CANADIAN FORCES COLLEGE
CSC 30

EXERCISE NEW HORIZONS

"Confessions of an Intranet Junkie"

Information Management Requirements for the CF

By LCdr P.R. Crain

Abstract

The revolution in military affairs has endowed the Canadian Forces with an increasing accessibility to information and data with which to manage warfare and make decisions. In this new environment of network-centric warfare, the principles of Information Management are key to organizing this newfound wealth of information. However, without a coherent strategy to implement a sound Information Management foundation, the benefits of network-centric warfare cannot be realized. This paper will prove that the CF will only be able to realize the operational advantages of speed of command and self-synchronization in a network-centric environment when a comprehensive Information Management strategy has been implemented to ensure that training, procedures and equipment support the goals of warfare management in a network-centric environment.

0630 – knock knock… "Morning file, Sir!" Clunk…a 3.5" disk lands on my desk. Up and off to the shower; back to the cabin to shave, dress and flash up the stand alone computer...Has it got the Secret Drive in it? Yes, ok put in the morning disk…whew! Only 150 messages this morning.
0800 – ahh, coffee… back to the staff office to flash up the MCOIN – a quiet night only 12 emails since 2am. Done – next flash up COWAN…uggh! 17 messages in the last 6 hours. Websites to check…was that posted yesterday or is it new? Hmm… oh well better bring it up anyway. Half hour to kill before the morning meeting…might as well go back to the cabin to check DWAN and log onto the Internet to see if an email from home has come in.
0925 – Oh, there we go – time for the Morning Staff Meeting. Pretty good read-in this morning – five different systems, a couple of hundred emails and a baker's dozen of websites surfed – yielded about 30 points to pass on at the staff briefing.

This was my life for six months while deployed on Operation Apollo in 2002…checking a number of network systems while dedicating my time throughout the day to Battle Rhythm events and normal staff duties. While it is not disputed that the addition of these deployed systems aided the CF in achieving a key Command and Control (C2) role during the Global War on Terrorism (GWOT), the fact that the systems were non-integrated and Information Management (IM) principles were embryonic, resulted in a less than efficient network-centric warfare (NCW) environment.

> …the information provided by systems like GCCS (M) [see Appendix One] …MCOIN III, [has] become "stove piped". The result is a cluttered Operations Room where decision makers must consult a number of systems in order to gather all the information necessary to perform their jobs – obviously not the most efficient arrangement in the heat of battle.[1]

What is this gift of the latest revolution in military affairs (RMA) called network-centric warfare? First, it must be clearly understood that NCW is not a "warfare area" like the traditional warfare domains of Anti-Air Warfare or Air Interdiction. NCW is a concept, or environment, in which traditional warfare is conducted more effectively. Perhaps the best explanation is that offered by Vice-Admiral Jay Johnson, the USN Chief of Naval Operations (1996-2000), during the introduction of deployed Information Technology (IT) systems, when he suggested that this RMA has initiated a change from platform-centric warfare to network-centric warfare.[2] This

---

[1] Paul T. Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?" *Naval War College Review*, Vol. LVL, No 2 (Spring 2000): 94.

[2] VAdm (USN) Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings Magazine*, (January 1998) [journal on-line]; available from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; Internet; accessed 29 February 2004.

means that the focus of warfare has shifted from an operational advantage based upon a platform or equipment capability to an environment in which the platform capability remains important but that operational capability is enhanced or leveraged by the use of networks to collect, analyze and disseminate information[3] while also using these networks to plan, make decisions and order actions. VAdm (USN) Arthur Cebrowski, one of the visionaries of NCW and current US Director of Force Transformation, has said "Network-centric warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization."[4] Roughly paraphrasing these concepts, speed of command refers to information superiority or the ability to collect, analyze, disseminate and display information to permit timely and informed decision-making. Self-synchronization refers to the state in which individual systems users input, access and use information permitting the decision cycle to function. The most popular of the decision-making cycles is the "OODA" loop consisting of the Observe, Orient, Decide and Act phases.[5] Cebrowski contends that the observe, orient and decide phases are periods of operational inactivity where the warfighters await direction.[6] The operational advantage afforded by speed of command and self-synchronization will diminish these periods of operational inactivity permitting the cycle to progress more rapidly and, in terms of operational success, progress more rapidly than the decision-making cycle of the enemy – getting inside the enemy's OODA Loop.[7]

The introduction of NCW into the CF is a serious issue. It is ironic that it was the Soviet Union that first recognized the RMA in the late 1970s that eventually gave birth to NCW.[8] This irony is further exacerbated by the fact that the US led the integration of NCW in the mid 1990s

---

[3] *Ibid*

[4] *Ibid*

[5] Col. John Boyd, "Patterns of Conflict," available from http://www.mindsim.com/MindSim/Corporate/OODA.html; Internet; accessed 19 March 2004.

[6] Cebrowski, *Network-Centric Warfare*…

[7] Australia, Department of Defence, *AF2025 - Information Operations: A new War-fighting Capability*, available from http://www.au.af.mil/au/2025/volume3/chap02/v3c2-2.htm; Internet; accessed 19 March 2004.

[8] Stephane Lefebvre, Michel Fortmann and Thierry Gongora, "The RMA: Its Implications for Doctrine and Force Development Within the US Army" in *Operational Art: Development in the Theories of War*, ed. B.J.C. McKercher and Michael A. Hennessy (Westport, CT: Praeger Publishers, 1996), 173.

fuelled by successful network introduction during the 1991 Gulf War[9] while Canada, a world technology leader, finally made mention of the RMA and its potential impact upon interoperability and command and control in 1998.[10] A lot of effort is now being expended on implementing secure LANs, deployed networks and a joint command and control system – the equipment component of NCW, but the IM aspect of NCW remains neglected. Additionally, perhaps the most important, if the least visible, is the human dimension of successful NCW operations for it is the people and their training in IM that will exploit information superiority to achieve that operational advantage coveted by VAdm Cebrowski. As the Canadian Forces continue to integrate warfare into a network-centric environment, a comprehensive Information Management strategy is required to ensure that training, procedures and equipment support the goals of warfare management in a network-centric environment.

In focussing upon the need for a comprehensive IM strategy, a short précis of network equipment concerns as they relate to IM will be introduced to delineate the background environment necessary to support successful NCW operations. Once this need for a basic understanding has been addressed, the requirement for a comprehensive IM strategy, including a proposed framework, will be demonstrated. This analysis will develop the requirement for dedicated IM personnel and IM training. IM in a joint and combined environment will then be discussed to expose the security issues that arise in combined operations and the need for interoperable systems and procedures in joint operations. Security, as it concerns the integration of systems that handle information of varying classification, will not be addressed due to the highly technical and evolutionary concepts involved. Furthermore, while understanding that NCW tends toward an acronym rich environment and that principles such as the differences between data, information and knowledge are important to one's understanding of this topic, several appendices have been included for reference.

---

[9] Timothy J. Gibson, "Rapid Preparation and Distribution of Battlefield Information," in *The First Information War*, ed. Alan D. Campen, (Fairfax, VA: AFCEA International Press, 1992), 111.

[10] Andrew Richter, *The RMA and Its Impact on Canada: The Challenge and the Consequences*, Working Paper 28 (Vancouver: Institute of International Relations, University of British Columbia, 1999), 9-11.

IT equipment is not a specific focus of this essay, however, a general understanding of the technical requirements to support the IM strategy is apropos. There are three equipment requirements that will foster a coherent NCW environment – a single networked system, a robust communications network linking all users and an equipment replacement philosophy. Currently there are at least seven systems varying from secret to unclassified that operate either independently or have some degree of integration that is less than complete.[11] A brief description of each system is included at Appendix One.

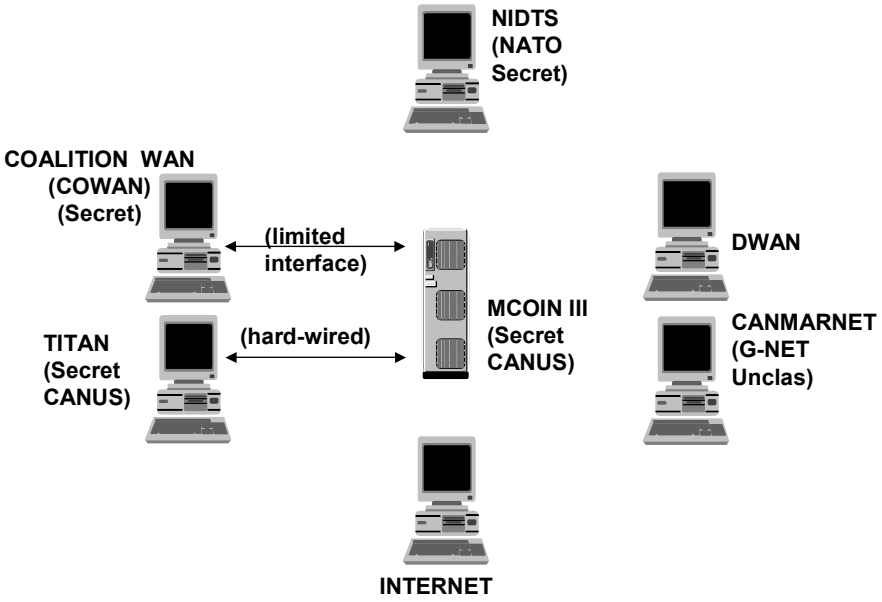

Figure 1 – Current non-integrated Family of Systems

A single system, with layered access corresponding to security classification and "need to know" will support the proposed IM framework and facilitate the realization of the principles of speed of command and self-synchronization. Secondly, the system must be supported by a communications system of sufficient bandwidth. The communications path must interface with satellite systems, civil or military, to support deployed operations. Finally, the procedures by which the system is acquired, installed and supported must be tailored to permit timely updating

[11] Adapted from Cdr Tom Aquano, *Naval Use of the Operational Planning Process*, presentation to CFC 10 March 2004.

of the system as technology advances.[12] Moore's Law states that data densities will double every 18 months.[13] This defines the pace of technological change and, while it is not proposed that the entire CF suite of IT equipment be replaced every 18 months, an appreciation of Moore's Law does offer a flavour of the rate of change. These leaps in technology far outpace the CF's current capability to acquire, support and deploy new equipment. Meeting this requirement requires Commercial-Off-the-Shelf (COTS) equipment and software systems that are quickly acquired and easily integrated into newer systems while preserving data integrity. These three requirements are not prerequisites for an IM strategy but are factors that will influence its success. It is not intended to explore these requirements further but rather to highlight them as issues that require attention in transitioning to a NCW environment.

The CF is in a state of transformation with the goal of learning to operate effectively in an environment characterized by new technologies. Key goals in this transformation are to transform "the way we [the CF] perceive and think; transform our [the CF] management structures and decision-making processes; and, transform our [the CF] force structure."[14] A transformation in the information age must include a strategy to manage the information and as such, IM forms part of each of the transformation goals. The Associate Deputy Minister, Information Management Group (ADM (IM)) was established to serve "the information needs of both the operational commanders and the departmental business managers."[15] ADM (IM) subsequently issued an IM administrative directive to highlight the requirement for "an IM policy to maximize the efficiency with which they [DND and the CF] plan, collect, organize, control, disseminate, use, safeguard and dispose of information."[16] However, while the directive goes on to catalogue a list of general requirements, it falls short of defining an IM strategy, rather

---

[12] David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (Washington, DC: CCRP Publication Series, 2000), 201-202.

[13] Moore's Law, available from http://www.webopedia.com/TERM/M/Moores_Law.html; Internet; accessed 19 March 2004.

[14] Department of National Defence, *A Time for Transformation: Annual Report of the Chief of Defence Staff 2002-2003*, available from http://www.cds.forces.gc.ca/00native/pdf/CDS-R2003_e.pdf; Internet; accessed 19 March 2004.

[15] Department of National Defence, *Defence Plan Online*, Article 307, available from http://www.vcds.forces.gc.ca/dponline/main_e.asp; Internet; accessed 30 January 2004.

[16] Department of National Defence, *DAOD 6000: Information Management*, available from http://www.dnd.ca/admfincs/subjects/daod/6000/0_e.asp; Internet; accessed 30 January 2004.

reserving for ADM (IM) the role of reviewing and approving the various departmental (Environmental and Group) IM plans and policies. This approach serves to encourage diversity in the ways that individual sections of the CF approach IM. This lack of a comprehensive IM strategy has created a disparity in IM between the environmental services and has done little to enhance CF-wide interoperability.[17]

The foundation of a coherent IM strategy is the establishment of an IM framework. It is useful at this point to review exactly what is expected in a NCW environment to achieve speed of command and self-synchronization. The network consists of several components, which include data – websites, databases and search agents; communications – voice/video telephone, chat, email, and whiteboarding; situational awareness – common operational picture (COP), Command and Control Personal Computer (C2PC)[18], tactical displays, Global Command and Control System (GCCS)[19], and Data Link; and, collaborative planning tools – presentations, programmes and decision-making aids. It should further be noted that at the periphery of the network, a variety of sensors and legacy data collection systems interface with the network situational awareness applications and tactical level situational awareness displays. The IM framework must include all these NCW components to define the collection, dissemination, organization, analysis, evaluation and display of information in terms of responsibility, organization and format to ensure that a NCW environment is achieved and that it enhances CF operations.

The basic premise of the IM framework is that it must cater to all aspects of operations, which include both force generation and force employment as well as the corporate/business practices of the CF. Far too often IM is thought of in parts of the whole – either from the perspective of operations – battlespace awareness; C2 and decision making; and, execution[20] – or, is conversely considered strictly from a business process point of view – personal administration, financial management and like activities. The ADM (IM) Information Management Strategic Review (IMSR) of 2002 highlights the need for an enterprise[21] or total systems approach to IM.[22]

---

[17] Hugh Robertson, *Future Direction for IM in DND/CF*, presentation on the IM Strategic Review; available from http://img.mil.ca/DGIMSD/IMSR/index_e.htm; Intranet; accessed 7 March 2004.

[18] See Appendix One.

[19] See Appendix One.

[20] Alberts et al, *Network Centric Warfare*…, 123.

[21] Robertson, *Future Direction for IM in DND/CF*, Slide 11.

As a result, data and information will be accessible by all authorized personnel in the pursuit of their duties.

With the understanding that the IM framework caters to the information needs of the CF as a whole, it is useful to visualize how the information environment will transcend traditional corporate borders to provide resources to users. A notional IM framework has been developed and included at Figure 2 to give an architectural depiction of a CF-wide network centric environment. The vertical separation indicated by the dotted lines refers to the conceptual differences between data, information and knowledge explained in Appendix Two. Conventional thinking in terms of

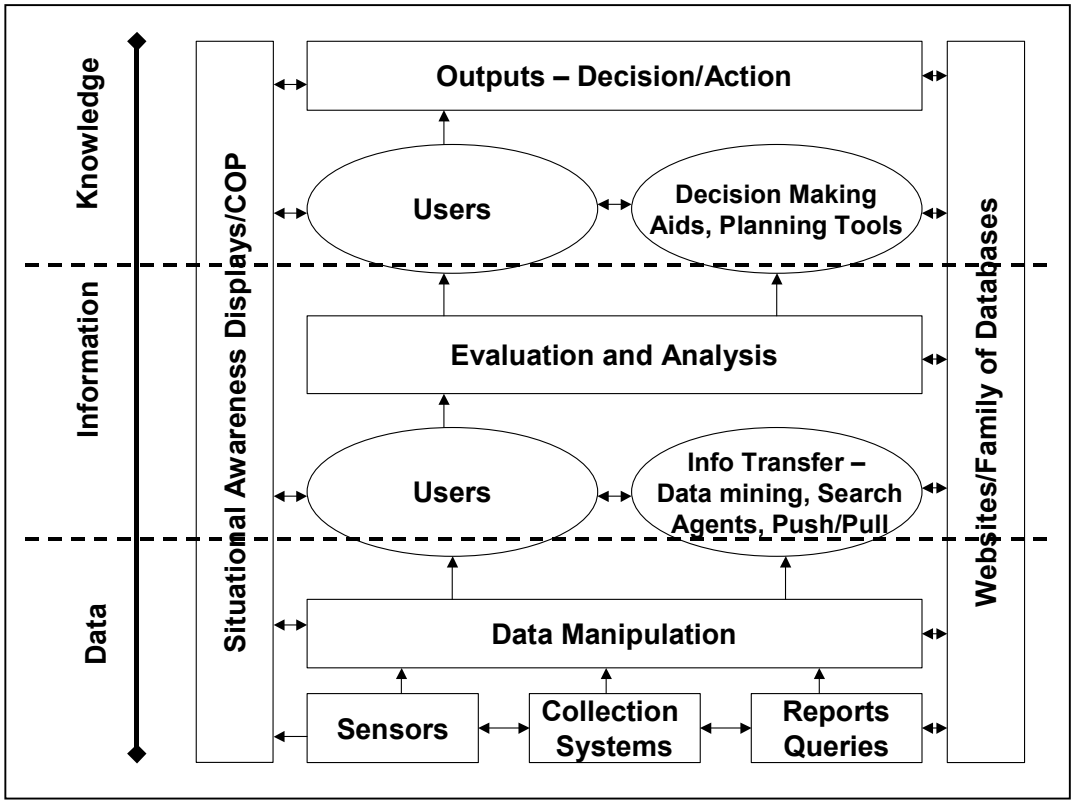

Figure 2 – Notional IM Framework

organizational structure has been set aside; as has stratification by strategic, operational and tactical levels of command; and, so to has separation by operational, administration and business practice barriers. To put the framework in context, one must accept that any person in the CF or "user" may have need for, or require access to, any information and may then be permitted to self-

[22] Department of National Defence, *Information Management Strategic Review Executive Summary*, (Ottawa: Canada Communications Group, 2002), 8.

synchronize in an all-access system protected only by need-to-know and security classification barriers.

The natural desire to critique the notional framework as being deficient or as misrepresenting chains of command must be resisted for it is offered only as an example of the total systems approach required in an IM framework. The completed IM framework will define the production and collection of all data in terms of who provides, who collects and who displays each data parcel with additional definition of how it will be stored (database) and displayed (website or other means) and disseminated. Clearly this is a daunting task and much reliance must be placed upon the environments and group principles to provide the necessary level of detail. It should also be noted that much of this infrastructure and information management detail exists but is operating in isolation. The IM framework must also address the uses and manipulation of the collected and displayed data. In this, the information stage, the data will be analyzed and evaluated. The IM framework must define how and by whom this will be done and how the fruits of their labours – the information – will be distributed and to whom. Appropriate collaborative planning tools and how they will interface with the data collection/storage systems will be introduced at this stage. In the knowledge management stage, decision-making aids, more advanced planning tools and tools for ordering and monitoring actions must be defined.

An example to illustrate the functionality of the notional IM framework is useful at this point. Deployed units, through their tactical HQs will post/report information – this can occur through networks or traditional communications paths depending on the level of sophistication. This information is then passed manually or automatically onto the network where it is seen, accessed by higher-level HQs and incorporated into the planning process. At the same time, strategic direction may be flowing down the information chain that must also be factored into the planning and decision-making process. Other critical information such as weather, intelligence and related data are available on the network for consideration. As the OODA loop continues, additional information is received, providing for constant shaping of the decision-making process. When a decision is taken, actions are ordered via the network and appropriate communications paths. As the course of action is implemented, the speed of command is realized by the rapid collection and dissemination of the results permitting the OODA cycle to continue at an accelerated pace. The rapidity of information transfer and availability permits all involved to self-synchronize in the manner proposed by Cebrowski. While this is a typical information exchange on the force employment side; consider also the reporting of a defect through both the operational

and logistical chains to simultaneously report a reduction in operational capability and initiate the repair/supply process.

Equipped with this notional IM framework and understanding thereof, it is appropriate to look at some of the processes that will enable the IM framework to serve the needs of the CF. Underlying the framework must be a comprehensive compendium or family of databases that are widely accessible with access limited only by that protection necessary to safeguard privileged information. To demonstrate the wide scope of these databases, consider the repetitive actions when conducting an in-routine. How many times has one had to various offices with an in-routine card gathering signatures in exchange for identical parcels of information – service number, rank, name? By implementing the principles of effective IM, a CF-wide database would exist that contains all personal information and thus, the only in-routine required would be transparent as one's in which one's personal data would be accessed upon posting to a new unit. This capability exists now through the PeopleSoft® database, but access to the system is significantly limited. CFB Esquimalt, for example, has new arrivals report to the Base Orderly Room, collects the information manually and then disseminates it to the offices that have need of it – simple and elegant but still not maximizing the potential efficiencies of a fully networked system and an existing database. Expand this example to include operational databases of units' readiness and logistical preparedness and the CF is well on its way towards a coherent IM strategy – the IM framework establishes a home for the data, determines who collects it, who posts it, who can access it and what is done with it and how – the simple functions of collect, display, disseminate, analyze, evaluate and decide. One approach that may work to begin the large task of integrating the CF IM system in one framework is that proposed by Johanna Ambrosio:

> [Don't build] the grand database in the sky to house all your company's knowledge. Instead, think "communities of practice," …Figure out who works together regularly because they have a job in common and then find out what they want or need to know to be more successful or to save time. Then provide that information – through databases, easy to use front-end tools and other means – so users can act on the information. …It's only knowledge if someone actually does something with it.[23]

It is necessary to discuss two of the common pitfalls of a wide-access system like NCW. These pitfalls are that of voyeuristic curiosity and micromanagement. The first was revealed

[23] Johanna Ambrosio, "Knowledge Management Mistakes," *Computerworld* Vol.34, Issue 27, 7 March 2000: 44.

during a conversation with a USN officer at US Central Command in Tampa.[24] During a particular operation in Afghanistan, a live feed was available of an especially compelling event. It was discovered after the event that virtually every person who had access to the live feed at various tactical and operational headquarters around the world, was watching the live events unfold rather than attending to their immediate duties. The inherent danger, of course, was that during the period of vulnerability/inaction, an enemy counterattack might have occurred. NCW operations do not remove the requirement for self-discipline and supervision to ensure that self-synchronization is driven by one's duties – not curiosity. Unfortunately for the voyeur, that which is most interesting is not always that which is most important. Micromanagement is familiar to all and is related closely to the issue of voyeurism. The ability to drill down into lower levels of information, often into an area of familiarity where one has previous experience, is irresistible and, at best, results in a commander becoming overwhelmed with minutia. At worst, it leaves a vacancy at a higher level of command where action and decision are required to exploit the operational advantage of speed of command. Once again, NCW operations require self-discipline to limit the occasions when self-synchronization occurs at too low a level.

The IM framework must determine if a "push" or a "pull" distribution system is appropriate for each type of information available. For example, a pull system for access to personal data necessary for an in-routine may be quite acceptable, however, the same distribution path may be inappropriate for intelligence information. Time-sensitive information must be pushed to the end user and decision makers. In today's NCW environment there is a significant chance that critical information may be missed because those who require it have been expected to demand it or worse, it has been posted to intranet sites without notification. Technology now offers smart search agents that are capable of watching databases and collections to alert users of items of interest and automatically retrieve information that meets user-defined criteria.[25] The inclusion of search agents in the IM framework to automatically bring items of interest to users' attention may alleviate the need for manual data/information forwarding.

Finally, the IM framework must govern the format of information and data. This serves two purposes – first it allows for some degree of standardization and bandwidth management but

[24] Meeting, Author and N3 Staff USCENTCOM Tampa Fla, February 2002

[25] Smart Search Agents, available from http://www.caseshare.com/technology/verity.cfm; Internet; accessed 26 April 2004.

more importantly, it ensures that the information is available to those who need it in an appropriate format. In today's NCW environment it is usually the collector or producer of the information who determines how and what will be displayed. This is often inconsistent with the expectations of those accessing the information. A prime example of this arose from an examination of commercial vessel information available to deployed ships – the shore-based database was comprehensive but of limited use to deployed ships because of its complex format and the excessive bandwidth required to access it. The ensuing discussion revealed that the database was designed for the use of the unit that compiled it and not for the deployed units.[26] Had there been an IM framework that defined the format of the database, perhaps mandating the use of a "data-driven website" that displays information from a database and thus updates all related pages automatically [27] this information rich resource would have been useful to more agencies than just the originator. The IM framework, in specifying the format of data and information storage and display, must ensure that information is available when needed by the user, in useful format and that bandwidth limits are respected.

The IM framework is the first and most important step in transitioning to an effective NCW environment in which speed of command and self-synchronization are enabled. However, in keeping with the CF priorities for transformation,[28] the IM strategy must also address training and personnel requirements necessary to

at spected.

duties to all those involved and it is the IM strategy that must define those duties (within the IM framework) and, who will perform them (based on the advice of environmental and occupation subject matter experts (SME)).[30] However, there is a need for an IM professional at each unit and organization to ensure that the IM framework is being correctly implemented and maintained. These positions will require individuals with specific skills and duties to perform effectively as the Unit IM SME. The IM SME should be responsible for network security (within the unit), database management and IM troubleshooting. This position does not necessarily include the responsibility for equipment, communications or data collection. The role of IM SME can be fulfilled by the addition of personnel to units or by current personnel through the elimination or re-allocation of existing duties. It is beyond the scope of this paper to suggest how duties should be eliminated or reallocated – that must be done in consultation with environmental SMEs. Care must be taken to appreciate that the addition of IM duties to existing workloads may detract from the effectiveness of NCW. That is not to say that a massive influx of new people will be required to implement NCW. For the most part, existing operators and supervisors will conduct data entry and analysis. Consider intelligence production – the existing Intelligence Operators (IntOp) will continue to do their jobs in the current fashion, but they will conduct their collection and display functions on the network. The intelligence analysts will conduct their evaluation by accessing the IntOps' work and publish the analysis to a web page (or whatever vehicle the IM framework defines). These existing operators will, of course, require training to complete their duties but it is anticipated that the transition to NCW will replace some previous methods of conducting day-to-day business. It must be an integral part of the IM strategy to establish the requirement for an IM SME or Information Manager to ensure that the IM framework is implemented, conduct local database management, and oversee network security. With the personnel requirements defined, the IM strategy can then define the training/retraining requirements for both the IM SME and all others involved in the NCW environment.

It will be necessary for all personnel to be trained in NCW operations. This training will need to be incorporated into core occupation training. Training must be tailored to the tasks of the individual that will be accessing or inputting information to the network. It is common in CF units today that the duties of Webmaster fall to whoever happens to have an interest in web management and that individual is often self-trained. Training in software applications and IT in general is lacking. Few people have formal keyboarding training and although many are sent on civilian courses for software applications like Microsoft Word or Excel, few receive training in

[30] *Information Management Strategic Review Executive Summary*, 12.

database management. In an NCW environment, many personnel will be required to post data to websites but few are trained to do so. One has only to surf the Internet briefly to discover a plethora of poorly managed web pages rife with errors and broken links clearly demonstrating that the ability to manage and post data to a web page while preserving the integrity of content and format is not a duty to be taken lightly. In NCW operations, this lack of appropriate training has the potential to mask critical information and confuse the decision-making process vice facilitate speed of command and self-synchronization. The ad hoc method of training and existing training shortfalls will need to be addressed to permit the benefits of NCW to be fully realized. Whereas the IM framework can mandate the use of data-driven web pages to lessen the technical proficiency required of each operator, the IM strategy must still define training baselines and skill-sets necessary for network operators and for those who will access and manipulate information.

There remain two requirements of the IM strategy – it must be able to support joint and

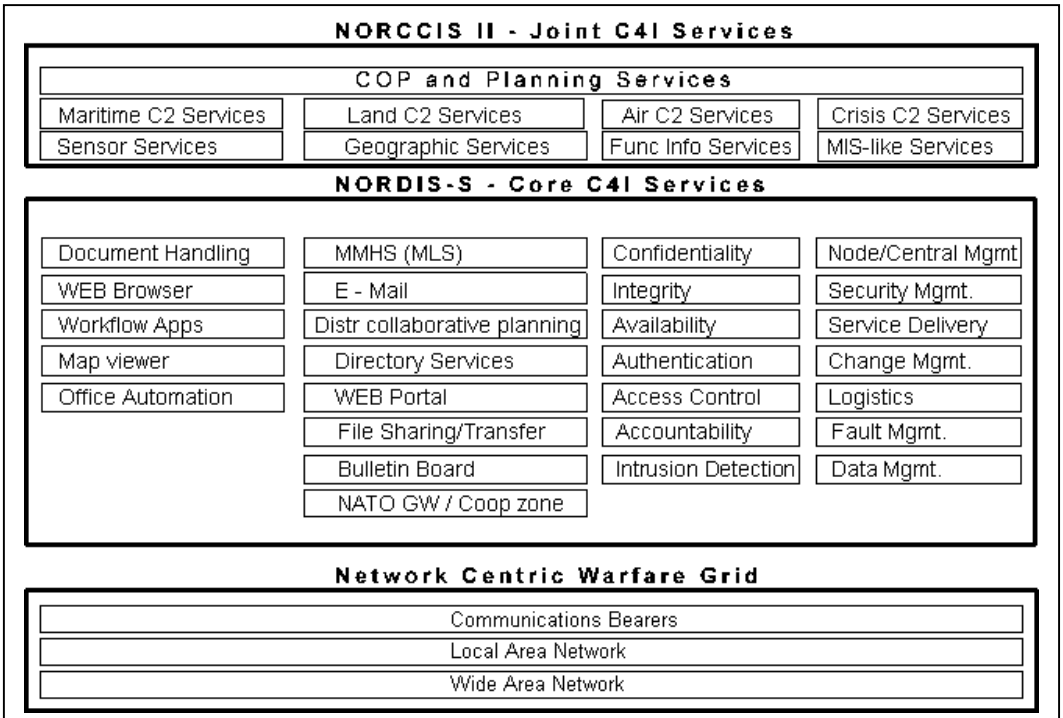

Figure 3 – NORCCIS Architecture

combined (coalition) operations. The joint operations requirement[31] is relatively easy to fulfill at

[31] Department of National Defence, *Shaping the Future of the Canadian Forces: A Strategy for 2020*, available from http://www.cds.forces.gc.ca/00native/docs/2020_e.doc; Internet; accessed 19 March 2004.

the national level since the IM framework will be CF wide. It will be important, however, to ensure that the databases, terminology and decision-making aids support each of the services without undue compromise. It may also be necessary to have specific modules that cater to particular environmental needs. The Norwegian Command and Control Information System (NORCCIS)[32] provides a good model to support joint operations. Unlike the IM framework proposed in this paper, the NORCCIS supports solely operations rather than the business functions of defence. However, the joint functions support each of the land, maritime and air environments environmental specific applications that are tied together through a common database and a common network. Mapping and COP functions are also common but can filter information by environment.[33] NORCCIS is worthy of consideration for inclusion into a Canadian NCW initiative to meet the joint operations support requirement.

The combined capability will be more difficult to achieve since a combined force often consists of a wide variety of allies with varying capabilities in NCW. Consider the differences between NATO, AUSCANUKUS, and Global War on Terrorism (GWOT) operations. In addition to the obvious technical problem of incompatibility, coalition operations are also hampered by the release of information restrictions between allies.[34] To address these issues, it is necessary to define the country with whom Canada wishes to be most closely aligned in terms of NCW capability. Integration with the US is the Canadian desired end-state[35] since the US is likely to remain the driving force in NCW for the foreseeable future and, operations in which Canada participates will most likely include the US. Therefore, to address the technical issue, Canada must ensure that when choosing the components of the NCW environment (software applications, databases, etc) that they are the same as those used by the US or, at the very least, transparently interoperable. The security issue is more complicated to address due to the sensitivities of information exchange and, as a result, may be the ultimate hurdle that defines coalition

---

[32] Norwegian Command and Control Information System, available from http://www.teleplan.no/products/software/quick_summary/command_and_control/c4is_net_prod_20030506.pdf; Internet; accessed 27 April 2004.

[33] Norwegian Command and Control Information System: Joint Command and Control Services, available from http://www.c2is.net/norccis/jointc2.html; Internet; accessed 27 April 2004.

[34] Mitchell, *Small Navies and Network-Centric Warfare*…, 88.

[35] *Shaping the Future of the Canadian Forces: A Strategy for 2020*.

interoperability.[36] Although both Canadian and US national classified networks have some rudimentary interoperability with the coalition network (COWAN), it is functionally limited to web site replication (Canada) and an email capability with email attachments being prohibited (US). The technology exists to support a more robust interface as proven with the NORCCIS,[37] however, the national authorities of both the US and Canada have yet to approve these technologies due to security concerns. This reticence must be overcome on both sides of the border to establish a CANUS NCW link. It is inadvisable to cater to the least NCW capable potential coalition partner because that may reduce the network classification to little more than an unclassified level. The technologies employed by NORCCIS may also permit a NATO or AUSCANUKUS interoperability. Therefore, it may be concluded that the technologies exist to establish a common NCW environment supportive of joint and combined operations and that only national security barriers remain. Interoperability with the US will put Canada at the forefront of NCW operations with other allies aspiring to that standard. The IM strategy should define the combined operations standard as interoperability with the US; and, that system, when integrated with a CF-wide system that facilities joint Canadian operations, should result in a joint interoperability with US forces that will meet or exceed the existing NCW capabilities of all other allies.

The current state of IM in the CF is below the standard required to support NCW operations. This has been noted in the IM Strategic Review Tiger Team Report of April 2002[38]. This paper has proposed some solutions to the current deficiencies by expanding upon the need for a coherent IM strategy that addresses the need for a CF wide IM framework, trained personnel and dedicated IM personnel. These observations have been explored in some detail to propose solutions that will meet the needs of the CF and enable the transformation envisaged by the CDS.[39]

In particular, there is an immediate need for a comprehensive IM framework that will support the operational and business functions of the CF in a NCW environment. The IM

---

[36] Mitchell, *Small Navies and Network-Centric Warfare*…, 89

[37] Norwegian Command and Control Information System: Core and Cross Domain Services, available from http://www.c2is.net/Core%20and%20Cross%20Domain%20Services%20Briefing.pdf; Internet; accessed 27 April 2004.

[38] *Information Management Strategic Review Executive Summary*, 12.

[39] *Chief of Defence Staff Annual Report 2002-2003*, II-III.

framework must include provisions to support data management, information management and knowledge management through databases, websites, and communications in addition to situational awareness displays, collaborative planning tools and decision-making aids. The integration of these functions into the IM framework will support the cornerstones of NCW – speed of command and self-synchronization – by providing an environment where information can be collected, displayed, analyzed, evaluated and disseminated. The IM framework must define how data is to be displayed and accessed including database and search agent requirements. The "push or pull" access to information is critical to ensure that information is available to those that require it in a timely fashion. It is only through the creation of this comprehensive IM framework that the personnel and training requirements will be revealed. The personnel requirements may indicate a need for additional, dedicated IM SMEs to be employed in each unit to execute the duties of network security, database management, network troubleshooting and Information Manager. Consultation with environmental representatives will be required to determine the best way of fulfilling the new duties. The training requirements to meet the objectives of the new IM framework will include both the training of the IM SMEs and all others who will use the network. These training requirements will be derived from the IM framework and will need to be incorporated into the core training of all occupations.

NCW changes the environment in which the military operates from a platform-based advantage to an operational advantage based upon information superiority where battlespace awareness and the collection, display, evaluation and analysis of data and information permits decision-making and actions to be undertaken with rapidity that overwhelms the enemy. This is the principle of speed of command and it can only be achieved in an environment where information is available to all in the decision-making cycle in order to permit self-synchronization. As this paper has proven, the CF will only be able to realize the operational advantage of a network-centric environment when a comprehensive Information Management strategy has been implemented to ensure that training, procedures and equipment support the goals of warfare management in a network-centric environment.

> *0130 – (Yawn) Boy am I tired. Soon be time for bed. Jut press send on this last email and log off my MCOIN, COWAN and DWAN accounts. I should just have time to log onto the Internet and send a quick email home then into bed.*
> *0155 –Done – oops got to shut off that stand-alone computer…that screen will keep me awake all night.*

Appendix One

Key Definitions

MCOIN III – Maritime Command Operational Information Network

- Interface with the national system Titan.
- Classified to CANUS level.
- Web, chat, database and email capability.
- Display the COP via C2PC.
- Display COWAN web pages only.

SIPRNET – Secret Internet Protocol Router Network

- US Joint Command and Control Network
- Secret US-only classification
- Interface with COWAN (air-gapped, Web and email without attachments)
- Chat, web, database, COP and collaborative planning tools

COWAN – Coalition Wide Area Network

- Interface with MCOIN (Web pages only) and US SIPRNET (Web pages and Email without attachments)
- Various subsystems and classifications (AUSCANUKUS, US-Japan, GWOT)
- Web, chat, database and email capability

DWAN – Defence Wide Area Network

- Interfaces with Internet
- Unclassified (up to Protected B permitted with secure card)
- Web, chat and email capability
- Largely administrative system
- No interface with classified systems

GCCS – Global Command and Control System

- US modular C2 system that interfaces with SIPRNET
- Canada has partial system in stand-alone format (limited by fewer modules)
- Message passing capability
- COP
- Modular Tactical and Strategic planning tools

C2PC – Command and Control Personal Computer

- Software application that interfaces with systems like GCCS to display COP
- Fitted on select MCOIN III terminals
- Varying levels of client participation (view only, read/write privileges)
- Planning tools and tactical displays

NORCCIS – Norwegian Command and Control Information System

- Joint C2 System with application packages to serve component commands
- Layered security classification
- GIS, message handling, parsing applications
- NATO trials ongoing

TITAN – Secret part of Canadian Joint Command and Control Information System (JC2IS)

- Top Secret part is SPARTAN
- No unclassified part
- Similar to MCOIN
- Partial interface with MCOIN
- Messaging, chat, email, COP and Web capable
- Intent was to have interface (tunneled) with DWAN (not yet implemented)
- Largely operations and operations admin oriented

CANMARNET – Canadian Maritime Network

- DND led network to link Coast Guard, RCMP, CCRA, Immigration and DFO
- East Coast only
- Unclassified
- Database Oriented – Vessel location, name and amplifying information only
- Very limited in utility but is only common system between federal departments

VOIP – Voice over Internet Protocol

- Telephone system using Internet or Intranet as transmission medium
- Poor quality from VOIP to traditional telephones
- Very good on VOIP to VOIP connection
- Significant bandwidth requirement
- Burgeoning technology
- Unclassified but can be classified through bulk encryption (mil or civil std)

Tactical Data Link – Digital data transfer of tactical information

- Transfer of Tactical information including contacts, engagement orders and amplifying information
- Interfaces with Strategic and IP based systems
- Several different protocols exist (LINK 11 – aging technology, LINK 16 US/Cdn Link, LINK 22 – evolving NATO LINK standard)
- Gateway capable between LINK protocols but some data is sacrificed in translation

PeopleSoft® - Commercial Human Resource Management Software

- Used by DND to record and manage personnel data
- Limited read/write authority to preserve database integrity and privacy
- Habitually out of date
- Poorly understood and managed

Data-Driven Websites

- Website displays information from linked database(s)
- Web pages are not static – i.e. information is not resident on web page
- When Web page is loaded, database is polled for information, then displayed
- When database is changed, each linked web page will access updated information
- Emerging commercial technology
- Essential for large websites

Smart Search Agents

- Evolved search engine
- Data and text mining
- Variable and topic weighting
- Combines several search technologies (Boolean, proximity, natural language, fuzzy, etc)
- “Watch-dog” technology – agent watches document/database collection and brings forward user-specified information

Appendix Two

Data, Information and Knowledge Management

There is much discussion currently about the difference between data, information and knowledge. It is important to realize that the term "knowledge" refers to evaluated information that is managed by knowledge where knowledge is defined as the human understanding of procedures, doctrine and military experience. The term "information" refers to the collection, display, and analysis of raw data. Data is a collection of facts and inputs to the information system. Clarity of this differentiation is provided by the following definitions:

> Wiig defines information as facts and data organized to characterize a particular situation and knowledge as a set of truths and beliefs, perspectives and concepts, judgments and expectations, methodologies and know-how.[40] Therefore, information can be seen as data made meaningful by being put into a context and knowledge as data [information] made meaningful through a set of beliefs about the causal relationships between actions and their probable consequences, gained through either inference or experience.[41]

To put this in a military context, consider a platoon of enemy troops observed moving toward one's own position while another platoon is observed moving towards the flank. When combined with an intelligence officer's assessment that it is the enemy's standard procedure to feign a frontal attack while intending a flanking manoeuvre, this observed troop movement becomes information. This information, when presented to command becomes knowledge when a commander assesses, based on his experience and knowledge, that the enemy will make a determined attack on his flank within the next X hours and orders own forces re-oriented in sufficient numbers to repel a platoon sized attack. The importance of data, information and knowledge in developing the IM framework is to ensure that data and information are formatted to support analysis, evaluation, dissemination and decision-making.

---

[40] K.M. Wiig, "Introducing Knowledge Management into the Enterprise," in *Knowledge Management Handbook*, ed. J. Liebowitz (NY: CRC Press, 1999): 3.1-3.41. As quoted in *Understanding Knowledge Management and Information Management: the need of an Empirical Perspective*, France Bouthillier and Kathleen Shearer, available from http://information.net/ir/8-1/paper141.html; Internet; accessed 6 March 2004.

[41] K D. Mitchell, "Knowledge Management: The Next Big Thing." *Public Manager*, Vol. 29 (2) 2000, 57-60. As quoted in *Understanding Knowledge Management and Information Management: the need of an Empirical Perspective*, France Bouthillier and Kathleen Shearer, available from http://information.net/ir/8-1/paper141.html; Internet; accessed 6 March 2004.

Bibliography

Australia. Department of Defence. *AF2025 - Information Operations: A new War-fighting Capability*. Available from http://www.au.af.mil/au/2025/volume3/chap02/v3c2-2.htm; Internet; accessed 19 March 2004.

Alberts, David S. John J. Garstka and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd ed. (Washington, DC: CCRP Publication Series, 2000), 201-202.

Ambrosio, Johanna. "Knowledge Management Mistakes." *Computerworld* Vol.34, Issue 27, 7 March 2000.

Boyd, Col. John. "Patterns of Conflict." Available from http://www.mindsim.com/MindSim/Corporate/OODA.html; Internet; accessed 19 March 2004.

Canada. Department of National Defence. *DAOD 6000: Information Management*. Available from http://www.dnd.ca/admfincs/subjects/daod/6000/0_e.asp; Internet; accessed 30 January 2004.

Canada. Department of National Defence. *Defence Plan Online*, Article 307. Available from http://www.vcds.forces.gc.ca/dponline/main_e.asp; Internet; accessed 30 January 2004.

Canada. Department of National Defence. *Information Management Strategic Review Executive Summary*. Ottawa: Canada Communications Group, 2002.

Canada. Department of National Defence. *Shaping the Future of the Canadian Forces: A Strategy for 2020*. Available from http://www.cds.forces.gc.ca/00native/docs/2020_e.doc; Internet; accessed 19 March 2004.

Canada. Department of National Defence. *A Time for Transformation: Annual Report of the Chief of Defence Staff 2002-2003*. Available from http://www.cds.forces.gc.ca/00native/pdf/CDS-R2003_e.pdf; Internet; accessed 19 March 2004.

Cebrowski, VAdm (USN) Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." *Naval Institute Proceedings Magazine*, (January 1998). Journal on-line; available from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; Internet; accessed 29 February 2004.

Data-Driven Websites. Available from http://www.caseshare.com/technology/extranets.cfm; Internet; accessed 26 April 2004.

Gibson, Timothy J. "Rapid Preparation and Distribution of Battlefield Information." in *The First Information War*, ed. Alan D. Campen, (Fairfax, VA: AFCEA International Press, 1992).

Lefebvre, Stephane, Michel Fortmann and Thierry Gongora. "The RMA: Its Implications for Doctrine and Force Development Within the US Army" in *Operational Art:*

Development in the Theories of War, ed. B.J.C. McKercher and Michael A. Hennessy (Westport, CT: Praeger Publishers, 1996), 173.

Mitchell, Paul T. "Small Navies and Network-Centric Warfare: Is There a Role?" *Naval War College Review*, Vol. LVL, No 2 (Spring 2000).

Mitchell, K D. "Knowledge Management: The Next Big Thing." *Public Manager*, Vol. 29 (2) 2000, 57-60. As quoted in *Understanding Knowledge Management and Information Management: the need of an Empirical Perspective.* France Bouthillier and Kathleen Shearer. Available from http://information.net/ir/8-1/paper141.html; Internet; accessed 6 March 2004.

Moore's Law. Available from http://www.webopedia.com/TERM/M/Moores_Law.html; Internet; accessed 19 March 2004.

Norwegian Command and Control Information System: Core and Cross Domain Services. Available from http://www.c2is.net/Core%20and%20Cross%20Domain%20Services%20Briefing.pdf; Internet; accessed 27 April 2004.

Norwegian Command and Control Information System: Joint Command and Control Services. Available from http://www.c2is.net/norccis/jointc2.html; Internet; accessed 27 April 2004.

Norwegian Command and Control Information System – Summary. Available from http://www.teleplan.no/products/software/quick_summary/command_and_control/c4is_net_prod_20030506.pdf; Internet; accessed 27 April 2004.

Richter, Andrew. *The RMA and Its Impact on Canada: The Challenge and the Consequences.* Working Paper 28 (Vancouver: Institute of International Relations, University of British Columbia, 1999), 9-11.

Robertson, Hugh. *Future Direction for IM in DND/CF.* Presentation on the IM Strategic Review. Available from http://img.mil.ca/DGIMSD/IMSR/index_e.htm; Intranet; accessed 7 March 2004.

Smart Search Agents. Available from http://www.caseshare.com/technology/verity.cfm; Internet; accessed 26 April 2004.

Wiig, K.M. "Introducing Knowledge Management into the Enterprise." In *Knowledge Management Handbook*, ed. J. Liebowitz (NY: CRC Press, 1999): 3.1-3.41. As quoted in *Understanding Knowledge Management and Information Management: the need of an Empirical Perspective*. France Bouthillier and Kathleeen Shearer. Available from http://information.net/ir/8-1/paper141.html; Internet; accessed 6 March 2004.