occupations are best suited for this employment (Aerospace Controllers have inherent command and control background, CELE officers certainly have the technical competence). Tactical CF units have recognized this serious shortfall. Unfortunately, there is a lack of understanding of the significance of this problem at the Air Division level. When the problem was brought to the division staff, instead of seeking to grapple the problem at the HQ level, the A1 (Pers) cell sent the request back to the unit to develop a Needs Assessment and Job Task Analysis Requirement. This is not a question of a tactical unit proposing the creation of one or two new positions, but represents a fundamental shift in the way the CAF does business and hence this issue needs to be managed from the top down.

6.1 - VISION AND LEADERSHIP

The biggest impediment to NEOps implementation in the CF is the current lack of vision and leadership on the issue. Currently, oversight of CF datalink initiatives, C4ISR and other NEOps related projects is held with the ADM (IM) group. While this arrangement may have been appropriate during the project initiation phase, NEOps is simply far to critical to operations to be relegated to a largely administrative organization. Recommend that NEOps by either the Chief of Force Development or the Strategic Joint Staff. It would be inappropriate to manage NEOps from CEFCOM, CANCOM or CANOSCOM because these are operational level commands and NEOps must first be implemented and controlled at the strategic level.

Next, and second in priority, there is a serious requirement to establish NEOps cells at each element level (CNS, CLS, CAS). Recommend that the Air Force NEOps office be established at 1 Canadian Air Division HQ.

6.2 - DOCTRINE

First and foremost Canada needs to articulate NEOps doctrine – that is to say exactly how the CF intends to incorporate NEOps into the ongoing transformation initiatives. National and Environmental staffs must draft this doctrine, referring to lessons learned and areas covered by allies but taking ultimate direction from CF commanders, academics and defence scientists. Currently the CF has no national level NEOps doctrine.

6.3 - CONOPS

Having developed doctrine, strategic and element staffs would then work together first to define a national joint CONOPS, then to further refine supporting elemental CONOPS. Currently only the Canadian Navy has anything resembling a CONOPS (a developed section in the NCPM 231 Naval Combat Procedures Manual). Part of this doctrinal and CONOPS process would include establishing the minimum personnel required to man these organizations (since they would initially be established with a start-up skeleton staff). The establishment of positions, designation of MOCs and allocation of required training must come as direction from leadership, not percolate up from the tactical level as seems to be happening today.

6.4 - JOINT, COMBINED OR BOTH?

The limited practical NEOps work that has taken place to date in the CF has been across Joint (i.e. multinational) lines. The Canadian Air Force regularly exercises and trains with the USAF, similarly the Canadian Navy trains and fights alongside the USN. For these pragmatic reasons, development of CF NEOps capability has been along combined lines among like elements. It is time for the CF to shift that focus to joint NEOps. This is not to say that the combined capability should be neglected. This, as we have seen above, will continue to be the most likely option in future conflict. However, CF NEOps must be developed jointly for two key reasons. First, CF elements must integrate together under NEOps for the same reason it is not called NCW. Canada's implementation is and should be different than our allies and it is important that CF element units have a clear understanding and capacity to work together under NEOps (without, of course, foregoing interoperability with allies). Second, as the complexity of a national NEOps concept increases, standardization between elements in equipment acquisition, training, and procedures will become increasingly important.

6.5 - DEGREES OF NETWORKED CAPABILITY

Clearly it is unrealistic for smaller nations such as Canada to attain the level of networking and information exchange necessary to achieve true NCW-capacity as defined in the US context. Is it perhaps possible to identify and target a lower, but acceptable level?

A Network Centric Maturity Model has been developed which helps categorize the developmental stage of a network centric application. The model is based on the two key dimensions: the degree to which the C2 system (including humans) is capable to develop situational awareness through information sharing and the degree to which the same system

(including organizational elements and doctrine) are capable of self-synchronizing (see diagram below).[158]

The model identifies five value levels ranging from 0 to 4. Value 0 represents platform centric operations with low situational awareness and traditional C2 relationships. Value 1 involves the ability to share information, which in turn provides enhanced situational awareness. Value 2 involves the availability of collaborative planning to maximize the benefit of the enhanced situational awareness. Value 3 involves richer information engagement involving more participants and integrating more aspects of the operation. There may actually be less communication between participants because of the shared SA achieved. Finally Value 4 requires the integrated capability (including doctrine, training and processes) necessary to permit self-synchronization.[159]

Although this model seems primarily aimed at tracking progress towards a goal of complete network centricity, it may also serve a useful role in setting targets for those defence forces aspiring to that goal, but recognizing that, for the foreseeable future, such goals are unattainable. A realistic near-term goal for the CF would be Value 2 with serious planning and budgeting to achieve Value 3. The astronomical expense involved in fielding and maintaining a CF equivalent to the GIG and the associated sensors may make Value 4 unachievable within CF resource limitations. A good compromise of operational necessity and fiscal reality would see the CF eventually achieve Value 3 NEOps capability whereby they could effectively "plug and play" with coalition forces in a wide-area networked coalition operation.

---

[158] Alberts, *Understanding Information Age*…, 241.

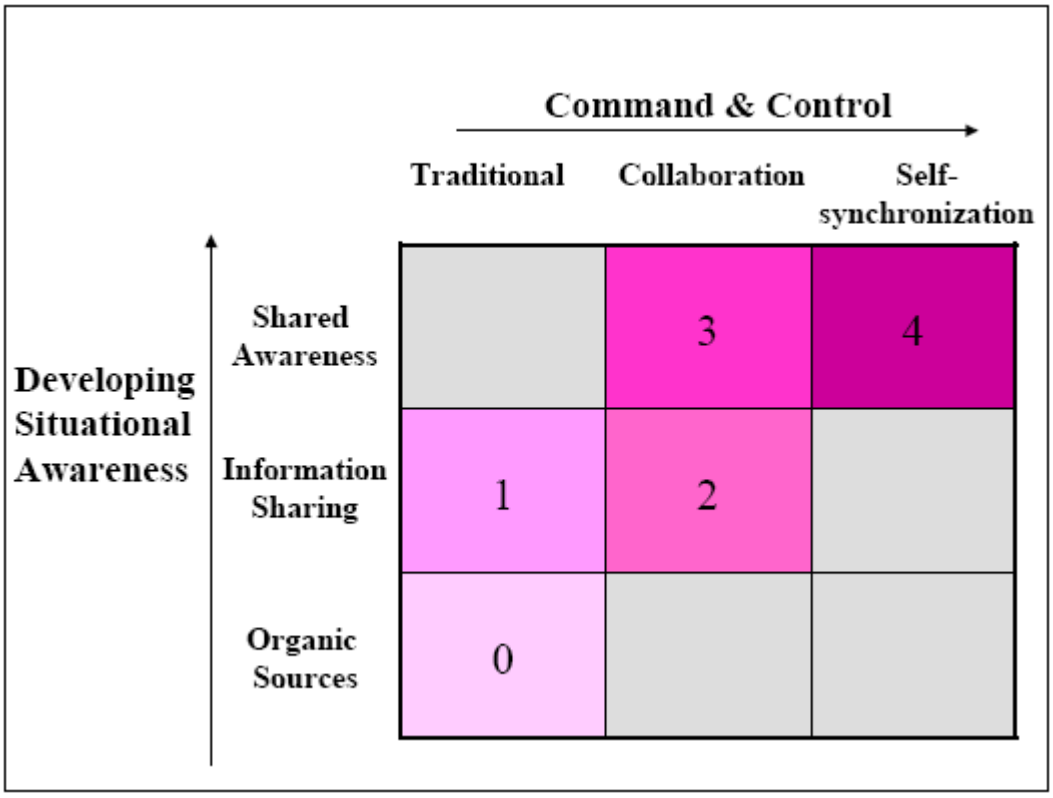

Figure 11: Network Centric Maturity Model
Source: Alberts, David S. *et al*, Understanding Information Age Warfare, 241.

6.6 - CHAPTER CONCLUSION

Successful CF NEOps implementation hinges on senior CF leadership support *as soon as possible*. Further delays in developing doctrine, CONOPS and standardizing equipment and procedures between CF elements will only exacerbate the inevitable (and expensive) back-pedalling that will be required to correct these problems at a later date.

Joint CF training and operations must be stressed in order to bring about a unified network-enabled Canadian Forces.

---

[159] Ibid, 242.

CHAPTER 7

CONCLUSION

> Warfare is not "network centric." It is either "people centric" or it has not centre at all[160]

As with any military concept, the successful implementation of NCW will depend heavily on good leadership. This will require courage and commitment to change, resolute direction and the ability for non-parochial fusion of Army, Navy and Air Force branches into a network enabled force.

There are two key recommendations for successful CF NEOps implementation. The first involves debate, discovery, innovation, and experimentation amongst warfighters and defence scientists. Translating the promises of NEOps into capability-enhancing reality for the CF will not be easy. The challenges will be as much organizational as technological. Their will be new technology required and this will involve significant capitol investment. In some areas upgrade of legacy systems, structures and processes may be possible, but other areas will require radically new force structures and systems. Once the information grid has been established, the CF would need to proceed with integration of the sensor and shooter grids. Organizationally, the CF must adapt doctrine and training to incorporate the NEOps impact on military operations (speed of command, flattened hierarchy, etc) while consistently resisting the temptation to micromanage.

The second recommendation concerns the importance of ensuring complete interoperability among warfighters, both jointly among the three CF services and in

---

[160] Ralph E. Giffin and Darryn J. Reid, *A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy,* 8th International Command and Control Research & Technology Symposium (Ottawa: NDHQ, 2003), 21.

combined multi-national operations with other militaries. CF NEOps systems must be capable to readily "plug" into an integrated battlefield operating system and forces will require interoperable communications, standards, doctrine, tactics and procedures. All this change towards NEOps must ensure that the human occupies the central position, with all the systems, procedures and doctrine built for and around him/her.

> Any new theory of C2 must, therefore, assert the fundamental importance of the human as its central philosophical tenant. It is the human – e.g., the CF member – who must assess the situation, devise new solutions, make decisions, co-ordinate resources and effect change. It is the human who must initiate, revise and terminate action. It is the human who must (ultimately) accept responsibility for mission success of failure. All C2 systems, from sensors to weapons to organizational structures and chain of command, must exist to support human potential for accomplishing the mission.[161]

> We want our leaders and their subordinates to be enabled by appropriate information technologies and architecture in order to develop the situational awareness essential for mission success. However, confident battlespace awareness will only result from the appropriate fusion of technology, organization, doctrine and personnel. There is no point in generating more information about the battlespace if: a) the doctrine is not well enough developed to assist in managing the information; b) the technology cannot rapidly and securely transfer vast amounts of data over long distances; c) the organizations is so layered and compartmentalized that the right information never reaches the right people in time; and d) operator are unable to derive action-relevant knowledge for the information displayed to them. [162]

Implementation of NEOps in the CF requires vision and leadership, **and it needs them both now**.

> People – men of frailty, judgment, and human decision – must control machines. Not vice versa. Loudon Wainwright, 1965

---

[161] English, *Beware of Putting the Cart Before the Horse…,* 13.

[162] Ibid, 17.

BIBLIOGRAPHY

Airforce Technology, "RQ-4A/B Global Hawk High-Altitude, Long-Endurance, Unmanned Reconnaissance Aircraft." http://www.airforce-technology.com/projects/global/; Internet; accessed 17 February 2008.

Ackerman, Robert K. "British Warfighters Exploit Network Centricity." *Signal* (September 2003). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=147&zoneid=6; Internet; accessed 8 December 2007.

———. "Iraq War Operations Validate Hotly Debated Theories." *Signal* (July 2003). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=105&zoneid=57; Internet; accessed 13 January 2008.

———. "Afghanistan is Only the Tip of the Network-Centric Iceberg." *Signal* (April 2002). Journal on-line; available from http://www.google.com/search?sourceid=navclient&aq=t&ie=UTF-8&rlz=1T4GGLR_enCA260CA261&q=afghanistan+Is+Only+the+Tip+of+the+Network%2dCentric+Iceberg; Internet; accessed 8 December 2007.

———. "Military Crystal Ball Portends Network-Centric Supremacy." *Signal* (June 2001). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=542&zoneid=54; Internet; accessed 13 January 2008.

Ail, Irena. *Is NCW Information Sharing a Double Edged Sword? Voices from the Battlespace.* Department of Defence, Australia. Human Factors in Network-Centric Warfare Symposium. Canberra: DSTO Fernhill, 2006.

Aitken, Larry. "Network-Centric Warfare: Just Another Dot.Com?" Toronto: Canadian Forces College Advanced Military Studies Paper, 2003.

Alberts, David S. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series, 2001.

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series. 2nd (Rev.) ed. Washington, DC: National Defense University Press, 2000.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. Washington, DC: CCRP Publication Series, 2004.

Almén, Anders, Markus Anderson, Johan Lagerlöf, and Krister Pallin. *The Role of Command in Network Centric Warfare*. Swedish National Defence Research Establishment, Stockholm, Sweden. 5th International Command and Control Research and Technology Symposium, 2000.

Alston, Anthony. "Network Enabled Capability - the Concept." *Journal of Defence Science* 8, no. 3 (2003): 106-116.

Australia. Department of Defence. *Force 2020*. Canberra: National Capitol Printing, 2002.

———. Department of Defence. *NCW Roadmap*. Canberra: Defence Publishing Service, 2005.

Babcock, Sandy. *DND/CF Network Enabled Operations Working Paper*. Toronto: Defence Research and Development Canada, 2006.

———. *Policy Challenges in the Development of Integrated Network Enabled Operations in Canada*. Ottawa, ON: 10th International Command and Control Research and Technology Symposium, 2005.

———. *Policy Changes in the Development of Integrated Network Enabled Operatons in Canada*. NDHQ, Ottawa, ON: International Command and Control Research and Technology Symposium, 2005.

Barabasi, Albert-Laszlo. *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. New York: Plume (Penguin Group), 2002.

Barnett, Thomas P. "The Seven Deadly Sins of Network-Centric Warfare." *US Naval Institute Proceedings* 125, no. 1 (January 1999): 36-39.

Bashow, David L., Dwight Davies, André Viens, John Rotteau, Norman Balfe, Ray Stouffer, James Pickett, and Steve Harris. "Mission Ready: Canada's Role in the Kosovo Air Campaign." *Canadian Military Journal* 1, no. 1 (Spring 2000): 55-61.

Beckerman, Linda P. "The Non-Linear Dynamics of War." Science Applications International Corporation, 1999. Available from http://www.calresco.org/beckermn/nonlindy.htm; Internet; accessed 4 April 2008.

Bland, Douglas L. "Finding National Defence Policy in 2004." *Canadian Military Journal* 4, no. 4 (Winter 2003-2004): 3-10.

Blash, Edmund C. "Network-Centric Warfare Requires a Closer Look." *Signal* (May 2003). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=235&zoneid=62; Internet; accessed 8 December 2007.

Boland, Rita. "Keeping Track of the Troops." *Signal* (November 2007). Journal on-line; available from http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1415&zoneid=219; Internet; accessed 13 January 2008.

Canada. Department of National Defence. *1994 White Paper on Defence*. Available from http://www.forces.gc.ca/site/Minister/eng/94wpaper/white_paper_94_e.html; Internet; accessed 11 December 2008.

———. Department of National Defence. B-Ga-400-000/af-000 *Canadian Forces Aerospace Doctrine*. Ottawa: Director General Air Force Development, 2007.

———. Department of National Defence. *Canadian Forces Integrated Operating Concept*. Ottawa: DND Canada, 2005.

———. Department of National Defence. *Shaping the Future of the Canadian Forces: A Strategy for 2020*. Ottawa: DND Canada, 1999. Available from http://www.cds.forces.gc.ca/pubs/strategy2k/intro_e.asp; Interent; accessed 3 January 2008.

———. Department of National Defence. *The Aerospace Capability Framework*. Ottawa: Director General Air Force Development, 2003.

Carr, James. "Network Centric Coalitions: Pull, Pass, Or Plug-in?" Newport, RI: United States Naval War College Paper, 1999.

Caterinicchia, Dan and Matthew French. "Network-Centric Warfare: Not there Yet." *Federal Computer Week* (June 9, 2003). Journal on-line; available from http://www.fcw.com/print/9_20/news/79869-1.html; Internet; accessed 11February 2008.

Cebrowski, Arthur K. "Network-Cenric Warfare: An Emerging Military Response to the Information Age." *Military Technology* 27, no. 5 (2003): 16-22.

Cebrowski, Arthur K. and Thomas P. M. Barnett. "The American Way of War." *Proceedings* 129, no. 1 (2003): 42-44.

Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origins and Future." *US Naval Institute Proceedings* 124, no. 1 (January 1998): 28-35.

Central Intelligence Agency. *The World Fact Book*. https://www.cia.gov/library/publications/the-world-factbook; Internet; accessed 11 March 2008.

Chan, John. "Network-Centric Warfare" : Fulfilling the 3C's Litmus Test." Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2005.

Chekan, Robert. "The Future of Warfare: Clueless Coalitions?" Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2001.

Clark, Wesley K. *Waging Modern War : Bosnia, Kosovo, and the Future of Combat*. 1st ed. New York: Public Affairs, 2001.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston: Little, Brown, 2002.

Cordesman, Anthony H. *The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo*. Westport, Conn.: Praeger, 2001.

Daalder, Ivo H. and Michael E. O'Hanlon. *Winning Ugly: NATO's War to Save Kosovo*. Washington, D.C.: Brookings Institution Press, 2000.

Dahl, Erik J. "Network Centric Warfare and the Death of Operational Art." *Defence Studies* 2, no. 1 (2002): 1-24.

Deptula, David A. *Effects-Based Operations: Change in the Nature of Warfare*. Arlington, VA: Aerospace Education Foundation, 2001.

Diamanti, Stan. "Multinational Knowledge Sharing." Toronto: Canadian Forces College Command and Staff Course Paper, 2005.

English, Allan D., Richard Howard Gimblett, and Howard G. Coombs. *Human Factors Implications and Issues in Network Enabled Operations*. Toronto: Defence R&D Canada, 2006. Available at http://pubs.drdc.gc.ca/inbasket/CEBsupport.060829_1504.CR_2006_217.pdf; Internet; accessed 15 November 2007.

English, Allan D., Carol McCann, Richard Howard Gimblett, and Howard G. Coombs. *Beware of Putting the Cart before the Horse : Network Enabled Operations as a Canadian Approach to Transformation*. Toronto: Defence R&D Canada, 2005.

Fadok, David S. "John Boyd and John Warden : Air Power's Quest for Strategic Paralysis." Maxwell AFB: United States Air Force School of Advanced Airpower Studies Paper, 1995.

Fogarty, Gerard. *Progressing the Human Dimension of NCW in the ADF*. Department of Defence. Human Factors in Network-Centric Warfare Symposium. Canberra: Russell Offices, 2006.

Forgues, Pierre. "Command in a Network-Centric War." *Canadian Military Journal* (Summer 2001): 23-30.

Free, Jennifer. "Network-Centric Leadership: Why Trust is Essential." *US Naval Institute Proceedings* 131, no. 6 (June 2005): 58-60.

Garstka, John J. "Network-Centric Warfare Offers Warfighting Advantage." *Signal* (May 2003). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=234&zoneid=62; Internet; accessed 8 December 2007.

Gentry, John A. "Doomed to Fail: America's Blind Faith in Military Technology." *Parameters* 32, no. 4 (2002): 88-104.

Geraghty, Barbara A. "Will Network-Centric Warfare be the Death Knell for Allied/Coalition Operations?" Newport, RI: United States Naval War College Paper, 1999.

Giffin, Ralph E. and Darryn J. Reid. *A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy.* 8th International Command and Control Research & Technology Symposium. Ottawa: NDHQ, 2003.

———. *A Woven Web of Guesses, Canto Three: Network Centric Warfare and the Virtuous Revolution.* 8th International Command and Control Research & Technology Symposium. Ottawa: NDHQ, 2003.

———. *A Woven Web of Guesses, Canto Two: Network Centric Warfare and the Myth of Inductivism.* 8th International Command and Control Research & Technology Symposium. Ottawa: NDHQ, 2003.

Gimblett, Richard H. *Command of Coalition Operations in a Multicultural Environment: A Canadian Naval Niche? the Case Study of Operation Apollo*. Canadian Forces Leadership Institute. Command and Control Research and Technology Symposium, 2006.

Gonzales, Daniel, John Hollywood, Gina Kingston, and David Signori. *Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16*. Santa Monica, CA: RAND Corporation, 2005.

Gonzales, Daniel, John Hollywood, Jerry M. Sollinger, James McFadden, John DeJarnette, Sarah Harting, and Donald Temple. *Networked Forces in Stability Operations: 101st Airborne Division, 3/2 and 1/125 Stryker Brigades in Northern Iraq*. Santa Monica, CA: RAND Corporation, 2007.

Gosselin, Daniel and Craig Stone. "From Minister Hellyer to General Hillier: Understanding the Fundamental Differences between the Unification of the Canadian Forces and its Present Transformation." *Canadian Military Journal* 6, no. 4 (Winter 2005-2006): 5-15.

Hammond, Grant Tedrick. "From Air Power to Err Power: John Boyd and the Opponent's Situational Awareness." In *Air Power Leadership: Theory and Practice*, edited by Peter W. Gray and Sebastian Cox, 107-128. London: The Stationery Office, 2002.

———. *The Mind of War: John Boyd and American Security*. Washington: Smithsonian Institution Press, 2001.

Hammonds, Keith H, "The Strategy of the Fighter Pilot." *Fast Company* (May 2002). Journal on-line; available from http://www.fastcompany.com/magazine/59/pilot.html; Internet; accessed 15 February 2008.

Hardesty, David C. "Fix Net Centric for the Operators." *Proceedings* 129, no. 9 (2003): 68.

Hazel, G. and Derek Bopping. *Linking NCW and Coalition Interoperability: Understanding the Role of Context, Identity and Expectations*. Australian Department of Defence. Human Factors in Network-Centric Warfare Symposium. Canberra: DSTO, 2006.

Horn, Bernd. "Complexity Squared: Operating in the Future Battlepace." *Canadian Military Journal* 4, no. 3 (Autumn 2003): 7-15.

Hunt, Peter C. "Coalition Warfare: Considerations for the Air Component Commander." Maxwell AFB: United States Air Force School of Advanced Airpower Studies Paper, 1998.

Jogerst, John. "What's so Special about Special Operations? Lessons from the War in Afghanistan." *Aerospace Power Journal* (Summer, 2002). Journal on-line; available from http://www.airpower.au.af.mil/airchronicles/apj/apj02/sum02/jogerst.html; Internet; accessed 15 November 2007.

Johns, Eric. "Beware of Geeks Bearing Gifts." *Proceedings* 124, no. 4 (1998): 74-76.

Johnson, Chris. "Net-Centric Fogs Accountability." *Proceedings* 129, no. 5 (2003): 32.

Kenyon, Henry S. "Israel Targets Network Centricity." *Signal* (May 2005). Journal on-line; available from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=915&zoneid=7; Internet; accessed 13 January 2008.

Kibbe, Jennifer D. "The Rise of the Shadow Warriors." *Foreign Affairs* (March/April 2004).

Kilford, Christopher R. "On 21st Century Operational Art." Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2003.

Kiszely, John. "Learning about Counterinsurgency." *Military Review* (March-April 2007): 1-11.

Krepinevich, Andrew, F. "Cavalry to Computer; the Pattern of Military Revolutions." *National Interest* (Fall 1994).

Lamb, Michael W. "Operation Allied Force: Golden Nuggets for Future Campaigns." Maxwell AFB: United States Air Force Air War College Paper, 2002.

Lambeth, Benjamin S. *Air Power Against Terror: America's Conduct of Operation Enduring Freedom*. Santa Monica, CA: RAND Corporation, 2001.

———. *NATO's Air War for Kosovo : A Strategic and Operational Assessment*. Project AIR FORCE Series on Operation Allied Force. Vol. MR-1365. Santa Monica, CA: RAND Corporation, 2001.

Larsen, Stephen. "Coalition Multinational Network Ready in Time to Support Operations Vs. Insurgents." *Army Communicator* (Spring 2005). Journal on-line; available from http://findarticles.com/p/articles/mi_m0PAA/is_2_30/ai_n15342954; Internet; accessed 13 January 2008.

Libicki, Martin C. "Information & Nuclear RMAs Compared." *Instutute for National Strategic Studies Strategic Forum* no. 82 (July 1996).

Lim, Seng Hock. "Myth Or Reality : Network-Centric Warfare and Integrated Command and Control in the Information Age?" Toronto : Canadian Forces College Advanced Military Studies Course Paper, 2003.

Lind, William S. *Maneuver Warfare Handbook*. Westview Special Studies in Military Affairs. Boulder, Colo.: Westview Press, 1985.

Luddy, John. *The Challenge and Promise of Network-Centric Warfare*. Arlington, VA: Lexington Institute, 2005. Available from http://www.lexingtoninstitute.org/docs/521.pdf; Internet; accessed 15 November 2007.

MacMillan, Kym. *Evolving Command & Control - the Challenge for Smaller Defence Forces*. Command and Control Research and Technology Symposium. Canberra, Australia, 2004.

McCarter, Mickey. "FORCEnet at the Helm." *Military Information Technology* 12, no. 3 (9 April 2008).

McLean, J. A. "Network-Centric Warfare and the Canadian Forces." Toronto: Canadian Forces College Command and Staff Course New Horizons Paper, 2004.

McNamara, Louis E. "Riding the Information-Revolution Tiger." *Aerospace Power Journal* (Fall 2001). Journal on-line; available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj01/fal01/mcnamara.html; Internet; accessed 15 November 2007.

Michaud, Samuel M. "Lost ... but Making Good Time : The Urgent Need for a Canadian Forces C4ISR Framework." Toronto: Canadian Forces College Command and Staff Course Paper, 2004.

Middlemiss, Danford W. and Denis Stairs. "The Canadian Forces and the Doctrine of Interoperability: The Issues." *Policy Matters* 3, no. 7 (2002): 1-33.

Miller, Eric S. *Interoperability of Rules of Engagement in Multinational Maritime Operations*. Center for Naval Analyses Research. Alexandria, VA, 1995.

Mitchell, Paul. T. "A Transformation Agenda for the Canadian Forces: Full Spectrum Influence." *Canadian Military Journal* 4, no. 4 (Winter 2003-2004): 55-62.

———. "International Anarchy and Coalition Interoperability in High-Tech Environments." In *Peacekeeping Intelligence : New Players, Extended Boundaries,* edited by David Carment and Martin Rudner, 87-104. London: Routledge, 2006.

———. *Network Centric Warfare : Coalition Operations in the Age of US Military Primacy.* Adelphi Paper 385. New York: International Institute for Strategic Studies, Routledge, 2006.

———. "Small Navies and Network-Centric Warfare: Is there a Role?" *Naval War College Review* 56, no. 2 (Spring 2003): 83-99.

Modeen, Roy, John J. Garstka and Frederick P. Stein. *Network Centric Warfare*. Bedford, Mass.: Mitre Corporation (DVD), 2005.

Murdock, Paul. "Principles of War on the Network-Centric Battlefield: Mass and Economy of Force." *Parameters* (Spring 2002): 86-95.

Näsström, Staffan. "We can definitely become world champions in network-based defence." *Framsyn Magazine*, no. 6 (2003). Available from http://www.foi.se/FOI/templates/Page____3787.aspx#; Internet; accessed 2 April 2008.

North Atlantic Treaty Organization. *Allied Command Transformation - History*. Available from http://www.act.nato.int/content.asp?pageid=240; Internet; accessed 18 March 2008.

———. *Examining NATO's Transformation*. Available from http://www.nato.int/docu/review/2005/issue1/english/special.html; Internet; accessed 18 March 2008.

"Network Centric Operations Center Launches Crisis Management Program." *Market Wire,* June 2006. http://findarticles.com/p/articles/mi_pwwi/is_200606/ai_n16500806; Internet; accessed 13 January 2008.

Nissen, Thomas Elkjer. *The Taliban's Information Warfare*. Royal Danish Defence College. Copenhagen, 2007.

Pascoe, Celina. *Network Centric Warfare and the New Command and Control: An Australian Perspective*. 11th International Command and Control Research and Technology Symposium. Canberra, Australia, 2006.

Perry, Walt L. *Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Operations*. National Defence Research Institute. Santa Monica, CA: Rand, 2002.

Phillips, Charles E., T. C. Ting and Steven A. Demurjian. *Information Sharing and Security in Dynamic Coalitions*. The University of Connecticut: 2002.

Pigeau, Ross and Carol McCann. "Re-Conceptualizing Command and Control." *Canadian Military Journal* 3, no. 1 (Spring 2002): 53-64.

Randall, Bobbie L. "Sun Tzu: The Art of Network Centric Warfare." Carlisle Barracks, PA: United States Army War College Paper, 2001.

Richter, Andrew. "The Revolution in Military Affairs and its Impact on Canada: The Challenge and the Consequences," Working Paper, University of British Columbia, March 1999.

Roberts, David W. and Joseph A. Smith. "Realising the Promise of Network-Centric Warfare." *Military Technology* 27, no. 7 (2003): 8-14.

Robertson, George I. "Rebalancing NATO for a Strong Future." Remarks Given at the NATO DefenceWeek Conference, Brussels, Belgium, 31 January 2000. Available from http://www.nato.int/docu/speech/2000/s000128a.htm; Internet; accessed 16 March 2008.

Robinson, David "Network-Centric Warfare: Maneuver, Attrition and the American Way of War." Toronto: Canadian Forces College Joint Command and Staff Programme Paper, 2007.

Roman, Gregory A. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide." Department of Defense, Air Force 2025 Paper, 1996.

Rousseau, Christian. "Complexity and the Limits of Modern Battlespace Visualization." *Canadian Military Journal* (Summer 2003): 35-43.

Saunders, Clayton D. "Al Qaeda: An Example of Network-Centric Operations." Newport, RI: United States Naval War College Paper, 2002.

Scales, Jr., Robert H. "Trust, Not Technology, Sustain Coalitions." *Parameters* 28, no. 4 (1998): 4-10.

Sharpe, Joe and Allan D. English. *Network Enabled Operations : The Experiences of Senior Canadian Commanders*. Toronto: Defence R&D Canada, 2006.

Sloan, Elinor. "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities." *Canadian Military Journal* 1, no. 3 (Autumn 2000): 7-14.

Smith, Jr., Edward A. *Effects Based Operations : Applying Network Centric Warfare to Peace, Crisis, and War*. Information Age Transformation Series. Washington, DC: CCRP Publication Series, 2002.

———. "Network Centric Warfare what's the Point?" *United States Naval War College Review* LIV, no. 1 (Winter 2001): 59-75.

———. "Network Centric Warfare: Where's the Beef?" *United States Naval War College Review* (1999).

Smith, D. F. "Network Centric Warfare for the Canadian Forces." Toronto: Canadian Forces College Exercise New Horizons Paper, 2000.

Stewart, Keith G. *Mission Command: Elasticity, Equilibrium, Culture, and Intent*. Toronto: Defence R&D Canada, 2006.

Stone, Paul. "Network-Centric Warfare Key to Combat Power." *American Forces Press Service,* 15 January 2004. Available at http://www.defenselink.mil/news/newsarticle.aspx?id=27492; Internet; accessed 15 November 2007.

Stuart, II., Robert M. "Network Centric Warfare in Operation Allied Force: Future Promise Or Future Peril?" Newport, RI: United States Naval War College Paper, 2000.

Sullivan, Gordon R. and James M. Dubik. "War in the Information Age." Carlisle Barracks, PA: United States Army War College Paper, 1994.

Tan Chong Ming, James. "Embracing Network-Centric Warfare in the Information Age: Buying the Sizzle but Not the Steak?" *Pointer* 28, no. 2 (2002). Journal on-line; available from http://www.mindef.gov.sg/safti/pointer/back/journals/2002/Vol28_2/2.htm; Internet; accessed 15 December 2007.

Thomson, Michael H., and Barbara D. Adams *Network Enabled Operations : A Canadian Perspective*. Toronto: Defence R&D Canada, 2005.

Toffler, Alvin. *The Third Wave*. Toronto: Bantam, 1984.

———. *Future Shock*. Toronto: Bantam, 1971.

Toffler, Alvin and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century*. 1st ed. Boston: Little, Brown, 1993.

Toomey, Christopher J. "Army Digitization: Making it Ready for Prime Time." *Parameters* 33, no. 4 (Winter 2003/2004): 40-53.

Truswell, M. C. "The Canadian Approach to Network Centric Warfare: Data Links and Multi-Sensor Integration." Toronto: Canadian Forces College Exercise New Horizons Paper, 2004.

United Kingdom, Ministry of Defence. *Defence White Paper: Strategic Defence Review New Chapter*. London, UK: HMSO, 2002.

———. Ministry of Defence. *Network Enabled Capability - Network Enabled Capability Vs. Network Centric Warfare*. Available at http://www.mod.uk/issues/nec/nec_vs_ncw.htm; Internet; accessed 17 January 2008.

———. Ministry of Defence. *Network Enabled Capability - Working Definintion.* Available at http://www.mod.uk/issues/nec/working_definition.htm; Internet; accessed 15 March 2008.

United States. Department of the Army. *Operations. Field Manual. Vol FM 3-0.* Washington, D.C.: Headquarters, Department of the Army, 2001.

———. Department of the Air Force. *Air Force Basic Doctrine*. Afdd 1. Vol. 1. Washington, D.C.: Dept. of the Air Force, 2003.

———. Department of Defence. Joint Chiefs of Staff. *Joint Publication 3-16: Joint Doctrine for Multinational Operations*. Washington, D.C.: U.S. Government Printing Office, 1999.

———. Department of Defence. *Joint Vision 2020*. Washington, D.C.: Government Printing Office, 2000, http://www.dtic.mil/jointvision/jv2020.doc (accessed January 3, 2008).

———. Department of Defence. Office of Force Transformation. *Network Centric Operations.* Office of Force Transformation. Available from http://www.oft.osd.mil/initiatives/ncw/ncw.cfm; Internet; accessed 19 November 2007.

———. Department of Defence. Office of Force Transformation. *The Implementation of Network-Centric Warfare*. Washington, DC: Office of Force Transformation, 2005.

———. Department of Defence. *US/UK Coalition Combat Operations During Operation Iraqi Freedom.* Washington, DC: Office of Force Transformation, 2005.

———. Congress. House. Committee on Armed Services. Subcommittee on Military Readiness. *Operations in Kosovo: Problems Encountered, Lessons Learned, and Reconstitution.* Hearing before the Military Readiness Subcommittee of the Committee on Armed Services, House of Representatives, One Hundred Sixth Congress, First Session. Hearing Held October 26, 1999. Washington DC: U.S. G.P.O., 2000.

Valin, P., É Bossé, and A. Jouan. *Information Fusion Concepts for Airborne Maritime Surveillance and C2 Operations*. Valcartier, QC: Defence R&D Canada, 2006.

Van Creveld, Martin L. *Command in War*. Cambridge, Mass.: Harvard University Press, 1985.

Van Nederveen, Gilles. "Technology for the Future Leader: International Command and Control Enhancements." *Aerospace Power Journal* (Summer 2001). Journal on-line; available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj01/sum01/phisum01.html; Internet; accessed 15 November 2007.

Vego, Milan. "Net-Centric is Not Decisive." *Proceedings* 129, no. 1 (2003): 52-58.

Villa, Jiancarlo. "Network Centric Warfare: A Tool Or Hinderance to the Commander." Newport, RI: United States Naval War College Paper, 2004.

Wallace, William S. "Network-Enabled Battle Command." *Military Review* (May-June 2005): 2-5.

Walters, Eric M. "Synchronization: The U.S. Inheritance of Soviet Military Doctrine?" *Marine Corps Gazette* 78, no. 8 (1994): 23-26.

Warne, Leoni, Irena Ali, Derek Bopping, Dennis Hart, and Celina Pascoe. *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*. Edinburgh, Australia: DSTO Information Sciences Labatory, 2004.

Warne, Leoni, Derek Bopping, and Irena Ail. *NetworkER Centric Warfare: Outcomes of the Human Dimension of Future Warfighting Task*. Canberra, Australia: Department of Defence, 2006.

Wathen, Alexander M. "Joint Airspace Management and Deconfliction: A Chance to Trade in a Stovepipe for Network-Centric Warfare." *Air & Space Power Journal* (Fall 2006). Journal on-line; available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/wathen.html; Internet; accessed 15 November 2007.

———. "The Miracle of Operation Iraqi Freedom Airspace Management: How the Skies Over Iraq were Kept Safe." *Air & Space Power Journal* (Fall 2006). Journal on-line; available from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/wathen.html; Internet; accessed 15 November 2007.

Wentz, Larry K. *Lessons from Kosovo: KFOR Experience*. Washington, DC: CCRP Publication Series, 2002.

Wesensten, Nancy J., Gregory Belenky, and Thomas J. Balkin. "Cognitive Readiness and Network-Centric Operations." *Parameters* (Spring 2005): 94-105.

White, Orrick. *Network Centric Operations*. Toronto, ON: Defence R&D Canada, 2005.

Wikiquote. "Niccolo Machiavelli." Available at http://en.wikiquote.org/wiki/Niccol%C3%B2_Machiavelli; Internet; accessed 2 March 2008.

Zimm, Alan D. "Human-Centric Warfare." *Proceedings* 125, no. 5 (1999): 28-32.