



FUTURE NETWORKS

The development of a future network capability is a complex evolution toward emerging information systems technology that will increasingly empower people, organizations and processes. It must be reiterated, however, that command is and remains a human endeavour, and consequently the first and foremost requirement of any future network will be to facilitate better human performance and interaction. The Canadian Army will constantly strive to become increasingly network enabled, capable of exchanging information laterally and vertically between sensors, weapons, vehicles and command and control nodes, so that the right person can access the right information at the right time. Properly implemented, future network-enabled operations will involve a community of soldiers and supporting elements on the ground supported by joint sensor, fire support, and command and control systems linked by voice and data to create a level of improved situational awareness, battlefield mobility and fire support that will combine to overwhelm the adversary's understanding of the battlespace and his ability to react within it.

The future network capability, while aiming to empower commanders, must enable faster soldier decision cycles, encourage decisions to be made at the lowest appropriate level, and allow soldiers and commanders to recognize and capitalize on opportunities as they arise. Significant goals for the future network include improved reach, or an expansion of the audience; improved range, particularly on the move; improved information management, with an emphasis on analyzing the vast quantities of collected data and information; and improved collaboration between any users. The success of the Canadian Army of Tomorrow in the conduct of adaptive dispersed operations will be underpinned by the delivery of a robust future network.

CANADIAN ARMY LAND WARFARE CENTRE

The Canadian Army Land Warfare Centre serves as the army's intellectual foundation for the development of overarching concepts and capability definition for tomorrow and into the future. It is responsible for the delivery of concepts-based, capabilities driven, force structure design tenets and specifications, the development of the army's concept development and experimentation plan, serving as a focal point for connection with other warfare centers, government departments, partner nations, and external agencies and academia, and the delivery of high quality research and publication in support of the Canadian Army's force development objectives.



Future Networks: A Concept for the Army of Tomorrow



FUTURE NETWORKS

A CONCEPT FOR THE ARMY OF TOMORROW

CALWC



FUTURE NETWORKS: A CONCEPT FOR THE ARMY OF TOMORROW





**THE NETWORK:
A CONCEPT FOR THE ARMY OF TOMORROW**

Canadian Army Land Warfare Centre
Kingston, Ontario, 2013

Publication Data

Designing Canada's Army of Tomorrow

English

IDDN—NDID B-GL-007-000/JP-005

French

IDDN—NDID B-GL-007-000/JP-006

Print—English

GC Catalogue Number—D2-327/2013E

ISBN—978-1-100-23023-8

Print—French

GC Catalogue Number—D2-327/2013F

ISBN—978-0-660-21574-7

Online—English

GC Catalogue Number—D2-327/2013E-PDF

ISBN—978-1-100-23024-5

Online—French

GC Catalogue Number—D2-327/2013F-PDF

ISBN—978-0-660-21575-4

This official publication is published on the authority of the Commander Canadian Army. No part may be reproduced or republished elsewhere without the express permission of the Director Land Concepts and Designs through the Department of National Defence.

© 2013 Department of National Defence

Design & Layout: Army Publishing Office, Kingston, Ontario  **BEAT**

All photography © Combat Camera



NOTICE

This documentation has been reviewed by the technical authority and does not contain controlled goods. Disclosure notices and handling instructions originally received with the document shall continue to apply.

AVIS

Cette documentation a été révisée par l'autorité technique et ne contient pas de marchandises contrôlées. Les avis de divulgation et les instructions de manutention reçues originalement doivent continuer de s'appliquer.





FUTURE NETWORKS: A CONCEPT FOR THE ARMY OF TOMORROW



CANADIAN ARMY LAND WARFARE CENTRE
KINGSTON







TABLE OF CONTENTS

Table of Contents	5
PART 1 – Introduction	7
Constraints/Restrains	9
PART 2 – The Future Technological Environment	10
Technology-Induced Societal Change	15
Military Technology Change	17
Human Factor Implications	18
PART 3 – Network-Enabled Operations and Networks	22
A Simplified Explanation of Network-Enabled Operations	22
Opportunities and Risks	27
What is a Network?	36
A Taxonomy of Network Functions	40
What Kind of Information?	43
Information Presentation	44
Conclusion	45
PART 4 – Command and The Network in ADO	46
Enduring Tenets of Command	46
The Human in Command	48
The Network in ADO	50
Summary	54
PART 5 – Overarching Network Capability Objectives	55
General Goals	55
Specific Network Objectives	59
User Segments	67
Other Objectives	72
End State	73
PART 6 – Recommendations and Conclusions	74
Appendix 1 – Review of Network-Enabled Operations Documents	75
Appendix 2 – Abbreviations	77
Appendix 3 – Glossary	79
Primary Source	83
Secondary Sources	85







“On the first of February 2003, a space shuttle falls out of the sky. Within 90 minutes, we had to set up a critical information exchange environment with 15 organizations that we had not even so much as made a phone call to. What elements of planning can you do when you don’t even know who your partners are on an event-driven basis? You have to figure out how to dynamically create trusted information exchange environments, dynamically merge them, and have them go away when no longer required.”

—MAJOR GENERAL DALE W. MEYERROSE¹

PART 1 – INTRODUCTION

As a result of a history of separate “stovepiped” projects delivering capabilities in the absence of a coherent network strategy, the Army has seen a steady introduction of often incompatible networking capabilities. Thus formation headquarters, manoeuvre units and base/garrison sites have seen the introduction of networked capabilities delivered under different mandates, largely unable to exchange information with each other and failing to deliver seamless information-sharing between and within operational and tactical commanders. As a result, the Army is faced with a situation where Army simulators do not easily exchange information with tactical Battle Command Systems, which in turn are unable to exchange information with baseline office applications. Indeed, to date, the Canadian Army network capabilities may be described as enclaves of networks characterized by poor information exchanges and connectivity (incompatible data formats, high latency, low bandwidth, and limited ranges) between those enclaves. That means that although there exist sufficient network resources within a combat team or battle group for the element to conduct its primary tasks, it is hampered by the quite limited means to exchange or access information stored in any other organization than itself.

Recent operations and contemporary research illustrate that a force is far more effective when information necessary to the decision-making process is made available to the right person at the right time.² Indeed, the sheer amount of information available to commanders and the requirement to be accountable (and, in some cases, personally liable) for it is driving a need to be able to not only manage the volume but also to sift it for relevancy and deliver high confidence in

1. Meyerrose, Major General D.W., Statement to Joint Warrior Interoperability Demonstration (JWID) final planning conference at Chesapeake, V.A. 30 March 2004. Quoted in Bubbers, L. “Transforming Homeland Defence Through Network Centric Operation,” IBM Business Consulting Services, April 2005.

2. Alberts, D., “Power to the Edge.” www.dodccrp.org/publications/pdf/Alberts_Power.pdf



the accuracy of that information. As a consequence of the ability of current and evolving technology to deliver increasing volumes of information, the provision of robust networked capabilities between commanders, soldiers, sensors and weapons is envisioned as a core component of the Future Land Combat System (FLCS). Connecting decision makers to information sources and weapons will require a flexible approach to information sharing and a careful study of the cognitive stresses implied in managing the resulting volume of information. What differentiates the FNC from a typical commercial network is the nature of the environment in which it must operate, and the potentially lethal consequences for soldiers if it fails. The FNC must therefore be designed to facilitate military operations, endure under extreme environments and be capable of adapting to rapidly changing situations, reflecting the mobile and ad hoc nature of combat operations.

The goal of the FNC is to deliver a networked capability nested within a comprehensive CA C4ISR strategy,³ fielded within the Canadian Army at the formation level and below, delivering relevant, effective information and decision support to deployed forces. It aims to enable land tactical operations by providing an evolving, sustainable, fully secure, integrated and interoperable network capability that is flexible to the needs of the land operations community. The FNC will be a coherent package of information, hardware (networked sensors, weapons platforms), software (e.g., decision support tools) and people (decision makers, staffs and soldiers), all aimed at delivering an integrated, seamless capability.

Given the multitude of end-user requirements, the diversity of software applications, the rapid pace of technological change and the demand for flexibility, and faced with a dynamic adaptive adversary situated within a complex operational environment, no one system will likely be able to satisfy all of the requirements that encompass the FNC. Accordingly, this capability is envisioned to be a system of systems (SoS) comprised of a mix of complementary capabilities delivered variably to the appropriate Canadian Army users. Indeed, this paper will not define the perfect mix of capability, as it will necessarily be delivered incrementally and be derived and evolve from the technology available at the time of definition. There are too many factors to be able to state categorically that the recommended capabilities will satisfy all interests. Therefore, this paper recommends optimal capabilities to meet most of the considerations while retaining flexibility and adaptability.

This FNC paper does not investigate the full details of life cycle management, equipment distribution levels or training methodologies. These issues are not driven primarily by operational considerations but instead by fiscal restraints, management

3. CA C4ISR Strategy (DLCI) promulgated spring 2011.

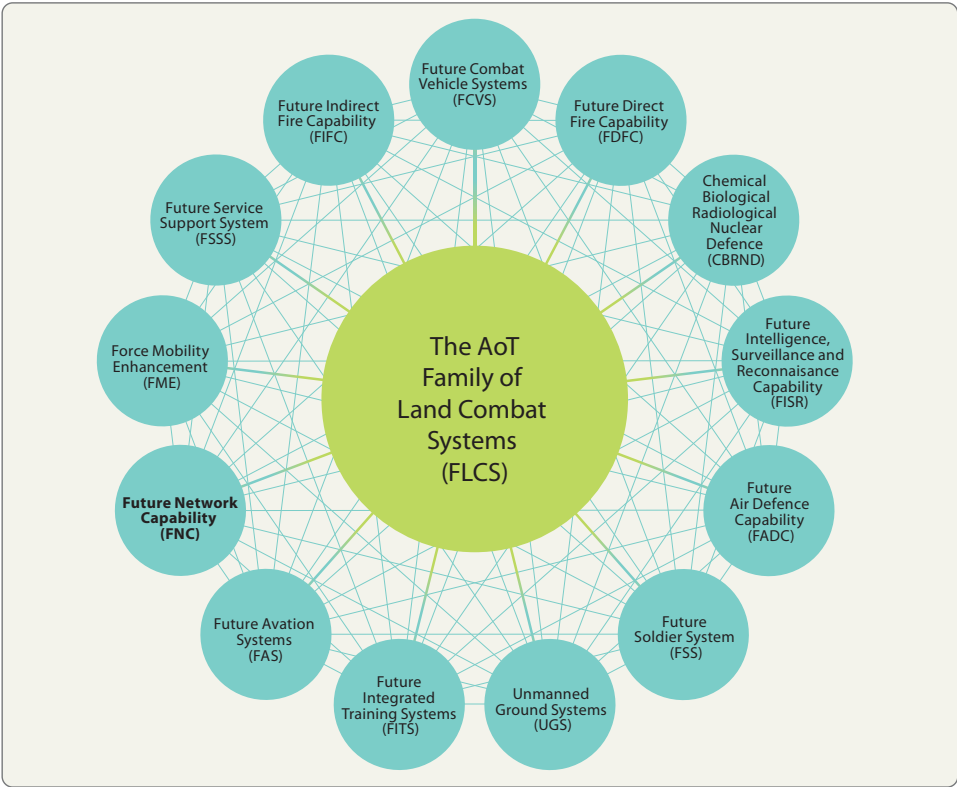


Figure 1: The Family of Land Combat Systems⁴

practices and learning requirements, and they merit special investigations by follow-on studies conducted by the responsible directorates.

CONSTRAINTS/RESTRAINTS

The FNC paper does not fully investigate the supporting communications infrastructure or bearer system required to support the capabilities and features desired of FNC. However, inferences applicable to changes in characteristics applicable to the bearer system may be drawn from the discussion of capability requirements. In addition, this paper does not concern itself with the human dimension within the network, especially possible changes to command and control processes necessary to realize the potential of an FNC within ADO, except to note that there are as yet poorly understood aspects to the cognitive domain that may arise as a result of the introduction of a near exponential increase in the volume of information and of networked devices in the military environment.

4. The Family of Land Combat Systems (FLCS) has evolved and will continue to do so over time.

PART 2 – THE FUTURE TECHNOLOGICAL ENVIRONMENT⁵

Throughout history, warfare has been profoundly altered by science and technology.⁶ Improvements in weaponry have yielded increases in accuracy and lethality, altering the way wars have been fought thereafter. The same trends are recognizable today—increasing accuracy, range, firepower, lethality, technological disparities, information-technology-enabled command and control, and troop dispersal. Each of these trends will be subject to frictions that may slow or change the course of developments. It is highly probable that legislators and regulators will likely be challenged to keep pace with the rate of change in science and technology (S&T) development. Moreover, it is expected that the technological advantage held by developed nations will decrease rapidly as technology flows to underdeveloped nations and non-state actors, including to potential adversaries. With those caveats in mind, it is fairly evident that three⁷ technology trends wield significant influence in driving change out to 2020: information and communication technologies (ICTs), biotechnologies, and energy and environmental technologies.

Computing. For the past several decades, escalating computing power has driven the growth of the information age, which has resulted in a concurrent democratization of information access and sharing as costs have plummeted even as computing capability has increased dramatically. The result of this remarkably consistent growth is that a personal computer with equivalent performance to the most advanced supercomputer of 1991⁸ can be purchased today for one ten-thousandth of the cost. The computing power of these widely available machines makes it possible to conduct such high fidelity simulations that they permit the simulation of events or phenomena that we could not even begin to attempt in the real “physical” world. This in turn means that the power of supercomputers can be harnessed into smart simulation tools, allowing plans to be rehearsed prior to committing forces. New modes of data manipulation that encourage more effective

5. Part 2, The Future Technical Environment, is an adaptation of Chapter 2, “Emerging Global Technologies and Trends” of “Towards Land Operations 2021: Studies in Support of the Army of Tomorrow Force Employment Concept” (Godfroy and Gisewski).

6. Science is defined as any system of knowledge that is concerned with the physical world and its phenomena and that entails unbiased observations and systematic experimentation. See www.britannica.com/eb/article-9066286/science.

Technology is the application of scientific knowledge to the practical aims of human life or to the change and manipulation of the human environment. Technology thus comprises machinery and equipment based on scientific knowledge and, in the military context, developed specifically for the purpose of fighting. See www.britannica.com/eb/article-9110174/military-technology.

7. According to the Canadian National Research Council (NRC) Renewal Futures Team www.nrc-cnrc.gc.ca/aboutUs/ren/nrc-foresight_e.html.

8. www.openfabrics.org/archives/aug2005datacenter/W8.pdf (slide 7).



access to digitized information will be enabled through simultaneous multi-touch interfaces, haptic⁹ devices and motion sensing controllers.¹⁰ Such multi-touch devices introduce possibilities such as interactive walls and tabletops, which are ideally suited to command and control information system displays in formation and unit headquarters. Similarly, the computational power available is being harnessed to solve tactical edge communications problems, yielding a generation of cognitive software defined radios¹¹ and thus allowing for a network of self-healing and ad hoc communications networks on the battlefield. Finally services such as “cloud computing” include the proliferation of Internet-hosted storage and retrieval from across multiple devices and platforms, offering an improved capability for people to connect (including social networking). What is perhaps unrecognized by military planners is that this increase in processing power has become readily available to both state and non-state actors, some of whom will undoubtedly harness the computing ability to pursue actions and activities harmful to the interests of Canada.

Artificial Intelligence. Artificial intelligence (AI) research has experienced a resurgence in activity as a result of the progress made in ICT. As AI systems achieve greater levels of ability, they may increasingly replace or augment functions and procedures that were once the sole purview of humans, such as, for example, managing a power grid¹² or guiding missiles or satellites and assembling other machines.¹³

At some point, military AI will reach a threshold of ability that threatens to cross moral, ethical and/or legal boundaries. An autonomous system that is able to make life and death decisions within chaotic or dynamic environments is not unimaginable. Given recent progress in AI and the likelihood that it will reach a point of sophistication that challenges human abilities in broad areas, *it is prudent for those within capability development organizations to be mindful of the moral, ethical and legal ramifications of AI-related development decisions.*

Robotics. The Robotics is on the verge of becoming the next major commodity technology, perhaps surpassing the computer in importance.¹⁴ The US Department of Defense (DoD) appears to think so; in 2000 the US Congress mandated that a third of military ground vehicles and a third of deep-strike aircraft must become

9. A haptic interface is a device that allows a user to interact with a computer by receiving tactile feedback. See <http://wii.nintendo.com/controller.jsp>.

10. <http://cs.nyu.edu/~jhan/ftirtouch/>.

11. Cognitive radios analyze the radio environment to decide the best spectral band and protocol to reach whatever base station they need to communicate with, at the lowest level of power consumption.

12. <http://www.scientificcomputing.com>.

13. <http://www.kurzweilai.net/meme/frame.html?main=/articles/art0637.html>.

14. <http://www.sciam.com>.



robotic within a decade. A 2006 Australian¹⁵ paper concluded that, in strategic terms, robotics has passed the point of being a new strategic threat to being one that broadens the threat at the operational and tactical level. Robots, including unmanned ground vehicles (UGVs), are well suited to perform routine and boring tasks. They are fearless and tireless. They perform repetitive tasks with speed and precision. They can be designed to avoid or withstand enemy armaments and to perform specific military functions. Most importantly, robots can reduce casualties by increasing the combat effectiveness of soldiers on the battlefield.¹⁶ Furthermore, as robotic vehicles enter service by 2021, they could draw fire or spot targets, allowing legacy systems to engage and dominate while not having superior firepower or armour.

Deriving inspiration from the behaviour of ant colonies, researchers are achieving success with reconfigurable, biologically-inspired robots modeled on insect behaviour, producing swarm¹⁷ robots in which there is no central “control centre” directing the activity. Instead, the collective and adaptive behaviour emerges spontaneously without the need for sophisticated decision-making software. Efficient and robust¹⁸ against mechanical failure, such insect-like craft could fly unobtrusively around buildings, moving into open windows. When equipped with different sensor types, they may provide a better way of monitoring remote or inhospitable habitats.

Maturing at an accelerating pace, commercially available unmanned aerial vehicles (UAVs) are reaching the market with increasing frequency and with impressive performance specifications, achieving about 50% of the speed, range and endurance of much more expensive military spec UAVs.¹⁹ Fitted out with quiet electric drives and onboard video, it is now feasible for belligerents to use such systems for covert surveillance and target detection.

Virtual Reality and 3D Modelling. An area that is revealing a potentially radical effect on military planning is the application of virtual reality (VR) and three dimensional (3D) modelling augmented with near real time updates of changes to the actual environment. Thus sensors could easily “add” new objects or features immediately as they are observed, adding richness to the “known”

15. Hew, Patrick Chisan, “The Generation of Situational Awareness within Autonomous Systems – Near to Mid Term Study – Issues,” Australian DoD, Defence Science and Technology Organization, DSTO-GD-0467, Edinburgh South Australia 5111 Australia, July 2006. <http://dSPACE.dsto.defence.gov.au/dSPACE/handle/1947/4560>.

16. Technology Development for Army Unmanned Ground Vehicles, Committee on Army Unmanned Ground Vehicle Technology, Board on Army Science and Technology, Division on Engineering and Physical Sciences, National Research Council of the National Academies, The National Academies Press, Washington, D.C. Copyright 2002 by the National Academies Press, http://books.nap.edu/openbook.php?record_id=10592&page=13.

17. Swarm robotics: a collection of many small and cheap robotic units can act as an autonomous entity.

18. <http://www.sigmascan.org/ViewIssue.aspx?Issued=302>.

19. <http://www.rctoys.com/rc-toys-and-parts/DF-TANGORC/INDUSTRIAL.html>.



Figure 2: Big Dog Robotic Mule²⁰

environment, assisting, for example, near real time threat warning. Adding haptic resistance feedback interfaces will further enhance the experience by introducing a way to reduce fatigue.

At the opposite end of the same technological spectrum lies “embodied virtuality,” which has been described as the process of drawing computers out of their electronic shells, miniaturizing them, and placing them in everything—cars, buildings, appliances and human bodies. The likely outcome of this pervasive computing environment is the ability to create augmented reality (AR). The implications for military training establishments involve possibilities to deliver immersive education and training to anyone, regardless of time or location. Already, augmented reality gamers are turning the real world into virtual battle zones using existing technologies such as GPS and web-enabled cell phones.²¹ Those examples reveal the powerful potential of a fully network-enabled force—i.e., one that has communications, computation and location-based services,²² possibly all embedded into a single wearable device.

20. <http://www.bostondynamics.com/>.

21. <http://www.newscientist.com/article.ns?id=mg18625036.200>.

22. A location-based service (LBS) is an information and entertainment service, accessible with mobile devices through the mobile network and capitalizing on the ability to make use of the geographical position of the mobile device.





Biotechnology. Many of the same growth trends are evident in the realm of biology. Indeed, ICT has revolutionized the study of biology, making it, in essence, an information technology subject to similar exponential growth and accelerating return.

Despite early resistance, some researchers foresee a rapidly approaching era where biology hacking becomes commonplace, thus potentially amplifying the threat of bio hazard situations. New generations of sophisticated tools have resulted in research labs disposing of their “old” hardware at discount rates. This discounted equipment may easily find its way into the hands of criminal or terrorist organizations, thereby enabling a proliferation of bio-related threats. If insurgent groups succeed in harnessing the full disruptive potential of synthetic biology, our present capability development efforts—which in large measure rely upon kinetic energy weapons—may become irrelevant.

The biotechnology revolution holds equally important implications for the human dimension. For example, progress is being made towards understanding and manipulating the genetic basis of the fear response. While it is not unreasonable to think that such genetic manipulation can only be undertaken within a laboratory environment, recent advances point to capabilities that have both offensive and defensive implications both for the Army of Tomorrow and the Army of the Future and that raise a myriad of questions. For example, will the Army harness this capability to make its soldiers truly fearless warriors in the face of the enemy? Could this ultimately mitigate the effects of post-traumatic stress? While this may remain morally and ethically problematic for western democracies, it may not be so for a well-funded terrorist cell or crime network.

Nanotechnology. The race to research, develop, and commercialize nanomaterials is global. Advances in nanomaterials promise to revolutionize broad domains such as high-performance materials, coatings, energy conversion and storage, sensors, electronics, pharmaceuticals, and diagnostics. Nanotechnology is at a formative stage but is maturing quickly—so rapidly, in fact, that the first physical neural interface²³ between a computer and a human brain (probably serving a prosthetic function) may be demonstrated within the 2015 to 2020 timeframe.²⁴ With the advent of such interfaces, the possibility of humans being able to interact directly with computers by merely thinking may become reality.

The military, economic and security implications of nanotechnology are considerable and have prompted some U.S. federal agencies to commit significant

23. Neural interfaces will provide a direct connection between a human or animal brain and nervous system and a computer or computer network.

24. <http://humanitieslab.stanford.edu/2/290>.





resources to nanotechnology research and development (R&D).^{25, 26} Recognizing the importance and potential impact of nanotechnologies on future capabilities, the U.S. Army has provided \$50 million to stand up the Institute for Soldier Nanotechnologies at the Massachusetts Institute of Technology (MIT) in Cambridge in order to improve warfighters' protection, specifically in the development of new uniforms, better armour and improved sensors.

TECHNOLOGY-INDUCED SOCIETAL CHANGE

Technology is a key driver of societal change. Moreover, the *pace of change is leading to societal disruptions*, which in many cases are manifest in revised laws and policies. Legal disputes are arising as a result of groups using, or seeking to use, new technologies before the general public or any elected body has even considered the public policies that should surround them. Accordingly, and in order to help avoid being taken by surprise and thus having to make rash judgments that often result in unintended consequences, systematic study of future issues must become a routine part of capability developmental activities.

Open access databases and knowledge warehouses add to the potential risk; for example, current policies allow scientists and the public unrestricted access to genome data on microbial pathogens. Whether exploitable information such as that should be published for the public good or whether it should be safeguarded because of its threat potential remains a matter of debate. Policy-makers must also consider the possibility that the information could be used for destructive purposes, such as in bioterrorism or war. Given those risks, the need exists for continuous and thorough evaluation of scientific technology as it affects national security and health and welfare.²⁷ Force development activities must heed changes and potential scenarios that include such radical capabilities if we are to be prepared for future defence and security threats.

Another area that will continue to challenge societies is the ease with which digital data can be copied, shared and manipulated. Issues of inappropriate data and information manipulation notwithstanding, network-enabled social collaboration remains a powerful capability that will most likely continue to grow in popularity and importance. Open access to information, coupled with the addition of text mining software, will allow users to probe links within the data, thus facilitating

25. <http://chemicalvision2020.org/nanomaterialsroadmap.html>.

26. <http://www.afcea.org/signal/articles/templates>.

27. The CBRNE Research and Technology Initiative led by DRDC is an excellent example of the proactive approach being taken by Canada: <http://www.crti.drdc-rddc.gc.ca/en/default.asp>.



detailed analysis. *The liberation of information will empower individuals while at the same time reducing government monopoly on information.* Indeed, it may become a necessity for organizations to provide social networking tools to their personnel. These inexpensive capabilities, combined with near-instantaneous worldwide dissemination over the Internet, offer opportunities for misinformation, deception and fraud—intentional or otherwise—and will increase the need for due diligence in verifying sources. Given the institutional conservatism, and the desire for access control and information security policies within the CF, such openness and transparency is likely to be resisted within the defence environment.

While bandwidth and security restrictions may be legitimate in a military context, such measures may become increasingly intolerable²⁸ to individuals who expect social collaboration and communication tools to be made available to them. *In the future, any attempt by an authority to stifle user communication within these emerging Web 2.0 collaborative environments may ironically lead to greater proliferation of the information that they initially attempted to restrict.*²⁹ Thus we can imagine that civilian network-enabled operations capabilities will likely grow in sophistication and power, rivalling anything that can be implemented by large institutional and bureaucratic armies.

Armies as institutions are by their nature conservative and evolutionary, and its *organisational culture may not necessarily be well placed to accept the rapid pace and nature of technological change.* It is likely that the establishment of a networked force optimized to conduct ADO will impel organizational changes, resulting possibly in the creation of flatter, less hierarchical structures and more probably in the creation of ad hoc forces assembled for specific tasks. That said, the possibilities for collaboration fostered by social networking technologies could serve to undermine hierarchical structures familiar to the Army. The uncertainty produced by such changes will likely be met with considerable resistance in some quarters of the Army. Similarly, the development and rapid fielding of a variety of (evolving) network components may produce an asymmetrically equipped force with significantly different networking capabilities, perhaps giving rise to soldier/leader distrust or frustration with the information generated via the network and presented to them

28. Recently, Digg.com users posted links to a code that allowed software developers to copy encrypted content from HD-DVD discs. The code's creators, Advanced Access Content Systems, demanded that the Digg.com administrators remove the links. While the site's administrators cooperated with the request, the site's users rebelled. Digg's site was covered with thousands of links to the code and free speech protest statements. This social rebellion has forced Digg's administrators to abandon its attempts to remove the code and instead to develop a legal position in preparation for inevitable litigation by the code's creators.

29. This phenomenon is known as viral marketing, which can have positive advertising benefits but negative consequences if attempting to protect sensitive information. There are growing opportunities, however, to data-mine these flourishing connections. Intelligence agencies are seeking to track insurgent groups with social network mapping tools for example.



for decision making. To overcome resistance and issues of trust, considerable effort will need to be undertaken to educate the CA that the introduction of networked capabilities will not supplant human responsibility and control.

While the current approach is to ensure the presence of a human-in-the-loop to make such decisions, this may not be as suitable in the future. It is possible that there will be situations wherein events transpire so rapidly that typical human response times would be wholly inadequate. For example, automated countermeasures such as defensive aid suites (DAS) must deploy in milliseconds, well before human operators would be able to sense and respond to an impending threat.

The Army's capability development community will need to be aware of these issues and their human resources implications. Potential recruits in the year 2021 are currently four to eight years old and they will undoubtedly have well-developed expectations of network-enabled social collaboration. Moreover, an ability to operate in this environment will be a trait in high demand amongst recruits since the AoT ADO concept envisions a ubiquitous network environment. That said, balancing security policies against user demands for access to technology will continue to be a challenge for military system implementation.

MILITARY TECHNOLOGY CHANGE

The changes resulting from the proliferation of networking capabilities within the commercial sector will continue to influence Canadian society and the military. Operational imperatives obviously will demand that available bandwidth be prioritized for mission-specific use.

Beyond the social benefits provided by advanced networking, there is the ability to extend the life of legacy weapons platforms and systems by allowing them to be used in new and innovative ways— including dispersal with greater situational awareness and superior cooperative engagement potential. New fire control systems, sensors and software can offset deficiencies in armour protection with improved first hit/kill probability. Similarly, advances in materiel design and manufacturing and information technology will be leveraged to enhance protection and survivability. In that sense, network capabilities are expected to improve survivability, enhancing successive layers of protection, from mobility and stealth, to signature reduction and soft-kill defensive aids suites (DAS), to hard kill DAS, to improved armour, to spall suppression systems.





Navigation and navigation jamming³⁰ devices have become commercially inexpensive commodities that anyone, including our adversaries, may obtain. While these commercial systems sometimes lack robust security features, they are being purchased by troops before they deploy to theatre. When combined with commercially available communications technologies, they offer situational awareness capabilities rivalling those available to current deployed military systems. For example, Canadian soldiers have a long history of augmenting issued equipment with privately purchased enhancements, particularly commercial GPS-enabled products ensuring that at least one person per patrol and often everyone has GPS capability. This situation will likely continue as commercial innovation provides capabilities more quickly than military procurement programs can respond.

Israeli-owned ImageSat International, for example, offers customers the opportunity to task its EROS-A imaging satellite and download its data in total secrecy with few, if any, restrictions.³¹ The service essentially provides private customers with their own reconnaissance satellite at low cost. The private satellite industry is becoming so advanced and pervasive that many advanced militaries, including the U.S. military, now rely upon it to provide some of their imaging and meet much of their communications needs.

The confluence of all these trends is likely to influence the conduct of land warfare towards an environment dominated by much lighter, stealthier and information-intensive forces that make heavy use of robotics. Increased commercial and military use of space could lead to the emergence of a wide range of offensive and defensive space-control capabilities. Computer network attack (CNA) tools, GPS jammers and radio frequency weapons could be widely used to assault information infrastructures and information-intensive forces. Designer biological weapons and the emergence of biological operations could also figure prominently. Clearly, a failure to hedge capability development efforts to deal with these possibilities represents a significant future risk.

HUMAN FACTOR IMPLICATIONS

As society changes, the skills that citizens need to address challenges also change. Recruits of 2021 will need digital age proficiencies in order to thrive on a digital battlefield. The military training system must make parallel changes to prepare

30. At the present time, 28 countries are actively developing jammer systems. Source: Trial Gypsy Hotel planning conference documents.


31. <http://imagesat.pionet.com/?catid={38D9FD69-CE40-4E27-8F6D-85D35E50AFEF}>.



soldiers for that environment. In particular, the training system must understand and embrace the skills³² demanded by changing technology in the 21st century, including:

- **Visual and Information Literacy:** Good visualization skills are required to be able to decipher, interpret, detect patterns, and communicate using improved graphic user interfaces. Information literacy includes accessing information efficiently and effectively, evaluating it critically and competently, and using it accurately and creatively.
- **Cultural Literacy and Global Awareness:** In a global economy, with interactions, partnerships and competition from around the world, there is a greater necessity for knowing, understanding and appreciating other cultures, including the cultural norms of a technological society. Where there are cultural knowledge gaps within the CF, the FNC may be able to augment with such capabilities as cultural knowledge bases and real-time translation.
- **Adaptability/Managing Complexity and Self-Direction:** The interconnectedness of today's world generates unprecedented complexity. Individuals must be self-directed learners who are able to analyze new conditions as they arise, identify the new skills that will be required to deal with those conditions and independently chart a course that responds to such changes. They must be able to take into account contingencies, anticipate change, and understand interdependencies within systems.
- **Curiosity, Creativity and Risk-taking:** Individuals today are expected to adjust and adapt to changing environments. Curiosity fuels lifelong learning as it contributes to the quality of life and to the intellectual capital of the country. Equally important is risk taking—without which there would be few quantum leaps in discoveries, inventions, and learning. Amongst soldiers, new generations of technology-proficient individuals will have risen through the ranks of the Army, comfortable with configuring devices for their own use and expecting to be able to accomplish the same with Army C2IS devices. If presented with centralized information management, they will seek and implement workarounds—often in the field and in response to user-driven needs. The challenge for the Army will be how to understand and benefit from this creativity.

32. This list of 21st century skills is adapted from the enGauge 21st Century Skills study:
<http://www.ncrel.org/engage/skills/skills.htm>.

- 
- **Teaming and Collaboration:** The rapid pace of today's society and communications networks has caused, and enabled, a shift in the level of decision-making down to the individual. At the same time, the complexity of today's world requires a high degree of specialization by decision makers. This demands the teaming, in an increasingly virtual realm, of specialists to accomplish complex tasks in ways that are efficient, effective and timely. Email, faxes, voice mail, audio and video conferencing, chat rooms, shared documents, and virtual workspaces can provide timelier, iterative collaborations.
 - **Personal and Social Responsibility:** Emerging technologies often pose ethical and values dilemmas. As technical complexity increases, ethics and values must guide the application of science and technology at the personal, community, and governmental levels. Individuals must grasp this responsibility and contribute as informed citizens at all levels.
 - **Interactive Communication:** It is imperative that individuals understand how to communicate using technology. This includes asynchronous and synchronous communication such as person-to-person email, blog and wiki interactions, group interactions in virtual environments, chat rooms, multi-user gaming environments, interactive videoconferencing, phone/audio interactions, and interactions through simulations and models. Such interactions require knowledge of etiquette often unique to that particular environment. Information technologies do add new dimensions that need to be mastered so that they become transparent (e.g., scheduling over time zones, cultural diversity, and language issues). Otherwise, such technologies may interfere with rather than enhance communication.
 - **Prioritizing, Planning, and Managing Results:** High levels of complexity require careful planning and management as well as an ability to anticipate contingencies. That means more than simply concentrating on reaching the main goals of the mission or monitoring for expected outcomes. It requires the flexibility and creativity to anticipate unexpected outcomes as well.

Military technologies will undoubtedly continue to be augmented with improved intelligence, speed, range, stealth, lethality and autonomy in what amounts to a continuous race to outpace perceived threats. Indeed, despite the inherent inability to predict the future, there is sufficient trend data to suggest that technology (primarily commercial) will continue to advance exponentially and



converge (barring an unforeseen catastrophe). That offers the potential for small, well-funded groups to achieve an asymmetric technological advantage in niche areas, thus threatening current western military superiority.

Foreseeable advances in artificial intelligence, computation, simulation, communication, sensors, robotics and portable power are just beginning to influence today's Canadian Army capability development thinking. Unfortunately, given the snail's pace at which major new system capabilities are delivered, which is complicated by a procurement pipeline that is fully subscribed with mainly traditional equipment and platforms, it will be difficult to respond in a timely manner to the continuing rapid technological change, let alone to a potential (perhaps looming) security disruption caused by new commercial technological breakthroughs.

While this section presents a short and necessarily incomplete survey of future technological trends, it illustrates the degree to which change will affect the development of military capabilities. PART 3 will attempt to summarize the concepts contained in network-enabled warfare, provide some cautionary insights regarding the wholesale adoption of these concepts and conclude with a description of what a network is and what its functions are. It will furthermore set out some broad types of information exchanges relevant to the ADO concept.





“Finally, the general unreliability of all information presents a special problem in war: All action takes place, so to speak, in a kind of twilight, which like fog or moonlight, often tends to make things seem grotesque and larger than they really are. Whatever is hidden from full view in this feeble light has to be guessed at by talent, or simply left to chance. So once again for lack of objective knowledge one has to trust to talent or to luck.”

—CLAUSEWITZ³³

PART 3 – NETWORK-ENABLED OPERATIONS AND NETWORKS

Network-centric warfare (NCW), network-enabled operations (NEOps), network-enabled capability (NEC), etc., are conceptual frameworks developed by the United States, Canada and their allies to explain an approach to transforming military capabilities by changing the way people think, thereby promoting smart processes to share and exploit information and the linking or networking of people, platforms and sensors with technology. Part 3 will outline in very simplified form the principles of NEOps, suggest some opportunities and risks inherent to pursuing a NEOps framework and conclude with a short discussion of what constitutes a network and its generic functions.

A SIMPLIFIED EXPLANATION OF NETWORK-ENABLED OPERATIONS

Military endeavours are characterized by their violent, lethal, fluid, chaotic and mobile nature, exacerbated by a lack of information about the battlespace. It is this overarching need for information that has remained constant even as the nature of warfare has changed that has inevitably impelled the creation of networks, no matter how simple, to accomplish this exchange.

Human beings have been organizing into social networks to share information between themselves from the moment they first collaborated to achieve a task. The evolution of human networks from ad hoc and informal arrangements, arising first from the need to exchange ideas, into trade arrangements and, finally, into formal military and bureaucratic networks intertwined with the rise of the nation state placed a premium on

33. Carl Von Clausewitz, *On War*. Translated by Michael Howard and Peter Paret (Princeton University Press, 1984).





sharing, storing and organizing information. Indeed, the demands placed on the state to defend its domestic, territorial and international interests led to specialized bureaucracies tasked with formalizing the systematic practice of civil and military affairs.

Networks, in the military context, evolved from temporarily formed campaign staffs (typically disbanded or much reduced upon the conclusion of conflict) into a retained formal staff structure epitomized by the Prussian Army in the post-Napoleonic era. The vastly increased size of conscript or “levée en masse” armies resulted in efforts to develop and apply scientific management to their manoeuvre, movement, provisioning and training. At the conclusion of the Napoleonic campaigns, most European countries recognized an enduring need to maintain and manage peacetime standing armies. Thus the general staff emerged as a concrete manifestation of a desire to retain formal and persistent networks of people, information and methods of transmission. The fact that most western armies continue to this day to require a method of command and control is an acknowledgment of the need for a network of information.

Notwithstanding the substantial improvements in organizing militaries, control of military forces remained over time and, until very recently, a largely laborious and process-oriented industrial age effort. What has changed, and which marks a clear departure from the past, is the advent of lightweight, easily portable information and communications technologies introduced into the military milieu. Capable of transmitting, processing and manipulating vast amounts of data and converting it with analysis into contextualized information, armies have fielded complex command and control information systems (C2IS) throughout the battlespace in significant quantities.

The rapid propagation of portable information systems at all levels has allowed commanders and staffs to move from mechanistic processing of information (i.e., simple arithmetic calculations) through to enhanced processing (i.e., shared document publishing), to automated processing (rules-based analysis) of information and ultimately to the virtual representation of the battlespace. Simultaneously, the adoption of a mission command philosophy in Canadian and allied armies has led to renewed attention being paid to the art of war. Voice and data communications systems have increased both their range of transmission and their capacity (bandwidth). Finally, the increasing use of personal computers, video



games and multifunctional mobile phones has created a generation of soldiers entirely comfortable with the rapid pace of technological change. Commanders at all levels expect to be able to leverage information quickly, producing more accurate situational awareness and situational understanding, thus achieving the potential for faster decision–action cycles than the adversary. The coherence of those attributes has revealed the potential to link together sensors, weapons platforms and decision makers quickly and accurately in the Army of Tomorrow time frame.

Recognizing this potential application of technology, Cebrowski and Gartska set out in a seminal article, *Network-Centric Warfare: Its Origin and Future*,³⁴ that the exploitation of the increasing persistence of links between sensors and weapons platforms would allow better communications and information sharing and thus increased flexibility and combat effectiveness. Since the publication of *Its Origin and Future*, NCW has been further articulated by the Canadian Directorate of Land Strategic Concepts (DLSC) in *Towards the Brave New World: Canada's Army in the 21st Century*, arriving at network-enabled operations (NEOps).³⁵ Regardless of nomenclature, network-centric warfare subscribes to the following tenets:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhance the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization,³⁶ and it enhances sustainability and speed of command.
- Those in turn dramatically increase mission effectiveness.³⁷

Key benefits of a networked capability, summarized in the UK joint publication *Network-Enabled Capability* (JSP 777), are:

- **Full Information Availability.** Enabling a user to search, manipulate and exchange information of different classifications captured by or available in, all sources internal and external to the battlespace.
- **Shared Awareness.** Providing a shared understanding and interpretation of a situation, the intentions of friendly forces, and the potential courses of action amongst all elements in the battlespace.

34. Cebrowski, VAdm A.K., and Gartska, J.H., "Network-Centric Warfare: Its Origin and Future." *Proceedings*, January 1998: 139.

35. Other similar terms in use in allied nations refer to the same or similar concepts but are differentiated somewhat in terminology, for instance: Network Enabled Capability (UK), Network Centric Operations (US Army) and Network Based Defence (SWE), etc.

36. Alberts, Gartska (1999): "[...] two or more robustly networked entities, shared awareness, a rule set, and a value-adding interaction." In essence, self-synchronization is about independent military units automatically orchestrating their actions in accordance with a commander's intent rather than waiting for direct orders or explicit instructions.

37. Alberts, Gartska and Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority" (Washington D.C. DoD Command and Control Research Program, 2002).



- **Flexible Working.** Enabling assets to rapidly reconfigure to meet changing mission needs, allowing them to work together with minimum disruption and confusion.
- **Agile Mission Groups.** Enabling the dynamic creation and configuration of mission groups that share awareness and that coordinate and employ a wide range of systems for a specific mission. In broad terms, ADO posits that ad hoc and adaptive groups may form for a specific mission. Once the mission has been completed, the group members will disperse back to their constituent organizations. In order for the ad hoc organization to perform effectively, it needs to be able to develop and maintain a high level of shared awareness in order to ensure that the group has coordinated goals and synchronized actions (synchronized effects). Furthermore, while the concept of agile grouping implies autonomy (in that there need not be a direct link to a central command), it is likely that some form of overall command will need to be exercised, implying some form of hierarchy in the command structure, particularly as the group responds to orders or rules of engagement.
- **Synchronized Effects.** Achieving overwhelming effects within and between mission groups by coordinating the most appropriate assets available in the battlespace through dynamic distributed planning and execution.
- **Resilient Information Infrastructure.** Ensuring information resources can be managed and that secure and assured access is provided with the flexibility to meet the needs of agile mission groups.
- **Fully Networked Support.** Allowing the ready use of non-frontline government bodies, industry, academia and public service capabilities to support operations.



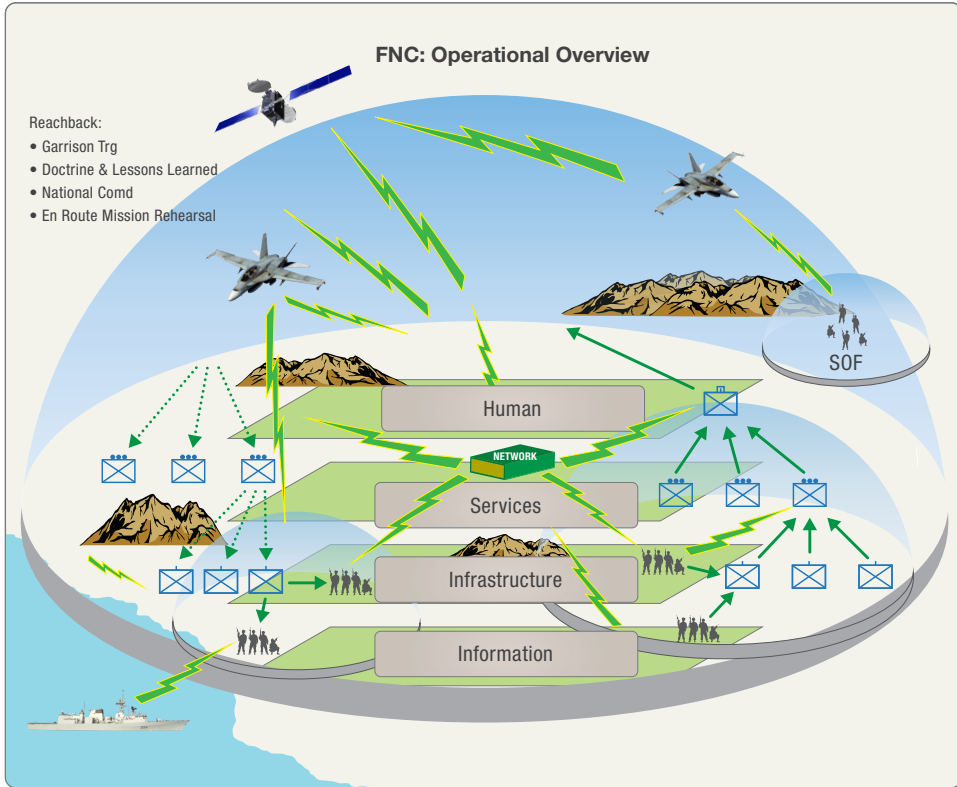


Figure 3: FNC Operational Overview

Canadian approaches to NEOps emphasize that, while the role of technology in furthering NEOps is important, the primacy of manoeuvre warfare doctrine with the human commander at its centre cannot be undermined. Babcock defines NEOps as “the conduct of military operations characterized by common intent, decentralized empowerment and shared information, enabled by appropriate culture, technology and practices,”³⁸ while the CA has separately defined it as “an evolving concept aimed at improving the planning and execution of operations through the seamless sharing of data, information and communications technology to link people, processes and ad hoc networks in order to facilitate effective and timely interaction between sensors, leaders and effects.”³⁹ The FNC, building on the NEOps body of work, will leverage information and technology to achieve decision superiority rather than focus entirely on a type of technology solution to be

38. Babcock, S., “Canadian Network Enabled Operations Initiatives.”

39. Army Terminology Repertoire: Endorsed for Commander Canadian Army and Doctrine Training System (LFDTS) approval, 17 May 2006.





applied to a command and control problem.⁴⁰ It must be absolutely clear that while technology will play an important role in realizing a future network capability, the components of any network delivered to the Canadian Army can only be viewed as an enabler of the human in command.

The Canadian Army will require leaders who can accommodate unpredicted and rapid change in organizational processes, who are capable of leading and implementing adaptive command and control arrangements, and who function in a climate that accepts greater risk and uncertainty. The Canadian Army may no longer assume that it will plan and conduct operations with organizations that have similar structures that are well known to them. Indeed, the norm may become operations in which ad hoc organizations coalesce for the period of an operation and then, upon completion of the task, disaggregate to return under the command of a higher echelon formation.

In summary, network-centric operations are characterized by information-sharing across multiple levels of established echelons of command and control. The keys to the effectiveness of the FNC will be a widespread and complete adherence to mission command philosophy, a shift in focus away from developing platforms in a stovepiped environment, revised command and control practices and procedures and updated doctrine and training that moves the Canadian Army from a culture of “need to know” to one of “willingness to share.”⁴¹ That, coupled with a high degree of availability of information and the status and disposition of friendly and enemy forces and any other relevant aspect of the operational environment, will be a force multiplier in the Army of Tomorrow.

OPPORTUNITIES AND RISKS

Not surprisingly, when considering the potential proposed by the introduction of networked capabilities, there will be opportunities to be recognized and risks to be overcome. The following section highlights certain opportunities to be gained, and cautions against particular risks that should not be ignored.

Opportunities

- **Coherence.** Historically, CA network(ed) components have been conceived, developed, engineered and delivered asymmetrically with poor coordination between project offices. The result has seen the Army take delivery of sensors, platforms and applications that have been

40. CANADA, Command Domain Capability Alternative Report 2008, Chief Force Development (CFD).

41. *Land Operations 2021*, 23.





poorly integrated and require considerable support to be able to even minimally share information. A significant opportunity exists then to bring coherence to the development of CA network(ed) components, ideally with the promulgation of a comprehensive C4ISR strategy⁴² for the Canadian Army. Such a strategy would outline strategic goals, identify broad capability objectives against which specific equipment purchases could be measured and allow the CA to incrementally deliver capabilities over time.

- **Culture.** A significant opportunity exists to socialize the Canadian Army, influencing its culture towards acceptance of networked capabilities. The CA should proceed with a deliberate plan to incrementally introduce select components of a network capability well in advance of the expected full operational capability (FOC). As it is likely that components of the FNC will be developed and delivered over time, the Army leadership must take great care to ensure that *expectation management* is carefully shaped, educating leaders that technology injection is a process of spiral development and evolution resulting not in the delivery of a complete package but rather in a process of managed capability injections that will result in a Future Network Capability.
- **Command and Control.** A networked capability presents new opportunities to review command and control processes, specifically the operational planning process (OPP). As the amount and quality of information increases and is coupled with sophisticated analysis tools, the value of devoting staff resources to planning (which is essentially anticipation in the absence of information) may decrease. Instead, the ability of commanders and staff to react quickly and adapt to analyzed information, aided by artificial intelligence, may become a more desirable feature, rather than adherence to a mechanistic planning process. Michael Schrage points out that “another perverse consequence of the RMA/net-centric argument is that investing in responsiveness yields disproportionately higher returns than investing in planning. That means training exercises and experiments should logically focus less on comprehensive plans of attack and more on the ability to flexibly respond to the unanticipated and unplanned.”⁴³ There is also potential to examine what is meant by “control” in command

42. Promulgated by the Directorate of Land Command Information (DLCI) 2011.

43. Schrage, M., “Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency,” 16.





and control. Control, as an element of C2, may not remain as sufficient terminology for use in the highly variable and complex environment envisioned in the ADO construct. As Czarnecki⁴⁴ concludes, “it is time to dispose of the word, with all its baggage, at least from the military arts. Instead, if one wishes to retain the acronym C2, call the second C ‘coordination’, or ‘collaboration.’” Alberts⁴⁵ goes further, suggesting that the very language of command and control may not be sufficient to enable *complex decision making*. In a recent article, he proposed that “agility,” “focus,” and “convergence” might be the semantics that replace the linguistics of the term “command and control,” inviting new approaches to thinking about C2 by removing the “restrictive legacy of language and connotation.” Certainly, it is desirable to investigate whether the problem-solving paradigm of our current C2 process is sufficiently adaptable to rapidly changing environments and whether the very process as it is currently practised impedes commanders and staff from viewing the complexities of the problem as a system to be understood, complete with competing stakeholders.

- **Interoperability.** Significant opportunities exist to achieve interoperability, not only between the Canadian Army and the CF, but also between coalition networks. As technology coalesces around commercial standards, it may reasonably be expected that interoperability can be more easily achieved, particularly in the sphere of common services.⁴⁶ Nevertheless, interoperability of data and methods of exchange will continue to be of concern, as there remain substantial suites of military equipment and sensors that rely on proprietary data models and inconsistent or incompatible methods of exchange.⁴⁷
- **Costs/Sustainment.** Opportunities⁴⁸ exist to reduce the overall costs of implementing the FNC in the areas of project management, sustainment and training.

44. Czarnecki, Dr. J., “The Failed Thermostat: The Illusion of Control in an Information Rich Age.”

45. Alberts, D.S., “Agility, Focus, and Convergence: The Future of Command and Control,” XX.

46. For example, certain services have coalesced around common standards such as email (SMTP), chat (jfire), and transport layers (TCP/IP) and so on.

47. For example, several distinct exchange protocols exist, often not interoperable with each other, such as Tactical Data Links (TADL), ADatP3 and VMF formats.

48. For instance, an omnibus FNC project aided by Industry Canada within which competing vendors are encouraged through open competition and experimentation to rapidly identify and implement capabilities. Successful vendors could compete and qualify for tranches of funding predicated on positive user feedback.





Risks

As the Canadian Army embarks on implementing the concepts contained within Land Operations 2021, and specifically the FNC, it must be recognized that there will be risks inherent in evolving to a network-enabled Canadian Army. In developing and implementing a networked force, the risks must be acknowledged and may not be assumed away.

The first risk is one of premise.⁴⁹ Adherents of NEOps, NCW and the like assert that networked forces will be more effective, achieve a faster speed of command and achieve self-synchronization. The premise rests on the ability to transmit and process substantial amounts of data and transform it into actionable information. However, faster decisions based on greater volumes of information do not necessarily translate into better decisions. Or, as Van Creveld noted in *Command in War*,⁵⁰ the more one knows, the less one is certain of what he or she understands. As Malcolm Gladwell also points out,⁵¹ the results of the single largest exercise⁵² designed to test this premise revealed that commanders were “gorging on information [...]. Experts from every conceivable corner of the U.S. Government were at their service [...]. But once the shooting started, all of that information became a burden.” Nor is it the case that self-synchronization is necessarily viewed amongst all services as a commonly understood or equally desirable goal. In particular, air and maritime forces, with their focus mainly on strategic outcomes, might argue that a land-centric method of decentralized decision making focused on achieving the commander’s *intent* is, in its most basic form, unsuitable for the bulk of their operations, wherein the allocation of scarce resources (airframes and hulls) require a more traditional directive top-down method of command and control. One would hardly feel comfortable with a method of command and control that, for instance, left the decision to release nuclear weapons dependent upon merely an “understanding” of the commander’s intent. Rather more detailed and directive arrangements might be prudent. Theories of network-enabled operations tend to gloss over the social and cultural aspects (leadership, presence, etc.) of command, focusing instead on the promise of technology. Finally, devotees of net-centricity like to cite the “wisdom of crowds,”⁵³ asserting that networked crowds are better at solving problems, fostering innovation, coming to wise decisions, and even predicting the future

49. Some critics go further and suggest that the foundation premise of Cebrowski and Gartska’s theory of Network Centric Warfare may itself be incomplete at best or entirely wrong at worst (Giffin/Reid)

50. VanCreveld, M., “Command in War.”

51. Gladwell, M., *Blink: The Power of Thinking without Thinking*.

52. US Joint Forces Command (JFCOM) Exercise Millennium Challenge 2002.

53. Surowiecki, J., “The Wisdom of Crowds: Why the Many Are Smarter Than the Few.”

than (presumably) traditional hierarchical organizations. The wisdom of crowds may be, at best, nothing more than a wide sampling of opinion, arriving inevitably at the lowest common denominator. While this might be sufficient to address a shortcoming in a marketing strategy, as a method of organizing warfare it is hardly acceptable. The dangers inherent in the “wisdom of the crowds” have been identified and elaborated by Norman Dixon⁵⁴ as follows:

- *An illusion of invulnerability* shared by most members of the group.
- *Collective attempts to ignore or rationalize away items of information* that might lead the group to reconsider shaky but cherished assumptions.
- *An unquestioned belief in the group’s inherent morality*, thus enabling members to overlook the ethical consequences of their decision.
- *Stereotyping the enemy* as either too evil for negotiation or too stupid and feeble-minded to be a threat.
- *A shared illusion of unanimity* in a majority viewpoint, augmented by the false assumption that silence means consent.
- *Self-appointed “mind-guards”* to protect the group from adverse information that might shatter complacency about the effectiveness and morality of their decisions.

Before investing considerable resources into obtaining ever more complex networked devices, it is also worth considering whether or not the tenets of network-centric warfare stand up to criticism. Giffin and Reid⁵⁵ provide an excellent summary criticism worth repeating in some detail here:

- *‘A robustly networked force improves information sharing.* It is not the network, or its robustness, that determines the quality of information sharing. What matters is the nature of our thought processes, our attitudes toward the information we may theoretically have access to, the situation we are in and our requirements for information. Let us cite a counter example: where one specific data element is sufficient for our purposes, access to a terabyte of data that we do not need constitutes no meaningful improvement.’
- *‘Information-sharing and collaboration enhance the quality of information and shared situational awareness.* By “quality of information,” this tenet must mean to imply something like “truthful and complete information.” By “quality [...] of shared situational awareness,” it must mean to imply something like “a true, complete and accurate understanding of the situation held in common by more than one observer.” If inductivism

54. Dixon, N., *On the Psychology of Military Incompetence*, 399.

55. Giffin, R. and Reid, D., “A Woven Web of Guesses,” Canto Two, 17.



is the methodological means by which these states are supposed to be achieved, then this tenet is insupportable, for inductivism fails to provide such a means. In addition to arguments already presented, it is worth noting that inductive inferences are not necessary inferences in the logical sense; in other words, *it is logically possible to draw differing conclusions from the same body of observed facts*. Thus it is perfectly reasonable for different observers to draw different conclusions from observation of the same body of facts, and nothing in inductive logic can prevent this outcome or justify this tenet. *It must be incumbent upon its supporters to describe the precise method by which the implied certainty, completeness and commonality is achieved. Until they do so, the assertion surely cannot be granted.* We submit that this tenet is dangerous in a common sense way. We may share information and collaborate all we like. We may come to a perfectly harmonious agreement in all respects. And we can still be dead wrong. History is full of examples of this phenomenon; the set of failed military plans includes more than a few instances. Consensus and truth are not synonymous.’

- *Shared situational awareness enables self-synchronization.* Shared situational awareness is neither a sufficient nor necessary condition for the behaviour described as self-synchronization; two actors with a perfectly harmonious understanding of the situation could still conceivably act at cross-purposes as a result of, for example, different personal interests and intentions. Conversely, two actors may disagree dramatically concerning the nature of a situation but still work together without being compelled to do so by higher authority because of open-mindedness or shared intent. *It is not compelling homogeneity, but managing the inevitable and actually beneficial diversity intrinsic to the battlefield, that constitutes the more fundamental and important challenge of command.*
- *These, in turn, dramatically increase mission effectiveness.* We are in complete agreement with proponents of the NCW thesis that recent progress in the domains of information and communication technology has dramatically improved and will continue to improve military capability. We also agree that this progress creates a compelling case for organizational, materiel, doctrinal and behavioural change. But for the reasons presented, we cannot accept that the three preceding tenets justify this final assertion.



Left unexamined, the gaps in the Network Centric premise may undermine the successful implementation of a networked capability. Considerable effort should be applied to investigating who consumes information in the military domain, how they do it and for what reason, otherwise we may succeed in constructing a set of networked components that are very adept at collecting and disseminating information but inadequate when it comes to helping humans make sense of it.

Training. Two training issues can be identified with the implementation of networked capabilities, particularly (1) the potential for degradation of basic soldiering skills, and (2) cognitive demands in adopting new technology. The requirement to train on a wider variety of new technologies coupled with a finite amount of resources applied to individual and collective training may negatively affect the retention of basic soldiering skills. Furthermore, there is a risk that, with the proliferation of networked devices, dependencies may develop such that, absent the network, certain commonly held soldier skills may disappear altogether. For example, with the introduction and widespread use of handheld GPS technologies, the ability for soldiers to skilfully navigate by map and compass may become endangered. Likewise, as weapons platforms become semi-autonomous, skills such as manual plotting of artillery missions may weaken or disappear altogether. A concerted effort to conserve core skills within the Canadian Army will be required so that, in the event that the network is unavailable, the Canadian Army may continue to carry out its assigned tasks. In addition, with the proliferation of personal computers, gaming consoles and high speed Internet access and ongoing exposure to commercial technology, soldiers possess high expectations of the reliability and performance of FNC components. They will expect functionality that works “out of the box,” that is easy to use and that has immediately responsive technical support. There will be very low tolerance for technology that is seen to be cumbersome, duplicative and non intuitive. In fact, any FNC component that does not offer immediate and clear improvements in job performance will likely be rejected out of hand. Much effort will have to be devoted to ensure that soldiers experience low “frustration” scores⁵⁶ and low effort⁵⁷ scores. The CA may wish to investigate opportunities for self-learning⁵⁸ and beta testing⁵⁹ as a means of reducing the training overhead associated with the introduction of a wide variety of FNC components. With the increase in the sheer volume of data, much more effort will

56. Frustration Scores – realized when soldiers encounter products with an uneven technological development or performance.

57. Effort Scores – displayed when products work yet are deemed difficult or time consuming to use.

58. Self-learning opportunities could include the creation of a game-like training package, perhaps set up as a Multi User Domain in which multiple users learn system components in a gaming environment. A secondary benefit would be to create or encourage a community of beta testers amongst soldiers of the CA.

59. Versions of the software, known as beta versions, are released to a limited audience outside of the programming team. The software is released to groups of people so that further testing can ensure the product has few faults or bugs. ([www.wikipedia.org // search “beta testing”](http://www.wikipedia.org//search%20beta%20testing))

be required to design tailorable and decluttered user interfaces and test components of the FNC to ensure that subscribers may easily access the information they need whilst keeping frustration and effort scores to a minimum. Warne et al⁶⁰ identify specific skills that would be vital for NEOps to succeed, including:

- An understanding of what fielded systems are capable of.
- Freedom to risk, innovate, and learn.
- An ability to interpret and make decisions from incomplete data.
- An ability to deal with information overload.
- An ability to absorb substantial quantities of information and discern what is most important.

Network Dependency and Control. There is the possibility that commanders and staff may come to rely on the widespread availability of networked capabilities, thus introducing a significant vulnerability should there be a catastrophic loss of the network. Indeed, the Army will need to identify a minimum set of network tools, or a “no fail”⁶¹ subset of the network, which must possess a high degree of survivability. A complementary risk that has been recognized generally by the western militaries is a suspicion that the networked capabilities will allow or encourage senior commanders to micromanage their subordinates. The “all informed” network delivering a detailed “window” to every level presents the possibility that commanders without sufficient trust in their subordinates will desire the capability to view the battle through the rifleman’s scope, so to speak. While the inclusion of predictive intelligent agents and tools in the FNC may help to anticipate upcoming threat courses of action, prior to and during engagements, not everyone will be comfortable with the air of certainty implicit in the term “predictive.” A firm and uncompromising *adherence to mission command* in doctrine, training and network design will be necessary to alleviate this risk.

Threat Forces. It has been demonstrated repeatedly that advancements in military technology rarely remain in the hands of the leading power for very long. Market forces will combine to lower the acquisition cost to threat forces of obtaining network capabilities of their own. Open source documentation will permit adversaries to exploit much of the work being accomplished by allied transformation efforts. Also, threat forces are expected to not only be highly adaptable, making use of commercial technologies in their own networks, but the types of social- and relationship-based networks they use may very well operate below the detection threshold of many of the sensors available to the CA. In conflicts of the future, the

60. DSTO 2004, The Network Centric Warrior.

61. A no fail capability implies a high degree of availability, which may lead to increased costs due to hardening and protection, redundant paths and so on. Careful consideration of what exactly constitutes a no fail component/capability of a network will be necessary in order to assess costs and complexity.



enemy's resort to asymmetric attacks and the significance of human interaction and social contacts and of improvisation, endurance, commitment, and trust may well render the technological capabilities of the network irrelevant. Additionally, much technological effort in support of network-enabled operations has been expended on more sophisticated electro-optical sensors that, while they may be very good at discerning threat platforms for weapon engagement, do not appear to be optimized to be able to sense threat forces enmeshed with a local civilian population. A reliance on networked sensors and weapons platforms may also expose the AoT to sophisticated computer network attacks from opportunistic criminal organizations and third parties seeking to experiment against our network (hackers, etc.) or indeed from threat sympathizers with access to the latest technology. In other words, NEOps and NCW may very well optimize the Canadian Army's ability to operate against peer or near peer competitors but may not function quite so well against an asymmetric threat. Possible risk mitigation efforts could include the creation of standing multidisciplinary "red teams" charged with brainstorming countermeasures to a networked force and the inclusion of their analysis into any [exercise] simulation.⁶²

Costs/Sustainability. One potential risk that should be of particular concern to a resource-constrained force is the costs and sustainability associated with the development, engineering and institutionalization of a future network capability. As technology evolves, there will be a potential for overall costs to increase as more platforms become network "aware." That, coupled with requirements for the network to be available and reliable in all environments, may also place considerable cost pressures on the development of networked components. Adoption of commercial standards including COTS products may help mitigate costs; however, the requirement to integrate military security policies into commercial products will require additional effort and resources. Assuming that whole fleet management continues as a sustainment methodology, then a model in which multiple capability releases (CRs) require simultaneous support may tax the ability of the CF and CA to sustain the capability in training establishments and on deployed operations.

Infrastructure Bandwidth Throughput and Performance. As the CA adopts a network-based communications infrastructure with interconnected sensors, weapons and commanders, there will continue to be greater amounts of information demanded, placing pressure on the network's capacity to transmit, receive and store information. The performance of every network is related to the optimal number of users and nodes, yet it is difficult to identify that in advance and even more difficult to prevent the number of nodes and users on the network from increasing above the

62. *Towards Land Operations 2021, Studies in Support, Chap 7 (terfry), XX.*





optimal number. For instance, there is a growing recognition of the phenomenon of network degradation. As the number of nodes on a network increases, the potential for degradation via effects such as delay, packet loss, and packet jitter⁶³—or variable packet delay—affects the performance of the network in wholly unpredictable ways. Thus, as the design of the FNC and its component nodes evolve, considerable attention will need to be given to features such as redundancy, intelligent routing and so on.

Despite the risks elaborated above, each may be mitigated with careful attention to the identification and protection of core network services, training and experimentation and with a commitment to supporting technological development.

WHAT IS A NETWORK?

Much of the literature surrounding network-enabled operations or net-centric warfare presupposes that the reader is familiar with the terminology, assuming that the terms are understood. A misunderstanding of what networks are has led to a pronounced tendency in the army to immediately assume that “networks” are only about hardware and communications and are thus a signals branch issue. This tendency has led in turn to some confusion over what is actually meant by networks, network-enabled operations and so on. Therefore, a short and necessarily imperfect working description of a network and its components is worthwhile.

An understanding of what constitutes a network, its generic elements and their properties and the types of information to be exchanged will allow the capability development process to move from conceptual through to more detailed design and ultimately to building and managing the FNC. At its most basic, a network is simply one entity or *node*⁶⁴ (human or nonhuman) *linked*⁶⁵ to interact with another entity or node. Accordingly, for a network to exist there must be entities (or nodes) present, a means of communication, and an understandable or measurable interaction. Thus, for example, two humans (entities/nodes) speaking (means of

63. Miller, M.A., “Do You Hear What I Hear? – Part II: Defining Key Transmission Impairments.” (<http://www.voipplanet.com/backgrounders/article.php/3517541>) In Voice over Internet Protocol (VOIP), automatic speech processing can be affected by phenomena such as packet jitter, which measures the variation in arrival rates between individual packets. Since each packet can (theoretically) follow a unique path, it is possible that the time delay between successive packets can vary. In other words, packets number 1 and 2 might arrive 30 milliseconds apart, while packets 2 and 3 might arrive 40 milliseconds apart, because packet 3 took a different route from the first two. Excessive packet jitter adds complexity to the packet reassembly process, which must present the received voice signal to the end user as a continuous, smooth stream of information.

64. “Nodes are defined as elements in a process that are deciders, sensors, influencers or targets. By definition, sensors receive observable phenomena from other nodes and send them to deciders. Deciders receive information from sensors and make decisions about the present and future arrangement of other nodes. Influencers receive direction from deciders and interact with other nodes to affect the state of those nodes. A target is a node that has some military value but is not a sensor, decider or influencer.” (From Cares, J.R., “An Information Age Combat Model,” 6.)

65. A link is “an observable phenomenon that emanates from a node and is detected by a sensor. For example phenomena detected by sensors and communicated to deciders, or deciders issuing orders to nodes and influencers typically in an effort to destroy or render useless other nodes – constitute links.” Paraphrased from Cares, J.R., “An Information Age Combat Model,” 7.





communication: vocal chords coupled with a measurable interaction: language/grammar) to each other constitute a very basic network. Similarly, a manned aircraft complete with weapons, sensors, and a communications link to a ground station and target designator constitutes a more complex network, composed in this example of many interconnected nodes. However, regardless of their complexity, each meets the definition above.

Building on the definition, it is possible to further identify network components, classify them, and specify their functions and properties. It should be understood that the components and their properties in the sections that follow are conceptual⁶⁶ in nature. These network types and their functions exist regardless of the technology available now or in the future, providing a framework against which all potential FNC components may be assessed.

Fortunately, two excellent papers are available from which detailed network component descriptions may be drawn. The first, “An Information Age Combat Model,”⁶⁷ simplifies all networks into four nodes: “Deciders,” “Sensors,” “Influencers” and “Targets,” each possessing two rudimentary properties, “side” (blue/red/friend/foe, etc.) and “contracted,” wherein functions of more than one node can be contained in a smaller number of nodes. Subscribers employ links between nodes to transmit and receive information and data, the type and complexity of which depends on the nature of the network and the requirements of other participants in the network. Significantly, this model, in identifying any recipient of information as a node type of “target,” allows for a framework to model network effects (particularly influence activities) on friendly, neutral *and* adversary nodes. The Cares model possesses advantages, chiefly, in its suitability in the area of mathematical representation of networks. However, its representation of node types is perhaps too simplified for the purposes of this study.

The second paper, “Netforce Principles,”⁶⁸ proposes six node types characterized by the *actions* they perform (“collectors,” “information providers,” “deciders,” “effectors,” “communicators,” and “supporters”) combined with one or more *properties* (“identity,” “status,” “capability,” “structure,” “control,” “security,” “integration,” and “interaction”) to create a complex set of network capabilities. Using either set of definitions, the network can be defined and understood. Keus, however, offers greater richness and is grounded in operational constructs and therefore this study will adopt the Netforce terminology. Accordingly, the following section draws heavily on the Keus model.

66. As opposed to narrowly specific definitions found for example in the Open Systems Interconnection computer networking model.

67. Cares, J.R., “An Information Age Combat Model.”

68. Keus, H.E., “Netforce Principles: An Elementary Foundation of NEC and NCO.”



Nodes and Node Types. A *node* is an entity that performs one or more actions and is able to interact with other nodes. A node type is the characterization of a node according to its main action. In military networks, the components must be able to (1) collect, process and interpret data and information (to date, interpretation has been largely a human function), (2) provide quality information to decision makers, (3) enable decision makers to cooperate and create measures, and (4) provide an ability to execute these measures. For example, using the Keus model, a human may be classified as a node, while a commander through his actions fulfils the *node type* of “decider.” Furthermore, the node type of human commander may also possess certain properties, including “identity” (“Smith”), “status” (trained/active/operational, etc.), “structure” (company commander), and so on. Indeed, the functional model proposed by Keus is applicable to any type of network, whether comprised entirely of humans, of machines, or of a combination of both.

- Collector nodes collect data and information passively, actively or through a combination of both. A collector node could be a sensor (radar, MET, etc.) or a data collection agent such as a data mining program. Their behaviours can be defined and controlled.
- Information-provider nodes process, interpret, correlate, fuse and provide information in the right format to information requestors. Information provider nodes perform the functions of processing, fusion, interpretation, and administration of situational awareness data. “In an optimized [FNC] architecture, the information provider node capability should ideally be distributed in such a way that the information needs (speed, latency, accuracy, level of detail, format, etc.) of deciders can be fulfilled”.⁶⁹
- Decider nodes process the information to decide on possible courses of action. Accountability and responsibility reside in these nodes.
- Effector nodes are the entities that cause a change in the status of a target (for example, a behavioural change or change of physical condition). Thus an effector could be lethal (an artillery round) or non-lethal (a PSYOPs product).
- Communicator nodes transport data from one place to another. At their simplest, communication nodes receive or transmit and do not interact with the data itself. Communicator nodes include security mechanisms.
- Supporter nodes perform the functions of node management, data management and security management.

69. Ibid., 13.

Node types may be further combined to perform multiple functions, and when so grouped they can be formed into sub-networks or network enclaves, optimised to perform specific tasks such as network control. A federation of sub-networks or enclaves may also allow for the creation of virtual teams, perhaps sequestered into multi-caveat work spaces, or to enable areas of the network to be optimised for performance over low bandwidth communication suites suitable for dismounted users and so on. This combination of nodes and their functions promotes specialized network functions such as monitoring and remote system administration and helps strengthen the network against intrusion and threats.

Each node is, in turn, connected to others via links, commonly understood as communications paths. As such, these paths are characterized by qualitative attributes and quantitative performance metrics. Qualitative characteristics include complexity, quality of service, scalability and topology, while performance metrics could include latency, efficiency, fault tolerance and so on.

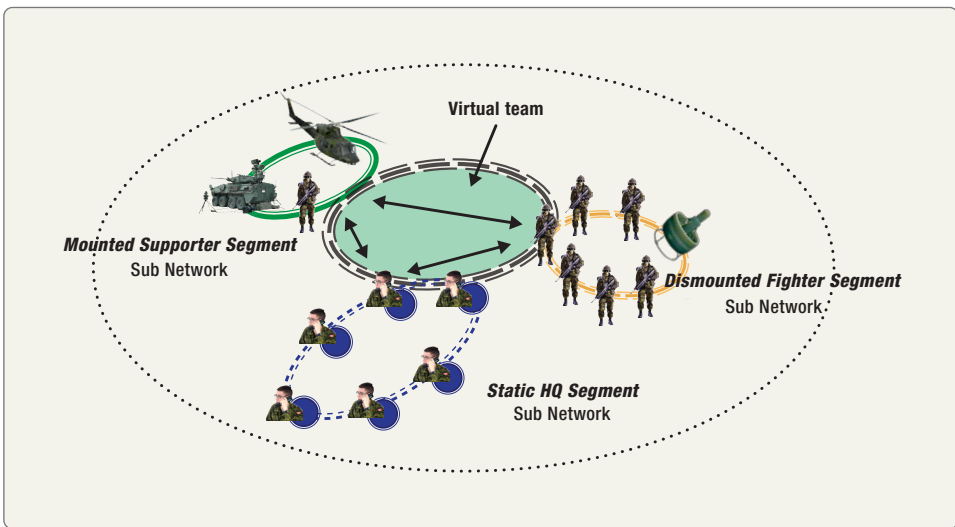


Figure 4: A Notional Federation of Networks

Nodes rarely exist exclusively in the purest forms described above; rather, they are designed as composites to increase effectiveness (for example, an optically guided munition can perform the simultaneous network node functions of collector and effector). Similarly, nodes must be able to interact with each other and, as a consequence, they will combine one or more of the following interface features:

- Registration and Discovery. Nodes are able to join the network (plug and play) and be known to other nodes in the network. To achieve discovery, nodes possess properties of *identity*, *integration* and *interaction*—that is, they “know” themselves, they have a means to interact and they share a degree of integration in order to “know” or discover other nodes on the network. As nodes undergo changes to their capabilities, so to do they need a means of advertising the change through a *status reporting* function.
- Subscribers and nodes will require varying degrees of *access* to some or all of the nodes within the FNC. Another basic category of interaction with the network is the need for *timeliness* of information. Again, subscribers will require that information is exchanged between nodes with varying degrees of latency. For some subscribers, timeliness will not be a great factor, but for others, timeliness will be crucial. And finally, there is a need for *information assurance*.

A TAXONOMY OF NETWORK FUNCTIONS

For the network to be of use to the intended user, it must deliver distinct, operational, value-added functions, or the activities and tasks that we want it to do. Turning again to Keus, *network functions* can be identified and, taken together, present a useful taxonomy representing operational value and against which every component piece of an FNC can be measured.⁷⁰ More than one network function may be combined within a single component, while other components, for reasons of cost, operating efficiency, or specialized capability, may be optimized to deliver only a single function. Nevertheless, every component considered for inclusion in the FNC should be assessed against the degree to which it meets the functions below:

- **Collect.** The collection function enables the supply of rich data for analysis and inclusion into the shared picture. It includes the tasking, management and control of sensors and their configurable characteristics. Supporting collection activities include orientation, exploitation and tasking and are enhanced by sub-functions such as assignment, threat evaluation, identification and engagement prioritization. In a COIN environment, mechanisms to enable the human collection⁷¹ of information will be important.

70. Note also that the network functions fit very closely into the cognitive hierarchy and reveal those areas of the chain of data to decision where machines are optimized for performance.

71. Human collection of information is characterized by its randomness and chance encounters, particularly in the COIN environment.



- ✦ Orientation: Includes but is not limited to validation of RFIs, CCIRM, track management and assisting in compiling the COP.
- ✦ Exploitation: Includes but is not limited to tracking, discovery and fusion.
- ✦ Tasking, or *assignment*, is the function of analyzing the set of available effector nodes (units, sensors and weapons), conducting deconfliction and scheduling tasks, and then assigning a node to engage a target.
- **Disseminate.** The communication of information between nodes necessitates the existence of a physical means of transmission or a bearer system. The bearer system includes the hardware, wiring harnesses and transmission protocols, which may take several forms, from over the air (UHF, VHF, WiMax, cellular, etc.) to wired. The method of dissemination may include voice, structured and unstructured data exchanges, full motion video and so on.
- **Analyze.** The processing of data to produce information suitable for judgment.
 - ✦ **Planning and Coordination.** This function is the process of considering the available information to prepare for operations. Software support in the form of smart Decision Support Tools (DST), war gaming and simulation tools are key to the efficient execution of this function.
 - ✦ **Situational Evaluation.** This function is the process of assessing or analyzing a specific object or entity to determine its potential to cause harm and would also include a post-engagement assessment if an engagement had occurred.
- **Compile.** This is the function of assembling the relevant information from contributing collectors for presentation to users (i.e., *Create a Common or Shared Picture*). The effectiveness of picture compilation is, in part, dependent upon the ease of access to information, the applications available to portray this information and how it is then consumed to



inform decision and planning cycles.⁷² Because it supports the planning process and because individual users will likely have different views of the operation, the effective compilation of a common or shared picture will of necessity become the subject of a managed process.

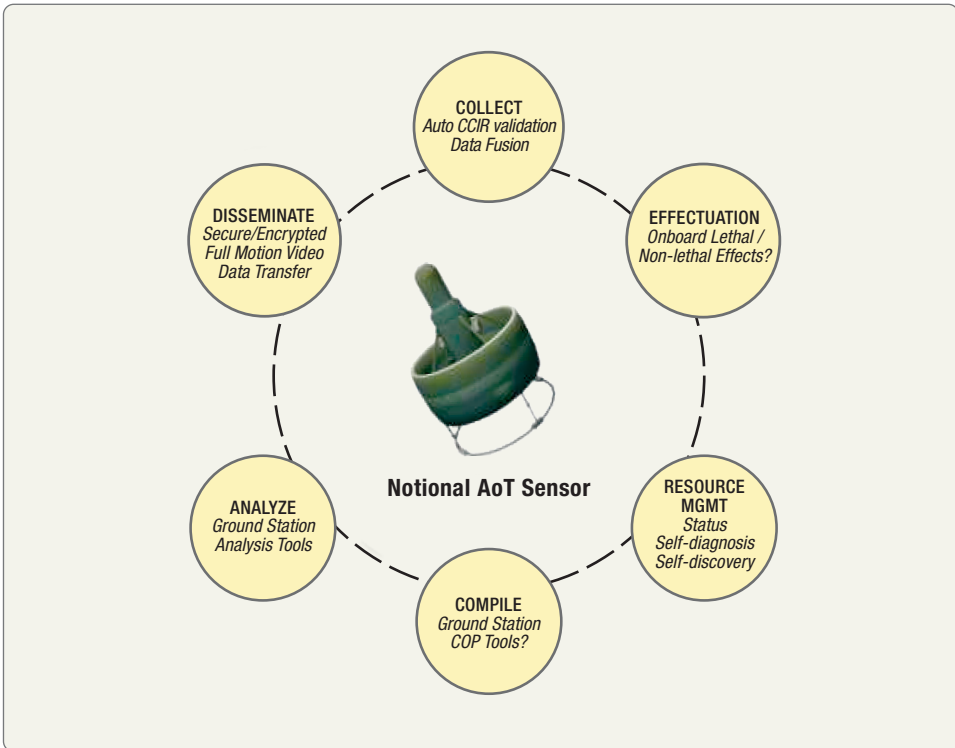


Figure 5: Network Functions Represented in a Notional Network Sensor Node

- **Effectuation.** This is the function of execution or actions of one or more nodes (units/weapons/sensors) aimed at bringing about the desired effect. Effectuation comprises all of the actions necessary to direct nodes to engage a target. It supports the function of effects synchronization, including of sensors and fire support.
- **Resource Management.** This is the function of logistics and maintenance of the various components of the network. It is not limited to simply system management, but includes the analysis necessary to support units in close combat.

72. ABCA Report 068.1 (FOUO) ABCA Lessons Collection Deployment Summary Report, 30 Sept 2008.



The difficulty for capability developers is that one cannot simply go out and buy “a network,” or at least one which will be of utility to a deployed Canadian Army. Careful consideration must be given to understanding end user requirements in order to determine the nature, quantity and characteristics of each node and the links between them.

WHAT KIND OF INFORMATION?

The purpose of exchanging information between users is to define the environment. Building on an understanding of what constitutes a network and the functions it may perform, we can turn to the question of what kind of information the FNC will need to exchange. The premise of ADO accepts that the network-enabled force will need to leverage information superiority to gain an advantage over its adversaries, yet little effort has been devoted to describing the nature of the information itself. According to Keus: “For any multi-node environment, where the nodes work together to achieve common goal(s) there are four generic *types of information* sets, (1) self-awareness, (2) situational awareness, (3) intent and (4) current operations.” Additionally, we can propose a set of information about the organization itself, calling it (5) enterprise services.

Self-awareness is information about the available resources, particularly about the nodes and their capabilities. This information set is concerned with the defining characteristics (performance parameters) of the node itself and changes to those characteristics (diagnosis). It could include information about the organizational hierarchy of the node, command and control status, etc.

Situational awareness, or information about the operational situation (the real world) at all hierarchical levels. This set represents compiled information derived from many sources, including raw, fused and/or analyzed information, and it is enabled by the network functions of collecting, evaluating and managing. In its presentation, it must be customizable to the commander’s needs. It will be comprised of information about the environment in which operations are being planned and conducted.

Intent, or *information about the commander’s intent and plans*. This information is concerned largely with either future operations or the projected conduct of the current operation. It concerns itself with the organization’s goals. The set is necessary to monitor the direct actions of the various networked components to determine the success or potential for success of the commander’s stated intent. When fused and analyzed with current operations information, it contributes to the achievement of both situational awareness and the development of subsequent plans.





Current operations, or information about the conduct of an operation. Information contained within the current operations set consists of largely *perishable information of immediate relevance* to those conducting the current or close fight. It will of necessity be comprised primarily of actions and events, both friendly and hostile (or of other hostility, for that matter), or information about actual actions and events that have been taken to achieve the stated intent and used to take into account imminent actions and determine successive actions for purposes of de-confliction and synchronization. Information in this set is closely coupled with information contained in the intent and situational awareness information set and, with analysis and judgment applied, is a significant contributor to the situational awareness set.

Enterprise services, or information about organizing principles of the institution itself. This information supports enterprise-wide business processes across organizations that are geographically dispersed. Thus *doctrine, policies, information management, personnel management and training* could be included here. The inclusion of enterprise services allows the components of the FNC to be extended into training and garrison activities and training material to be made available in the operational environment where appropriate.

INFORMATION PRESENTATION

Describing the types of information to be exchanged clearly enables an understanding of the nature and scope of information exchanges, but equally important is a discussion of how this information is made available to end users. Indeed, there is a direct connection between the network function of “*compile*” and the form in which information is presented. The Oxford English dictionary defines form as “a way in which a thing exists or appears.” Using this definition, we can easily understand that information is customarily perceived by users primarily in visual and auditory form (supported by touch, smell and taste). Thus users such as dismounted soldiers may reasonably expect to continue relying heavily on auditory and visual perception as their primary means of information consumption. The dissemination of information from dismounted soldiers may continue to be heavily reliant upon voice communications, aided perhaps by simplified graphical and textual information, while other recipients may rely on tools that are optimized for high-volume textual presentation such as spreadsheet applications, email and the like. Of course, while information is initially perceived in raw format, it is





consumed or processed using a set of filters, be it cultural, psychological and so on. This customization of information occurs regardless of the means of dissemination, and users will continue to demand that technology allow them to filter or customize the presentation of information.

CONCLUSION

In conclusion, networks exist to *share* and *exploit* information. Each component must satisfy one or more of the network functions in order to deliver operational value. While the definition of a network, its types and functions is a suitable starting point from which to begin to describe the generic components of a network, it does not tell us very much about what makes a network useful, nor in particular how a network enables the ADO concept. In PART 4 we describe the relationship of the network to the human in command and, in general terms, how the network might function in Land Operations 2021.





“There is nothing common about the operating picture. We create our own understanding of the situation and we impose our own meaning on the facts. We each have our own unique and personal operating picture. It is not the commander’s task to eliminate these diverse operating pictures but to identify and manage any contradictions between them. To the extent that we employ a homogeneous database, our decision to accept it is voluntary, and its purpose is not to create a common understanding but to provide an agreed basis for exchanging and comparing our conjectures and the results of our tests.”

—LCOL RALPH E. GIFFIN⁷³

PART 4 – COMMAND AND THE NETWORK IN ADO

As the CA embarks on a program of realizing a network-enabled force, it should not be forgotten that, regardless of technological trends, armies will continue to place the exercise of command and trust in the hands of humans and that is not likely to change. Part 4 begins with a summary introduction to the tenets of command, continues with a short discussion of the network in ADO, and concludes with a description of generic information required by the ADO-enabled force.

ENDURING TENETS OF COMMAND

Perhaps the compelling reason that command remains as a human function is that, despite the rapid advances in machine logic and artificial intelligence, it is only humans who possess the true capacity to react to unanticipated threats or recognize when an opportunity of chance arises. Command, therefore, is an art, bringing together personality, competence, knowledge and experience and creativity. The CA recognizes⁷⁴ that command is the “most important activity in war, garrison and throughout the breadth of the spectrum of operations.” Current doctrine⁷⁵ places the exercise of command within the human domain, noting that “land combat occurs as primarily a human interaction,” and that is not expected to change in the AoT timeframe. Human command of military forces relies heavily on the attributes [of *leadership*, *competency*, *responsibility* and *trust*, etc.] of individuals who play a role in the decision process and on the interpersonal dynamics between commanders

73. Giffin, Lieutenant-Colonel Ralph E., “A Woven Web of Guesses,” Canto Two.

74. B-GL-300-003/FP-001, *Command In Land Operations*, dated 27 July 2007, 1–3.

75. *Ibid.*, 1–5.



and their subordinates.⁷⁶ Therefore, it is important to understand that the design and operation of the FNC must not interfere with the exercise of human command; rather, it must complement it.

It is this ability to take advantage of the intangible aspects of human nature that reinforces the fundamentally human role of command and has been recognized by several writers, including Col Forgues in his article, *Command in a Network-Centric War*:

The fundamentals of command, as defined in CFP 300-1, are: unity of effort, decentralization, trust and mutual understanding, and timely and effective decision making. Command promotes force cohesion to achieve unity of effort. Whenever possible, command must be decentralized and rely on the ability of sub-units to operate independently, while maintaining unity of effort. This favourable situation is made possible through the development of trust and mutual understanding. In such an environment, commanders can exercise timely and effective decision-making. Maintaining unity of effort is of course more difficult when command is decentralized. CFP 300-1 argues that the conflict between unity of effort and decentralization is resolved by ensuring that the commander's intent is communicated and understood, the main effort is clearly designated, a proper command climate is maintained, and the forces operate based on a common doctrine. The role of the leader in establishing purpose, providing direction, and generating cohesion and motivation is stressed.⁷⁷

Two themes stand out: first is the issue of *trust* and second is the imperative to communicate, in unambiguous terms, the commander's *intent*. Trust has always been a significant factor in the success of military operations, but it is likely to become even more vital as we extend the circle of decision makers to persons (and possibly non-human entities) and organizations outside the immediate chain of command. Because trust and the understanding of the commander's intent are fundamental to the success of an operation, any future network that is incapable of delivering an uncompromising information assurance has the potential to undermine users' confidence in it. The clear communication and understanding of the commander's intent is such a key component of mission command that the challenge for those implementing the FNC will be to find ways to communicate this intent, particularly to nonhuman entities, beyond the traditional methods of voice and written communication.

76. Directorate of Army Doctrine; Command Capability Development Record, September 2006.

77. Forgues, Colonel P., "Command in a Network-Centric War," Canadian Military Journal, (Summer 2001), 23–30.

It should also be noted that only humans are currently capable of *applying judgment* to knowledge. That is significant because, while data, information and, to a certain extent, knowledge may be mastered by machines, the understanding gained from experience, intuition and training is not likely to be acquired by machine intelligence in the near future.

THE HUMAN IN COMMAND

Command is a fundamentally human endeavour relying on the intangibles of human nature, including, for example, a moral and ethical code, judgment, interpersonal relationships and bonds of trust. However, the complex nature of warfighting demands that mechanisms to reduce risk and uncertainty and increase the speed of decision making be made available to support the commander. It is in this supporting role of control that technology and, in particular, a network capability, excels. As armies engage in a cycle of planning, preparation, execution and assessment, the commander “must be supported by a control system that supports his ability to overcome time-uncertainty challenge through the management and production of timely, relevant and accurate information and knowledge upon which he can realize an understanding of the situation and visualize what needs to be done next.”⁷⁸ Key to achieving the commander’s battlefield visualization is a process of transforming raw facts into understanding⁷⁹—a process illustrated by the information hierarchy, depicted below. As we shall see later, technology can help with the speed and accuracy of this process, complementing human effort.

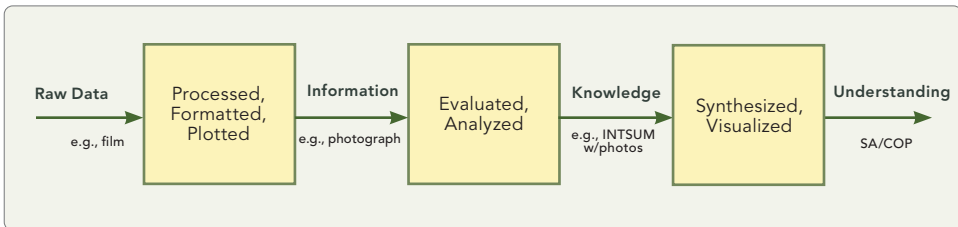


Figure 6: Information Hierarchy

78. B-GL-300-003/FP-001, *Command in Land Operations*, 1–11.

79. The transformation of data to knowledge leading ultimately to decision involves a chain of cognitive dependencies in which machines and humans are differentially optimized to perform specific tasks. Machines are much more capable of collecting volumes of data, collating it into information and conducting rough analysis of it to transform it into knowledge, which in turn contributes to situational awareness. Humans too provide analysis of information, but are far better at taking knowledge and applying judgement to build understanding and arrive at decisions.



Canadian Army network needs are different from those of the other services—for instance, the very personal exercise of command leadership will drive CA network requirements that differentiate a CA network solution from those of the CF or air and maritime environments. Command of soldiers very much depends on bonds of trust, motivation, leadership and teamwork—that is, an army commander is expected to display courage, moral strength and personal presence, wielding his influence at the right place and time on the battlefield. However, because the commander cannot be everywhere at all times and because of the vast amount of information available to him and from which he must extract relevant nuggets, a complex yet intuitive information network is required. This network must firstly be absolutely capable of allowing a commander to communicate his intent or purpose in concise, unambiguous terms down to the soldier, thus equipping the subordinate with enough information for him to make decentralized decisions sufficient to carry out the plan. This decentralized decision-making capability is in and of itself nearly unique to armies, and a one size fits all CF network design will not be adequate for it.

In addition, the Canadian Army network must cater to a wide variety of users, from dismounted fighters carrying nearly everything they need on their bodies, to mounted fighting and support elements where the physical network components must co-exist with vehicle/platform weapon systems, to static headquarters and garrison training facilities where, with higher bandwidth and resources, the component footprint need not be optimized for deployment. This breadth of user elements means that the FNC will likely be comprised of a federation of specialized sub-networks, each optimized for specific user elements and the environment it will operate in but also capable of sharing information amongst them.

What is more, transmission of information within the CA is moving towards more digitized systems, opening the possibility that humans will no longer be the sole consumers of information and that information will also be consumed by automated sensors and weapons platforms. However, the most critical information, the *commander's intent*, does not currently flow as data, limiting our ability to provide direction to non-human entities within the battlespace.

To date, the Canadian Army network capabilities may be characterized as highly provisioned enclaves of network ability connected by poorly provisioned information exchange (high latency, low bandwidth, and limited ranges) between those enclaves. It is also worth noting that the networking capabilities adopted within the CA have largely digitized pre-existing analogue processes, leading to a condition where the CF and CA have become quite adept at storing or “warehousing” information. Unfortunately, lacking smart information sharing tools, the CA is largely incapable of efficiently delivering relevant information to commanders. Furthermore, there





is little or no integration of networks that exist at garrison (baseline), training establishments (simulation tools) or tactically deployed networks. Thus, while it may be claimed that a network does exist, it does so in a poorly realized form. The inability to easily share the contents of the information warehouse gives rise to the frustration of “knowing” the information exists somewhere within the several disjointed information repositories but not where to find it. Recent wiki-based information management tools developed in theatre show some promise of breaking out of this paradigm.

Finally, the conduct of full spectrum operations in an ADO context will require a networked suite of FLCS systems to support the fundamentals⁸⁰ of dispersed operations developed from the manoeuvre principles of find, fix and strike. Therefore the FNC will, as a minimum, require characteristics and features that allow it to operate in the AoT under the ADO construct.⁸¹

Another way to put it might be that, notwithstanding advances in the arenas of science and engineering set out in the preceding section, in the foreseeable future, humans will remain the masters of the *art* of war while machines may come to dominate the *science* of war.

THE NETWORK IN ADO

The Army of Tomorrow will be a medium weight, high-technology-enabled force optimized for full spectrum operations in failed or failing states, operating in a JIMP environment and capable of operating across the spectrum of conflict. Land Operations 2021 acknowledges that key to its success will be the “integration of information systems, weapons and other effects-producing platforms,” positing a force that will operate in complex environments, across non-contiguous areas of operations (AO); form ad hoc organizations; disperse and reassemble anywhere in the battlespace; and may not always rely on mass to achieve its desired effects. “By linking knowledgeable entities in the battlespace, forces will be more capable of gaining information superiority and ultimately greater mission effectiveness.” While the conceptual underpinnings admit the requirement for a network, Land Operations 2021 “does not provide doctrinal details on the deployment of Canadian Army formations and units,”⁸² and questions such as how the ADO force might employ a future network are left unanswered.

80. (1) Developing situations prior to contact, (2) Enabling manoeuvre to positions of advantage, (3) Influencing the adversary beyond the range of his weapons with lethal and nonlethal capabilities, (4) Enabling the destruction of the enemy, when necessary, with precision and area effects, (5) Enabling the conduct of close engagement, when necessary, at the time and place of own choosing; and (6) Transitioning between operations without loss of focus or momentum.

81. B-GL-310-001/AG-001, *Land Operations 2021: The Force Employment Concept for Canada's Army of Tomorrow*, 18.

82. Chapman, Major B., “Bounding the Force Employment Concept,” 4.





Significantly, implicit in Land Operations 2021 is the notion that sub-units and platoons will no longer just carry out what can be thought of as conventional military operations—they will also be expected to be executed across the spectrum of operations, complete with (possibly tactically deployed) JIMP enablers, and they will be physically dispersed and likely beyond the range of organic direct and indirect fire support. This means that the physical components of the FNC will need to be lightweight, capable of operating on low power for extended periods of time, and deliver a wider range of services to the end user.

Bounding the Force Employment Concept. The ADO force may expect to operate in any one of four basic areas of operations (AO) while maintaining the ability to rapidly change and operate in the other types of AOs.⁸³ Chapman (2008) proposes a list of factors that will “limit the ability of a unit to disperse,” including factors such as indirect and direct fire support, casualty evacuation, resupply (sustainment), C2 and communications, reinforcement, surveillance and aggregation of forces within prescribed timeframes. Expanding on the factors within Chapman’s thesis, some generalized assumptions about the nature of the FNC in ADO may be proffered:

- Indirect fire support resources will remain in high demand, scarce, and generally centralized in their allocation, particularly joint fire support assets. Furthermore, indirect fire support will continue to be characterized by a high degree of centralized control, pre-planning (ROE and target selection criteria) and special request procedures. By the 2021 timeframe, it would be expected that both indirect and direct fire weapon systems will possess a self-discovery protocol, thus being capable of registering their availability, exchanging information about the target sets they can engage, conducting automated queuing of target selection (and handoff, or “defection”), and incorporating onboard analysis tools that can aid in the automatic selection of appropriate munition types. To support indirect fire requests the FNC will need a high degree of availability, and most likely a path dedicated to the exchange of fire orders.
- Direct fire support weapons will continue to be employed in mutually supporting positions, thereby limiting the area that may be dominated with fire. Increased range, lethality and smart target acquisition should allow area coverage to increase. Direct fire systems will need to

83. Ibid.



possess many of the same capabilities as indirect fire systems above, but additionally may also possess capabilities such as integrated defensive aid suites (DAS), cooperative engagement capabilities (CEC) and so on.

- Casualty evacuation. A high quality of HSS will continue to be demanded, and that expectation will impose limitations on the degree of spatial dispersion. To mitigate limitations on the degree of spatial dispersion, it may be desirable to outfit dismounted segment fighters and mounted segment fighters with biometric monitors such that, in the event of emergency CASEVAC, information on the condition of the patient is available to HSS specialists and combat first aiders, thus enabling better on-site care or preparation at specialized HSS facilities.
- Sustainment. It is expected that sub-units will consume ammunition, food and water at rates exceeding planning⁸⁴ figures. Therefore, the FNC will need to provide a CSS network that enables adaptive logistics and resupply, analysis tools and a customized CSS view of the battlespace. Network components optimized for deployment within the ADO context will need to be configured for a *reduced logistics footprint* (for instance, a reduced demand for consumable power supplies and/or the provision of regenerative power supply). Analytical tools and intelligent agents provided to the CSS community will need to be able to provide quick CSS options analysis, coupled with real time asset and commodity tracking to enable quick configuration of re-supply loads. Significant network benefits may be realized in the area of sustainment via the provision of location-based services, particularly proximity actuation (i.e., low fuel/low ammunition alerts cue resupply tasks), and proximity notification.
- Command and control. A core network capability such as secure voice everywhere on the battlefield, supplemented with reliable positional awareness (PA), will of necessity form the core of a tactical network—one that is available, survivable and easy to use. Careful consideration will need to be given to information presentation on mobile and wearable devices. For instance, components delivered to dismounted fighting elements will need to present simplified information but allow greater fidelity as desired. Furthermore, information requirements will

84. For instance, the issued tactical vest contains storage for four magazines of ammunition, which matches the planning figure of 1 day of supply of 5 magazines (one on the rifle). However, it was not uncommon during Op ARCHER for soldiers to carry between 12–15 magazines on daily patrols, greatly exceeding all scales of consumption.

be varied, rapidly changing and sufficiently broad in nature that it is conceivable that soldiers will want access to a broad range of information at almost any time.

- Communications. It is assumed that satellite communications will not be available for all nets and that current, or evolutionary radio capabilities will be used. Mounted Sub-units must maintain connectivity with the higher headquarters (HQ) through tactical radios with a range of at least *40 km*.
 - ✦ Competing demands will necessarily introduce design tradeoffs that will continue to exist in the AoT timeframe. For instance, efficiencies in size, weight and power (SWaP) suggest that the soldier may have to accept constraints on bandwidth and thus tradeoffs in the capabilities that he may have access to. Contra wise, users at the static HQ/garrison segment may demand significant increases in bandwidth and be willing to sacrifice size, weight and power (SWaP).
 - ✦ Voice communications will continue to be a necessary standard and specifically must be available as a “no fail” capability when other means are interrupted.
 - ✦ Voice communications will be in high demand from elements of the force that are not currently equipped with communications suites (CSS “B” vehicles for instance). Thus many more platforms will be fitted with voice communications suites than is the case now; dramatically increasing the number of discrete network nodes that will fall under signals planning and that will require system management and maintenance.
 - ✦ Bandwidth will remain a critical commodity and continue to be particularly constrained below sub-unit level. We can further assume that, in this bandwidth-constrained environment, voice communications will remain as a high priority method of communication.
 - ✦ With the proliferation of databases (at static headquarters and on mobile platforms), information will persist throughout the battlespace, thus necessitating agile system management policies and an improved information security model.



SUMMARY

It is the human who exercises command and leads through presence and force of will who must assess situations, devise new solutions and make decisions. It is the human who remains responsible for the results of his actions, including those of non-human entities. As components of the FNC are designed, careful attention must be paid to ensuring that, throughout the system, a mechanism for holding humans accountable for their decisions is implemented. Therefore, all FNC systems from sensors and weapons to organizational structures and change of command must exist to support the human potential for accomplishing the mission.⁸⁵

By accepting that the commander remains paramount and the manner in which the force uses information, we can imagine how the network provides specific utility to the commander. Taken together, network functions and information exchanges must support the commander's overarching need to be able to specify mission details to principle subordinates. That is typically formulated as mission statements in which such elements as *who* [resource] will *do what* [action/task] *to whom* with *which* [resource], *where* [location], *when* [date/time], *why* [purpose/intent] and *how* are expressed.⁸⁶ Incidentally, and importantly for potential applications within the FNC, formulations such as the preceding lend themselves easily to the creation of machine-readable instructions, suitable for autonomous non-human actors.

In Part 4, a brief description of the relationship of the network to the human in command and how the network might function in Land Operations 2021 was provided. Part 5 continues with a description of general goals, specific objectives and a discussion of user elements.

85. English et al: Beware of putting the cart before the horse.... 13.

86. STANAG 2287 Mission Task Verbs.





As the Canadian Army will be highly dependant on the network, special efforts must also be made to ensure that it is dependable, secure from physical and cyber attack and that it has built-in redundancies should system elements fail. The Canadian Army will stress a blanket approach to networking—with emphasis placed on the network’s technological and human dimensions. This will involve selecting the right technologies at the right time to complement the ever-crucial human dimension of a network-enabled Canadian Army.

—LAND OPERATIONS 2021

PART 5 – OVERARCHING NETWORK CAPABILITY OBJECTIVES

GENERAL GOALS

The FNC, characterized by a *human-focused, modular and integrated federation of sub-networks/enclaves*, supported by an *integrated architecture*, will deliver an AoT land network capability that allows commanders, soldiers, sensors and weapons to access information across tactical, theatre, inter-service and JIMP boundaries to share actionable information, all in support of manoeuvre. The key overarching capability goals are as follows:

- ***A Core Network.*** The FNC will need to possess a “no fail” or reversionary set of capabilities that make it highly available, robust and self-healing,⁸⁷ secure and sustainable. An all-informed secure voice capability is identified as the core network capability that must be available to all user segments.
- ***Dismounted Users.*** Dismounted users will require low power configurable devices and small footprint applications and/or services. Dismounted network components will need to seamlessly integrate with vehicle-mounted devices. Devices designed for employment at the tactical edge will need to feature a variety of push and pull information services configured depending upon the user identity/credentials/role. Thus, services such as proximity notification, location-based alerts and warnings, near real time translation services, cultural lexicons, doctrinal

87. Software defined radios are being realized now with the implementation of the Soldier Radio Waveform into the US Army Battle Command on the Move project. Self-healing allows communications components of the network to “find” an alternative path to the intended recipient in the event that a dedicated communications path becomes disrupted. Technology required to enable self-healing also introduces the capability to form ad hoc networks as communications nodes discover each other. The formation and use of ad hoc networks will likely be crucial to successful operations in urban and complex terrain as small teams of soldiers rapidly form transitory teams.



documentation, simple text messaging and so on could be offered on an as needed basis, either over the air (similar to “cloud” computing) or configured and preloaded onto the device, all based on user profile.

- **Information Presentation.** FNC components must offer a simplified and configurable human system interface (HSI), enabled perhaps by augmented reality (AR) technologies. FNC components must possess interfaces that easily emulate the user’s decision-making process, encourage confident interaction⁸⁸ and enable the user to better perform his/her tasks.
- **Modular System of Systems.** Recognizing that technology and the rate of institutionalization within the CA coupled with a necessity to support legacy systems, a modular approach to the design and delivery of the FNC components is desirable. Such an approach allows for components of the FNC to be designed and engineered to be interoperable, incorporating a common exchange protocol and data model.
- **Collaborative Information Sharing Environment.** Considerable effort should be applied to delivering distributed collaboration tools⁸⁹ allowing some or all users to be physically remote from the central HQ whilst still promoting team cohesion. Indeed an ability to achieve collaboration across any set of users (including sensors or unmanned systems), particularly an ad hoc grouping of users, is a highly desirable JIMP and domestic operations enabler. The ability to form ad hoc connections between individuals or between shared information spaces, offered by such social networking constructs as Facebook and Twitter, might offer near term⁹⁰ collaboration solutions.
- **Assured Information Integrity.** An information assurance capability focusing on guaranteed information quality and trustworthiness will be a necessary feature. Information quality will be greatly improved with investments in the unambiguous definition of data (ontologies, terminology, etc.) such that its representation is consistent across applications. Since not every individual within a user segment will require

88. The three-click rule is an unofficial web design rule concerning the design of website navigation. It suggests that a user of a website should be able to find any information with no more than three mouse clicks. It is based on the belief that users of a site will become frustrated and often leave if they cannot find the information within the three clicks. Critics of the rule suggest that the number of clicks is not as important as the success of the clicks. Regardless, what is clear is that as information is delivered to the “edge” of the network, to tactical users, devices must be able to present information quickly.

89. Such capabilities enable team brainstorming, document assembly and information manipulation.

90. A sharing space in a wiki environment was developed on Op ARCHER Roto 3-07 and demonstrated the operational utility of collaborative information sharing tools within the TF.



the same degree of access to the network, role-based and credentialed access protocols will enable security of information. Together with common encryption methods, trusted and rapid guards and filters, the FNC will be able to operate in multilevel security environments.

- **Accountability.** Mechanisms of accountability throughout the network, including from those nodes operating on the edge of the network, will help to cultivate trust in the quality and accuracy of information. The design of FNC components must ensure that where practicable, subscribers are credentialed and that their decisions are tracked and retained.

In addition to the overall capability objectives above, the FNC will be characterized further by a philosophy that promotes:

- **System Management.** A fully realized FNC will result in a substantial increase in the number of networked nodes, which will necessarily imply a comprehensive system management plan. However, it may be advisable to adopt a philosophy that recognizes and attempts to resolve the CA tendency to centrally control IS systems against the desire of individual users to experiment (“improve”) on the tools delivered to them. Thus a system management philosophy that accepts that there will be certain “no fail” services that must remain under central management, while other services might be devolved to formations and units to manage, could be adopted. Such a philosophy offering some responsibility for developing and managing some services to the “edge” could foster a climate of experimentation, improvement and, ultimately, user acceptance.
- **Information Management.** The sheer amount of information exchanged between network components, coupled with unique and variable user requirements, will mean that the FNC must be characterized by a comprehensive information management strategy. Such a strategy would be enabled with a common and formal ontology of the military domain, thus enabling the consistent representation of information throughout FNC components.
- **Knowledge Management.** The FNC will need to provide a robust knowledge management (KM) ability to allow users to distil information from a wide variety of sources, including humans, sensors and weapons. KM should incorporate intelligent agents to enable automatic notifications, smart tracking, dynamic information packaging, natural





language parsing,⁹¹ and semantic searches.⁹² Features such as intelligent agents,⁹³ smart data histories, web applets, and avatars,⁹⁴ etc., all enabling a subscriber to assemble relevant and composable information, are significant to enabling a networked force. An automated KM capability enabling human analysts would need to be supported by comprehensive analysis engines that can parse sensor data, chat logs, emails, and reports against CCIRs, RFIs, plans and running estimates for useable information. Notably, automated KM need not necessarily be deployed into theatre; rather, it could be supplied from remote locations. Such a capability would allow unstructured information to be transformed into structured information suitable for data queries, thus extending collaboration to non-human components of the FNC. In addition, data that JIMP contributors provide⁹⁵ will need to be incorporated into a KM capability goal. Notwithstanding technological assistance, human analysts are expected to continue to perform a necessary KM role.

- **Information Dissemination.** As elements of the Canadian Army carry out dispersed operations, information will need to be disseminated to a variety of user segments over wide areas. To enable this, a high bandwidth *communications infrastructure* capable of transmitting voice and data will be a necessary feature of the FNC. High bandwidth radios configured for installation in vehicles and personal tactical harnesses and radio rebroadcast (RRB) systems (integrated into airborne UAS, or into small, tethered aerostats) available at least down to platoon level could be considered as potential components of the FNC.

91. Natural language parsing systems convert samples of human language into more formal representations that are easier for computer programs to manipulate. Smart applications incorporating natural language processing could deliver a capability that helps to discern the correct intent or meaning of a term or acronym for which there are multiple definitions. Parsing an unstructured text field in an email, chat or other medium, NLP agents could search for known terms and acronyms and then prompt or suggest to the composer possible meanings for the term being used. Similarly, NLP could aid a receiver by parsing the entire phrase in which a term or acronym appears to derive context and suggest a narrow set of probable search matches/data records to the term.

92. Web 3.0, A Web Beyond Words. <http://www.pcmag.com/article2/0,2817,2102861,00.asp>.

93. Incorporating intelligent agents similar to Amazon's purchase recommendations feature ("the last five staff officers planning an information operations campaign used this plan as a starting point"), or TripAdvisor's group-based rating recommendation feature ("four out of five previous subscribers found this source of intelligence data to be useful") or Google Maps -based web applet mashups presenting user defined information on a specific point or area will allow subscribers to quickly find and assemble information of immediate relevance to their operations.

94. An avatar is a computer user's representation of himself or herself, whether in the form of a three-dimensional model used in computer games, a two-dimensional icon (picture) used on Internet forums and other communities, or a text construct found on early systems such as MUDs. It is an "object" representing the embodiment of the user. ([www.wikipedia.org // search "avatar"](http://www.wikipedia.org//search%20%22avatar%22))

95. *Towards Land Operations 2021: Studies in Support of the Army of Tomorrow Force Employment Concept*, Chap 7.



SPECIFIC NETWORK OBJECTIVES

Certain objectives⁹⁶ could assume a higher priority based on need balanced against the risk of adopting the technology. Similarly, decisions to proceed with capability objectives should avoid wherever possible the tendency to deliver “one-off” solutions tailored to perceived branch/functional needs. At all times it must be remembered that capabilities as they are scoped should further the ability to communicate and share information amongst commanders and subordinates. The following objectives are considered in priority:

Improve Information Presentation. Soldiers in the course of their duties will be subject to prolonged periods of stress and fatigue that, when combined with unpredictable threat actions, can contribute to errors of perception, cognition and decision making. To address this, some considerable effort will need to be devoted to understanding the human dimension⁹⁷ as it relates to multifaceted information flows and information sharing, resulting ultimately in a useable and improved user interface. High fidelity battlefield visualization tools, ideally incorporating augmented reality⁹⁸ (AR) or virtual reality (VR) features aimed at improving information display, performance, system supportability and design integration, will be ideal areas for investment:

- Functional capabilities supporting improved information presentation include but are not limited to:
 - ✦ *Own positional awareness* to provide own location information making use of available geolocation devices is identified as a “no fail” capability.
 - ✦ Navigational support to enhance own positional awareness, facilitated with limited planning functions, focused on route support with turn by turn navigation.
 - ✦ *Own positional awareness* enhanced with the addition of location and activities of friendly, neutral and hostile forces, proximity alerts and so on.
 - ✦ Support the shared SA of distributed decision-makers through collaborative planning and information representation tools.

96. This section does not attempt to specify the tools or technology, although it will occasionally point to some existing examples to describe the potential characteristics of a toolset that could meet a capability objective.

97. The human dimension will include understanding social, organizational, task and skill structures of user groups.

98. <http://www.wired.com/gadgetlab/2009/08/augmented-reality/#more-22882>.

➤ Enabling Tools:

- ✦ An augmented reality⁹⁹ (AR) / virtual reality (VR) enabled integrated tactical display to provide a customisable display to the user of information available from multiple data sources. At the lowest levels, the degree of user configuration might well be constrained due to bandwidth and security limitations; however, at other user segments, there may be increased demand for individually or user-defined operational picture¹⁰⁰ (UDOP):
 - Focus on any particular areas of interest in the world, and obtain data using feeds from relevant regional and national assets.
 - Create relevant operational pictures at multiple levels of abstraction, from theatre-level C2 perspectives aimed at the strategic decision-making team to detailed, tactically oriented views suitable for individual soldiers or sections to make decisions.
 - Transform large amounts of raw data into a meaningful storyboard that can be understood at a glance and animated backwards and forwards in time.
- Three-Dimensional Rehearsals – A highly desirable feature would be a visualization of the battlespace in three dimensions—linking digital imagery, digital terrain elevation data (DTED) information and real time updates of changes in the physical environment— allowing commanders and staff to conduct more realistic war games/rehearsals.
- Concepts such as a lightweight, multi-touch, multi-user (MTMU),¹⁰¹ compact and horizontal *digital “bird table”* around which commanders and subordinates may gather to plan and that incorporate layers of near real time and real time information to augment sensor feeds would be an ideal enabling tool.

99. FNC devices, particularly sensor viewfinders, could be enabled with additional information overlaid on top of the sensor feed to provide rich detail about the target area. For instance, an AR-enabled viewfinder leveraging location-based services and thus “knowing” where the operator and target are could provide the operator with additional and customizable contextual information such as (human) target personality profiles, target capabilities, and so on.

100. A UDOP provides a customized and tailorable view of operationally relevant information to different subscribers depending upon their need.

101. A MTMU is a touch screen elevated vertically or horizontally above ground level. The standard mode of operation is for the operator to stand to the side, working the screen. Controlling the screen is done by gesturing while simultaneously touching the screen. Typical gestures include simple mouse-like gestures (poking, dragging, etc.) and more complex gestures like making circles. An arbitrary number of points or gestures can be recognized by the device. Any form of graphical media can be displayed on the screen. A working example is the CNN Election Centre multi-touch screen.

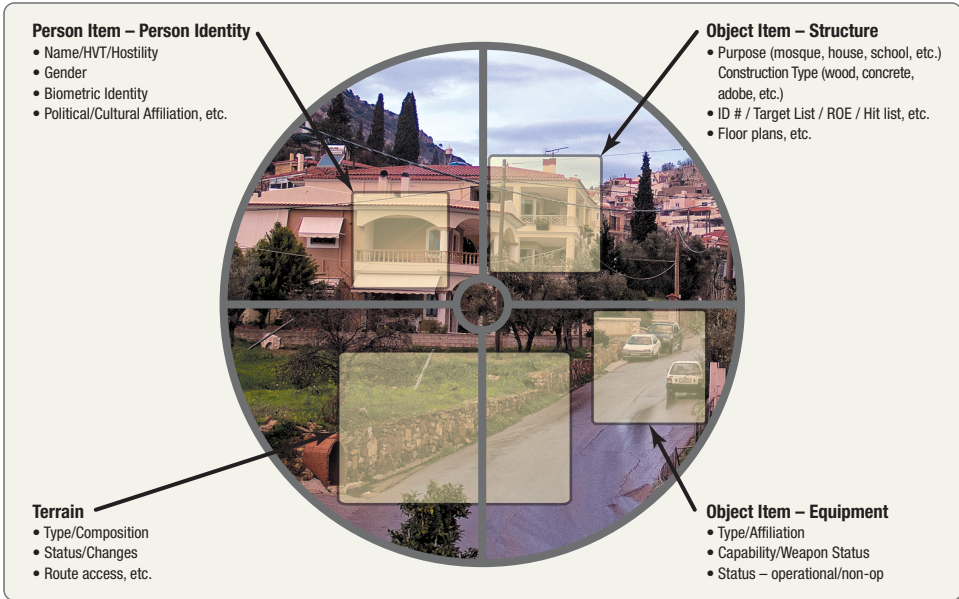


Figure 7: Example Augmented Reality Sensor View

Improve Reach. The purpose of improving reach is to expand the audience or recipients of information within the network. The most significant and “no fail” capability to enable reach will be in the form of an all informed secure voice network. It will need to offer a high degree of availability, be redundant, offer multi-protocol transmission, and allow users to communicate by voice, by text or graphically:

- **All informed secure voice network service.**
 - ✦ All informed secure voice everywhere, all the time, provides a CNR-like voice capability. It is a “no fail” capability.
 - ✦ Private voice everywhere, all the time, provides telephone-like functionality, meaning that private, one-to-one voice communications may be established between those nodes so equipped.
- **Multi-Caveat – Multi-Level Security Nodes.** In ADO, Canadian soldiers may expect to have to exchange information in a JIMP environment. Such information exchange agreements are likely to be temporary, to change rapidly, and to be conducted in an environment where the coalition networks may not be certified and accredited (trust) to the same degree of interconnectivity as our own. Therefore, devices/nodes delivered to most user segments will need to be capable of exchanging information under multi-caveat, multi-level security



contexts. FNC devices will require a *cross domain security* solution that extends the reach of information between security domains—indeed, a model that expands on the current classification of information types from Top Secret (strategic INT, etc.), through Secret (tactical INT, long-term planning, etc.) and Unclassified. A suggested classification known as *Sensitive but Unclassified* (SBU) accompanied by sensitivity caveats could allow inclusion or exclusion of trusted JIMP partners in the (largely perishable) information exchange.

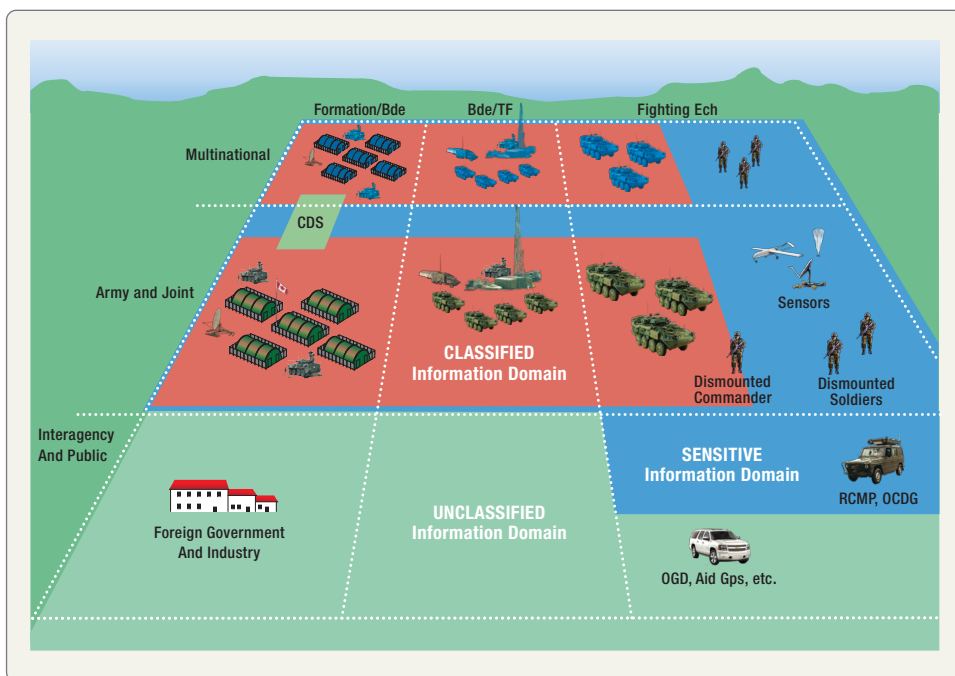


Figure 8: Multiple Independent Levels of Security – Extended to the JIMP environment

- **Integration and Interoperability.** An FNC goal should be to be interoperable with joint and coalition networks, initially at the edge of the CA network domain between the CA and coalition partners.
 - ✦ Integration of as many FNC components as possible is a desirable capability objective if only to reduce or eliminate the instances of middleware (as points of failure) that is currently necessary to allow disparate systems to exchange with each other.



- ✦ Networked components will need to be interoperable at the network-bearer system level (physical connectivity of the various components), at the data level (a common data model), at the application/services level and at the security policies level.
- ✦ Given the requirement to operate in a JIMP¹⁰² environment, there is an operational need for the FNC to be interoperable with our allies, particularly the ABCA armies, the CF (joint and services) and other governmental departments (OGDs).

- **Improve Throughput.** The AoT network should be enhanced with the provision of high capacity bandwidth throughout the AO.
- **Real Time Online Communications (RTOC).** The capabilities¹⁰³ could allow soldiers to quickly “chat”—one to many or private, point-to-point, unstructured text messages—without having to resort to voice communications. RTOC could be enhanced with parsable search, integrated address books, embedded media, message priority settings and digital signatures.

Networked Sensors. Linking various sensors to each other will not only allow the sharing of the sensor product but will also allow the smart allocation of sensor resources, enable machine-to-machine collaboration, etc.:

- **Shared Sensor Product.** The sensor product in multi-media format should be shareable, through many levels of user segments.
- **Sensor Allocation.** All sensors should not only be “visible” to the tasking authority, but also to each other (discovery).
- **Machine-to-Machine Collaboration.** Sensor/weapon queuing (defection) is a particularly useful capability that enables standoff target identification and acquisition and engagement.
- **Active and Passive Threat Discrimination.** Capabilities that, in conjunction with the human user, enable the identification of threats in a high clutter environment.

102. In an environment where information is expected to be shared amongst JIMP partners, the CF Integrated Command and Control project has identified “three types of information that could be shared as part of interdepartmental mission collaboration”:

- List (database) of problems/questions for which there are yet no solutions/answers.
- List (database) of assets that could be available in a crisis across all applicable departments/agencies.
- A “Recognized Operational Picture” for each on-going mission from the lead department confirming what they are collectively doing and with what degree of success.

103. Any Chat service as an example.



Improved Range

- Extend the range of communications suites by offering range-extending capabilities such as aerostat-borne radio rebroadcast capabilities.
- Mobility, particularly in optimizing communication- and network-device size, weight and power (SWaP).
- Location-Based Services. Given the expected physical dispersion of the ADO force, components of the FNC will need to be not only “aware” of their location but must also be able to “discover” other devices (sensors, for instance) and be able to access services on demand that are customized to the user and location. LBS can include services such as traffic conditions, turn-by-turn navigation to specific addresses, resource tracking, proximity-based notification or alerts, and so on.

Improve the Distribution of Intelligence Product. The network should deliver actionable intelligence in a variety of multi-media formats to a wide variety of users. The ADO force will need to be better able to share raw data from soldier to soldier, from soldier to dismounted or mounted commander and from soldier to supporting elements than is the case now. For instance, the provision of individual rifle scopes with digital technology enhancing the soldier’s ability to act as an initial sensor could allow, for instance, the near real time sharing of (a) digital image(s) between soldiers while simultaneously informing the intelligence analysis tools.

Improve Lethality

- Elements of the ADO force will need networked access to joint fire support assets. As indirect fire support to a force is typically characterized by a high degree of centralized control, high demand, pre-planning (ROE and target selection criteria) and special request procedures, the FNC will need to allow observers to collect and disseminate target information to joint fire support.
- Secondly, many user segments will need to possess an ability to control the engagement of targets with indirect fire support than is currently the case. This need may be met with a combination of organic sensors and trained and authorized observers resident at levels much lower than is currently the practice. Regardless, there will continue to be both a high demand for fire support coupled with competing priorities for the use of limited resources, thus the FNC will need to provide access to and encourage agile fire support allocation mechanisms.

- Weapons Platforms as FNC nodes. The network will need to enable surveillance and target acquisition data exchange between manned and unmanned weapons platforms, treating these as nodes on the network.
 - ✦ Implement a Cooperative Engagement Capability¹⁰⁴ in a variety of weapon and sensor systems, including in indirect and direct fire mounted and dismounted systems. CEC allows the soldier or weapons system out of contact with the threat to engage a target that a soldier or sensor in contact has designated. Both the sensor/designator and the shooter are able to see the target through the sensor.
 - ✦ Smart Weapon/Platform Collaboration. Targeting software will need to be “smart,” fostering collaboration between sensors and weapons platforms. A capability that enables calls for fire to be automatically parsed for availability of a platform to service the target, munitions selection, smart fire mission queuing and defection¹⁰⁵ should be the core capability objective within the networked fire support capability.
 - ✦ Allow the soldier to act as a target designator and to share that information between a wide variety of FNC nodes (command nodes, other soldiers, sensors and weapons platforms, etc.).
 - ✦ Enable the decider to alter the munitions effect post firing or launch.

Protection of the Network

- **Information Security.** The FNC will need to deliver secure computing platforms. Available solutions include possibly the NSA-sponsored High Assurance Platform (HAP) architecture, which supports multiple security domains on a common computing platform and virtual machines running over a trusted computing platform.

104. A “Cooperative Engagement Capability (CEC).” CEC allows a providing weapon sensor to communicate target data to a receiving weapon sensor or sensors and decision maker(s). The decision maker accepts or rejects the cue and, until the cue is accepted, the decision maker retains complete control of the weapon system. If the decision maker accepts a target cue, then the weapon system will automatically slew to the bearing of the target. The decision maker then resumes control of the weapons system and completes the engagement process.

105. For more on queuing and defection modelling, particularly the effectiveness of systems in answering calls for fire considering responsiveness, distance between delivery systems and targets, and the number of targets yet to be prosecuted, see Wheeler, S., “An Application of Queues to Offensive Support Indirect Fire Weapon Systems.”

- **Self-protection.** Given the expected proliferation of unattended sensors, remote networked nodes, dissemination paths and data storage, the FNC will need to possess a significant protection capability against computer network attack (CNA), jamming and sabotage.

Lower the Cost of Ownership

- **Simplified Training.** The delivery of a network capability will not be successful without a comprehensive fielding and training plan. Recognizing this, the Army will need to ensure that delivery of FNC components is coordinated with the road to high readiness, incorporate self-learning tools, encourage user feedback on the usability of the systems and ease of use, and commit to the evolutionary introduction of technology. In other words, “sorting out how to properly employ new technology in the midst of a fire fight is a recipe for failure”.¹⁰⁶
- **System Support.** FNC will require a very high degree of reliability, availability, maintainability and durability (RAMD) and not impose a maintenance burden on the individual soldier.
 - ✦ Reliability. FNC components must be able to dynamically self-heal and reform the network when one or more communications paths between FNC nodes are disrupted.
 - ✦ Availability. There is an operational need for the FNC to be able to operate 24/7 in all climates and under all weather and terrain conditions.
 - ✦ Maintainability. Leveraging lightweight materials technology, FNC components will be optimized for reduced size, weight and power (SWaP).
 - ✦ Durability.
- **System Management.** System management capabilities should be aimed at reducing the burden of managing FNC devices on system managers, operators, technicians, and end users.
 - ✦ Device integration via auto detect capabilities wherein networked devices discover and register with each other.
 - ✦ Signal Planning Service. Semi-automated signals planning capability to aid in the development of the signals plan.
 - ✦ Platform “Dashboard.” Monitoring and control of integrated platform devices and services from a single point of entry.

106. Callahan, Lieutenant Colonel W.E. (USMC), “The Effects of Network-Centric Enabled Distributed Operations Forces on the Principles of War,” 18.



- ✦ Automated initiation of system actions based on device or service status (for example, on detection of “fuel low,” a networked vehicle might automatically trigger a POL request).
- ✦ Increased data throughput to all user segments.

Sustainment. With dispersion in space as a given, the network will need to be designed to enable smart CSS functions while also reducing the requirement for specialized system support:

- **CSS Functions.** The ADO force will require a reduced logistics footprint (for instance, a reduced demand for consumable power supplies, and/or the provision of regenerative power supplies) and an ability to intelligently configure re-supply loads. Thus, an FNC capability objective could be the provision of automated reporting of consumable materials, realized perhaps through technologies similar to radio frequency identification (RFID) devices for example—attached to ammunition pallets, water and food and so on.
- **HSS Functions.** Physiological monitoring systems can improve soldier survivability by providing triage information en route to medical support and ensuring timely medical intervention, thus an HSS capability objective for the FNC could be the provision of individual biometric devices to support casualty diagnostics.

USER SEGMENTS

Having described the general goals and some specific capability objectives of the FNC, we can turn to the question of what generic user¹⁰⁷ segments exist and the information they will consume. This study purposely avoids identifying the very specific needs of branches and specialty trades, since CA structures are likely to evolve over time with capabilities moving from one branch to another. Thus a useful construct containing broad classes of users is required and fortunately exists in the form of the categories of users identified for the LCSS LE project. Deliberately missing from this section is any specific discussion of users groups outside of the FNC; these could include for example corporate networks within DND, or user segments we may wish to exchange information with, but for whom the FNC is not designed for. Finally, it is important to note that these broad classes of user

107. Different users will place variable demands on the network and will often consume the same information in different contexts and thus will require that the network offer a variety of applications and capabilities suitable to manipulate that information.



may be comprised of both human and non-human entities. By extending the class of users to non-human actors, it is possible to incorporate autonomous systems into the discussion of FNC.

The user segments are as follows:

- ***Dismounted Segment – Fighter.*** This users segment is typically made up of combat arms soldiers. They are the basic building block of the section or detachment and is a common and significant human level of entry of information into the FNC. Soldiers engage in close combat and may be physically dispersed in the conduct of their tasks, which could include but are not limited to close combat in open and complex terrain and air-mobile operations. Engagements are likely to be short in duration and high in physical exertion and require substantial cognitive resources to achieve clearly defined tasks. Dismounted soldiers possess a high degree of mobility and must be completely self-sufficient for up to 72 hours of high intensity contact. The highest priority capabilities that the soldier will demand from FNC will be secure voice everywhere and battlefield visualization tools that deliver a simplified presentation of a local tactical picture. Thus the soldier requires that FNC components be capable of supporting soldier needs under rapidly changing situations, when there is little time for deliberate planning, or for generating and evaluating detailed courses of action (COAs).¹⁰⁸ In close combat, the soldier will need easy mechanisms to retrieve and send information, including for the purposes of amending plans and resynchronizing with flanking friendly forces. Components offered to this segment will need a “glance and select” interface with few initial input options linked to an overarching design principle offering components that are (1) *simple to operate*, (2) *lightweight and wearable*, (3) do not interfere with individual movement, and (4) do not distract attention from localized view of the battlespace. “Information¹⁰⁹ that should be rushed to the platoon member should be limited to only the critical information that affects their decisions or actions. This would result in less cluttered displays that are easily read and understood. Soldiers should be allowed to ‘pull’ information that is less critical or that is only needed occasionally.

108. Tate, A., Levine, J., Jarvis, P., and Dalton, J., “Using AI Planning Technology for Small Unit Operations.” See <http://www.ai.ai.ed.ac.uk/~oplan>.

109. Redden, E., “Virtual Environment Study of Mission-based Critical Information Requirements,” ARL-TR-26-36, March 2002, 2.

Criticality of knowledge of threat forces locations beyond small arms range from the objective increases as the level of leadership increases”.

- **Mounted Segment – Fighter.** *This segment* is comprised of soldiers who are normally combat arms. In this role, they conduct the fight from mobile platforms, engaging targets with direct fire weapons at ranges often greater than when employed as dismounted segment fighters. They may be expected to conduct movement through the battlespace over extended distances, conduct combat estimates with simplified tools, and provide and receive orders and other instructions whilst moving. In addition to the capabilities provided for the dismounted segment fighter, FNC nodes installed within mounted segment fighter platforms will be expected to be (1) simple to operate, (2) capable of providing voice, text and graphical communications, and (3) a view of organic and inorganic sensor feeds; all of which is optimized for a bandwidth constrained environment.
- **Tactical CP / HQ Segment.** At the tactical CP / HQ segment, the FNC is optimized to support a unit or sub-unit commander while simultaneously providing some support to his battle staff. Commanders at all levels need a high degree of situational awareness and situational understanding. The commander employs the components of FNC to receive and disseminate a common operating picture, communicate with subordinates, plan and control operations, and collaborate with other users. The commander’s information needs may be summarized as an interest in the status of an ongoing operation, the COAs available for future operations and information regarding his higher commanders’ intent. The commander’s information needs will comprise a balance between timeliness, quality and relevance—in other words, he may have a high demand for a variety of information needs under rapidly changing circumstances.

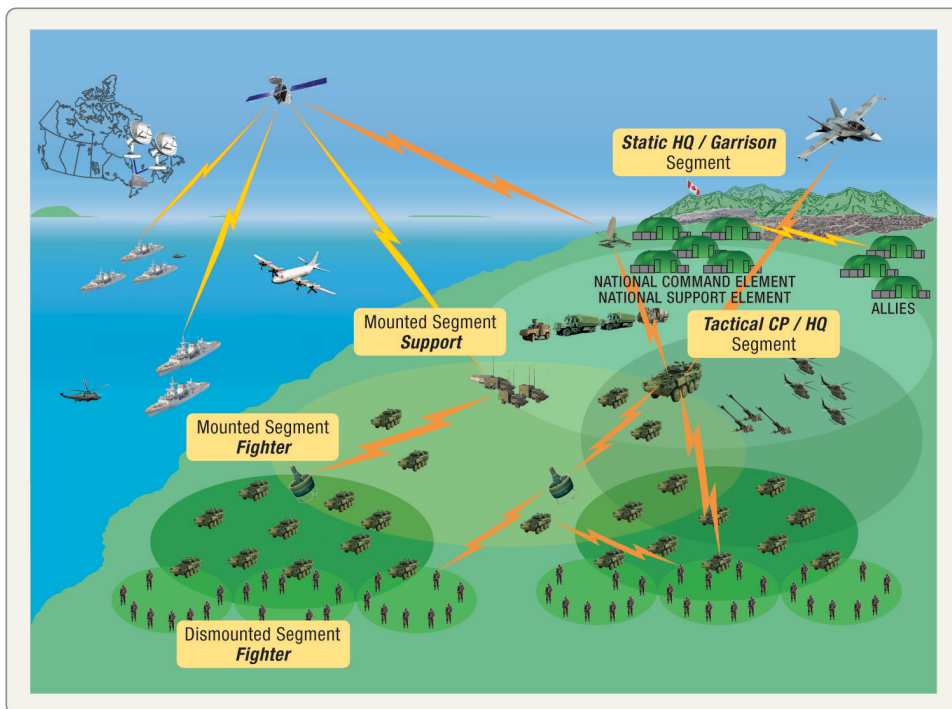


Figure 9: User Segments

- **Mounted Segment – Support.** Supporters are grouped loosely into those whose primary function is to assist the commander with specialized combat support to operations (fire sp, cbt engr, etc.) and/or to sustain (CSS, HSS, etc.) the force. This segment may be further broken down into those whose primary function is to support the availability of the network and communications infrastructure. As supporters, their information needs are complex; they consume a high volume of information and require access to specialized analysis tools. Their network needs are somewhat different than for the fighter in that their role is primarily one of resource management; they have less demand for lightweight wearable components but rather require components that can provide greater analysis tailored to the support specialty (for instance, a CSS supporter needs greater access to and more complex information about, the status of resources).
- **Static HQ / Garrison Support.** At this segment, the FNC components are optimized for use by the commander and HQ staff in a static environment. The static HQ/garrison support segment supports the



commander with analysis and advice. The staff requires access to analytical and collaborative planning tools, to enterprise services and doctrinal and operational documents and, of course, to situational awareness. Commanders and staff at all levels need a high degree of situational awareness and situational understanding. The commander employs the components of FNC to receive and disseminate a common operating picture, communicate with subordinates, plan and control operations, and collaborate with other users. The commander's information needs may be summarized as an interest in the status of an ongoing operation, the COAs available for future operations, and information regarding his higher commander's intent.

- **Non-Human Actor.** As more sensors, weapons platforms and other non-human actors proliferate on the battlefield, commanders will need a means to issue unambiguous instructions and communicate the commander's intent¹¹⁰ to machine or non-human-actor elements of the FNC. Indeed, considerable effort will need to be devoted to developing and delivering a technical solution¹¹¹ to effect human to non-human C2. Additionally, non-human actors will need to be equipped with validation protocols to determine the applicability of such decision discriminators as rules of engagement, shoot/no shoot, task selection, survivability and more.

Much still remains to be explained about how an ADO force might be organized, equipped and trained to fight, and without this employment model it will be difficult to fully describe the required network capabilities. Finally, it is important to remember that the network will be designed for the warfighter, possibly a senior officer commanding a formation or an NCO commanding a section, and that, with that in mind, the technology to be implemented must enhance decision making rather than overwhelm the decision maker. Key to achieving this must be advanced and realistic training on the use of new technologies, coupled with the enabling of the soldiers to be empowered as discriminators and deciders.

110. Work conducted to date within the Simulation Standards Interoperability Organization (SISO) aimed at creating a Battle Management Language (BML) suitable for transmitting C2 information to non-human nodes may point the way towards achieving this objective.

111. While simple instructions (where, what, when, how, etc.) between humans and non-human nodes may be achievable now, considerable effort should be made to realize a method of communicating commanders intent (why) coupled with moral imperative between humans and non-human nodes.



OTHER OBJECTIVES

The objectives below do not easily fit within the user-segments construct, yet they are important to the realization of an FNC:

➤ **Training**

- ✦ Self-training. Components of the FNC should be designed to encourage use, experimentation and enable “self-training” modules as a part of an integrated training package. Concepts such as embedded multi-user domains (MUD) could be considered.
- ✦ Human Factors:
 - (a) These are focused on the end user and do not create an additional burden or otherwise impede the user from completing his usual tasks.
 - (b) They are intuitive and easy to manipulate, with an intuitive human-systems interface, simple user procedures and a high degree of simplicity.
 - (c) They have as few parts as possible. The components of the FNC must not hinder movement, either mounted or dismounted, and must be lightweight (ideally 4.5 kg or less, complete with batteries and cables).
- ✦ Requires Intensive Education and Training. Inevitably, as a system of systems, some components of the delivered FNC will be comprised of complex systems of communications hardware and application software. Therefore, it is highly probable that some components of the FNC, particularly those involved with the system administration, may continue to require intensive education and training, although the goal is to reduce this as much as possible.

- **Flexibility:** The FNC must be flexible in its physical and logical configurations. Flexible configurations will allow the FNC to be adapted for use in a wide range of organizations and environments and a variety of operational circumstances. It must be recognized that not every component of the FNC requires the same degree of flexibility; for instance, certain communications suites may have certain physical or logical properties (size, security, etc.) that, in effect, restrict

their flexibility. The ideal is to achieve universal flexibility, but it is recognized that that still may not be possible given technology and unique employment demands constraints of the day:

- ✦ Components of the FNC should be able to rapidly and automatically adapt themselves to the configuration of the user segment and to the type of operation. For example, the FNC will be able to automatically configure services based on user profiles, mission-specific requirements and the type of operation. Ultimately, components of the FNC should be designed to adapt to any operational structure or circumstance.
- ✦ Some components of the FNC, because of their complexity or as a result of security requirements, may still require specialist intervention on site to configure for the end user.

In addition to these general capability requirements, FNC components should demonstrate a high degree of adaptability and potential evolution to meet the post-2021 army requirements.

Each potential FNC component must also be carefully studied to understand the full implications of PRICIE¹¹² and to ensure it is sustainable within the overall AoT resource envelope.

END STATE

The Future Network Capability will connect commanders, soldiers, sensors and weapons in a seamless network of information exchange, empowering the Army to dominate the battlespace. The FNC will offer a secure, robust network that provides the necessary connectivity to all Canadian Army operational nodes—including reach back to national/joint networks—and that is extensible to the JIMP environment.

112. The mnemonic PRICIE provides a standardized analytical framework to assess/build new capabilities. The letters of PRICIE represent the following: Personnel, Leadership and Individual Training. Research & Development and Operational Research (plus Experimentation). Infrastructure, Environment and Organization. Concepts, Doctrine and Collective Training. Information Management and Information Technology. Equipment and Support.

PART 6 – RECOMMENDATIONS AND CONCLUSIONS

Recommendations

- Develop a Canadian Army C4ISR strategy to identify and manage the implementation of capabilities, acknowledging resource constraints, a need to accommodate life extension plans for legacy systems, and a need to introduce a network capability in an evolutionary manner.
- Develop a comprehensive Army information management strategy, extended to encompass the JIMP environment.
- Develop an overarching LF network architecture to govern implementation of the FNC out to 2028. The architecture should be compliant with the CF C4ISR architecture (DNDAF).
- Develop a force employment model for ADO, complete with elaborated use cases for FNC components across selected operations.
- Develop a comprehensive ontology of the military domain. Coordinate overlapping areas of interest between the military ontology and the JIMP environment.

Research areas to optimize the FNC

- Develop a detailed command and control ontology.
- Develop a model for automated direct and indirect fire discovery/registration, queuing and defection and the methods of command and control in a semi-automated environment.
- What will be the nature of JIMP information exchanges within the AoT HQ?
- Investigate simplified¹¹³ pictographic representations of battlefield objects.¹¹⁴

113. See Apple iPhone.

114. The development of graphical icons for military use originates in the need to represent in simplistic and analogue form military objects on map overlays. In recent years, little research has been done to simplify the representation of military symbols in the digital domain, especially for the purposes of rendering in digital format on a small display screen. To communicate semantically complete information onto handheld devices without cluttering the display, it is likely that FNC components will require even more simplified graphical presentation of battlefield objects than are available in the doctrinal lexicon of military symbols.

APPENDIX 1 – REVIEW OF NETWORK-ENABLED OPERATIONS DOCUMENTS

General. The literature devoted to network-enabled operations has expanded greatly in the last few years. Beginning with Cebrowski and Gartska, development of the concept remained generally within the realm of U.S. capability development. Recently Canadian and Allied doctrine and capability developers have produced a wider body of thought with the purpose of examining and explaining in significant detail the requirements necessary to achieve NEOps. A short and necessarily incomplete listing of readings is detailed below; however, requirement developers are strongly advised to consult the bibliography. Documents listed below are not arranged in any particular order:

➤ **Beware of Putting the Cart Before the Horse: Network Enabled Operations as a Canadian Approach to Transformation.**

A report prepared by Dr Allan English, Dr Richard Gimblett, and Mr Howard Coombs for Defence Research & Development Canada (DRDC) concludes that “Canada and the CF should be cautious about using NCW as the foundation for NEOps because the context and needs that are the basis for NCW may not be congruent with Canadian requirements.” It explicitly cautions that theories of NCW and NEOps may not be sufficiently developed to address the unique needs of Canadian experience and military culture. It suggests that the human network and not the technical network “should be the basis for future approaches to CF transformation” and that, therefore, the design of future networks and indeed the FNC will require “network architects not only to consider the use of information technology as an enabler, but also for them to address the much more complex issue of the creation of effective social networks”.

- **A Woven Web of Guesses.** A presentation delivered by Lieutenant-Colonel Ralph Giffin (CAN) and Mr Darryn J. Reid (AUS) to the 8th International Command and Control Research and Technology Symposium (ICCRTS) in Washington, D.C., in June 2003 in which the premises underpinning Cebrowski and Gartska’s “Network-Centric Warfare: Its Origins and Future” were challenged, specifically and among others they “predict[ed] that



the military network will be constructed primarily to satisfy the needs of centralized controllers, and not the needs of operators.” It is a thought-provoking piece, serving as a wake-up call to those designing the military networks of the future.

- **LandWarNet 2015.** Produced by the U.S. Army Training and Doctrine Command (TRADOC), LandWarNet 2015 provides a concept of operations (CONOPS), including a small vignette, and captures capabilities in currently approved concepts and articulates a single network reference across the operational functions.
- **Operational Requirements Document for the Future Combat Systems.** Produced by the Unit of Action Maneuver [sic] Battle Lab in January of 2005, this document explicitly states the key performance parameters (KPP) of each element of the U.S. Army Future Combat System of systems, from manned to unmanned vehicles, future networks and sensor suites, giving each system a “threshold” and “objective” KPP. It is a comprehensive resource for the development of requirements for the entire family of land combat systems (FLCS).
- **NATO Network Enabled Capability Feasibility Study, Volume 1.** Produced by the NATO Consultation, Command and Control Agency (NC3A), this volume seeks to address transformation within NATO and to strengthen the ability of the alliance to better carry out the full range of its missions and respond collectively to new security challenges.





APPENDIX 2 – ABBREVIATIONS

AAP	Allied Administrative Publication
ABCA	America, Britain, Canada, Australia Armies Standardization Program
ADO	Adaptive Dispersed Operations
AoT	Army of Tomorrow
BDA	Battle Damage Assessment
BLOS	Beyond Line of Sight
C2	Command and Control
CF	Canadian Forces
CID	Combat Identification
CNA	Computer Network Attack
COP	Common Operating Picture
CSS	Combat Service Support
DLCD	Directorate of Land Concepts and Designs
EW	Electronic Warfare
FEC	Force Employment Concept
FEM	Force Employment Model
FCS	Future Combat System (U.S. Army)
FLCS	Family of Land Combat Systems
FNC	Future Network Capability
FSE	Future Security Environment
FTS	Force Tracking System(s)
ISSP	Integrated Soldier System Project
ISTAR	Intelligence Surveillance Target Acquisition and Reconnaissance
JIMP	Joint, Interagency, Multinational Public
CA	Canadian Army
LOS	Line of Sight



NLOS	Non Line of Sight
NCO	Network-Centric Operations (USA)
NEOps	Network-Enabled Operations
OBG	Optimized Battle Group
PRICIE	Personnel, Research and Development, Infrastructure, Concepts and Doctrine, Information Technology and Equipment.
ROE	Rules of Engagement
RTOC	Real Time Online Communications
SU	Situational Understanding
VOIP	Voice Over Internet Protocol



APPENDIX 3 – GLOSSARY

Actor

An actor is an implementation independent unit of responsibility that performs an action to achieve an effect that contributes to a desired end state. Each actor can perform one or more roles. An actor can be a consumer of a service. This is typically the role of a commander. An actor can also be the producer of a service. This is typically the role of those who are ordered to conduct a task by a commander. An actor can perform several roles, e.g., a commander can require a service from his subordinates but he is also delivering a result to his higher echelon commander. Common similar terms are (1) Business Actor, (2) Performer, (3) Logical Node.

Architecture

The fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.

An architectural framework¹¹⁵ is simply a method of classifying and organizing complex information and processes. It is fundamentally a structure within which system designs may be placed, a set of generic components that may (or must) be used in the systems, a set of generic relations (interfaces) that may (or must) be used between these components, and some rules about all of those that guide and constrain their use, and the addition of new parts of the framework or new components. Note that by using generic relationships and components, it is possible to discuss desired capabilities and features of the FNC without being constrained by the limitations of specific technologies.

Client–Server Architecture

A client–server architecture separates a client node upon which resides the user software from a server upon which resides the data that the user software will manipulate. A typical client–server architecture is a web browser.

Combat Identification (CID) (Joint Publication JP1-02)

Combat identification is the process of attaining an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision.

115. For detailed information on Architectural Frameworks, please consult the Department of National Defence and Canadian Forces Architecture Framework (DNDAF), or the NATO Architectural Framework (NAV v3).



Common Operating Picture (Army Terminology Bank, approved 2 Oct 2002)

A representation of operations based on common data and information that is shared by more than one command and that can be tailored by users.

Force Tracking System (Chairman Joint Chiefs of Staff Instruction (CJCSI) 8910.01A)

Employment of techniques to actively or passively identify and track U.S., Allied or Coalition forces for the purpose of providing the combatant commander with enhanced battlespace situational awareness and reducing fratricide.

Information Object

An information object is an implementation independent representation of the facts that need to be known about objects and their coherence in order to turn the set or representation into information. The objective of capturing information objects is to identify and unambiguously describe all the elements of information and their properties that are relevant for execution of tasks in the mission space.

Integration

Integrate: complete (imperfect thing) by addition of parts; combine (parts) into a whole. *For* FNC: 1. the state of combination or the process of combining into completeness and harmony. 2. In computer science, allows data from one device or software to be read or manipulated by another.

Interoperability (Army Terminology Repertoire, approved 15 September 2005)

The ability of military forces to train, exercise and operate effectively together in the execution of assigned missions and tasks. NATO: (1) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.

Physical Interoperability – The connection of communications and information systems infrastructure between users.

Syntactic Interoperability – The users speak the same language, for example verbally or using machine language.

Semantic Interoperability – The users have the same understanding of the linguistic concepts. Thus, for example, the users have the identical interpretation of the information being exchanged.





Pragmatic Interoperability – The receiver is able to anticipate how to act. The addressee realizes the communicative intent of the sender. This ability to act in concert is regarded as a pre-condition to perform self-synchronization.

Knowledge Management (Army Terminology Repertoire, recommended 2003)

A comprehensive strategy that permits the effective collection, sharing, utilization and retention of the critical knowledge possessed by Army personnel.

Latency (Defence Terminology Bank, approved 3 May 2005)

The time interval between the instant at which an instruction control unit initiates a call for data and the instant at which the actual transfer of data starts.

Location

A location is a geographical spot, e.g., a place, represented by spatial coordinates. The objective of capturing locations is to understand where activities are executed by the actors. The same actor can carry out the same on different locations.

Mission Command (Army Terminology Repertoire, approved 10 October 2002)

The philosophy of command that promotes unity of effort, the duty and authority to act, and initiative to subordinate commanders.

Near Real Time (Defence Terminology Bank, approved 11 November 1991)

Pertaining to the timeliness of data or information that has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. The distinction between near real time and real time is somewhat nebulous and must be defined for the situation at hand.

Ontology ([http://en.wikipedia.org/wiki/Ontology_\(information_science\)](http://en.wikipedia.org/wiki/Ontology_(information_science)))

- (1) The branch of metaphysics concerned with the nature of being.
- (2) In *computer science* and *information science*, an *ontology* is a formal representation of a set of concepts within a *domain* and the relationships between those concepts. It is used to *reason* about the properties of that domain, and may be used to define the domain.

Process

A process is a composition of activities that are triggered by an event and transforms a specific input into a meaningful output.

Real Time Online Communications

Real time online communications are a set of digital communication standards and protocols in voice and text that chat, instant message, etc.



Service-Oriented Architecture

A service-oriented architecture (SOA) is a construct for a distributed system wherein applications are decomposed into separate services that are made available to consumers. Thus an SOA consists of *producers of information* (sensor nodes, soldiers, and commanders) and *consumers of information* (commanders, planners, weapon systems, etc.). The producer/consumer relationship is the basis for the term SOA. The main premise of SOA is that services do not have to be bound to a system; instead, they are loosely coupled to the system and function independently of any particular platform or operating system (OS). This allows a consumer to “discover” and consume a service without the client needing to know where the service originates from. This characteristic allows SOA to support multiple users simultaneously. To leverage the power of SOA and ensure interoperability, the many services need to be implemented according to a standard and protocol. For consumers to determine which services best suits their needs, (a remote sensor feed, for example), the service must be advertised (or published) to the end user. Network security policies restrict access to services and information and deliver varying amounts of capability to different users depending on their access credentials.

Situational Understanding (Army Terminology Repertoire, approved 10 Oct 2002)

Situational awareness to which human judgment has been applied.

Endsley proposes three levels of situational awareness, Level 1 Perception (of data), Level 2 Comprehension (fusion of fragmented data into information) and Level 3 Projection (transforming information into understanding).

System of Systems

A large, complex, enduring collection of interdependent systems under development over time by multiple independent authorities to provide multiple, interdependent capabilities to support multiple missions.

Time to Live

Time to live (sometimes abbreviated as TTL) is a limit on the period of time or number of iterations or transmissions in *computer* and *computer network* technology that a unit of data (e.g., a *packet*) can experience before it should be discarded.

PRIMARY SOURCES

- Australia. ADDP-D.3.1. *Enabling Future Warfighting: Network Centric Warfare*, February 2004.
- Australia. Defence Science and Technology Organization. *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*. DSTO-CR-0373, July 2004.
- Australia. Defence Science and Technology Organization. *An Application of Queues to Offensive Support Indirect Fire Weapons Systems*. DSTO-TR-1662, January 2005.
- Australia. Defence Science and Technology Organization. *Network-Centric Warfare Prioritisation and Integration*. ACPL-Report 20-2005-J53v1.0, issued 24 April 2006.
- Canada. Department of National Defence. *Beware of Putting the Cart Before the Horse: Network Enabled Operations as a Canadian Approach to Transformation*. Drs Allan English and Richard Gimblett, and Mr Howard Coombs. Defence Research and Development Canada, CR 2005-212, 19 July 2005.
- Canada. Department of National Defence. *Human Factors Implications and Issues in Network Enabled Operations*. Drs Allan English and Richard Gimblett, and Mr Howard Coombs. Defence Research and Development Canada, CR 2006-217, 26 August 2006.
- Canada. Department of National Defence. *Capability Development Record – Command: Enabling Command for the Contemporary Operational Environment*. Majors Darryl Gutscher, and Robert Hart, project directors. Kingston, Directorate of Army Doctrine, September 2006.
- Canada. Department of National Defence. *Department of National Defence and Canadian Forces Architecture Framework (DND/AF)*, Associate Deputy Minister (ADM) Information Management (IM), Ottawa, March 2007.
- Canada. Department of National Defence. *Land Operations 2021, Adaptive Dispersed Operations: A Force Employment Concept for Canada's Army of Tomorrow*. Major Andrew B. Godefroy, ed. Kingston Directorate of Land Concepts and Designs, 2007.
- Canada. Department of National Defence. B-GL-323-004/FP-003, *Counter-Insurgency Operations*, (Nov 2007 draft).
- Canada. Department of National Defence. B-GL-351-001/FP-001, *Signals in Land Operations*, 1 May 2008.



- Canada. Department of National Defence. *Toward Land Operations 2021: Studies in Support of the Army of Tomorrow Force Employment Concept*. Major Andrew B. Godefroy, ed., Kingston, Directorate of Land Concepts and Designs, 2009.
- NATO. *NATO Network Enabled Capability Feasibility Study, Volume 1: NATO Network-Centric Needs and Implications for the Development of Net-Centric Solutions*, October 2005.
- NATO. *NATO Network Enabled Capability Feasibility Study, Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing and NNEC Networking and Information Infrastructure (NII)*, October 2005.
- NATO. *NATO Architectural Framework (NAF) Version 3*, 2007.
- NATO. Allied Administration Publication (AAP) 6, Glossary of Terms.
- NCOIC. Network-Centric Operations Industry Consortium. *Interoperability Framework, Communications*, February 2006.
- New Zealand. New Zealand Defence Force. *Future Land Operating Concept: Precision Manoeuvre 2020*, January 2007.
- United Kingdom. Ministry of Defence. *Network Enabled Capability, JSP 777, Edition 1*, London, 2005.
- United States. Department of Defense. Office of Force Transformation. *The Implementation of Network-Centric Warfare*, 5 January 2005.
- United States. Congressional Research Service RL32411. *Network Centric Operations: Background and Oversight Issues for Congress*, 15 March 2007.
- United States. Department of the Army. *The United States Army Functional Concept for Battle Command 2015–2024*, TRADOC Pamphlet 525-3-3, Leavenworth, April 2007.
- United States. Department of the Army. *The United States Army Functional Concept for Strike 2015–2024*, TRADOC Pamphlet 525-3-4, Leavenworth, 30 April 2007.
- United States. Department of the Army. *The United States Army's Concept of Operations: LandWarNet 2015*, TRADOC Pamphlet 525-5-600, Leavenworth, February 2008.
- United States. Department of the Army. *The United States Army Commander's Appreciation and Campaign Design, Version 1.0*, TRADOC Pamphlet 525-5-500, Leavenworth, January 2008.
- United States. Department of the Army. *Air Assault Expeditionary Force (AAEF) Spiral D Experiment Final Report*. US Army Test and Evaluation Command, Alexandria VA, March 2008.



SECONDARY SOURCES

- Alberts, David S., and Gartska, John J. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised). Washington, D.C. Department of Defence (DoD) Command and Control Research Program (CCRP), 1999.
- Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military* (revised). Washington DC: Department of Defence (DoD) Command and Control Research Program (CCRP), June 2002.
- Alberts, David S., and Hayes, Richard E. *Power to the Edge: Command and Control in the Information Age*. Washington D.C. Department of Defence (DoD) Command and Control Research Program (CCRP), June 2003.
- Alston, Anthony, and Dodd, Lorraine. *C2 and Agility: Complex Adaptive and Inquiring Systems Theory for Contemporary Military Operations – A Multiperspective Approach*. Presentation to the 14th International Command and Control Research and Technology Symposium, 2009.
- Barnes, Dr. D. *A Vision of the Infantry Soldier in 2020*, RUSI Defence Systems, Spring 2005.
- Barnett, Thomas P.M. *The Seven Deadly Sins of Network-centric Warfare*. Proceedings, January 1999.
- Bain, Matthew D. *Supporting a Marine Corps Distributed Operations Platoon: A Quantitative Analysis*. Naval Post Graduate School, Thesis, September 2005.
- Callahan, LCol W.E. *The Effects of Network Centric Enabled Distributed Operations Forces on the Principles of War*, Strategy Research Project, U.S. Army War College, March 2008.
- Cebrowski, VAdm A.K., and Garstka, J.H. *Network-Centric Warfare – Its Origins and Future*, Proceedings, January 1998, 139.
- Craig, Clayton A., and Tsirlis, Christopher S., *Command and Control for Distributed Operations: An Analysis of Possible Technologies, Structure and Employment*. Naval Post Graduate School, Thesis, June 2007.
- Czarnecki, Dr. Jonathan, E. *The Failed Thermostat: The Illusion of Control in an Information-Rich Age*. Submission to the 13th International Command and Control Research and Technology Symposium, 2008.
- Deakin, Colonel S. *Managing FIST (Future Integrated Soldier Technology)*, RUSI Defence Systems, Spring 2005.

- Foltz, Kevin, and Chandrasekaran, Coimbatore. *Sharing Resources Through Dynamic Communities*, Institute for Defence Analyses, Presentation to the 10th International Command and Control Research and Technology Symposium, 2005.
- Forgues, Colonel P. *Command in a Network-Centric War*. Canadian Military Journal, Summer 2001.
- Garth, Dennis J. *Network Centric Warfare and Its Impact on Operational Functions*. Naval War College, 3 February 2003.
- Giffin, Lieutenant-Colonel Ralph E., and Reid, Darryn J. *A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy*. Presentation to the 8th International Command and Control Research and Technology Symposium, 2003.
- Giffin, Lieutenant-Colonel Ralph E., and Reid Darryn J. *A Woven Web of Guesses, Canto Two: Network Centric Warfare and the Myth of Intuitivism*. Presentation to the 8th International Command and Control Research and Technology Symposium, 2003.
- Giffin, Lieutenant-Colonel Ralph E., and Reid, Darryn J. *A Woven Web of Guesses, Canto Three: Network Centric Warfare and the Virtuous Revolution*. Presentation to the 8th International Command and Control Research and Technology Symposium, 2003.
- Gizewski, P. *The Future Security Environment 2021 – Implications for Canadian Armies*. Defence Research and Development, DRDC CORA TM 2007-61, September 2007.
- Gladwell, M. *Blink: The Power of Thinking Without Thinking*. Little, Brown and Company, New York 2005.
- Gompert, David C., Lachow, I., and Perkins J. *Battle-wise: Seeking Time-Information Superiority in Networked Warfare*. NDU Press 2006.
- Gonzales, D., Johnson M., McEver J., et al. *Network-Centric Operations Case Study: The Stryker Brigade Combat Team*. RAND Corporation 2005.
- Gonzales, D., Hollywood, J., Sollinger, J.M. et al. *Networked Forces in Stability Operations 101st Airborne Division, 3/2 and 1/25 Stryker Brigades in Northern Iraq*. RAND Corporation, 2007.
- Grau, Lester M. *Urban Combat: Confronting the Spectre*. Military Review, July–August 1999.
- Johnson, Chris. *Net-centric Fogs Accountability*. US Naval Institute Proceedings, Vol. 129, No. 5, May 2003.
- Kaplan, Robert D. *The Coming Normalcy?* Atlantic Monthly, April 2006.



- Keus, H.E. *Netforce Principles: An Elementary Foundation of NEC and NCO*. Presentation to the 10th International Command and Control Research and Technology Symposium, June 2005.
- Libicki, Martin C., Gompert, D., Frelinger, D.R., et al. *Byting Back: Regaining Information Superiority against 21st Century Insurgents*. RAND Corporation 2007.
- Luddy, John. *The Challenge and Promise of Network-Centric Warfare*. The Lexington Institute, February 2005.
- McCaskill, Lawrence P. *Beyond PowerPoint Deep: A Concept of Operations for Implementing Net-Centric Warfare*. Presentation to the 12th International Command and Control Research and Technology Symposium, September 2007.
- McKenna, T., Moon, T., et al. *Science & Technology for Australian Network-Centric Warfare: Function, Form and Fit*, Australian Defence Force Journal, No. 170, 2006.
- Murphy, Colonel (Ret'd) D., and Groh, Dr. J.L. *Landpower and Network-Centric Operations: How Information in Today's Battlespace can be Exploited*. U.S. Army War College, Centre for Strategic Leadership, 2006.
- Nwana, H.S. *Software Agents: An Overview*. Knowledge Engineering Review, Vol. 11, No. 3, 1–40, Sept 1996. © Cambridge University Press, 1996.
- Polydys, M.L. *Interoperability in DOD Acquisition Programs through Enterprise Architecting*, Acquisition Review Quarterly, Summer 2002.
- Shade, U., and Hieb, M.R. *Development of Formal Grammars to Support Coalition Command and Control: A Battle Management Language for Orders, Requests and Reports*. Presentation to the 11th International Command and Control Research and Technology Symposium, September 2006.
- Schade, U., and Hieb, Michael R. *Improving and Replanning: Using a Formal Grammar to Automate the Processing of Command and Control Information for Decision Support*. The International C2 Journal, Vol. 1, No. 2, 2007.
- Schrage, Michael. *Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*. Massachusetts Institute of Technology, Security Studies Program White Paper, May 2003.
- Schmidtchen, Lieutenant-Colonel D. *Network-Centric Warfare: The Problem of Social Order*. Land Warfare Studies Centre, Working Paper 125, June 2005.
- Smith, Edward Allen. *Complexity, Networking, and Effects-based Approaches to Operations*. Department of Defence Command and Control Research Program, 2006.





Sparks, E. *Soldier System Technical Risk Assessment. An Approach for Identification of Current and Future Integration Challenges*. Land Warfare Conference 2007, October 2007.

Unewisse, M., Wilson S., Perry, A., and Boyd, C. *An Australian Approach to Assessing Force-Level Network-Centric Warfare (NCW) Readiness*. Presentation to the 11th International Command and Control Research and Technology Symposium, September 2006.

Wallace, William S. *Network Enabled Battle Command*, RUSI Defence Systems.

