DRDC Toronto No. CR-2005-162

Network Enabled Operations: A Canadian Perspective

by:

Michael H. Thomson and Barbara D. Adams

Human*systems*® Incorporated
111 Farquhar St., 2nd floor
Guelph, ON N1H 3N4

Project Manager:
Barbara D. Adams
(519) 836 5911

PWGSC Contract No. W7711-3-7893/01-TOR
Call-up No. 7893-03

On behalf of
DEPARTMENT OF NATIONAL DEFENCE

as represented by
Defence Research and Development Canada - Toronto
1133 Sheppard Avenue West
North York, Ontario, Canada
M3M 3B9

DRDC Scientific Authority:
Carol McCann
416-635-2190

May 13, 2005

Author

Carol McCann - on behalf of the Author

Michael H. Thomson
Humansystems Inc

Approved by

Carol McCann

Carol McCann

Head/Command Effectiveness & Behaviour

Approved for release by

K.M. Sutton
Chair, Document Review and Library Committee

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada

Abstract

This report outlines the concept of Network Enabled Operations (NEOps), both as a whole, and from a uniquely Canadian perspective. This report is the culmination of an extensive literature survey, and of two think tanks convened on 1 March 2005 and 30 March 2005 with Canadian subject matter experts (SMEs), both military and non-military, who are currently working to define and drive forward the Canadian concept of NEOps.

Results showed that the Canadian conception of NEOps must be interpreted in light of the new security environment and what role the Canadian Forces (CF) is likely to play. As such, NEOps must be understood within emerging concepts in defence policy, such as the JIMP framework (joint, interagency, multinational, public) and the 3-D (defence, diplomacy, development) approach to international affairs. SMEs questioned how the stated benefits of NEOps would actually manifest themselves in operations, such as warfighting, peacekeeping, humanitarian, nation building, etc., without fully appreciating the cognitive and socialization processes that underlie them. Moreover, SMEs pointed to a number of challenges that require greater attention prior to full implementation of NEOps. These include: trust; ensuring common mental models, cognitive processes, and understanding; information overload; authority (including common intent) and accountability; attempts to implement NEOps universally, across the three arms of the CF; CF structure and culture (e.g., distributed decision making and information sharing); education and training; and affordability.

Résumé

Ce rapport décrit le concept des opérations réseaucentriques (NEOps), d'une manière générale et du point de vue canadien seulement. Ce rapport constitue l'aboutissement d'une étude approfondie des ouvrages portant sur le sujet et de deux exercices de réflexion qui se sont tenus le 1er et le 30 mars 2005. Les groupes de réflexion étaient composés d'experts en la matière (EM) canadiens, militaires et civils, qui s'occupent actuellement de définir et de faire progresser le concept canadien des opérations réseaucentriques.

Il en découle que la conception canadienne des NEOps doit être interprétée à la lumière du nouveau contexte de sécurité et du rôle qui devrait être attribué aux Forces canadiennes (FC). Ainsi, il faut envisager les NEOps dans des concepts nouveaux de la politique de défense, par exemple, le cadre JIMP (interarmées, inter-institutions, multinational et public) et l'approche des trois D (défense, diplomatie et développement) à l'égard des affaires internationales. Les EM se sont interrogés sur la manière dont les avantages mentionnés des NEOps se manifesteront concrètement dans les opérations, notamment au combat, dans le cadre du maintien de paix, de l'aide humanitaire, de la construction de nation, etc., sans parfaitement comprendre les processus cognitifs et de socialisation qui les sous-tendent. En outre, les EM ont soulevé un certain nombre de défis dont il faudrait se préoccuper davantage avant de passer à la mise en œuvre complète des NEOps. Il s'agit notamment de la confiance, de la compréhension, des processus cognitifs et des modèles mentaux communs, d'une surdose d'information, du pouvoir (y compris l'intention commune) et de la responsabilisation, des tentatives visant à appliquer les NEOps universellement dans les trois armes des FC, de la structure et de la culture des FC (p. ex. le partage du pouvoir de décision et l'échange d'information), de l'éducation et l'instruction et, enfin, de la capacité financière.

Executive Summary

Network Centric Warfare (NCW) is essentially a concept of operations that seeks to maximize advances in information technology in military operations by linking all sensors, platforms, and decision makers through an integrated system of robust networks, thereby lifting the fog and friction of war. Fundamental to the theory is the belief that power in the "Information Age" derives from accessing and sharing information at increased rates of speed. Adopting a NCW approach to warfighting, it is argued, will lead to information and decision superiority over potential opponents.

This report outlines the concept of Network Enabled Operations (NEOps), both as a whole, and from a uniquely Canadian perspective. This report is the culmination of an extensive literature survey, and of two think tanks convened on 1 March 2005 and 30 March 2005 with Canadian subject matter experts (SMEs), both military and non-military, who are currently working to define and drive forward the Canadian concept of NEOps.

Results of these efforts suggest that the current conception of NEOps has a number of hidden assumptions that derive, on the one hand, from simply extending the US conception of NCW to fit a uniquely Canadian perspective and, on the other hand, from a lack of research regarding the potential benefits and challenges. For example, the Canadian conception of NEOps must be interpreted in light of the new security environment and what role the Canadian Forces (CF) will likely play. Emerging concepts in defence policy, such as JIMP (joint, interagency, multinational, public) and the 3-D (defence, diplomacy, development) approach to international affairs, will inform this role and need to be significant in delineating the concept of NEOps.

SMEs questioned how the stated benefits of NEOps would actually manifest themselves in operations, such as warfighting, peacekeeping, humanitarian, nation building, etc., without fully appreciating the cognitive and socialization processes that underlie them. SMEs also mentioned a number of challenges that will arise from network enabled operations. These include the following: trust; ensuring common mental models, cognitive processes, and understanding; information overload; authority (including common intent) and accountability; attempts to implement NEOps universally (across the three arms of the CF); CF structure and culture (e.g., distributed decision making and information sharing); education and training; and affordability.

Sommaire

Les opérations réseaucentriques (NCW) sont avant tout un concept d'opérations visant à maximiser les progrès réalisés au titre de la technologie de l'information dans le cadre des opérations militaires. Les opérations réseaucentriques consistent à relier tous les capteurs, les plates-formes et les décideurs au moyen d'un système intégré constitué de réseaux robustes, ce qui permet ainsi de venir à bout du bouleversement provoqué par la guerre. La théorie se fonde principalement sur la croyance que la puissance de « l'ère de l'information » découle de l'accès à l'information et du partage de celle-ci à des vitesses plus rapides. On prétend que l'adoption d'une approche NCW au combat assurera une maîtrise de l'information et une supériorité décisionnelle par rapport aux adversaires éventuels.

Ce rapport décrit le concept des opérations réseaucentriques (NEOps), d'une manière générale et du point de vue canadien seulement. Ce rapport constitue l'aboutissement d'une étude approfondie des ouvrages portant sur le sujet et de deux exercices de réflexion qui se sont tenus le 1er et le 30 mars 2005. Les groupes de réflexion étaient composés d'experts en la matière (EM) canadiens, militaires et civils, qui s'occupent actuellement de définir et de faire progresser le concept canadien des opérations réseaucentriques.

Il en découle que la conception canadienne des NEOps doit être interprétée à la lumière du nouveau contexte de sécurité et du rôle qui devrait être attribué aux Forces canadiennes (FC). Ainsi, il faut envisager les NEOps dans des concepts nouveaux de la politique de défense, par exemple, le cadre JIMP (interarmées, inter-institutions, multinational et public) et l'approche des trois D (défense, diplomatie et développement) à l'égard des affaires internationales. Les EM se sont interrogés sur la manière dont les avantages mentionnés des NEOps se manifesteront concrètement dans les opérations, notamment au combat, dans le cadre du maintien de paix, de l'aide humanitaire, de la construction de nation, etc., sans parfaitement comprendre les processus cognitifs et de socialisation qui les sous-tendent. En outre, les EM ont soulevé un certain nombre de défis dont il faudrait se préoccuper davantage avant de passer à la mise en œuvre complète des NEOps. Il s'agit notamment de la confiance, de la compréhension, des processus cognitifs et des modèles mentaux communs, d'une surdose d'information, du pouvoir (y compris l'intention commune) et de la responsabilisation, des tentatives visant à appliquer les NEOps universellement dans les trois armes des FC, de la structure et de la culture des FC (p. ex. le partage du pouvoir de décision et l'échange d'information), de l'éducation et l'instruction et, enfin, de la capacité financière.

Table of Contents

This page intentionally left blank.

1. Purpose of this Report

This report outlines the concept of Network Enabled Operations (NEOps), both as a whole, and from a uniquely Canadian perspective. It is the culmination of an extensive literature survey, and of two think tanks convened on 1 March 2005 and 30 March 2005 with Canadian subject matter experts (SMEs), both military and non-military, who are currently working to define and drive forward the Canadian concept of NEOps. The following outlines the broad concept of Network Centric Warfare (NCW) and then considers the unique Canadian perspective on this topic before considering the benefits and the challenges of NEOps. To conclude, we outline the Canadian implementation efforts.

This page intentionally left blank.

2. Introduction

Network Centric Warfare (NCW) is essentially a concept of operations that seeks to maximize advances in information technology in military operations by linking all sensors, platforms, and decision makers through an integrated system of robust networks, thereby lifting the fog and friction of war. Fundamental to the theory is the belief that power in the "Information Age" derives from accessing and sharing information at increased rates of speed. Adopting a NCW approach to warfighting, it is argued, will lead to information and decision superiority over potential opponents. As the Deputy Director of the US Office of Transformation Terry Pudas (2004) reported, NCW is ultimately about translating an "information advantage into a decisive warfighting advantage" (*Network Centric Warfare and US Transformation*, 2004). Proponents of NCW hold that greater information sharing and collaboration will enhance the quality of information and shared situation awareness of the battlespace, increase the speed of command, lead to self-synchronized activities with dispersed amassed forces, and increase combat power and mission effectiveness (Albert & Hayes, 2003; Report from the US Office of Transformation, *The Implementation of Network Centric Warfare*, 2005). In this sense, NCW can be understood as a means to an end.

Though the roots of NCW derive from the United States, it is not limited to the United States. Other countries, such as Australia, United Kingdom, Sweden, New Zealand, and Canada, all recognize the importance of NCW as a "central concept" for shaping military transformation, and yet all have unique definitions and give varying emphasis to the key components of NCW. For example, the UK refers to NCW as Network Enabled Capabilities (NEC), and, according to the UK Ministry of Defence, distinguishes it from the theory of NCW in a number of ways. NEC does not place "the network at the centre of capability in the same doctrinal way as NCW". Captain Dick Hemsley (2004), for example, describes NEC as "commander-centric" rather than "network centric". Some writers have suggested that while the US has focused its efforts on warfighting at the tactical and operational levels, other countries (such as the UK and Canada) have not restricted the application of NEOps to mere "theatre level combat operations" (Kennedy, 2004).

The Australian Defence Force (ADF) describes NCW similarly to the US and Britain. In the Capstone Series ADDP – D.3.1, NCW is described as "a simple concept that involves the linkage of engagement systems to sensors through networks and the sharing of information between force elements". In its infancy, attention focused on the information network and networking. However, the ADF conception emphasizes that information is only useful if it contributes to the overall effectiveness of the human actors using the network. The human dimensions – for example, professional mastery and mission command – are fundamental in the Australian conception of NCW. Networks enable warfighting effectiveness, but these descriptions of NCW assert that in no way should the network replace the skill, intuition, and willpower of ADF's people (Capstone Series ADDP – D.3.1, 2004). For the ADF, NCW merely enhances the six warfighting functions of Multidimensional Manoeuvre, which include information superiority and support, force application, force protection, force generation and sustainment, force deployment, and command and control (Capstone Series ADDP – D.3.1, 2004). At the core of the ADF conception is the human dimension, reinforced by "high standards of training, education, doctrine, organization, and leadership" (Capstone Series ADDP – D.3.1, 2004).

Despite these differences in emphasis, however, all countries hope to advance the “effectiveness and efficiency” of their militaries through robust networking. Moreover, there is a general expectation among these national accounts that robust networking will foster shared situation awareness, increased tempo of operations, self-synchronization, and mission effectiveness. There is, therefore, general convergence regarding the adoption of the principles and tenets of NCW among allied nations. As SMEs in our think tanks suggested, however, simply importing the NCW concept into the Canadian context may present several problems. It is, therefore, important to turn our attention to the Canadian conception of NEOps.

3. The Canadian Conception of NEOps

Canada's developing NEOps concept is articulated in the capstone document, the *CF Strategic Operating Concept* (*SOC*)[1]. NEOps, alongside Effect-Based Approach (EBA), make up the "integrating concepts" in Canadian Forces' *Strategic Operating Concept*. Accordingly, these concepts "describe how various broad core operational activities relate and will be integrated into a cohesive operating system" (*SOC*, 2004, p.13). Documented in the *CF Strategic Operating Concept* (2004), NEOps is described 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".

The emerging Canadian concept of NEOps is also likely to be closely linked with other Canadian initiatives. For example, the *CF Strategic Operating Concept* stresses the importance of fostering successful interactions among people through policy initiatives like the "3-D" approach to international security and affairs. In this concept, the CF function combines Defence, Diplomacy, and Development, and works closely with the Department of Foreign Affairs and the Canadian International Development Agency. The broad notion of 3-D security emphasizes that the CF will be participating to varying degrees with all elements of governmental departments in international efforts. In other words, the soldier will be simultaneously collaborating with the diplomat and the developer in the 3-D security environment, or the "three block war". The military's role will change depending on the "block". Moreover, 3-D security also underscores the Canadian perspective that the CF has a moral responsibility to protect and maintain security throughout the world. As such, Canada believes that there will be contexts where it has a humanitarian duty to intervene in a sovereign state to foster stability and safety for those citizens, and promote the good of humanity over the good of the tribe. The CF will be required to act on behalf of Canada to promote these good deeds around the world. Ultimately, it is believed that NEOps will offer the means to improve the ways that people throughout the system (i.e., the soldier, the diplomat, and the developer) work together, promoting information sharing and greater cooperation in a variety of defence, diplomatic and developmental contexts.

The development of the NEOps concept will also be influenced by the focus on the JIMP[2] (joint, intra-agency, multinational and public) framework as articulated in Canada's National Security Policy. This focus on the JIMP context stems from the recognition that military operations (and military business) increasingly require coordinated joint responses, cooperation with other agencies, and often occur at the multinational level. The Canadian joint services include not only Army, Navy, Air Force, but also the emergence of the Special Forces, which will require greater articulation around their purpose and role in NEOps. The focus on the public aspect recognizes that public support of military efforts is of increasing importance. Beyond this, however, SMEs noted that the full implications of this new security environment have yet to be ascertained.

---

[1] This document is to be replaced by the Integrated Operating Concept (IOC). The Defence Policy Statement, similar to the Quadrennial Defense Review (QDR) in the US, and the basis for the IOC, will also be released in the coming weeks.

[2] The JIMP framework appears implicitly rather than explicitly in the new IOC.

Like other conceptions of networked operations, the Canadian approach recognizes the four basic tenets described in *Power to the Edge* (Albert and Hayes, 2003). These are:

- A robustly networked force improves information sharing;
- Information sharing and collaboration enhance the quality of information and shared situational awareness;
- Shared situational awareness enables self-synchronization; and
- These, in turn, dramatically increase mission effectiveness.

Exactly how influential these tenets should be in defining the Canadian concept of NEOps, however, seemed to differ within the two focus groups that we conducted. On one hand, one group (comprised primarily of military personnel, but with some academic representation) seemed to mostly endorse Canada basing its conception of NEOps on the US view. This group argued that these tenets should not be stated so deterministically or absolutely, for fear that they may take on an "assumed reality". Another group member argued that the tenets did not seem to specify exactly how networking was likely to lead to the proposed benefits, and argued that substituting the network concept with words like "training" or "familiarity", for example, would lead to similar outcomes. This group also argued that although increasingly networked operations may lead to some benefits, it is important not to view NEOps as a panacea. Despite these reservations, however, this group did not emphasize the need for Canada's concept of NEOps to be wholly different from the prevailing US concept.

Another focus group (comprised of academics and some military personnel) was more insistent about the need for Canada to develop its own conception of NEOps, and argued that this was necessary because of the unique nature of Canada's capabilities and goals in military operations. For example, some SMEs felt that the US tenets are primarily focused on combat power rather than on the kind of operations that Canada is most likely to undertake (e.g. peacekeeping). One SME believed that NEOps included gathering information and sustaining it outside of combat, i.e., "NEOps across the entire spectrum of military business". For example, he agreed with the implied logic of the tenets, but questioned their application to UN Humanitarian missions. Participants also noted that differences in assets and resources also underlie the need for Canada's concept of NEOps to be distinct. This has also been noted in the Canadian working paper, *Network Enabled Operations: DND/CF Responding to the New Security Environment*, (2004), which argues that national differences regarding NEOps (NEC, NCW) are based partly on the resources nations have available to them, as well as the level of involvement and the role that each decides to assume. Not surprisingly, then, Canada's view of NEOps would not always put Canada at the centre of the network, particularly in warfighting operations, but would require "plug and play" capabilities that are interoperable with those of US or other coalition partners.

The Canadian conception of NEOps also switches the emphasis from technology and networks to the human elements. As underscored by the Canadian Parliamentary Secretary to the Minister of National Defence, Keith Martin, NEOps is the practical "use [of] networks to build effective partnerships" that are more central to the debate than technology itself (Martin, 2004). Canada's conception places more emphasis on the human elements and the need for cooperation and collaboration than the original US version of NCW. As one SME suggested, the real "power" of

networks is the potential to form groups. As such, the Canadian emphasis includes collaboration and shared knowledge as well as the mechanisms that enable these capabilities.

A critical theme running through our focus groups was that whatever definition of NEOps Canada adopts, it should be consistent with Canada's military culture and ethos. Therefore, Canada should be careful not to simply adopt a conceptual structure from the US that may not be consistent with the nuances and priorities of the Canadian military. Moreover, some participants were also emphatic that the concept of NEOps requires more than simply overlaying a networking capability onto an existing underlying organizational (or command and control) structure. In short, some participants felt that adopting NEOps in Canada would require a core paradigmatic change in the military as an organization, and the reworking of its relationships with all other members of the network. For example, enabling network capability within the JIMP context requires the recognition that networks extend beyond the mere use of information technology and into the realm of social networks. There is a transformation in operational procedure from the "need to know" model to the "need to share" and collaborate model, which triggers new risks. These risks, of course, are not optional. SMEs explained that, for NEOps to be successful, these risks have to be undertaken, and this will require a substantial reconsideration of the CF enculturation and socialization process.

4. Benefits of NEOps

In our focus groups, we enumerated the benefits of NCW (NEOps) proposed in the literature, and elicited discussion around these asserted benefits, and their applicability to the Canadian view of NEOps. These discussions also elaborated on the definitions and implicit assumptions of each benefit, and helped to refine how these benefits can be best explored in the future.

Shared situation awareness can be understood as the ability to regularly translate information and knowledge into a common understanding for those involved in military operations. The belief is that "all involved have the capability to share and access needed information" (Fewell & Hazen, 2003). It is also believed that shared situation awareness will lead to a common operating picture, or COP (*Office of Force Transformation*, 2005). One group member held that shared cultural norms are a hidden assumption of shared situation awareness, which may lead to challenges. SMEs reported that though a COP can be easily conveyed visually, it will be important to understand how individuals "make sense" of this, i.e., select, interpret, incorporate information into existing mental models, etc., at varying "levels of analysis" (i.e., individual, small team, and system) to fully take advantage of this characteristic. One SME said exploring how individuals chunk and categorize information was a means for further understanding these processes. Moreover, participants also noted an incorrect implicit assumption in the second and third tenet, namely that shared information would entail shared understanding.

SMEs also thought that further knowledge regarding social processes would contribute to helping the military know how to achieve shared situation awareness. For example, investigation of how group processes, such as social norm formation in a military context, implicate shared situation awareness might be one possible avenue of exploration. As the JIMP model gains broader application in operations, it was suggested that the type of team (e.g., joint, multinational) will compound the complexity of ensuring shared situation awareness. For example, one SME explained that a Carrier Battle Group can achieve shared situation awareness easily because it consists of one entity, one organization. In essence, it was a "closed system". However, other environments, such as the army, are open systems. Therefore, ensuring shared situation awareness requires understanding of the individual within his or her respective culture and military culture, with its particular education.

Moreover, achieving shared situation awareness will require knowledge of the individual's position in the operation because commander's intent will be different for different people, creating a variety of operational pictures. It was pointed out that, ultimately, "there are multiple realities", and "how we understand, determines what we see". Thus, understanding how multiple realities emerge to reflect one shared reality will be invaluable for helping to achieve shared situation awareness.

Interoperability, simply put, is "the ability to work together" (Alberts & Hayes, 2003). As one SME pointed out, this definition suggests that interoperability is a prerequisite for NEOps, and therefore should not be considered as a benefit or end state. The TTCP[3] technical report underscores its multifaceted nature, i.e., interoperability refers to logistical interoperability (physical domain),

[3] TTCP Maritime-Systems-Group Action Group 1 (MAR AG-1).

information flow ("between platforms and units"), and information usage ("ease with which information passes into the cognitive domain to build knowledge"). Interoperability, as Warne et al (2004) explain, "goes beyond integrated infrastructure and encompasses the social psychological bases of interpersonal and inter-group cooperation, fundamental to the ability of individuals to work closely together as a group". In any operation, this will be a challenge that will depend on the willingness of players to cooperate. As one SME stated, the reality of nets is that they are closed, and furthermore, there are tight nets, which privilege some people, and loose nets, which discriminate to a lesser degree.

Nevertheless, as one SME said, interoperability can integrate the activities of individuals and small teams, who are "more noted by their differences than similarities". Thus, they can achieve more together than they can independently. In this sense, interoperability has the potential for complimentary activity. Interoperability is most salient in situations where two forces overlap as a response to critical needs. As such, interoperability does not mean that forces need to share doctrine and culture to work.

According to Fewell & Hazen (2003), speed of command can be understood as the "time required to complete one full cycle of Boyd's observe-orient-decide-act (OODA) decision loop". Speed of command will instantiate compressed decision making cycles. It will likely be a consequence of increased distributed decision making and information sharing among a dispersed force. As such, friendly forces should ideally be able to disrupt an enemy's decision loop by making quicker command decisions and frustrating an enemy's.

Though speed of command is desirable, one SME said that it should not be an objective in all cases. Rather, in some circumstances it is better to "let political dynamics play out first". In other words, "quick could be a bad thing". Another group member concurred explaining that speed of command is desirable when it is "unidirectional". However, it becomes more complicated when decision making is "multidimensional". In such cases, a "lag" makes it more likely that commanders will be able to distinguish those things that are relevant from those things that are spurious because the world is changing for many reasons outside one's own effects. This underscores the need to distinguish between how to judge, decide and when to act. As one SME suggested, NEOps might contribute to commanders' ability to judge quickly and effectively, thereby allowing action to be deferred.

One group member noted that speed perhaps should be understood as "response", and that command is ultimately the flexibility around Commander's Intent. As the operation unfolds, there will be shifts occurring. Speed of command allows participants to adjust and modify their position more quickly, thereby leading to more robust Commander's Intent. A hidden assumption to speed of command, therefore, is that the locus of command can rapidly shift, i.e., "command is allowed to fluctuate" based on who has the most relevant knowledge for the given situation. And this knowledge can be more than mere core knowledge. It will also include support knowledge. In response to this interpretation, however, one SME noted that this notion is possible in the Army, whereas it is difficult in the Air Force and Navy. For example, following 9/11, within the Air Force, the decision to shoot down a passenger airline emerged. As one SME explained, in an NEOps paradigm, a decision such as this would necessarily remain in the hands of the commander, because he is ultimately responsible for all activities and some decisions are simply "too important". In particular, there was a concern among SMEs that speed of command would lead to a faster means to make old mistakes.

Force agility is based on the following six attributes outlined by Alberts and Hayes (2003, p. 128): robustness, resilience, responsiveness, flexibility, innovation, and adaptation.[4] Force agility will be important because in a NEOps environment, there will be no way of determining, a priori, who will be on the team or who will be required to participate. SMEs wondered whether innovation should be simply subsumed under force agility. Instead, it was suggested that it might be a pre-condition to NEOps in order to do it properly. One SME suggested that a hidden assumption of force agility was the competing tensions (such as mission accomplishment, force protection, etc.), and these needed to be reconciled. Another hidden assumption of force agility was that the commander would be in a better position to shift and deploy the force elements, viz., commanders will be able to move force elements around where needed at the appropriate time. Of course, this will be dependent on greater situation awareness of the battlespace.

Fewell and Hazen (2003) describe self-synchronization as the ability of individual unit commanders to synchronize their unit's individual efforts in order to mutually support other commander's units, and accomplish the overall shared goal. Knowing the theatre commander's "promulgated common intent" as well as being able to predict the reactions of other unit commanders allows each individual commander to decide independently how his or her unit will deploy (Fewell, M. & Hazen, M., 2003). As described in *The Implementation of NCW* (2005), it is the ability of "low-level forces to operate nearly autonomously and to re-task themselves through exploitation of shared awareness and the commander's intent". According to SMEs, self-synchronization provides a bit of unpredictability to the adversary, increasing "their" fog of war.

SMEs discussed in depth the notion of self-synchronization deriving from shared situation awareness. On the one hand, optimists concerning NEOps described, by analogy, the high level of connectivity between "nodes" on the network. It was argued that like crickets' synchronization in song, when forces have a COP (common operating picture), units will be able to "see" what happens to other units, allowing them to move into a supportive position. Of course, the very notion of a COP was challenged. Unlike crickets, which share the same logic, complexity arises when actors from various military environments, or from other environments (such as the well intentioned public), with broad, multifarious agendas and different assumptions and objectives enter the fold. Under these circumstances, simply ensuring connectivity will not ensure common understanding and common goals.

One SME commented that self-synchronization might work in the Army, at lower levels, but would unlikely work, for example, in a Battle Fleet. It was also suggested that the notion of self-synchronization was based on a "sensor to shooter model". This might be too restrictive, given that Canadian operations adopt a 3-D approach, and function within the JIMP framework. From the Canadian perspective, self-synchronization needs to incorporate all of the players in the operation, including soldiers as well as diplomats and developers (e.g., NGOs). Thus, self-synchronization needs to be interpreted more broadly to include the multifaceted nature of Canadian military operations, such as peacekeeping, nation building operations, humanitarian efforts, etc. Moreover, self-synchronization requires a delineation regarding how much autonomy will be permitted. In other words, there is an assumption underlying NEOps with respect to flexibility – what can be bound and what can be free.

[4] For a detailed description of the six attributes, please see *Power to the Edge* (Alberts & Hayes, 2003) pages 128 – 159.

Reachback "refers to the ability of commanders and other force elements to access valuable resources relevant to military operations (e.g. databank, intelligence, imagery) despite being physically far removed from the information source" (Warne et al., 2004, p. 22). One group member said that reachback provided an opportunity to elicit knowledge on an as-needed basis, which allowed soldiers to go beyond previous boundaries. Of course, one potential challenge will be the requirement to take ownership for that need. Another potential challenge for Canada is the fact that logistics support of the CF is not agile. Military operations often amount to rationing scarce resources. It might therefore be difficult for Canada to take advantage of this capability in this sense. However, SMEs pointed out that reachback also meant soldiers could "leap the chain", and establish links in a diagonal manner, and thus "plot unique trajectories". The ability to "reachout" on a multitude of networks meant that individuals could discover all of the competing strategic obligations for the operation. One SME suggested that reachback will be enhanced when processes, such as conditioning, processing, and understanding information on the networks, are further understood. This includes knowledge of the conditions of reachback, i.e., the social context (norms, trust, communities of practice) in which it can occur.

Reachforward, an extremely beneficial capacity means "the emerging ability of commanders, far removed from theatre, to use the same infrastructure to manage tactical events that take place in theatre in real time" (Warne et al., 2004, p. 23). SMEs believed that this was very powerful, however, warned that it could foster micromanagement.

Effect-based operations (EBO) are efforts "to leverage the soft and hard power assets of a nation or coalition, including its political, economic, technological and social resources, in order to achieve a set of desired outcomes" (*CF SOC*, 2005). It seeks to establish influence over the mind of an adversary to affect his will to act while, at the same time, keeping collateral damage as well as combatant and non-combatant casualties to a minimum" (*CF SOC*, 2005) – thus winning on both the physical and moral planes. As SMEs explained, EBO, essentially, begins with the anticipated outcomes and traces back in order to determine what to do.

However, there appeared to be little consensus around what, exactly, EBO meant in a Canadian context. For example, one SME explained that EBO derived from a US Air Force model, which essentially meant "getting folks to do what they wanted them to do". Another stated that Canada could not implement EBO because it was a "US paradigm", and that any definition or implementation of EBO should reflect our national culture. One group member suggested that EBO was equivalent to the Canadian 3-D concept of operations. Another went so far to suggest that there was no theory underlying the Canadian concept of EBO. He continued to explain that Canadian operations are better understood as "outcome based", and the consequences are more at the macro level where they stand out from the background, the status quo. Another SME replied that EBO was a "confirmation of outcomes". For Canada, this means "doing good deeds" and, therefore, this is why the 3-D concept is so important. Thus, the Canadian concept of EBO needs to incorporate the kinds of missions in which Canada participates. As one SME explained, EBO largely revolves around ammunitions, which is contrary to missions that involve nation building. In the 3-D approach to international security and affairs, there will be many effects that are interconnected and multiple people will be defining what those effects, or outcomes, are.

Information superiority can be understood as the ability to generate and share relevant and accurate information across a well-networked and interoperable force on a timely basis while denying potential adversaries the same ability. According to one group member, it should not amount to

superiority in isolation. One SME suggested that the real emphasis of NEOps and information superiority was knowledge. Thus, “network enabled” did not mean “labouring on information fusion”, but rather successfully translating information to knowledge and then into sound judgement. Information superiority has to be understood as more than simply related to resources. It needs to accommodate the purposes and processes as well as the tools. SMEs believed that generating social norms that could produce the necessary capacity for judgement was important.

The ultimate outcome of NEOps is increased mission effectiveness, which can be understood as quicker submission of the enemy with decreased lethality and destruction. Of course, within a peacekeeping operation, this would need to be defined differently. For example, one SME noted that mission effectiveness might be understood as “improving quality of life”. Thus, the political and social outcomes are as important as military outcomes.

4.1 Summary

One group member pointed out that NEOps might not promote benefits at all levels of operations. He continued that clarity, confidence, and assurance around NEOps were huge and largely untested assumptions. The general sentiment among SMEs was that, in their current state, the tenets are relatively incomplete and likely to be easy to disprove. As such, for the future, it will be necessary to exact more precise definitions and to work to understand the potential benefits of NEOps under rigorous and well-defined conditions. Moreover, emerging concepts, such as the JIMP, 3-D, and the role of Special Forces, needed to be integrated into any NEOps definition to ensure the benefits. It was also argued that the real potential of NEOps was that it allowed Canada to plug and play in warfighting operations and enhance its international efforts under the 3-D security approach. Therefore, one focus group participant concluded that it will be important to take a “devil’s advocate” approach to assessing the purported benefits of NEOps, and to ask, “How can this all go wrong?”

5. Challenges of NEOps

SMEs identified a number of potential challenges for NEOps. Many of these challenges derive from purely human factors. For example, trust was considered a major issue. SMEs explained that Canada shares more information with the United States than with NATO, which is in part based on a similar geography, education, and training. Moreover, multinational operations involve many nations, some more friendly and trustworthy than others. There was concern among SMEs regarding the development of swift teams (i.e., ad-hoc teams) in an environment of low trust. One group member believed that Canada was at an advantage in fostering trust because the CF was smaller and its ethical standards were uniformly higher than many other nations. For example, Canada maintains a willingness to uphold these standards through its justice system (e.g., the Somalia Inquiry).

But trust was not only a concern between nations. It also meant building trust amongst the different governmental departments and agencies within Canada. The CF needs to expand its network to include capabilities that it does not have while maintaining a stable structure. As such, boundaries need to be expanded and retracted as required. One SME suggested that officers should be moved into other governmental departments for durations of a couple of years as an effort to integrate and establish relationships. Thus, trust in a NEOps environment might be fostered by reputation. Moreover, in an environment that is rapidly changing, SMEs suggested trust could be fostered by commitment to a shared goal or purpose. In any case, group members' discussion of trust underscored its multidimensional nature, and the need to understand it further. Some questions pertaining to trust that are immediately relevant include how do individuals trust themselves to make good decisions based on the information that they receive? How do individuals trust the information that they are receiving? How do organizations begin to trust what members or non-members will do with the information that they have access to, given the switch from a need-to-know to a need-to-share culture? Thus, there are many areas of trust to consider as military forces move to a networked environment.

Another key challenge in NEOps is the often implicit assumption that simply providing people with access to the same information will enable common understanding. Again, the issue of how "common intent" can actually be promoted among network players, often from diverse backgrounds and cultures (both national and organizational) represents a major challenge for the future. As such, there will need to be consideration around control mechanisms. For example, what is the role of doctrine and mission command?

Other challenges included information overload. SMEs asked how people would respond to the huge amounts of information to which they will have access and filter. As one group member said, the only scarce resource in the 21st century was "attention". It was feared that in an effort to minimize the vast amounts of information, people may focus on the familiar and ignore what is perhaps different but nevertheless relevant. People also may reinforce their beliefs and hunches, and fail to interpret what the information is telling them. Ironically, a more ubiquitous, self-imposed fog could engulf the user. To prevent this, people within the network at all levels would need to be skilled at deciphering relevant and accurate information on a timely basis. Closely related to this is the challenge of recognizing information presented on the network and what this

information represents. For example, visual displays and sound displays (such as colour coded alarms, sound amplitude and frequency for urgency) will need to be consistent for users, both nationally and internationally.

One SME believed that understanding individual mental models and cognitive processes was vital because, he believed, the limitations of human cognition will be the major limit of NEOps. For example, how do individuals confirm or disconfirm information such that it reflects a change in mental models? What is the range of this capability and how does time impact this? It would also be beneficial to understand the ways in which people "learn to learn". There was an agreement among group members that one of the challenges of NEOps is that people often process information based on their cultural background. This is a potential problem because CF is increasingly diverse, yet collaboration within the NEOps context may require at least some conformity in mental processes. Other SMEs noted that the key to reducing information overload in the future will revolve around how information within operations is managed. The NEOps context will require robust tools for tagging and searching, as a way of managing the sheer volume of information. Moreover, the potential for information overload also varies somewhat in amongst arms. In the Navy, for example, SMEs argued that there are a limited amount of "blips", whereas in the Army, every single shooter must be tagged. This suggests that deliberate decisions will need to be made about what aspects of the common operating picture are the most critical.

Moreover, working within a NEOps paradigm also raises issues of authority and accountability. It will be critical to explore both the pragmatic and ethical implications of decentralizing authority and the redefined the role of leaders. SMEs also raised concerns about the potential for micromanagement by commanders as a result of their having both access to more information about subordinates and the ability to "reachforward" to a greater extent than was previously possible. In addition, the need for increased accountability may oblige people to provide more information than previously. As such, sourcing low diagnostic information or attempting to integrate more than needed may lead to a degradation of the quality of judgements. This challenge will likely be compounded by time pressure.

SMEs also noted that another potential challenge to NEOps will be attempting to implement it universally within the CF. In other words, SMEs argued that a "one size fits all" approach would undermine the particular nuances across environments in the CF. One SME believed that the impact will be more dramatic on the Army than the Navy or Air Force, explaining that the interaction of the soldier on the ground with another member of the land force is very different from the interactions in a maritime or air context. Some of the literature tends to support this perspective. For example, the notion of joint interoperability has been questioned because of the belief that air, sea, and land combine to achieve a "'unified' battlespace" (McMaster, 2003). But as McMaster states, "the factors that preserve uncertainty in war despite technological superiority are mainly land-based". He continues "because people live there, land is where political, social and cultural factors interact with complex geography to generate uncertainties that can alter the best-laid plans." Furthermore, a "one size fits all" approach will not be appropriate to the variety of operations (e.g., 3-D) in which the CF will participate. Each operation will require a unique application of the network to satisfy various outcomes.

Finally, NEOps will be a challenge to the organizational culture and structure. According to MacNulty (cited in Warne et al., 2004), some changes to organizational culture will be reflected in command plans, the planning process, competition, attitude to change and risk, decision making

planning cycle, and resourcing systems. Currently, there appears a lack of scientific investigation regarding NEOps and its impact on and interaction with CF culture. As outlined in the *Tiger Team Transformation Analysis,* there is some activity regarding the issue of trust, but no activity with respect to how CF members will handle uncertainty and how CF members will understand others ("others" being those people who make up JIMP) in relation to military affairs.

For example, NEOps demands information sharing as opposed to the more current practice of information hoarding. The handling of information, therefore, will require a culture shift. All network users will be responsible for accessing and sharing information in order to make decisions that will contribute to the overall achievement of the commander's intent (*CF Strategic Operating Concept,* 2004). However, information sharing will not be completely transparent. How information sharing occurs will be contingent upon how "open" or "closed" the networks are. In some cases the relationships may be "hidden" like the relationship the military may conceivably have with NGOs. In any case, there will be a large culture shift in how militaries do business with those outside their sphere of influence regarding information sharing.

Moreover, there are huge cultural differences across governmental departments (i.e., inter-agency) that need to be addressed and overcome. SMEs explained that the development of the concept of NEOps has been done largely in isolation without substantive inter-agency involvement, which is, ironically, exactly counter to what the idea entails. SMEs argued that other agencies cannot be divorced from the NEOps-implied culture, and that their advice should be elicited at the lower levels.

It appears, then, that the kind of transformation required for NEOps – or more specifically something like self-synchronization – will be a product of culture and doctrinal change within the CF as opposed to technological implementation. Moreover, as one group member explained, from a Canadian perspective, not everyone will be working in the net at the same time. What, he asked, are the growing steps that take us to a potential NEOps? How will the CF operate in partially networked environments? And how will personnel be able to know and capitalize on the fact that they are in a NEOps environment?

SMEs also noted that within the NEOps paradigm, the hierarchical structure of the military will be changed into a flatter organization, which resembles a "web of command" instead of a chain of command. If one of the desired outcomes of NEOps is distributed decision making, then the CF needs to consider the changes to the organizational structure that are required. For example, current C2 is based on a central, hierarchical model. While thinking around greater horizontal command approaches has been emphasized (McCann & Pigeau, 2000), how does NEOps make this process more of a reality and hence more immediate? How does CF culture begin to embrace a "web of command" in place of a chain of command? This may require another form of leadership to reflect decentralized decision making, while still maintaining the essential level of authority. This leads to the question of how authority changes in a NEOps environment. One SME suggested that military structures may need to change concurrently. He asked what would happen if they changed in different directions, and how would possible misalignment impact international efforts?

Consequently, another challenge of NEOps raised by SMEs was education and training, and what that means for the organization. NEOps presents a particular challenge in that all CF operations will be increasingly computing-dependent, and yet familiarity and competencies with computing technologies and applications in the CF is currently not pervasive. As such, NEOps implementation

is likely to require more investment in experts with competencies with networking and computing technologies. SMEs explained that a further challenge is identifying the core competencies in a NEOps world without the benefit of knowing exactly what that world is likely to look like. SMEs argued that, in a NEOps environment, competencies would in some instances supersede rank. As such, there is a need for flexible authority. According to MacNulty (cited in Warne et al, 2004), change in education and training will manifest itself in style, the approach to learning and subject matter, access to knowledge, timing of education, orientation, how education is perceived, and the approach to teaching. For example, one group member believed that what was specifically absent from the conception of NEOps was the "whole issue of judgement". Another concurred, that simply having information does not ensure good decision making. Another issue facing the CF, therefore, is providing personnel with the means to determine what they need to know to make a good decision in an information-rich environment.

SMEs also noted other challenges likely in implementing NEOps in Canada. Working within a JIMP context, for example, was seen as likely to present unique challenges to working in networked operations. For example, SMEs pointed out that although NEOps needs to be understood within a broader operational context, evolving partnerships (e.g. with differing JIMP stakeholders) will require different sharing requirements. This may not present a huge challenge when the Army works at the joint level with the Air Force, but the level of information sharing may be very different than when the Army works with a non-governmental organization (NGO). Similarly, although NEOps may increase the potential for information sharing with the public, the degree of information sharing would vary, depending on the nature of the operation. SMEs pointed out that the military would not release everything to other agencies or the public. In fact, the public role would likely be limited to supporting governmental decisions regarding the military, and the public sphere would simply be the domain where operations are played out.

One SME argued that specific competency training, i.e., "controlled knowledge", for NEOps would amount to only a small percentage of the education and training. The significant changes in education and training would occur, he continued, in the social processes, which are based on expectations, beliefs, etc. Another SME added that the structure of education should change and not necessarily the content. For example, how does one learn how to learn on the net? What does it mean to be a professional in a net world? Coping with uncertainty, creativity, innovation, were attributes that SMEs identified as particularly salient for successful performance in a new NEOps environment because "linear thinking" would be less effective. The design of NEOps had to be human-centric to reduce the potential complexity. The design could not follow a strictly engineering approach.

In terms of more pragmatic issues, SMEs noted that affordability was also considered a major challenge for NEOps. Canada has a limited budget that it can spend on defence. Legacy issues, one SME stated, need to be carefully addressed. Of course, affordability was understood in another way. Can Canada afford *not* to invest in the changing means of warfare and operations? What would Canada lose if it failed to move forward with NEOps? As well, recognizing that information is power, SMEs thought that information security was an imperative. For example, how could information be shared but at the same time be secure? And, of course, how would security issues impact interoperability?

Interestingly, the *CF Strategic Operating Concept* (2004) identifies the implausibility of removing all of the fog and friction of war through networks. It is documented that "human intelligence,

obtained in part through human networking, will be key to achieving [an] information advantage" in the future battlespace. Though networks and sensor capabilities have improved the operational picture and decreased the uncertainty of war, certainty will never be realized because "[d]ifferences in individual cognitive processes, technological failures, and the actions of adaptive adversaries will all continue to frustrate achievement of a completely certain operating picture" (*CF Strategic Operating Concept*, 2004, p. 18). So despite the information advantage that arises from robust networking, commanders will still have to make decisions in the face of uncertainty. Networks themselves will not eliminate the uncertainty of war. These points highlight the caution in the Canadian perspective of NEOps when compared to the U.S. conception of NCW.

In conclusion, SME identified many challenges for NEOps, including building trust between partners connected by the network, creating common intent, preventing information overload and consequently reliance on familiarity and confirmation bias. At a broader level, NEOps also requires melding of often diverse organizational cultures and requires changes to both education and training for CF personnel, as well as revisions to organization structures and procedures.

6. Final Thoughts

The ability to link sensors, decision makers, and combatants in newly formed relationships to provide an information and decision advantage and to increase mission effectiveness and efficiency is a potential reality in today's battlespace. Based on the culmination of a broad, literature survey and two think tanks, we have elaborated some of the key aspects of the Canadian perspective of network enabled operations. On the one hand, there is a general acceptance among SMEs that military operations should take advantage of the technological advancements of our time in order to maximize the information edge over potential adversaries in combat missions.

However, there was a general concern among SMEs that, as the CF moves forward, it should not get "blind-sided" by the mere technological potential for combat operations. Rather, the CF also needs to embrace the full extent of transformation and the paradigm shift in military affairs and take into account the unique roles that Canada plays in international affairs. It also needs to consider the unique impacts that NEOps will have on the human actors and the CF organizational structure and culture. As such, SMEs identified a number of cognitive and social factors that require investigation as Canada moves forward. They feared that there might be many rapid organizational changes without the benefit of the robust research that they thought necessary. SMEs also thought that it was critical to integrate Canadian strategic operating concepts, such as the JIMP framework and the 3D approach, to international affairs through a fully articulated definition of NEOps. In fact, it was pointed out that NEOps is a governmental concept rather than a military concept. The question remains whether a military model will dominate in the governmental model. SMEs also thought it was important to differentiate the Canadian concept of NEOps from the US concept of NCW in order to ensure that all of the missions in which the CF participates are given adequate attention.

7. Bibliography

(2002). Australia's Navy for the 21st Century, 2002-2031, The Royal Australian Navy.

(2003). Network Centric Operations Conceptual Framework. Vienna, VA, Evidence Based Research Inc.

(2003). Network Enabled Capability: The UK's programme to enhance military capability by better exploitation of information, Ministry of Defence, UK.

(2004). Multinational Experiment - Presentation to Foreign Affairs Canada. Ottawa, National Defence.

(2004). Multinational Experiment 4 (MNE4): A Process-Refinement Test of Functional Warfighting., U.S. Joint Forces Command.

(2004). Securing an Open Society: Canada's National Security Policy. Ottawa, Privy Council Office, Canada.

(2004). Looking Forward Staying Ahead...Enabling Transformation. Ottawa, Defence Research and Development Canada.

(2004). Network Enabled Operations Symposium - The Future of NEOps within Canada. Ottawa, National Defence.

(2004). Canadian Forces Strategic Operating Concept. Ottawa, National Defence.

(2004). Delivering Security in a Changing World: Future Capabilities, Ministry of Defence, UK.

(2004). Future Capabilities: Factsheet 4 Network Enabled Capability, Ministry of Defence, UK.

(2004). *Australian Perspective on Network Centric Warfare.* Paper presented at the TTCP Multi-National Workshop on NCW. Defence Science and Technology Organisation (DSTO).

(2005). HUM - Human Resources and Performance Group.

(2005). Operations Analysis Support to Network Centric Operations. MORS Workshop, WG 2, "Operations Analysis Methods & Process" Outbrief, Alexandria, VA, Military Operations Research Society.

(2005). Network Enhanced Capability, Ministry of Defence, UK.

**(2005). The Implementation of Network-Centric Warfare. **Office of Force Transformation. Washington, DC: Office of the Security of Defense, Department of Defense.

Recent update of statement of NCW in US. Must read.

ADKINS, M., & KRUSE, J. (2003). *Case Study: Network Centric Warfare in the U.S. Navy's Fifth Fleet. Web-supported Operational Level Command and Control in Operation Enduring Freedom* (Case Study): University of Arizona.

AITKEN, L. (2005). *Network Centric Warfare: Just Another dot.com* (Student Paper). Kingston, ON: Canadian Forces College, AMSC 6.

ALBERTS, D. S., GARSEKA, J. J., & STEIN, F. P. (1999). *Information Superiority and Network Centric Warfare* (Presentation). Washington, DC: Command and Control Research Program, US Department of Defense.

ALBERTS, D. S., & HAYES, R.E. (2003). *Power to the Edge: Command, Control in the Information Age*. Washington: CCRP Publications.

ALMEN, A., ANDERSON, M., LAGERLOF, J., & PALLIN, K. (2000). *The Role of Command in Network Centric Warfare.* Paper presented at the 5th International Command and Control Research and Technology Symposium, Vienna, VA.

Australian Defence Headquarters. (2004). *Capstone Series ADDP-D.3.1. Enabling Future Warfighting: Network Centric Warfare*. Canberra ACT: Directorate of Future Warfighting.

**BABCOCK, S. (2004). *Canadian Network Enabled Operations Initiatives.* Paper presented at the 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark.

Provides an overview of NEOps issues and initiatives within DND/CF and how it has or will facilitate transformation. Discussion of fruitful areas of research and development. Required reading.

BAKER, M. E. (2002). *Human Factors in Network Centric Warfare* (Final). Newport, RI: Naval War College.

BARNETT, T. P. M. (1999). The Seven Deadly Sins of Network-Centric Warfare. *Naval Institute Proceedings Magazine*.

"A devil's advocate take on what [the author] sees as network-centric warfare's seven deadly sins". These sins are lust, sloth, avarice, pride, anger, envy, and gluttony. While lacking in supporting research and literature, Barnett makes some interesting points. Worth reading.

BARRY, K., STONEKING, C., CARPENTER, C., & GOSELIN, K. (2004). *Shared Situation Awareness for Networked Dismounted Soldiers.* Paper presented at the 24th Army Science Conference, Orlando, FL.

BONK, C. J., & WISHER, R. A. (2000). *Applying collaborative and e-learning tools to military distance learning: A research framework.* US Army Research Institute for the Behavioural and Social Sciences.

BORGU, A. (2003). *The Challenges and Limitations of Network Centric Warfare - The initial views of an NCW sceptic.* Paper presented at the Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations Conference, Australian Strategic Policy Institute (ASPI).

BORNHOLT, G. (2004). *Network Centric Warfare: The Australian Perspective* (Presentation). Washington, DC: Australian Defence Staff.

BOWES, L. R. L. (2003). The Advent of Digitization: A Doctrinal Perspective. *The Army Doctrine and Training Bulletin, 6*(1), 28-32.

BRADLEY, D. J., STRICKLAND, G. M., WALKER, C. R. V., WOODDISSE, R. W., & ANGLIAN, R. (2002). *Network Enabled Capability and British Command Culture - No. 6 DTC (MA).* Unpublished Master of Arts, Cranfield University, Royal Military College of Science.

BREHMER, B., & SUNDIN, C. *Joint and Coalition Command and Control for the Digitised Battle Space: A Swedish View*: Swedish National Defence College, Department of Operational Studies.

BROWN, T. (2004). *The NZ National Perspective on Net-Centric Warfare*.

CATERINICCHIA, D., & FRENCH, M. (2003). Network-Centric Warfare: Not there yet. *Federal Computer Week*.

CEBROWSKI, A. K., & GARSTKA, J. J. (1998). Network-Centric Warfare: Its Origin and Future. *Naval Institute Proceedings Magazine*.

CEBROWSKI, A. K. (1999). *Network-Centric Warfare: An Emerging Military Response to the Information Age.* Paper presented at the Command and Control Research and Technology Symposium, Naval War College, Newport, RI.

CHNG, K. (2001). *Preparing Military Leadership for Warfare in the 21st Century* (Seminar Paper): Canadian Forces College, AMSC 4.

CHRISTINER, G. (2001). *Command Versus Control in the Age of Information Technology* (Student Paper): Canadian Forces College, AMSC 4.

CIANCIOLO, M. (2003). *Network Centric Warfare: A Bridge Too Far?* Newport, RI: Joint Military Operations Department, Naval War College.

CLARK, V., & HAGEE, M. W. (2005). *FORCEnet: A Functional Concept for the 21st Century*. Washington, DC: Department of Defense.

COOK, M. J. (2004). *Network Centric Decision Making Performance* (Presentation). UK: University of Abertay, Dundee.

COSGROVE, P. J. (2004). *Enabling Future Warfighting: Network Centric Warfare*. Canberra, Australia: Australian Defence Headquarters.

CRAN, G. (2004). *Operations Analysis Support to Network Centric Operations - UK Overview* (Presentation): DSTL, UK Ministry of Defence.

DAVIS, C., FEWELL, M. P., & CHRISTIAN, R. (2004). *Network Centric Maritime Warfare Study: Key Issues in Coalition Network-Centric Maritime Warfare* (TTCP Technical Report TR-MAR-10-2003): Technical Cooperation Program, Subcommittee on Non-Atomic Military Research and Development.

DUFF, P. A. (2003). Project Minerva: Command and Control in the Army of Tomorrow. *The Army Doctrine and Training Bulletin, 6*(1).

ELCOCK, W. (2004). *An Integrated "Whole Country" Approach to National and International Security.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

ENEMO, G. *Analysis of Command and Control in Network Enabled Operations.* Norwegian Defence Research Establishment (FFI).

ENGLISH, A. (2004). *The Operational Art: Theory, Practice, and Implications for the Future, Part 4: Future War and the Operational Art*: Canadian Forces College.

ENGLISH, A. (2005). *Selected Readings - The Human Dimension of NEO* (Reference List).

A listing of selected readings concerning the human dimension of NEOps.

FARRELL, P. S. E. (2004). *Measuring common intent during effects based planning.* Paper presented at the 2004 Command and Control Research and Technology Symposium: The Power of Information Age Concepts and Technologies.

FERBRACHE, D. (2002). *Strategic Defence Review - New Chapter: Network Enabled Capability* (Presentation): Ministry of Defence, UK.

**FEWELL, M. P., & HAZEN, M. G. (2003). *Network-Centric Warfare - Its Nature and Modelling* (Research Report DSTO-RR-0262). Australia: Defence Science and Technology Organisation.

A very good analysis of the characteristics of NCW. With the exception of reachback, they discovered that no characteristic was particularly "diagnostic" of NCW, when considered discretely and when the network meant a "high-capability communications network". They cited examples in which the characteristics could be achieved, without the assistance of a robust information network. They devised a list of other properties based on internet usage that they thought reflected more appropriately the nature of network centricity.

FEWELL, M. P., & HAZEN, M. G. (2003). *Network-Centric Warfare / Operations Definitions* (Annex). Australia: Defence Science and Technology Organisation (DSTO).

FORGUES, P. (2000). *Command in a Network-Centric War* (Student Paper): Canadian Forces College, AMSC 3.

FRASER, R. (2004). *Bi-National Civil-Military Coordination Challenge.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

GARSTKA, J. J. (2003). Network-Centric Warfare Offers Warfighting Advantage. *Signal Magazine*.

**GIZEWSKI, P. (2004). *Networked Enabled Operations: A User's Guide to the Literature*. Kingston, ON: Directorate Land Strategic Concepts.

Very good overview of major NEOps conceptual documents by Canadian defence scientist.

GOMPERT, D. C., LACHOW, I., & PERKINS, J. (2005). *Battle-Wise: Gaining Advantage in Networked Warfare* (Defense & Technology Paper). Washington, DC: National Defense University.

Gompert, Lachow, and Perkins, from the US National Defense University, indicate where research and analysis is needed on how to gain cognitive advantage through NCW. They indicate that the critical question at this juncture is how to gain advantage over enemies who also have networked forces, and that the answer is through our brains. By this they mean that the mind is the key to graduating from information superiority to time-information superiority as enemies develop their own networks. Acknowledging that the idea that brilliant command is not new, they argue that networking offers unprecedented opportunity to prevail in battle by permitting better problem-solving, mobilizing more minds, and by honing the collective intelligence of whole units and teams.

GRAHAM, B. (2004). *NEOps and DND/CF Transformation.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

HATCHARD, P. J. (2004). *NATO Networked Enabled Capability (NNEC) Foundation Document*. Norfolk, VA: North Atlantic Treaty Organization, Headquarters, Supreme Applied Commander Transformation.

HAYES, R. E. (2004). *Network Centric Operations (NCO) The Evidence Emerging from Case Studies.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

HAYES, R. E. (2004). Network Centric Operations Today, Between the Promise and the Practice. *RUSI Defence Systems*(Summer), 82-85.

HEMSLEY, D. (2004). *Network Enabled Capability: A Personal UK Perspective* (Presentation): Command & Battlespace Management, UK Ministry of Defence.

HENAULT, R. (2004). *NEOps and Future Operations.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

HUGHES, S. C., DRISKELL, J.E., & WILLIS, R.P. (1994). *Distributed Team Decision-Making*: US Army Research Office.

HURA, M., MCLEOD, G., & AL, E. (2000). A Broad Definition of Interoperability, *Interoperability: A Continuing Challenge in Coalition Air Operations*. Santa Monica, CA: Rand.

JEFFERY, L. R. (2004). *Opening Remarks by Master of Ceremonies.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

JOHNSON, C. (2003). Net-Centric Fogs Accountability. *Naval Institute Proceedings Magazine* (May).

KAUFMAN, A. (2005). Caught in the Network. *Armed Forces Journal, February*, 20-22.

> *In this short article, Kaufman, of the Institute for Defense, discusses his perspective on how the doctrine of network-centric warfare allows technology to dictate military strategy. Noting that NCW underestimates the enemy's ability to deceive even as it overestimates our own capacity to share understanding, he argues that the new doctrine tends to ignore the 'human character of information' and the perpetual nature of war. An interesting read.*

LAING, K. D. W. (2004). *The Atlantic Littoral ISR Experiment and NEOps - Networking for Future Surveillance.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

LEGGAT, J. (2004). *Australia-Canada-New Zealand-UK-US Collaborative Science & Technical Response to NEOps. The New TTCP NCW Enterprise.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

MATTE, G. C. P. (2004). *Improving Aircrew Interoperability in Coalition Warfare - Examining the Human Dimension of the Air Power Equation* (Student Paper): Canadian Forces College, AMSC 7.

MCMASTER, H. R. (2003). *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War* (Student Issue Paper): Center for Strategic Leadership, U.S. Army War College.

MIDDLEMISS, D. W., & STAIRS, D. (2002). *The Canadian Forces and the Doctrine of Interoperability: The Issues (Excerpts). Part 1 - Interoperability: The Way Ahead for Canadian-American Practice*

> *This article published in November 2002 reviews in brief the aspects emphasized in Canada's "Strategy for 2020" for achieving interoperability with its principle allies in general, and particular, the United States. Noting Canada's evident commitment to achieving this end, the authors warn that this objective must also imply Canada's commitment to US force goals, the political agendas that underlie them, and the acceptance of culpability for actions that occur within 'interoperational' missions. They also suggest that Canada has demonstrated "genuinely innovative approaches to achieving the interoperability objective", and given that Ottawa is unlikely to suddenly and dramatically increase Canadian defense spending, "interoperability with the Americans is the only game in town". Short read. Food for Thought.*

MITCHELL, P. T. (2003). *The Limits of Cooperation: Network Centric Warfare, Interoperability, and International Anarchy*. Santiago, Chile: REDES Strategic Studies Track.

MONEY, A. L. (2001). *Report on Network Centric Warfare Sense of the Report*. Washington, DC: U.S. Department of Defense.

NATO. (2004). Information Superiority & NATO Network Enabled Capability.

**NEOps Symposium Working Group. (2004). *Network Enabled Operations: DND/CF Responding to the New Security Environment (Background Info)*. Ottawa: Defence R&D Canada.

> *This paper, generated by the NEOps Symposium Working group, outlines the principles behind Canadian NEOps and the perspectives of allied nations and NATO. It provides an overview of how NEOps fundamental operational activities will be integrated into emerging concepts stated in the Strategic Operating Concept (SOC) and the future security environment with a number of national and international partners. It also suggests how NEOps will impact a number of functional concepts, such as command and sense, effective engagement, force generation, and support, sustainment, and mobility within the four domains, physical, informational, social, and cognitive.*

NEW, W. (2004). Military Culture Seen as Hurdle to Network Warfare. *National Journal's Technology Daily*.

NORDICK, B.-G. G. W. (2003). Command and Control Aspects of Digitization - Guest Editorial. *The Army Doctrine and Training Bulletin, 6*.

PHISTER, P. W., & PLONISCH, I. G. (2004). *Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare*. Rome, NY: Air Force Research Laboratory/Information Directorate.

PORTER, N., KENNEDY, J., BRIDGEWATER, B., FOURNIER, G., CHARLEBOIS, D., HALES, D., D'AGOSTINO, P., HANNA, D., HAZEN, M. G., SALMANIAN, M., HOLLANDS, J., & TIKUISIS, P. (2004). *Transformation Concepts and Technologies: DRDC Tiger Team Analysis of Transformation Implications*. Ottawa, ON: Defence Research and Development Centre.

PUDAS, T. J. (2004). *A Future Worth Creating* (Presentation). Washington: Office of Force Transformation, US Department of Defense.

SALAS, E., BURKE, C. S., FOWLKES, J. E., & WILSON, K. A. (2004). Challenges and Approaches to Understanding Leadership Efficacy in Multi-Cultural Teams. In M. Kaplan (Ed.), *Cultural Ergonomics* (Vol. 4, pp. 341-384): Elsevier.

SALAS, E., STAGL, K.C., & BURKE, C.S. (2004). 25 years of team effectiveness in organizations: Research themes and emerging needs. *International Review of Industrial and Organizational Psychology, 19*, 47-91.

SCALES, R. H. (2005). Human Intel vs. Technology. *The Washington Times*.

SHERRARD, L. B. (2003). From the Directorate of Army Doctrine: The Future Battlegroup in Operations. *The Army Doctrine and Training Bulletin, 6*(3), 5-14.

SMITH, E. A. (2005). *Network Centric Warfare: Where's the Beef? The Command and Control Research Program*: Naval War College Review.

STEWART, K. G., BONNER, M. C., & VERRALL, N. G. (2001). *Cultural Factors in Future Multinational Military Operations.* Paper presented at the Human Factors in the 21st Century, Paris, France.

SUTTON, J. L., & PIERCE, L.G. (2003). *A framework for understanding cultural diversity in cognition and teamwork*, Fort Sill, Oklahoma.

SUTTON, J. L., COSENZO, K.A., & PIERCE, L.G. (2004). *Influence of culture and personality on determinants of cognitive processes under conditions of uncertainty.* Paper presented at the 9th International Command and Control Research Technology Symposium.

TALBOT, D. (2004). "We got nothing until they slammed into us." *Technology Review, November,* 36-44.

Citing statements from a battalion commander that the objective was almost devoid of information about Iraqi strength, Talbot argues that the Pentagon's claim that the Iraq War had impressive digital connectivity and many characteristics of networked warfare is misleading. Talbot maintains that Objective Peach, the largest counterattack of the Iraq War which occurred on April 3, 2003, was the biggest test to date of the Pentagon's initial attempts to transform the military into a smaller, smarter, sensor-dependent, networked force, and that it failed. While relying mostly on evidence from a single event, and the testimony of a single individual, the article at least represents a critical perspective on NEOps. While critical, however, it rings of sensationalism, and therefore seems biased.

TAYLOR, R. K. (2001). 2020 Vision: Canadian Forces Operational-Level Doctrine. *Canadian Military Journal*(Autumn), 35-42.

VEGO, M. (2003). *Network-Centric Warfare is Not Decisive*: US Naval Institute Proceedings.

**VERDON, J. (2004) *Transformation in the CF - People Implications of Effects-Based and Network-Enabled Operations* (Draft).

Focuses on the human elements of NEC and EBO from psychological and philosophical perspectives. Required reading.

**WARNE, L., ALI, I., BOPPING, D., HART, D., & PASCOE, C. (2004). *The Network Centric Warrior: The Human Dimension of Network Centric Warfare* (DSTO Report CR-0373). Edinburg, SA: Defence Systems Analysis Division, Defence Science & Technology Organisation, Department of Defence.

This article from DSTO represents the most elaborated exploration of the human dimensions of NEOps that we found in our literature survey. It considers the concept of NCW, and new organizational paradigms that will be necessary. Requirements of warfighters in the past and in the future are then considered. Values that the ADF promotes are professionalism, trustworthiness, morality, teamwork and initiative, courage and compassion, fairness and carefully directed effort. In NCW paradigm, it will be necessary to add collaborative interoperability, cultural empathy, transparency of decision making and empowerment of individuals. Required personality traits include adaptability, making sense of contradictory information flows, dealing with ambiguity, comfort with change, skills in diplomacy and ability to innovate. Many human resource issues will also need to be considered, including recruitment, selection, values promulgation, people working in networks, human-machine interfacing, education and training as lifelong processes.

Issues for individuals and groups in NCW contexts

C2 issues are intent, self-synchronization, specialization and tempo.

Battlespace issues are multidimensional manoeuvre, EBO, interoperability, jointness, adaptability, reachback, shared SA

Information issues are volume of information, info. sharing, context and communication, reliability and quality, presentation, disinformation and conflicting information.

Several fundamental concept form bedrock for NCW. Because of the high levels of communication, shared understanding required, communication climate, social learning and learning style are important, as are innovation, creativity and problem solving. Organizational factors such as power and political dynamics will also be important to understand. Trust is argued to play a critical role, as are social cohesion and common identity.

Learning and knowledge development are addressed in detail. Organizational models that could be mapped on the NCW approach are considered.

Concludes with recommendations for establishing a coordinated research agenda (broadly applicable to Canada's efforts). A very important paper.

WHITE, O. (2004). *Harnessing the Power of Network Centric Operations: the role of ideas, norms and values.* Paper presented at the 2004 Command and Control Research and Technology Symposium, San Diego, CA.

ZACCARDELLI, G. (2004). *Cooperation and Coordination in the New Security Environment.* Paper presented at the Network-Enabled Operations Symposium: DND/CF Responding to the New Security Environment, Ottawa.

DOCUMENT CONTROL DATA
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document, Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Publishing: DRDC Toronto

Performing: Humansystems Incorporated, 111 Farquhar St,., 2nd floor, Guelph, ON, N1H 3N4

Monitoring:

Contracting: DRDC Toronto

2. SECURITY CLASSIFICATION
(Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification is indicated by the appropriate abbreviation (S, C, R, or U) in parenthesis at the end of the title)

Network Enabled Operations: A Canadian Perspective (U)

4. AUTHORS (First name, middle initial and last name. If military, show rank, e.g. Maj. John E. Doe.)

Michael H. Thomson; Barbara D. Adams

5. DATE OF PUBLICATION
(Month and year of publication of document.)

May 2005

6a NO. OF PAGES
(Total containing information, including Annexes, Appendices, etc.)

36

6b. NO. OF REFS
(Total cited in document.)

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The names of the department project office or laboratory sponsoring the research and development − include address.)

Sponsoring:

Tasking:

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant under which the document was written. Please specify whether project or grant.)

Contract No. W7711−3−7893/01−TOR
Call−up No. 7893−03

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document)

DRDC Toronto CR 2005−162

10b. OTHER DOCUMENT NO(s). (Any other numbers under which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILIY (Any limitations on the dissemination of the document, other than those imposed by security classification.)

Unlimited distribution

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11), However, when further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited announcement

DOCUMENT CONTROL DATA
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

(U) This report outlines the concept of Network Enabled Operations (NEOps), both as a whole, and from a uniquely Canadian perspective. This report is the culmination of an extensive literature survey, and of two think tanks convened on 1 March 2005 and 30 March 2005 with Canadian subject matter experts (SMEs), both military and non−military, who are currently working to define and drive forward the Canadian concept of NEOps. Results showed that the Canadian conception of NEOps must be interpreted in light of the new security environment and what role the Canadian Forces (CF) is likely to play. As such, NEOps must be understood within emerging concepts in defence policy, such as the JIMP framework (joint, interagency, multinational, public) and the 3−D (defence, diplomacy, development) approach to international affairs. SMEs questioned how the stated benefits of NEOps would actually manifest themselves in operations, such as warfighting, peacekeeping, humanitarian, nation building, etc., without fully appreciating the cognitive and socialization processes that underlie them. Moreover, SMEs pointed to a number of challenges that require greater attention prior to full implementation of NEOps. These include: trust; ensuring common mental models, cognitive processes, and understanding; information overload; authority (including common intent) and accountability; attempts to implement NEOps universally, across the three arms of the CF; CF structure and culture (e.g., distributed decision making and information sharing); education and training; and affordability.

(U) Ce rapport décrit le concept des opérations réseaucentriques (NEOps), d'une manière générale et du point de vue canadien seulement. Ce rapport constitue l'aboutissement d'une étude approfondie des ouvrages portant sur le sujet et de deux exercices de réflexion qui se sont tenus le 1er et le 30 mars 2005. Les groupes de réflexion étaient composés d'experts en la matière (EM) canadiens, militaires et civils, qui s'occupent actuellement de définir et de faire progresser le concept canadien des opérations réseaucentriques.

Il en découle que la conception canadienne des NEOps doit être interprétée à la lumière du nouveau contexte de sécurité et du rôle qui devrait être attribué aux Forces canadiennes (FC). Ainsi, il faut envisager les NEOps dans des concepts nouveaux de la politique de défense, par exemple, le cadre JIMP (interarmées, inter−institutions, multinational et public) et l'approche des trois D (défense, diplomatie et développement) à l'égard des affaires internationales. Les EM se sont interrogés sur la manière dont les avantages mentionnés des NEOps se manifesteront concrètement dans les opérations, notamment au combat, dans le cadre du maintien de paix, de l'aide humanitaire, de la construction de nation, etc., sans parfaitement comprendre les processus cognitifs et de socialisation qui les sous−tendent. En outre, les EM ont soulevé un certain nombre de défis dont il faudrait se préoccuper davantage avant de passer à la mise en œuvre complète des NEOps. Il s'agit notamment de la confiance, de la compréhension, des processus cognitifs et des modèles mentaux communs, d'une surdose d'information, du pouvoir (y compris l'intention commune) et de la responsabilisation, des tentatives visant à appliquer les NEOps universellement dans les trois armes des FC, de la structure et de la culture des FC (p. ex. le partage du pouvoir de décision et l'échange d'information), de l'éducation et l'instruction et, enfin, de la capacité financière

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of

Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

(U) Network Centric Warfare; Network Enabled Operations; benefits and challenges; new security environment; defence policy; international affairs