20 OCTOBER 2009

Integrated Capstone Concept

National Defence Défense nationale

Canada

Integrated Capstone Concept

CHIEF OF FORCE DEVELOPMENT • CHEF DU DÉVELOPPEMENT DES FORCES

INTEGRATED FORCE • FORCE INTÉGRÉE

Chief of Force Development
National Defence Headquarters
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Produced for the Chief of Force Development
by 17 Wing Winnipeg Publishing Office.
WPO30557

NDID # A-FD-005-002/AF-001

Library and Archives Canada Cataloguing in Publication

Integrated capstone concept.

Produced for the Chief of Force Development by 17 Wing Winnipeg Publishing Office.
Issued also in French under title: Concept cadre intégré.
Available also on the Internet.
Includes bibliographical references.
ISBN 978-1-100-16456-4
Cat. no.: D2-265/2010E

1. Canada--Military policy. 2. Canada. Canadian Armed Forces. 3. National security--Canada.
I. Canada. Canadian Armed Forces. Wing, 17 II. Canada. Chief of Force Development

UA600 I62 2010 355’.033571 C2010-980199-7

Printed in Canada.

1 3 5 7 9 10 8 6 4 2

FOREWORD

I am pleased to present the *Integrated Capstone Concept* to the Department of National Defence (DND) and the Canadian Forces (CF) for general reference. The purpose of this document is to provide the Defence Institution with an over-arching concept, informing a body of operating, integrating, and enabling concepts that will shape how the CF will meet the challenges of the complex future security environment. This document will underpin integrated CF Force Development and act as both a resource for CF Professional Development and other department needs.

Understanding the implications that complexity will present is essential to CF strategic success. It is also fundamental to understanding the changing nature of our adversaries, the domains in which we will operate, and the types of operations that the CF will be tasked to perform. In order to meet these challenges, we will need to create an integrated, multi-role, and combat-capable military force that will be comprehensive, integrated, adaptive, and networked in the execution of national intent.

Force Development organizations will use the *Integrated Capstone Concept* to guide integrated capability development across the CF functions for the new expanded strategic environment. Likewise, the Environmental Commands are strongly urged to use this document as a starting point to inform their concept and capability development.

The ideas in the ICC have already stimulated both concept development within the different organizations and feedback for the next version of the ICC. The next version will:

1. Include a human “dimension” to replace the human domain;
2. Clarify the intent, presentation, and explanation of the ICC Construct;
3. Enhance the description of the strategic function concepts; and
4. Expand upon the key ideas of Comprehensive, Adaptive, Integrated, and Networked.

I encourage all members of the Defence Team to use this document to maintain a high level awareness of the capstone concept and how it may impact our ability to remain strategically relevant, operationally responsive, and tactically decisive in the years to come.

S.A. Beare, Major-General
Chief of Force Development

ACKNOWLEDGEMENTS

CFD acknowledges the support and contribution from all Level 1 organizations within NDHQ, all Commands, and the concept development community writ at large through their membership in the Integrated Concept Working Group (ICWG).

The contributions provided by the following personnel deserve special acknowledgement:

BGen MD Kampman
BGen P Matte
Col JK Tattersall
Cdr KPL Hansen
Cdr HJ Henderson
Cdr NT Leak
Cdr WM Mooz
LCol FM Aubin
LCol RW Bell
LCol DJG Boucher
LCol JF Castonguay
LCol RW Clarke
LCol GL Couch
LCol SD Coveney
LCol TA Gibbons
LCol A Hirji
LCol MS Kostner
LCol JLD Lachance
LCol JMS Larouche
LCol JA Legere
LCol SRS Murphy
LCol JM Rettie
LCol MA Rostek
LCol RC Roy
LCol K Schramm
LCol RC Strum
LCol KP Truss
LCol JM Uchiyama
LCol WF Yee
LCdr DJ Harnett
LCdr JJ MacDonald
LCdr MD McKinley
LCdr PR Moller
LCdr ML Toth
Maj DE Allison
Maj RJ Aucoin
Maj MM Barbe
Maj DF Ceniccola
Maj ML Evans
Maj JT Fernandes
Maj BC Frandsen
Maj DA Goldsmith
Maj JDM Gratton
Maj TR Gushue
Maj CR Henderson
Maj PJ Kendall
Maj WK Little
Maj JSA Rollin
Maj MR Setter
Maj GO Sherwood
Maj JW Smith
Maj JA Stewart
Maj RD Trerice
Maj WR Wallace
MWO CC Deroche
MWO RP Nadeau
Darren Baker
Bill Bentley
G. Bergeron
Jean-François Born
Ann Bradfield
David Butcher
Neil Chuka
Kumar Dalvi
Scott Davey
Jamie Gibson
Phillipe Hebert
Rachel Lea Heide
Tony Humphreys
Karen Lahaise Mazur
Britton MacDonald
Carol McCann
Brian McCarthy
Charles Morrisey
Davide Pisano
Regan Reshke
Brian Staples
Keith Stewart
Tracey Wait

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

1.1 Challenge

There are numerous new challenges facing the Department of National Defence (DND) and the Canadian Forces (CF), such as the aging population demographic, the emergence of non-state actors, the access to disruptive technologies through globalization, and so on. Collectively, these challenges manifest themselves as increased complexity in the modern security environment.

Critics will say that complexity in the security environment has always existed, and in some aspects they are correct. What are changing are the varying degrees of complexity that characterize the security environment and the interactions of the complex systems involved. Since the mid-1970s, the study of complexity as a science has made much progress in dealing with complex issues. It is the contention of the *Integrated Capstone Concept* (ICC) that as the complexity of the security environment expands, so will the magnitude and nature of strategic stimuli that affect our national interests. Therefore, in order for the CF to remain strategically relevant, operationally responsive, and tactically decisive in the future security environment, it must rise to the challenges that increased complexity presents.

Analysis of current and future trends identifies that increased complexity will be at the core of nearly all future operations. *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations* investigates the challenges that military personnel are facing in current operations. Through a process of interviews with a number of personnel[1] with a variety of experiences and backgrounds, the Canadian Forces Leadership Institute Project Team reported that most of those interviewed "accurately described an operating environment of great complexity and unpredictability."[2] The findings from *Broadsword or Rapier?* show the immediacy of the current challenge. If there is a fundamental increase in complexity in our current operations, what does the future hold?

If there is a fundamental increase in complexity in our current operations, what does the future hold?

The Future Security Environment 2008-2030: Current and Emerging Trends (FSE) outlines a wide variety of trends that will influence how DND/CF will operate. Specifically, the FSE looks at economic, social, environmental, resource, geopolitical, science, technology, military, and security trends and concludes that the future security environment will undoubtedly follow the current trend of becoming increasingly complex.[3] Therefore, we must understand the implications of this paradigm and determine how to operate in this dynamic security environment.

INSIGHT 1

THE STRATEGIC ENVIRONMENT HAS ALWAYS BEEN DOMINATED BY ISSUES OF COMPLEXITY. HOWEVER, THE NUMBER OF FACTORS AND CHALLENGES RESIDENT IN THE FUTURE SECURITY ENVIRONMENT WILL SIGNIFICANTLY INCREASE THE LEVELS OF COMPLEXITY.

1.2 Aim

The aim of this paper is to describe the considerations that are strategically relevant to the Canadian Forces in the future security environment and to present the capstone construct required to inform capability development. The governing thesis is that the increasingly complex security environment demands approaches that are comprehensive, integrated, adaptive, and networked in the execution of national intent. These factors must become the tenets governing the nature of the future CF and the requirements for being strategically relevant, operationally responsive, and tactically decisive.

The increasingly complex security environment demands approaches that are comprehensive, integrated, adaptive, and networked in the execution of national intent.

The scope of the ICC is:

- To describe the considerations that are strategically relevant to DND/CF;
- To identify four necessary attributes (comprehensive, integrated, adaptive, networked) that future DND/CF concepts, approaches, and capability development must incorporate;
- To propose an expansion of the understanding of the strategic environment to include the land, maritime, air, space, cyberspace, and human domains; and
- To introduce the capstone construct as a tool to aid in concept, capability, and force development for DND/CF.

1.3 Assumptions

- The three enduring roles of the CF as described in the *Canada First* Defence Strategy (CFDS) will remain unchanged: Defend Canada and Canadians, Defend North America, and Contribute to International Peace and Security.

- Canada will remain a strategic ally with the United States and with a wide range of multi-lateral security partnerships.

- DND/CF will continue to be relevant to the Canadian public, the Government of Canada, and the allies of Canada and will hence continue to be an instrument of national power.

- Organizational bias, parochialism, and institutional inertia will always be an impediment to transformation.

1.4 Constraints

- Military capabilities will continue to be commensurate with levels of government funding.

- CF operations will continue to be guided by the laws and the direction of the GoC, the principles that guide the profession of arms in Canada, and the expectations of the people of Canada.

- Tolerance for collateral damage will continue to diminish – therefore, the requirement for greater precision which will place greater challenges on adaptability, comprehensiveness, and integration.

1.5 Section Highlights

Section 2 examines complexity theory and how it can be applicable to the study of the security environment. The trends described in the FSE are examined and contrasted with the strategic reality of today as a means of hypothesizing how the future strategic reality may look.

Section 3 provides a concise discussion of the importance of having a comprehensive, integrated, adaptive, and networked approach in the complex security environment.

Section 4 discusses the nature of future conflict and offers a model to portray the application of the elements of national power in a complex strategic environment. The section also examines the CFDS missions as condition sets within the ICC Construct.

Section 5 provides an overview of the future strategic environment. The section advocates an expansion of the strategic environment to include three new domains: space, cyberspace, and human. A discussion of how technology and globalization have empowered adversarial actors (state and non-state) with instruments of national power and influence that were previously unobtainable is also included in the description of the human domain.

Section 6 examines the CF functions of Command, Sense, Act, Shield, Sustain, and Generate with regards to being comprehensive, adaptive, integrated, and networked.

Section 7 introduces the capstone construct and describes its purpose. The information in the preceding sections is brought together, and the relationships between condition sets, domains, and functions are examined at a strategic level. The use of the capstone construct as a tool for capability and concept development is also discussed.

Section 8 articulates the strategic insights and impacts for DND and the CF in light of the central thesis that the increasingly complex security environment demands approaches that are comprehensive, integrated, adaptive, and networked in the execution of national intent.

STRATEGIC IMPACT

Complex future security challenges demand approaches that are comprehensive, integrated, adaptive, and networked. Therefore, these attributes must become the tenets that govern the nature of the future force and the requirements for being strategically relevant, operationally responsive, and tactically decisive.

2 COMPLEXITY, THE FUTURE SECURITY ENVIRONMENT, AND THE CANADIAN STRATEGIC REALITY

This section of the ICC examines complexity theory and how it can be applicable to the study of the security environment. The trends described in the FSE are examined and contrasted with the strategic reality of today as a means of hypothesizing how the future strategic reality may look.

2.1 Complexity

The international community and the inter-relationships amongst the various sub-communities clearly comprise a complex system. Consequently, the ICC contends that the study of complexity science is essential for any attempt to prepare DND/CF for the challenges they will face on operations in the increasingly complex future security environment. The term "complexity" can only be "situated in between order and disorder."[4] Complexity has also been called "the science of surprise,"[5] and this alone should be something all military audiences can appreciate.

> ***"Complex Systems is a new approach to science, which studies how the relationships between parts give rise to the collective behaviours of a system and how the system interacts and forms relationships with its environment."***
>
> **Yaneer Bar-Yam, *Making Things Work,* p.24.**

This science does study complex systems, their characteristics, and their properties and behaviours. A complex system is an aggregation of interacting agents.[6] These systems are neither rigid nor fluid; instead, they are a mixture and balance of regular, predictable, random, and chaotic behaviour. The parts that comprise the complex system are connected through their interactions; the sub-systems are simultaneously autonomous and mutually dependent. Models of complex systems treat the constituent parts as agents: "individual systems that act upon their environment in response to the events they experience." There is an underlying assumption that agents are goal-directed and aim to act toward their maximum benefit. Agents' actions affect the environment, which in turn will cause other agents to react. Although interactions begin at the local level, these actions can eventually cause global consequences.[7]

The interactions of complex systems are seldom linear: there is no directly proportional and predictable cause and effect relationship.[8] Nevertheless, complex systems do have the tendency to self-organize: "local interactions eventually produce global coordination," and this structure is often a network.[9] Agents within complex systems also co-evolve or adapt to one another's actions and reactions while attempting to move toward a beneficial or stable state.[10] The properties of complex systems cannot be deduced from identifying the properties of each unit part; the whole itself has emergent properties which are derived from "the pattern of interactions or relations between [the parts]."[11] Because complex systems are constantly experiencing non-linear interactions amongst agents, it is not surprising that these systems are unpredictable and uncontrollable in nature and "will never be able to be captured in a complete and deterministic model."[12] The relationship between parts can produce patterns or lead to self-organization. These are the emergent properties of adaptive systems. Emergent properties may lead to new organizations being formed or dissolved and could produce new behaviour locally or throughout the whole of the system. Any action within complex adaptive systems may also produce undesired side effects.[13]

Since the security and operating environment is composed of an abundance of complex systems, comprehending the science of complex systems (to the best of our ability) is essential to strategic success for DND/CF in the future security environment. Studying complexity theory is also fundamental to appreciating the growing number of agents impacting national and international security, the changing nature of our adversaries, the consequences of various groups' interactions, the unpredictable and non-linear nature of actions and behaviour, the domains in which we will operate, and the types of operations that the CF will be tasked to perform. The existing linear tools and legacy constructs that we currently use for problem solving may be inadequate for the challenges brought about by future complex systems. Evolving the Operational Planning Process (OPP) to include such tools as soft systems methodology or enhanced evolutionary engineering to address complex problems may be more appropriate in the future.

INSIGHT 2

UNDERSTANDING THE IMPLICATIONS THAT COMPLEX SYSTEMS WILL PRESENT IN THE FUTURE SECURITY ENVIRONMENT IS ESSENTIAL TO STRATEGIC SUCCESS FOR THE CF. THE FUTURE SECURITY ENVIRONMENT WILL BE INFLUENCED BY AN EVER-EXPANDING SPECTRUM OF DYNAMIC COMPLEX AND ADAPTIVE SYSTEMS.

2.2 The Future Security Environment

The FSE document examines a number of trends that will impact and influence how our operations may be conducted. Specifically, it outlines trends in the economic, social, resource, environmental, geopolitical, science, technology, military, and security dimensions, and it hypothesizes how the strategic environment may evolve out to 2030.

Globalization is a predominant trend affecting the future security environment. The proliferation of new technology facilitates and enables creative and dynamic means for people and systems to interact. This interaction builds interconnectedness, interdependence, and relationships, and it forms the basis of the complexity in the future security environment.

Many of the trends described in the FSE could generate indirect effects and give rise to conflict.[14] Social and economic trends may generate tension and aggravate existing hostilities and problems in regions already experiencing discontent, disparity, and desperation. Similarly, economic inequality, over-population, migration, urbanization, disease, poverty, and extremism all have destabilizing effects.

Global population trends exacerbate the triggers of instability and conflict. Urbanization trends towards mega-cities increases the probability of friction and allows previously disparate groups to interconnect for shared adversarial intent. The same is also true for sharing of strategic resources and the obvious health and pandemic issues that arise due to urbanization. Climate change and resource competition are also causing additional friction and population shifts.

Globalization, or more specifically the interconnectivity and access that globalization provides, empowers a wide range of actors with capabilities that were previously restricted to developed nation states. Global access to science and technology (such as space, cyberspace, and advanced disruptive technologies) means military advantage can belong to whomever is quickest and best able to acquire and exploit new capabilities, thus increasing the adversarial capability of non-state actors to levels that rival those of nation states. These trends have serious implications for defence and security within the context of the Canadian strategic reality.

INSIGHT 3

THE DYNAMIC AND COMPLEX STRATEGIC ENVIRONMENT WILL BE FURTHER INFLUENCED BY AN EVER-EXPANDING SPECTRUM OF TECHNICALLY AND SOCIALLY ENABLED ACTORS WHO WILL BE MORE COORDINATED, INCREASINGLY NETWORKED, AND WHO SHARE ADVERSARIAL INTENT.

2.3 The Canadian Strategic Reality

The *Canada First* Defence Strategy (CFDS) describes three enduring roles for the Canadian Forces:[15]

1) Defending Canada – Delivering Excellence At Home;
2) Defending North America – A Strong and Reliable Partner; and
3) Contributing to International Peace and Security – Projecting Leadership Abroad.

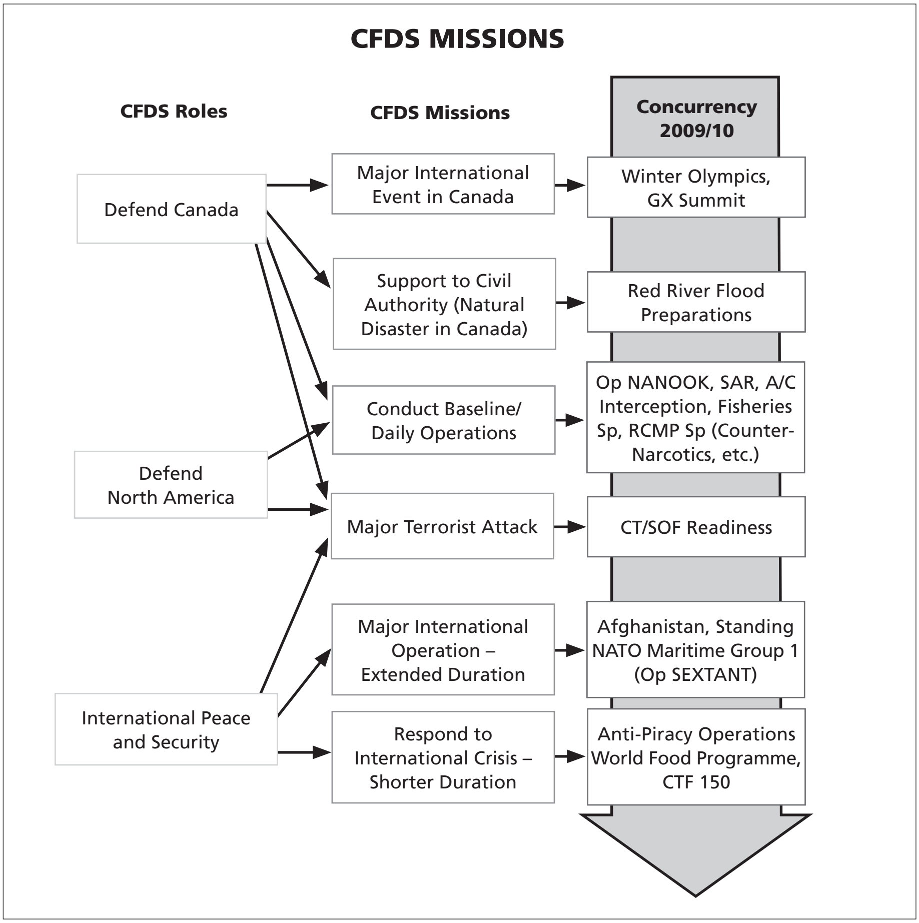

CFDS MISSIONS
CFDS Roles
CFDS Missions
Concurrency 2009/10
Defend Canada
Defend North America
International Peace and Security
Major International Event in Canada
Support to Civil Authority (Natural Disaster in Canada)
Conduct Baseline/ Daily Operations
Major Terrorist Attack
Major International Operation – Extended Duration
Respond to International Crisis – Shorter Duration
Winter Olympics, GX Summit
Red River Flood Preparations
Op NANOOK, SAR, A/C Interception, Fisheries Sp, RCMP Sp (Counter-Narcotics, etc.)
CT/SOF Readiness
Afghanistan, Standing NATO Maritime Group 1 (Op SEXTANT)
Anti-Piracy Operations World Food Programme, CTF 150

FIGURE 1: CFDS MISSIONS.

When comparing the trends within the FSE to the roles of the CF, a very demanding forecast for activity, both at home and abroad, becomes apparent. Non-state adversaries, empowered by modern technologies and possibly funded through criminal enterprise, will likely continue to be an issue. State-on-state conflicts will continue to be a reality; however, the depth and breadth of these conflicts is becoming far more expansive.

Globalization will continue to affect intra-state relationships, and new inter-dependencies will continuously manifest themselves within the wider strategic condition.

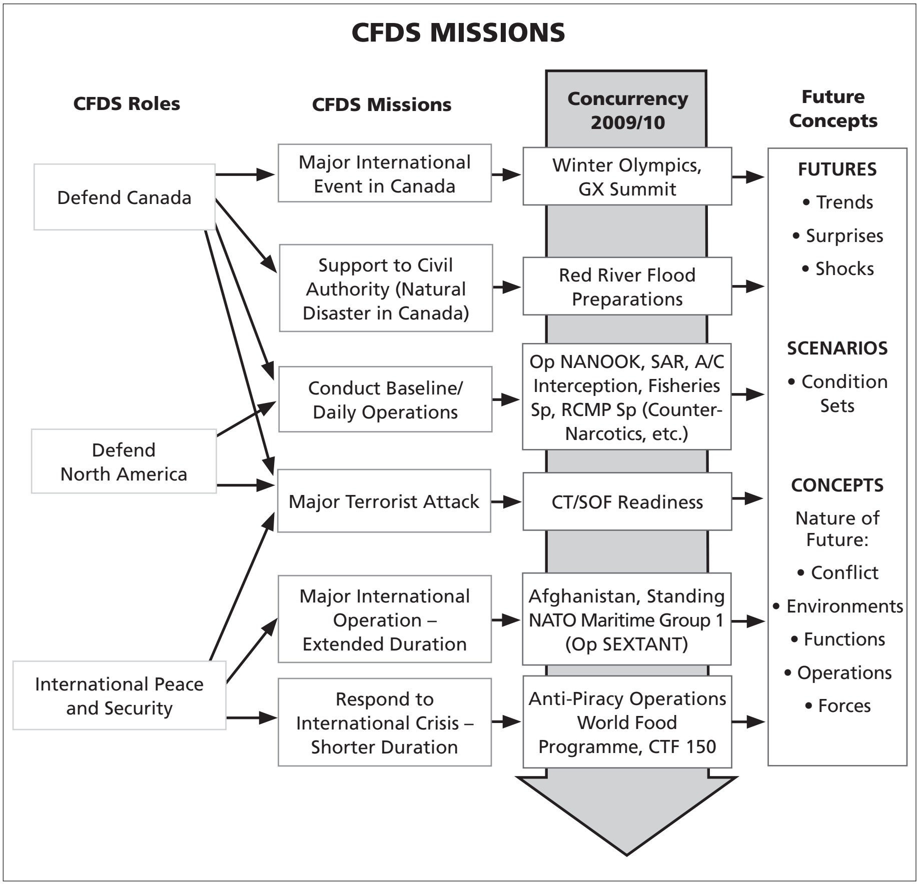

CFDS MISSIONS
CFDS Roles
CFDS Missions
Concurrency 2009/10
Future Concepts
Defend Canada
Defend North America
International Peace and Security
Major International Event in Canada
Support to Civil Authority (Natural Disaster in Canada)
Conduct Baseline/ Daily Operations
Major Terrorist Attack
Major International Operation – Extended Duration
Respond to International Crisis – Shorter Duration
Winter Olympics, GX Summit
Red River Flood Preparations
Op NANOOK, SAR, A/C Interception, Fisheries Sp, RCMP Sp (Counter-Narcotics, etc.)
CT/SOF Readiness
Afghanistan, Standing NATO Maritime Group 1 (Op SEXTANT)
Anti-Piracy Operations World Food Programme, CTF 150
FUTURES
• Trends
• Surprises
• Shocks
SCENARIOS
• Condition Sets
CONCEPTS
Nature of Future:
• Conflict
• Environments
• Functions
• Operations
• Forces

FIGURE 2: IMPACT OF UNCERTAIN FUTURE ON CFDS MISSIONS.

The security environment, as outlined in the FSE, will be constantly dynamic and uncertain. However, the three roles for the CF (defend Canada, defend North America, contribute to peace and security) should remain relatively unchanged. These roles must be fulfilled within the wider security environment, and each role has its own requirements for being comprehensive, integrated, adaptive, and networked. The combination of these roles and the security environment are referred to here as the *problem set*.

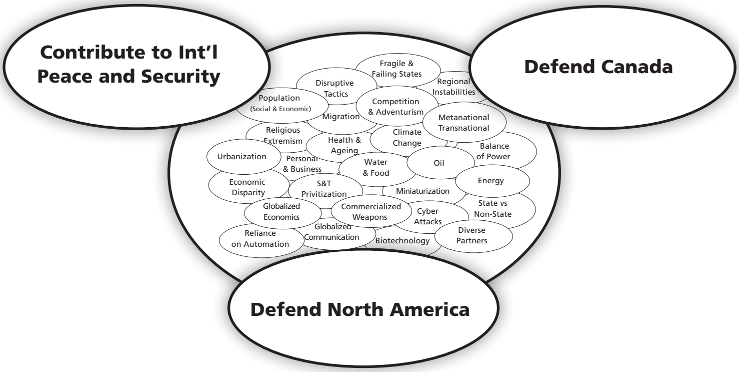


FIGURE 3: INTER-RELATIONSHIP OF CF ROLES AND THE FUTURE SECURITY ENVIRONMENT.

Equally important are the conditions under which CFDS missions will be conducted as well as the expectations of the Government of Canada (GoC). The combination of each CFDS mission and the expectations of the GoC are referred to here as the *condition set*. Each condition set will have unique requirements for being strategically relevant, operationally responsive, and tactically decisive.

With the aim of positioning the CF to operate successfully in the problem set, the ICC will explain the relationship of the nature of future conflict, the strategic environment, and functions as they pertain to the condition sets. Success in the increasingly complex security environment demands approaches that are comprehensive, integrated, adaptive, and networked.

STRATEGIC IMPACTS

It is fundamental to understand the growing number of agents affecting national and international security, the changing nature of our adversaries, the consequences of various groups' interactions, the unpredictable and non-linear nature of actions and behaviour, the domains in which we will operate, and the types of operations that the CF will be tasked to perform.

The linear tools and legacy constructs that we currently use for problem solving may be inadequate for to the challenges provided by future complex systems.

Global access to science and technology (such as space, cyberspace, and advanced disruptive technologies) means the military advantage can belong to whomever is quickest and best able to acquire and exploit new capabilities, thus increasing the adversarial capability of non-state actors to levels that rival those of nation states.

3 THE REVISED APPROACH AND THE FUTURE CF

This section provides a concise discussion of the importance of having a comprehensive, integrated, adaptive, and networked approach in the complex security environment.

There are methods to assist CF leadership in building a better framework within which our full capacities can be leveraged against a complex challenge. To appreciate the thesis, the idea of external and internal complexity must be clearly understood.

> ***"The external environment of an organization can also vary from relatively stable to dynamic and complex. If environmental complexity begins to exceed the internal complexity of the organization, chances of failure will loom higher unless the organization can increase its internal complexity sufficiently to generate successful responses to environmental demands."***
>
> **John Verdon *et al., The Last Mile of the Market*, p.54.**

In essence, our ability to respond to issues of external complexity is fully dependent upon our ability to resolve our issues of internal institutional complexity. Through CF Transformation, we are addressing uncertainty and better utilizing the full capacity of all the components of DND in an integrated manner. Nevertheless, for defence institutions to improve their performance in complex environments, issues of internal complexity must also be resolved through actions that are comprehensive, integrated, adaptive, and networked. Existing stovepipes may not be the answer.

3.1 Comprehensive

There are three different aspects of being comprehensive:

- a complete understanding of the strategic environment;
- an accurate definition of the problem(s) and appropriate goal-setting; and
- an ability to apply a multi-disciplinary approach.

Comprehensiveness must describe the complete strategic environment with all of the envisioned domains. Careful consideration must be given to physical aspects such as temperature, terrain, and location. However, more important to understanding the operating space are human aspects such as cultural, political, and social belief systems. Furthermore, if the adversary has the potential to operate outside the traditional domains (maritime, land, and air), then the CF must also be prepared to function there as well. Only by considering all of these aspects can a truly comprehensive understanding of the strategic environment be gained.

The second use of comprehensiveness relates to defining problems and goals. Aspects of the problem may not always be obvious, and consequently, the problem may have to be continually redefined. Goals may not be fully achievable and may initially be understated or unclear. All actions to achieve goals must be constantly monitored, and if necessary, leaders and planners may need to reconsider problems, goals, and courses of action. The unpredictable nature of the problem set means that decision support systems and operational planning processes cannot be linear.

The unpredictable nature of the problem set means that decision support systems and operational planning processes cannot be linear.

Finally, comprehensiveness[16] must describe a multi-disciplinary approach to resolve the challenges forecasted in the FSE document, which are well beyond the scope and the capacity of the CF alone. The CF is but one instrument of national power and influence available to the GoC. Additionally, non-governmental agencies may simultaneously be working in the complex space to solve other portions of a crisis and may or may not share the goals of the GoC. To best resolve or manage complex situations, a comprehensive framework is needed.

DND and the CF need to develop a full understanding of the shared strategic environment, to set and modify appropriate and relevant goals to achieve the strategic intent of the GoC and to work in a multi-disciplined team construct.

INSIGHT 4

COMPREHENSIVENESS MUST DESCRIBE A MULTI-DISCIPLINARY APPROACH TO RESOLVE THOSE CHALLENGES FORECASTED IN THE FUTURE SECURITY ENVIRONMENT WHICH ARE WELL BEYOND THE SCOPE AND THE CAPACITY OF THE CF ALONE.

3.2 Integrated

The term integrated is typically used to expand the meaning of joint and combined to include other actors and organizations within a Whole of Government Approach. For the ICC, the term has three distinct meanings:

- the coordination of effort between, and within, DND and the CF for force development, force generation, and force employment;
- the ability for two or more distinct organizations to work together; and
- the level of interoperability.

The first definition of integration speaks to DND and the CF. In order to resolve the issues of developing, generating, and employing military forces in support of national policy, DND/CF must integrate as force developers and force generators so that the CF can succeed as a force employer. This does not mean organizational integration, but rather integrating the effects required to achieve balanced and managed states of readiness. Integrating the efforts of both DND and the CF is a key process that will allow the defence institution as a whole to overcome establishment-wide inertia and organizational parochialism.

The second definition of integration goes beyond military terms such as "joint" and "combined." The term describes the relationships between DND/CF and external organizations, such as other governmental departments or allies. Such integration allows a multi-disciplined approach to complex situations. The most important relationships for DND/CF will be with other government departments for the security and sovereignty of Canada. Other transitory actors may include non-governmental organizations, high-tech business, and private military contractors. The team or force is integrated only as long as necessary to achieve success; the overarching issue is for all integrated partners to be working to achieve a common goal. It is assumed that DND/CF are always part of the integrated team or integrated force. However, it is not mandatory to be integrated from an organizational perspective in order to produce integrated effects.

The third definition of integration refers to the level of interoperability between the involved organizations that is needed to successfully achieve a goal. The level of interoperability (or integration), or minimum level at which interoperability is a critical factor, is dependent upon the mission. Highly complex problems and situations may demand higher levels of integration to realize success. Institutional culture, language, procedures, equipment, and legalities are all potential constraints to integration.

Building a Recognized Maritime Picture is an example of where integration is needed to contribute to good situational awareness. Many assets, including airborne or space-based sensors, belonging to DND/CF or Other Government Departments (OGD), can be integrated to provide information. Conversely, the requirement to conduct an expeditionary operation against a motivated opponent in a densely populated urban littoral area would require a much greater level of integration through all levels from the tactical to strategic, and through all activities from conception through to execution.

Both DND and the CF will need to evolve from organizational silos to processes, networks of relationships, and capabilities that enable integrated operations. Moreover, the entire institution will need to integrate as required with other agencies or actors. The aim must be to achieve a synergistic effect by exploiting the power of the whole rather than depending upon the sum of the parts.

INSIGHT 5

INTEGRATION WITHIN A MULTI-DISCIPLINARY APPROACH WILL PROVIDE A GREATER CHANCE OF RESOLVING THE COMPLEX ISSUES OF THE FUTURE SECURITY ENVIRONMENT THAN WILL WORKING INDEPENDENTLY.

3.3 Adaptive

Adaptation is the condition to respond to change and challenges in a positive manner, and it is integral for coping with complexity and complex systems. Understanding that complex situations and relationships are unpredictable, or uncertain, compels those coping with complexity to become adaptive or fail. In the military, this is reflected in the adage "no plan survives first contact with the enemy."

Adaptation also has a temporal quality. Systems are evolving all the time. The change may be very slow and unnoticed, or it may be very dramatic and pronounced. Slower changes are usually evolutionary, and quicker changes are often revolutionary. Evolutionary adaptation is normally based in the ability of an organization or individual to learn. Revolutionary adaptation is rapid and innovative. While learning remains an important component for an organization or individual, the emphasis during revolutionary adaptation will be on responsiveness, flexibility, and agility, which historically have been fundamental to successful military adaptation.

Adaptation has another quality known as co-evolution. It describes where a system is evolving not in isolation, but rather as a system of evolutionary systems that may be inter-dependent. Each system, or agent, not only interacts with agents at its own level, but also with superior and subordinate agents, all of which are evolving.

HALLMARKS OF ADAPTATION[17]	
Intelligent	Context-appropriate behaviour/decisions, discovery, and exploitation of advantages.
Resilient	Able to recover or adjust from shock, surprise, damage, or misfortune.
Robust	Effective across a range of conditions.
Flexible	Able to reconfigure.
Agile	Ability to redirect swiftly.
Creative	Process of generating novel and useful concepts, solutions, or product.
Responsive	Speed of recognition and action.
Enduring	Able to withstand prolonged strain.

The CF requires leaders who can discern the consequences of emerging trends and react to strategic shocks. The CF also needs commanders who are not afraid to pursue innovative and unconventional solutions. The CF requires individuals who, like our adversaries, can envision the use of equipment and capabilities in new and innovative ways. We require people who can sense a change in the adversary's course of action and exploit it to the benefit of the mission. Failure to create this capability within our people and institution will handicap us to the adversary's advantage. In short, the CF must be adaptive or risk failure.

INSIGHT 6

ADAPTATION IS IMPERATIVE TO COPING WITH UNPREDICTABLE AND UNCERTAIN COMPLEX CHALLENGES, SITUATIONS, AND RELATIONSHIPS. THE CF MUST BE ADAPTIVE OR RISK FAILURE.

3.4 Networked

Networks are about relationships and interconnectivity. Of specific relevance to the CF is the existence of national networks, the nature of social networks, the importance of organizational networks, and the impact of technology on networks.

There are two types of networks: human (or social) networks and technology-enabled networks. Both are equally important and are not mutually exclusive. Technological networks have created virtual social networks where distance is not a factor and where the boundary between a social network and a technical network is in some respects irrelevant.

Conflict is not merely between nation states; it also involves the underlying interconnected networks of national power. Traditionally, these were diplomatic, economic, and military networks. In a complex security environment, other elements of national infrastructure and resources such as information, financial, intelligence, and law enforcement[18] may be applied to the task at hand. These national networks may also be working with state, non-state, provincial, local, and other actors.

Social networks are defined by the relationship amongst groups, institutions, and individuals within a society. Cultural networks have grown to include shared identities, beliefs, values, customs, and behaviours.[19] In the future, networks of state and non-state actors with overlapping interests may form partnerships, act in cooperation, and disperse when no longer required. Human and social networks will be further discussed in the section on the human domain (section 5.2.3).

An organization's structure, or network, is also important. There are three structures that are of particular interest to the CF. In hierarchical relationships, information flows either up or down, and decisions are made by the superior component. This type of organization is a "weak" network because it can easily succumb to information overload, and it has limited capability to deal with complexity. More importantly, hierarchical organizations are easily targeted.

Integrated networks are well connected, and information is shared at all levels so that each node has decision-making capability. These structures can be very complex but are also well suited for dealing with high levels of complexity. An integrated network is more adaptable than a hierarchical one.

Hybrid networks are a combination of the two types of networks mentioned above. There is a hierarchical component, but decision-makers are empowered at various levels, and communication is lateral as well as vertical. A hybrid network may be suitable for a range of tasks from simple to complex. This hybrid structure has historical military foundations described as "centralized command, decentralized control." Such a structure will increase in importance in the future complex security environment; therefore, the CF should explore more integrated or hybrid networks as opposed to hierarchical ones.

Network technology has become a critical part of modern life and an essential aspect of the work place. The technological network includes the computers and information technology required for internal connectivity amongst all functions within the strategic environment. External connectivity to defence and security organizations, OGDs, allies, and partners will be required to the extent necessary and will be based on achieving goals.

Network technology is already embedded in each of the domains and in each of the functions. Networks are instrumental to the integration of both of these groups. In other words, "network your networks".

It must be remembered that there are limitations and constraints to networking.

- Although a highly integrated network can potentially share information and increase situational awareness, it is inherently impossible to provide access to all necessary information to make the perfect decision.
- The need to share is severely constrained by the need to shield and to protect. This applies within the CF, GoC departments, and partnerships.
- Creating *ad hoc* technical networks encounter the same problem as with creating *ad hoc* social networks: trust and relationships remain important.
- Consequently, while ideal technological network solutions may be a goal for the future, "good enough" solutions may be the best result that can be achieved.

Nevertheless, it is imperative that the CF continues to exploit technological and methodological advances in networking. Adversaries are becoming more technologically advanced and will be fully capable of exploiting any hierarchical weaknesses. Therefore, adaptive social and technical networks will play a pivotal role in being comprehensive and integrated in the complex security environment.

INSIGHT 7

BOTH SOCIAL AND TECHNICAL NETWORKS MUST BE EXPLOITED BY THE CF ACROSS THE STRATEGIC ENVIRONMENT AND WITHIN ALL DOMAINS IN RESPONSE TO ADVERSARIES' INCREASED TECHNICALLY AND SOCIALLY ENABLED CAPABILITIES.

3.5 The Revised Approach – Synergies and Inter-Relationships

The revised approach requires that the CF becomes comprehensive, integrated, adaptive, and networked in order to succeed in a complex security environment. These separate elements of the revised approach overlap to an extent: comprehensive approaches often lead to multi-disciplinary teams, which are in fact human networks; such teams and networks function best when integrated; and adaptation is enhanced when there are many partners from which to select the best combination of team members for a specific solution. More importantly, though, these approaches also provide mutual support to create a synergistic effect under all condition sets, across the strategic environment, and within the strategic functions.

Solutions to problems in the complex security environment will be a challenge. Cause and effect relationships may be problematic at best since each action will have desired and undesired effects. It is the unknown and undesired effects that are especially difficult. Therefore, to better assess solutions in a complex world, a comprehensive view of the intermediate effects will need to be monitored continually and goals adjusted accordingly.[20] These efforts will lead to synchronization of tactical effects to desired strategic effect.

A fundamental understanding of these cause and effect relationships is required if the CF is to be strategically relevant, operationally responsive, and tactically decisive.

STRATEGIC IMPACTS

The CF is but one instrument of national power and influence available to the GoC.

Non-governmental agencies may also be working in the complex space to solve other portions of a crisis and may or may not share the goals of the GoC.

To best resolve or manage complex situations, a comprehensive framework is needed.

Integration of DND and the CF must evolve from organizational silos to processes, networks, relationships, and capabilities that enable integrated operations.

The entire institution will need to integrate as required with other agencies or actors.

To be adaptive, the CF needs:

- *Leaders who can discern the consequences of emerging trends and react to strategic shocks;*
- *Commanders who are not afraid to pursue innovative and unconventional solutions;*
- *Individuals who, like our adversaries, can envision the use of equipment in new and innovative ways; and*
- *Soldiers, sailors, and air personnel who can sense a change in the adversary's course of action and exploit it to the benefit of the mission.*

Our current hierarchical networks may not be conducive to succeeding in a future complex security environment.

The CF should explore more integrated or hybrid networks as opposed to hierarchical ones.

Based on goals to be achieved, external connectivity with defence and security organizations, OGDs, allies, and partners will be required to the extent necessary.

Both special and technical networks provide the means to be comprehensive, integrated, and adaptive so that the CF can meet the challenges of the complex security environment.

4 THE NATURE OF FUTURE CONFLICT AND FUTURE CONDITION SETS

This section discusses the nature of future conflict and offers a model to portray the application of the elements of national power in a complex strategic environment. The section also examines the CFDS missions as condition sets within the Integrated Capstone Concept Construct.

4.1 The Nature of Future Conflict

There are "two dominant contrasting styles in warfare, regular and irregular (including terroristic) also classified by some today as symmetrical and asymmetrical."

Colin S. Gray, *Another Bloody Century,* p.23.

Globalization has played a role in the evolution of warfare. It has provided adversarial state and non-state actors with off-the-shelf capabilities such as global telecommunications, global positioning, information, intelligence, cryptography, remotely sensed imagery, and weapons. While such capability may not rival Western countries' military forces for endurance and effects, these capabilities are still strategically significant.

Recent conflicts have shown a shift from predominantly conventional warfare to asymmetric or irregular warfare, which contains elements of terrorism and guerrilla warfare (Figure 4). Although the number of interstate conflicts is nearly unchanged, analysis shows that there has been a significant increase in the number and duration of intrastate conflicts. The CF must be able to adaptively operate (both proactively and reactively) throughout the spectrum of conflict, whether in a conventional or irregular manner.

In intrastate conflicts, at least one party is characterized as an inferior non-state actor. This asymmetry forces the inferior non-state actor to resort to irregular warfare. The non-state actors constantly adapt their operations to new situations, either to gain an advantage or to counter the superior adversary's advantages in conventional capability. The increased effectiveness of this type of warfare has been enhanced by the continuously decreasing gap between highly sophisticated military equipment and commercially available technology.

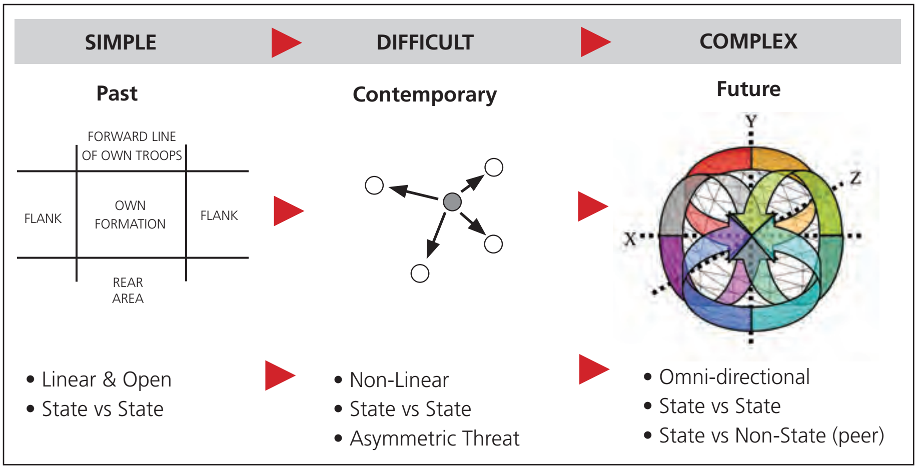


FIGURE 4: THE EVOLUTION OF CONFLICT.

We need to evolve from complex to omni-directional thinking since the number of potential fronts that can be opened by an adversary poses a threat that is omni-directional. Future conflicts involving failed states may require prolonged involvement by an intervening force to realize the desired results. Tactics and doctrine will likely need to be adapted for these conditions. When the CF is deployed in response to a conflict, it will face a complex environment involving a range of actors. The nature of future conflict must include a comprehensive appreciation of the evolution of future operations, the diverse range of state and non-state actors, and the elements of national power and influence increasingly available to all actors. Differences in nationality, language, culture, and motivation need to be understood in order to operate effectively in this environment. In addition, these conflicts often have no precise beginning and no clear conclusion.

In the future, a Canadian response to complex situations in difficult environments will likely require a wide range of government and non-government organizations. As the nature of conflict becomes increasingly dynamic, the spectrum of actors and solutions also increases and may necessitate actions that are no longer the exclusive realm of military forces.

4.2 The Conflict Model

Figure 5 portrays a traditional conflict model displaying peace, conflict, and war as three separate conditions. Such models also convey the sense that conflict is well-bounded and discrete and that a linear transition exists between the three conditions.

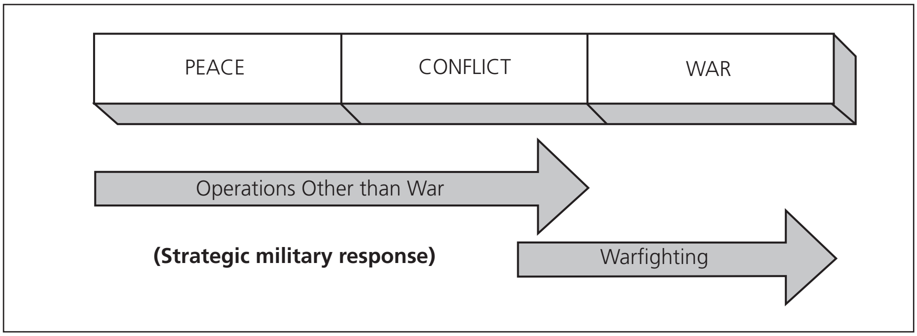


FIGURE 5: TRADITIONAL LINEAR MODEL OF CONFLICT.

History has shown that conflict is not a linear process and is not exclusively the domain of the military. Figure 6 provides a broader view of conflict which attempts to illustrate the application of the traditional three elements of national power – diplomatic, military, and economic. It represents moments in time where many actions, in differing degrees of intensity, are required to deal with a conflict.

Conflict does not have to be violent, and elements of national power other than the military may be used to resolve conflict situations. Violent conflict should always be considered, not as a necessity, but as a potential outcome of escalation.

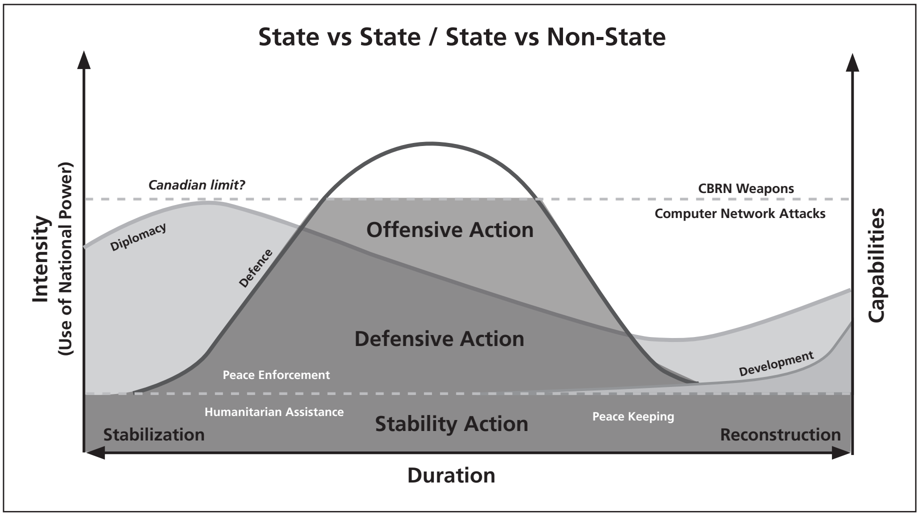


FIGURE 6: A COMPREHENSIVE VIEW OF CONFLICT.

What cannot be represented are the dynamic changes depicted by each line. One must envision that each of these curves or waves will move, depending upon the nature of the mission (see Figure 7 and Figure 8).

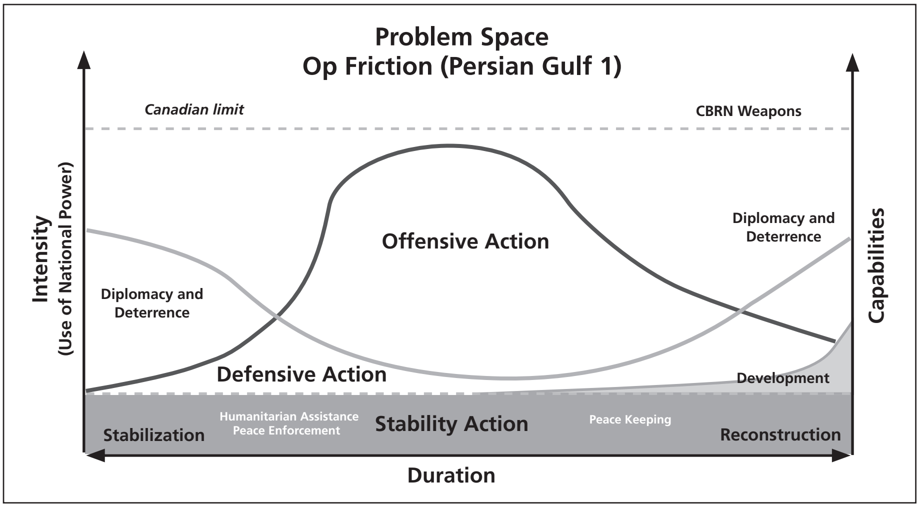


FIGURE 7: A COMPREHENSIVE VIEW OF OP FRICTION.

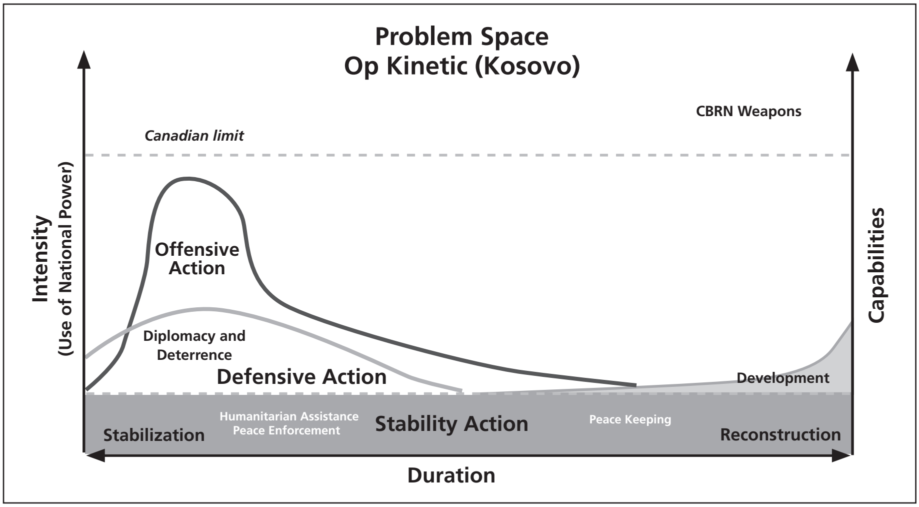


FIGURE 8: A COMPREHENSIVE VIEW OF OP KINETIC.

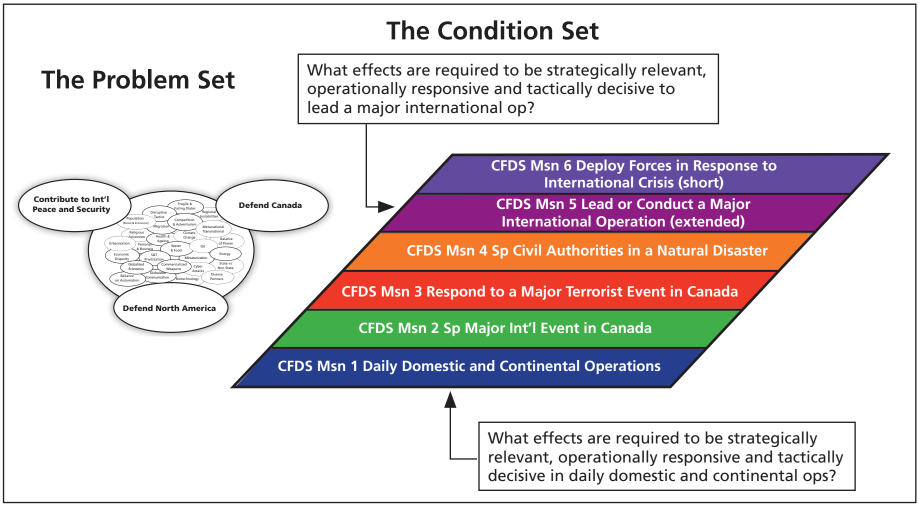
INSIGHT 8

THE SPECTRUM OF FUTURE CONFLICT IS NO LONGER A LINEAR UNDERSTANDING OF PEACE, OPERATIONS OTHER THAN WAR, AND WAR.

4.3 CFDS Missions – Condition Sets

Condition sets include the variables that can be encountered by the CF in fulfilling its roles and missions. At the strategic level, the variables can be grouped in broad categories such as geography, climate, and socio-political. Condition sets will almost never be the same for any two missions. Techniques, Tactics, and Procedures used in similar operations, or even at an earlier time in the same operation, will rarely achieve the same outcomes, or may in fact become counter-productive.

For the purposes of the ICC, the six CFDS missions will be used as the basis for the condition sets. Each of these missions will demand varying requirements for being comprehensive, integrated, adaptive, and networked in order for the CF to remain strategically relevant, operationally responsive, and tactically decisive.


The Condition Set
The Problem Set
Contribute to Int'l Peace and Security
Defend Canada
Defend North America
Fragile & Failing States
Disruptive Tactics
Regional Instabilities
Population (Social & Economic)
Competition & Adventurism
Migration
Metanational Transnational
Religious Extremism
Health & Ageing
Climate Change
Balance of Power
Urbanization
Personal & Business
Water & Food
Oil
Energy
Economic Disparity
S&T Privitization
Miniaturization
State vs Non-State
Globalized Economics
Commercialized Weapons
Cyber Attacks
Globalized Communication
Reliance on Automation
Biotechnology
Diverse Partners
CFDS Msn 6 Deploy Forces in Response to International Crisis (short)
CFDS Msn 5 Lead or Conduct a Major International Operation (extended)
CFDS Msn 4 Sp Civil Authorities in a Natural Disaster
CFDS Msn 3 Respond to a Major Terrorist Event in Canada
CFDS Msn 2 Sp Major Int'l Event in Canada
CFDS Msn 1 Daily Domestic and Continental Operations

What effects are required to be strategically relevant, operationally responsive and tactically decisive to lead a major international op?

What effects are required to be strategically relevant, operationally responsive and tactically decisive in daily domestic and continental ops?

FIGURE 9: THE CONDITION SET.

STRATEGIC IMPACTS

The CF must be able to adaptively operate (proactively and reactively) throughout the spectrum of conflict, whether in a conventional or irregular manner.

As the nature of conflict becomes increasingly dynamic, the spectrum of actors and solutions also increases and may necessitate actions that are no longer the exclusive realm of military forces.

5 THE NATURE OF THE FUTURE STRATEGIC ENVIRONMENT

This section provides an overview of the future strategic environment. The section advocates an expansion of the strategic environment, comprised of maritime, land, and air, to include three new domains: space, cyberspace, and human. A discussion of how technology and globalization have empowered adversarial actors (state and non-state) with instruments of national power and influence that were previously unobtainable is also included in the description of the human domain.

5.1 The Strategic Environment Described

The strategic environment is defined as where the elements of power and influence are exercised. The traditional elements of national power and influence are the diplomatic, economic, and military[21] capabilities possessed at the national level that can be directed toward effecting change in the human condition in the pursuit of national policy and intent. National policy and intent are those conditions, expectations, and desires set by government policy that direct the employment of the elements of national power.

The strategic environment is defined as where the elements of power and influence are exercised.

Non-state adversaries increasingly operate in the same strategic environment as DND/CF. Historically, the traditional elements of power and influence have been restricted to the state. In the modern security environment, the elements of power and influence are no longer exclusive to the state, and states no longer have exclusive dominion over the domains in the strategic environment. Current and future adversaries, whether state or non-state, have the power to create strategic effects directed against Canadian national interests. We must be aware that within states, new elements of power and influence are coming into being that challenge conventional perspectives.

States no longer have exclusive dominion over the domains in the strategic environment.

5.2 Three New Domains

Although maritime, land, and air are referred to as the traditional domains, these three did not always exist, nor is this number necessarily (or likely) to remain at three in the future. Access to each of the traditional domains within the strategic environment can be traced to technological developments. With the creation of sailing vessels, military forces could then carry out warfare on both land and sea. The advent of flight and subsequent technological improvements meant that conflict was extended there as well.

As these technological developments evolved, military forces were able to devise strategic uses for the technology and then exercise power and influence from ships and aircraft. The sea and air domains became part of the strategic environment when people developed the ability to generate national power and influence by accessing them.

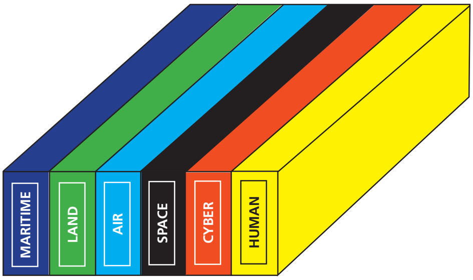


FIGURE 10: STRATEGIC ENVIRONMENT (DOMAINS) AXIS OF THE CAPSTONE CONSTRUCT.

Recent developments of spacecraft, communications, computing technologies, media, and behavioural sciences are expanding the strategic environment and creating new domains: space, cyberspace, human. State and non-state actors are already demonstrating that elements of power and influence can, and will, be exerted by them in the evolving domains.

5.2.1 Space Domain

Space must be considered a domain within the strategic environment. Technology continues to support growth in space, allowing more access to space and for longer durations. Space-based assets, along with their respective ground components, are part of Canada's national infrastructure.[22] Space is the medium for a number of communication facilities and supports many military and civilian capabilities. Space is also important from the aspect that an adversary can cause Canada serious strategic harm in and from this domain.

Space is not owned by anyone,[23] which essentially makes it accessible by both state and non-state actors who are capable and willing to project capabilities in that domain. Furthermore, in the conduct of global military operations, the availability of satellite services for DND/CF will be vital. In support of achieving Canadian strategic goals, such as exercising sovereignty in the Arctic, space-based assets are critical mission enablers. The CF will need to expand its role in space to protect and exploit vital information and communication sources.

Space will continue to grow in importance, as reliance upon space technology continues to increase. However, as recent examples have demonstrated, these space-based systems are increasingly vulnerable to attack from various weapons platforms.[24] This ability to destroy or disable satellites is currently limited to a select number of states, but the technology to disrupt, destroy, or disable satellites will likely become available to non-state actors or rogue nations in short order.

Many air forces have championed the space domain but have viewed space as a subordinate part of aerospace.[25] This subordinate relationship does not place enough emphasis on the rising importance of space. Space has become a joint domain and must be considered in all levels of operation. Space is a separate, unique domain where elements of national power and influence are exercised.

5.2.2 Cyberspace Domain

Cyberspace enables networks, both technical and social. Communications and information technology are essential components of national infrastructures and are the foundations for Canadian economic and financial power. Defence capability now, and into the future, is reliant upon the networks of communications and information systems that link sensors, weapons platforms, operators, and decision-makers.

The cyberspace[26] domain is also the virtual world where people meet, interact, exchange ideas, and "network" without a definable physical space. Military "communities of practice" and "communities of interest" already exist and use on-line collaboration and information sharing. Collaboration with OGDs and other defence and security agencies is also technically feasible. This access to data and information facilitates situational awareness and understanding, which combined with human intuition leads to insights and creativity.

The marketplace drives innovation and technology within cyberspace. All aspects of this domain – including the Internet, telecommunications networks, computer systems, and software – are in a process of continuous change. Trends such as media convergence of radio, television, and newspapers with the Internet only add to the shifting background. With each new technology and trend, new concepts, terminology, and jargon proliferate. It will be a challenge for the CF to keep pace with the rapid cycles of innovation and to keep abreast of leading edge concepts that are quickly discarded or replaced by newer concepts.

The cyberspace domain will be a mechanism for integrating all of the domains at the strategic level resulting in one common operational picture. This functionality will be complemented by the facility of the cyberspace domain to merge the strategic functions, producing integrated effects. Cyberspace may also be where the medium and the message are virtually inseparable.

Cyberspace has unique vulnerabilities. Accessible and affordable technology has made this the easiest domain for adversaries to exploit. In this domain, the distinction between criminal activity and threat to national security can be difficult to ascertain. Cyberspace recognizes no borders; servers located in neutral or friendly nations can be used by an adversary to conduct cyber attacks. The temporal aspects required to conduct cyber defence are extremely compressed. A continuing challenge will be to ensure our policy and doctrine keep up with the pace of change in the cyberspace domain.

Regardless of technologies or methods employed, the effects on national power and influence are governed by the nature of computer network operations (CNO) that can be conducted in the cyberspace domain. Most nations classify these as computer network exploitation (CNE), computer network attack (CNA), and computer network defence (CND) (Figure 11). These operations can be conducted at all levels of warfare, and DND/CF must concentrate on the effects produced rather than the means by which the operations are conducted.

By attacking or disabling our networks, an adversary can readily affect command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities in the maritime, land, air, and space domains. Furthermore, an adversary can attack at the core of our national infrastructure and support systems.

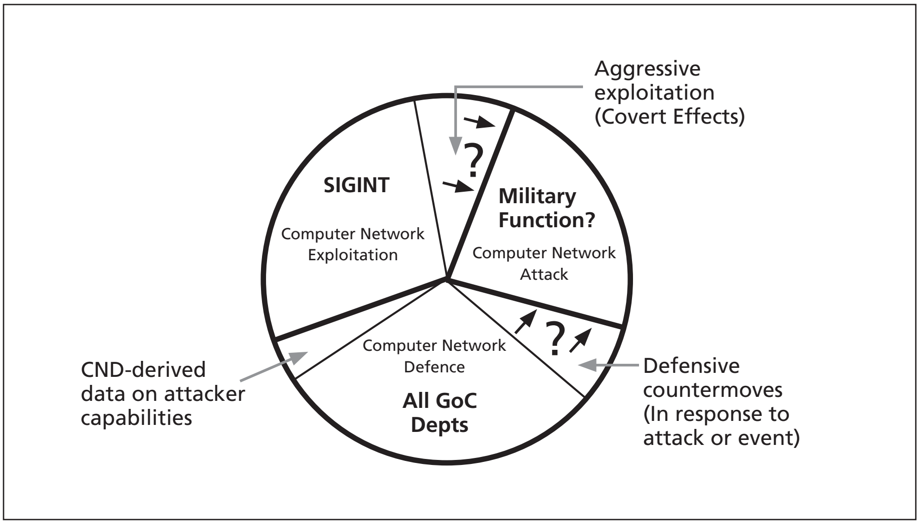

Aggressive exploitation (Covert Effects)
?
SIGINT
Computer Network Exploitation
Military Function?
Computer Network Attack
?
Computer Network Defence
All GoC Depts
CND-derived data on attacker capabilities
Defensive countermoves (In response to attack or event)

FIGURE 11: COMPUTER NETWORK OPERATIONS.

There are challenges with cyberspace as a unique domain. The current military definition and concept is a work in progress, but this work is anchored to legacy concepts based on an "Information Environment." This legacy concept was not well understood and was misapplied to psychological operations. Further confusion is created because the military definition of cyberspace is limited to the physical communications and information technology while the more commonly understood usage in the public domain also includes a virtual social networking component.

Can the virtual world of cyberspace create physical effects? Yes, the bulk of all economic power (financial instruments) is transferred electronically, and critical infrastructure relies on cyberspace. Consequently, it must also be recognized that cyberspace is becoming the predominant medium to influence the human domain.

The new question should be, "Can the physical world create effects in cyberspace (e.g. destroy information)?" The answer is certainly "yes" since individual nodes, sensors, and hardware components can be effectively destroyed; however, once video, imagery, data, information, and misinformation are placed within cyberspace, it becomes impossible to remove. For these reasons, cyberspace is a separate domain where elements of national power and influence are clearly exercised.

5.2.3 Human Domain

The human domain includes individuals, groups of individuals, and all aspects of human endeavour. Another method to describe this domain is a conflict-based view: adversaries, neutrals, or friendly actors. For the CF to succeed in the complex future security environment, it must understand individual and group motivations, technology as an enabler to human networks, and adversarial intent.

Within the individual (psychological) realm, perception, decision-making, and behaviour are the result of cognition (thinking, knowing, perceiving), emotive or affective (feeling, emotion, mood), and volition (will, striving, motivation); see Figure 12.[27] It is important to understand these biases and emotions in order to both degrade the adversaries' decision-making ability and enhance our own resilience.[28]

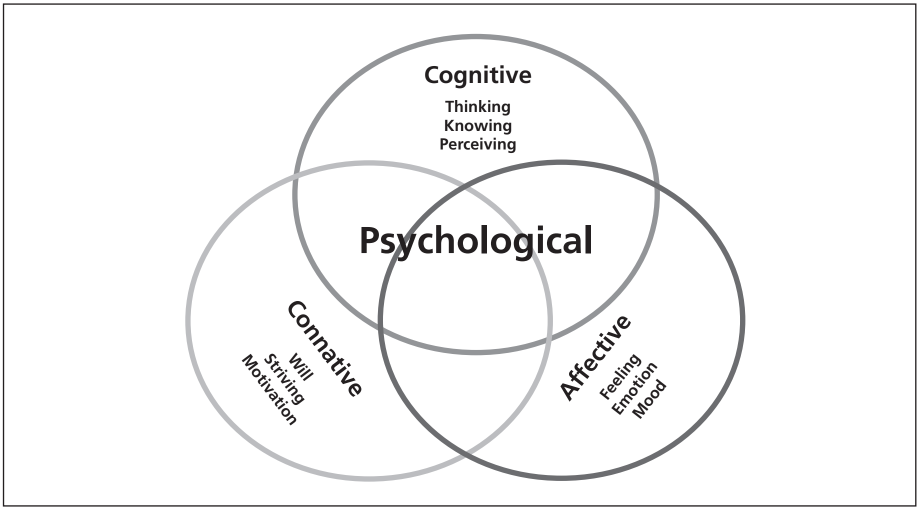


FIGURE 12: PSYCHOLOGICAL ASPECTS OF THE HUMAN DOMAIN.

Can physical and non-physical elements of national power be used to affect these things?

Yes, they always have!

More to the point, are these three psychological components relevant to national power and influence? Yes, absolutely, since these components are fundamental in the "clash of wills" or conflict. More social enabling technologies in the future will provide access to the individual, psychological realm.

Within the socio-cultural realm, there are several areas that are important for the CF with respect to networks: their nature (network analysis), their capability to learn and adapt, their various characterizations (e.g. organized crime), and the nature of relevant cultural and socio networks.

Within the CF human domain, there are three critical aspects: the institutional human where military capabilities are generated, the physical human who endures the challenges and dangers of the theatre of operations and is sustained in order to maintain operational capability, and the warrior who senses, acts, and shields. By necessity, the CF human domain will become comprehensive, integrated, adaptive, and networked and will be required to project effects in all the domains of the strategic environment.

The sociological and cultural (or group) networks that form are of particular interest because they are the basis for "other worldviews." A broad understanding not only of adversaries, but also of neutrals and potential friendly actors in the domain, is required to be strategically effective. The social and cultural networks that are of particular interest include:

- Family and tribal affiliations;
- Culture and language – shared identities, religions, beliefs, values, customs, behaviours;
- Other categories – political influence, criminal, economic; and
- Organizational categories – military, OGD, business.

Adversaries, neutrals, or friendly actors can all act as separate lenses to view the entire human domain. As an example, examining local and national economies is one means to gain perspective on the corresponding human behaviour. Each possible lens is a view of different complex systems comprising the human domain.

The key concerns within this domain are:

- How is the adversary creating effects that influence Canadian citizens, the CF, neutral actors, combatants, or non-combatants?
- Conversely, how should the CF create effects that influence adversaries, adversarial non-combatants, neutral actors, and our own citizens?
- What needs to change within the CF human domain to be able to operate in condition sets, across the strategic environment, and with the functions? Note that this domain is ultimately the source of military power.

The ultimate target for the elements of power and influence has always been the human domain. What is new is the capability to communicate ideas globally, with words and powerful images, in near real-time, to create a strategic influence. These capabilities to influence individuals and groups have dramatically increased. Enabling technology provides individual actors the ability to shape and influence large audiences globally with propaganda and misinformation. Such means were previously limited to state actors and the mass media.

EXAMPLES OF SOCIAL ENABLING TECHNOLOGIES	
Digital imagery	Still photographs and video
Television (24 hour news cycle)	CNN & Al Jazeera
Communications Technology	Cell phone, Internet telephones
Internet enabled activities	E-mail, banking, procurement, games, access to technologies
Web 2.0 (Social networking)	Twitter, Blogs, MySpace, YouTube

Powerful imagery and words crossing international boundaries to reach global audiences can expand conflict beyond the actors directly involved. More non-combatant state and non-state actors may become drawn into the conflict. In addition, global public opinion may transform into political influences within multi-national venues such as the United Nations and NATO. At the tactical level, adversarial use of propaganda may influence non-combatants and thus create a strategic effect. For example, non-combatant deaths and destruction, whether caused by adversaries or by the CF, may be used to adversarial advantage.

The human domain is the vital ground within the strategic environment.

The human domain is the vital ground within the strategic environment. The CF must understand friendly, adversarial, and neutral actors as well as the underlying factors motivating human behaviour. The CF must draw upon knowledge from human and behavioural sciences to better position itself to counter and mitigate conflict, to facilitate collaboration amongst all actors, to understand how human networks form, adapt, and evolve, and to facilitate threat assessment and threat reduction.

The CF must also understand the underlying factors that motivate individual and group behaviour, and specifically better understand friendly, adversarial, and neutral actors. Moreover, we must understand the adaptive nature of the adversarial human networks, as well as the strategic effect of adversarial influence operations when combined with new technology-enabled human networks.

Consequently, the human domain is a separate domain where elements of national power and influence are exercised to create a strategic effect. Moreover, failure in the human domain, regardless of the level of success in the remainder of the strategic environment, could result in national strategic failure.

INSIGHT 9

THE STRATEGIC ENVIRONMENT HAS EXPANDED BEYOND THE TRADITIONAL DOMAINS (MARITIME, LAND, AND AIR) AND NOW MUST INCLUDE SPACE, CYBERSPACE, AND HUMAN. THE STRATEGIC ENVIRONMENT WILL CONTINUE TO EXPAND, WHICH WILL PLACE AN EVEN GREATER EMPHASIS ON ISSUES OF COMPLEXITY AND THE NEED FOR BEING COMPREHENSIVE, INTEGRATED, ADAPTIVE, AND NETWORKED.

5.3 Relationship of the Domains

Figure 13 portrays the relationship amongst the components of the strategic environment. The human is central; the physical domains (maritime, land, air, and space) surround the human. More and more, cyberspace can affect our perception of the physical world, so in this depiction, cyberspace surrounds the human. Borders are blurring, and perception can be enhanced or deceived by technology. Cyberspace also enables many networks that are separated by distance in the physical world; thus, there is a direct relationship with the human.

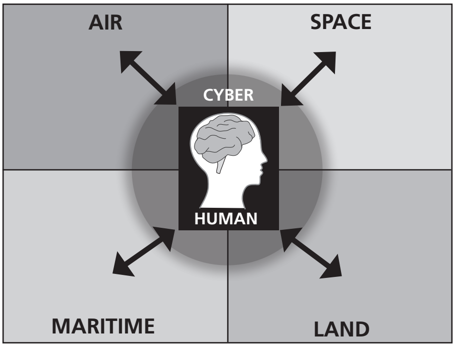


FIGURE 13: RELATIONSHIP OF THE DOMAINS.

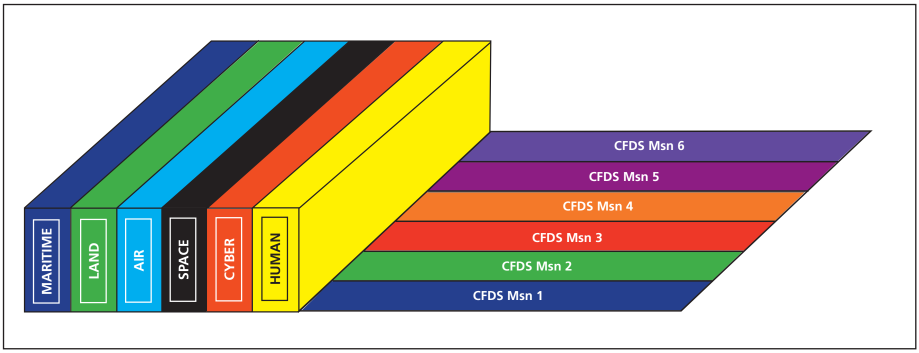


FIGURE 14: THE CONDITION SET AND DOMAINS AXES OF THE CAPSTONE CONSTRUCT.

The organizational components of the CF (Navy, Army, Air, and Special Forces) will continue to provide expertise and operate within their traditional domains and also contribute to realizing goals across the strategic environment. The new domains do not imply ownership, but rather demand leadership. Integrating the capabilities of a wide range of organizations will provide a more adaptive set of tools to cope with future complex problems.

The new domains do not imply ownership, but rather demand leadership.

As we proceed into the future, we must maintain a progressive attitude towards yet-to-be-discovered domains where elements of national power and influence can be exercised. Nano and quantum are distinct possibilities of future domains.

Our ability to be strategically relevant, operationally responsive, and tactically decisive within the entire spectrum of future conflict is fundamentally dependent upon our ability to project or to deny effects in all of these domains. Commanders at all levels must be prepared to have adversarial effects projected at them from all six domains, perhaps simultaneously. Depending upon the nature of the mission, commanders at all levels will also have to be prepared to generate effects in all six domains simultaneously and in an integrated and comprehensive manner.

Our ability to be strategically relevant, operationally responsive, and tactically decisive within the entire spectrum of future conflict is fundamentally dependent upon our ability to project or to deny effects in all of these domains.

STRATEGIC IMPACTS

States no longer have exclusive dominion over the domains in the strategic environment.

Current and future adversaries, whether state or non-state, have the power to create strategic effects directed against Canadian national interests.

By attacking or disabling our networks, an adversary can readily affect command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities in the maritime, land, air, and space domains. An adversary can also attack the core of our national infrastructure and support systems.

Strategic failure in any particular domain could result in national strategic failure.

Failure in the human domain, regardless of the level of success in the remainder of the strategic environment, could result in national strategic failure.

The CF must understand friendly, adversarial, and neutral actors as well as the underlying factors motivating human behaviour.

By drawing from the human and behavioural sciences, the CF can better position itself to counter and mitigate conflict, to facilitate collaboration amongst all actors, to understand how human networks form, adapt, and evolve, and to facilitate threat assessment and threat reduction.

The CF must understand the adaptive nature of adversarial human networks, as well as the strategic effect of adversarial influence operations when combined with new technology-enabled human networks.

These new domains do not imply ownership, but rather they demand leadership.

Commanders at all levels must be prepared to have adversarial effects projected at them from all six domains, perhaps simultaneously.

Commanders at all levels, depending upon the nature of the mission, will have to be prepared to generate effects in all six domains simultaneously, in an integrated and comprehensive manner.

Space, cyberspace, and human are all separate domains where the instruments of national power and influence can be exercised, with equal importance to the traditional domains.

Our ability to be strategically relevant, operationally responsive, and tactically decisive within the entire spectrum of future conflict is fundamentally dependent upon our ability to project or to deny effects in all these domains.

6 THE NATURE OF FUTURE FUNCTIONS

This section examines the CF functions of Command, Sense, Act, Sustain, Shield, and Generate with regards to being comprehensive, adaptive, integrated, and networked.

The six functions describe what the CF does in the course of daily routines and contingency operations. Failure in any one of the functions across the strategic environment may lead to strategic failure. Our current view of the strategic functions is governed by our historical experiences and knowledge of the traditional land, sea, and air domains. This planning for old battles may give us stereotypical views of the functions that may not necessarily speak to the future. At best, it may restrict us insofar as our ideas about future operations are governed solely by knowledge of current operations. In the worst case, it may cause us to plan for yesterday's conflict. To successfully carry out the direction of the GoC in an increasingly complex future security environment, comprehensive, integrated, adaptive, and networked approaches must be applied to the future functions.

The following table lists the proposed future definitions for the CF functions.[29]

Function	Definition
Command	The creative and purposeful exercise of legitimate authority to accomplish the mission legally, professionally, and ethically.
Sense	The acquisition and processing of information to enable commanders and authorities to understand the characteristics and conditions of the operating environment pertinent to military decision-making.
Act	The military use of capabilities to achieve desired effects in support of national policy
Sustain	The provisioning of all support services required to maintain routine and contingency operations – domestic, continental, and expeditionary – including prolonged operations.
Shield	The comprehensive approach to the protection of tangible and intangible elements through the integrating activities of detection, assessment, warning, defence (active and passive), and recovery.
Generate	The method by which DND and the CF recruits, trains, and develops personnel, procures equipment, infrastructure, and services, and all are made ready in order to meet the defence mission.

Our current view of the strategic functions (Command, Sense, Act, Sustain, Shield, and Generate) is governed by our historical experiences and knowledge of the traditional land, sea, and air domains. In the worst case, it may cause us to be planning for yesterday's conflict.

6.1 Command

The future Command function is defined as "the creative and purposeful exercise of legitimate authority to accomplish the mission legally, professionally, and ethically."[30]

Adaptive command comprises the toolbox that allows those in command positions, at all levels, to exercise mission command.

Adaptive command is the logical evolution of how this function is to be exercised in the CF in order to support the mission command concept. If mission command is an extension of command intent through an implicit understanding of that intent, then adaptive command comprises the toolbox that allows those in command positions, at all levels, to exercise mission command. An ingenious and organized adversary can achieve levels of surprise by taking action contrary to what was predicted. Conversely, adversaries' creativity can be mitigated and countered by those in command anticipating, adapting, and rapidly reacting to unpredictable adversarial action. Adaptive command is characterized by the hallmarks of adaptation.[31]

The future Command concept needs to describe the comprehensive factors that assist this function. Understanding the condition sets and the strategic environment will help commanders to define the problem and set (or reset) appropriate goals. The future Command concept should engender a multi-disciplined approach to integrate forces into a larger organizational construct in order to solve, manage, or contain the many challenges in the complex security environment.

6.2 Sense

The future Sense function is described as "the acquisition and processing of information to enable commanders and authorities to understand the characteristics and conditions of the operating environment pertinent to military decision-making."

The future Sense capabilities need to provide decision-makers with a comprehensive understanding of the information and intelligence that are required. There is a need to examine the human domain and understand the many networks formed within the strategic environment.

This function must be integrated to a high level to produce the best results for decision-makers. Information from a variety of sources – military and civilian networks – must be fused to provide situational awareness. Sense capabilities must be able to mitigate challenges such as climate and weather, terrain, language, beliefs, and cultural sensitivities. Nevertheless, even with total integration of all actors, perfect situational awareness is virtually unachievable.

The future Sense concept should employ highly integrated networks to share information in a timely manner, but the function should also be capable of employing *ad hoc* or mission-specific networks. Determining the organizations that form friendly, neutral, and adversarial human networks within the strategic environment will be difficult but is essential to strategic effectiveness.

6.3 Act

The future Act function is defined as "the military use of capability(ies) to achieve desired effects in support of national policy."

In the future security environment, the CF must be able to act in a comprehensive manner as one of the national instruments of power. Actions will produce a myriad of effects, some expected, some unpredicted, and some undesired. In a multi-disciplinary approach, not only our own actions, but also the actions of all other organizations, must be considered. A comprehensive understanding of the strategic environment, condition sets, our actions, and the actions of others will help to achieve desired goals and also mitigate side effects.

The future Act concept must encompass the notion of integration since the CF will be unable to solve complex issues in isolation. It is highly likely that the future CF will need to operate with a variety of other nations, other government departments, and non-government organizations. Integration of all participants, at the appropriate level, will produce convergent effects.

The forces directed to act need to be adaptive. By demonstrating the ability to reconfigure when faced with a new threat (flexibility), to redirect effects swiftly (agility), to do all this quickly (responsiveness) and in a manner that can be sustained over a prolonged period (endurance), the forces will be able to thwart unpredictable adversarial action.

6.4 Sustain

The future Sustain function is defined as "the provisioning of all support services required to maintain routine and contingency operations – domestic, continental, and expeditionary – including prolonged deployed operations."

To meet the challenge of sustaining the CF, whether at home or abroad, it is imperative for decision-makers to have a comprehensive understanding of the condition sets, the CF's changing needs, and the likely obstacles to be faced in addressing sustainment demands. Sustain capabilities will also require cooperation amongst all potential contributors: CF, allies, agencies, industry, academia, and NGOs – both national and international. Comprehensive sustainment will encompass materiel, personnel, and information.

Comprehensive sustainment will result in taking advantage of organizations, capabilities, systems, and processes from around the globe and deliberately building partnerships. Bringing together the capabilities in government (federal, provincial, municipal), industry, NGOs, academia, and amongst allies will require a carefully integrated approach so as to work as efficiently and as seamlessly as possible.

These partnerships of people and organizations from across the country and around the world will need to be brought together through information-age networks. Once such networks of contributors have been established and enabled, the CF can reach back into the network as needed to access point-of-need sustain capabilities directly from the source-of-origin.

As threats evolve and change, the CF's Sustain capabilities (and arrangements) will need to be able to reconfigure, reorganize, and reprioritize to meet the demands. In order to expedite precise delivery of sustainment, decision-makers must be solution-oriented in creating anticipatory and predictive tools and in arranging collective agreements between the GoC and national and international partners. Because of the wide variety of partners available to meet Sustain requirements, these networks can more easily be adaptive by bringing partners together as needed, when needed, and for only as long as needed.

6.5 Shield

The future Shield function is defined as the "comprehensive approach to the protection of tangible and intangible elements through the integrating activities of detection, assessment, warning, defence (active and passive), and recovery."

In order to successfully shield the CF in the future, a comprehensive understanding of the strategic environment, condition sets (specific circumstances), and especially the threats is required. The CF must have a broad understanding of what exactly needs to be shielded: this should encompass tangible defence assets (capabilities, platforms, people, as well as national telecommunications, business, transportation, and energy infrastructure) and intangible defence assets (national interests, culture, values, and will; economic well-being; public opinion). A comprehensive appreciation of the best actors with whom to establish partnerships for optimum shielding capabilities is also imperative.

A layered Shield response will require the seamless integration of the relevant military, civilian, OGD, NGO, and allied actors. Partners will need to depend upon each other for critical capability, information, and intelligence. Facilitating such integration is the creation of networks amongst national and international defence and security agencies. These human networks will be enabled by linking partner capabilities through information-age networks.

The Shield capability of the future must be more adaptive. Not only must the response be rapid, but it must also be able to re-scope, re-scale, and re-configure for any condition set and for any new or changing threat. The level of shielding should adjust to the requirements of the critical node in order to provide what is needed exactly when and where this need arises. Part of adaptation is the ability for Shield to take on the approach required at a particular moment: deter, prevent, pre-empt; or detect, deflect, counter-act.

The complex security environment has brought about an increase in threats from which Canada needs shielding: individuals have access to capabilities that were once the sole purview of states, and less-developed states have gained access to capabilities that once only rich nations could afford. The complexity of the security environment has also exposed new vulnerabilities; this includes the human domain and national well-being, identity, and unity. A key question remains: How do we shield within the cyber domain within a transparent society?

6.6 Generate

The future Generate function "is the method by which DND and the CF recruits, trains, and develops personnel, procures equipment, infrastructure, and services, and all are made ready in order to meet the defence mission." Generate is an institutional function. The future Generate concept should describe adaptive and integrated capabilities.

The increasingly complex strategic environment highlights the requirement for Generate capabilities that are highly adaptive. The CF must be able to adapt, reconfigure, reorganize, and reprioritize a finite Generate capacity to meet ever-changing defence requirements. This will be accomplished by progressively implementing information-age technology in concert with organizational and process changes.

In order to be more adaptive, DND and the CF must be able to recognize personnel with the aptitude to operate in a technically challenging environment where more networks, both human and technical, are pervasive. These people – whether CF Regular Force, Reserve Force, or civilian – will require training, education, and professional development that enables them to exercise the hallmarks of adaptation. This will provide the personnel needed to meet the expectations of the GoC, as reflected in CFDS.

> ***"To carry out these missions, the Canadian Forces will need to be a fully integrated, flexible, multi-role and combat-capable military, working in partnership with the knowledgeable and responsive civilian personnel of the Department of National Defence."***
>
> **Canada, *First Defence Strategy,* p.3.**

Future practice may see all members of DND and the CF employed and rapidly deployed to positions based upon a competency match that moves beyond labels of Regular Force, Reserve Force, and civilian. Integration becomes essential. The establishment of a civilian Defence and Security Professional is an idea that highlights potential integration of DND, Royal Canadian Mounted Police, Canadian Security Intelligence Service, and Canadian Border Service Agency civilian personnel.

There also needs to be a more integrated approach to generating and developing capability that will be adaptive to new threats in a dynamic and uncertain future. There is a need for strategic integration of force employment, force generation, and force development within a comprehensive managed readiness system that speaks to the complexity of all the condition sets, domains, and functions.

INSIGHT 10

THE CURRENT VIEW OF THE STRATEGIC FUNCTIONS IS GOVERNED BY OUR HISTORICAL EXPERIENCES AND KNOWLEDGE OF THE TRADITIONAL DOMAINS. THE FUTURE VIEW OF THE STRATEGIC FUNCTIONS MUST BE GOVERNED BY THE ATTRIBUTES OF BEING COMPREHENSIVE, INTEGRATED, ADAPTIVE, AND NETWORKED ACROSS ALL DOMAINS.

6.7 Way Ahead for the Future View of Strategic Functions

To avoid the pitfall of planning for yesterday’s conflict, concept developers and planners must avoid the limitations of our traditional thinking in maritime, land, and air domains. The future view of the strategic functions must be governed by the attributes of comprehensive, adaptive, integrated, and networked. Furthermore, in order to remain strategically relevant, operationally responsive, and tactically decisive in the complex strategic environment, a fundamental understanding of the effects required by each of these functions in each discrete condition set and domain is essential. Nevertheless, there are still fundamental questions that remain to be answered, such as “how will the three new domains change CF functions?”

STRATEGIC IMPACTS

Failure to understand the similarities and differences of the functions in relation to the expanding domains and dynamic condition sets will result in "planning for yesterday's conflicts."

Future function concepts (Command, Sense, Act, Sustain, Shield, and Generate) should describe comprehensive, integrated, adaptive, and networked capabilities.

The future Command concept must understand the effectiveness of a multi-disciplined approach to solve, manage, or contain many types of problems and to integrate forces into the larger comprehensive organization.

The future Sense concept should employ highly integrated networks to share information in a timely manner, but the function should also be capable of employing ad hoc or mission-specific networks.

In the future Act concept, forces must be adaptive. The CF will be better able to thwart unpredictable adversarial action if they can reconfigure to a new threat (flexibility), redirect effects swiftly (agility), do all this quickly (responsiveness) and in a manner that can be sustained over a prolonged period (endurance).

In the future Sustain concept, a network of the wide variety of partners available must be more easily adaptive and brought together as needed, when needed, and for only as long as needed to meet sustain requirements.

For the future Shield concept, the CF must have a comprehensive understanding of Canada's vulnerabilities: this should encompass tangible defence assets (capabilities, platforms, people, national telecommunications, business, transportation, and energy infrastructure) and intangible defence assets (national interests, culture, values, and will; economic well-being; public opinion).

In the future Generate concept, there must be strategic integration of force employment, force generation, and force development within a comprehensive managed readiness system that speaks to the complexity of all the condition sets, domains, and functions.

To be integrated and adaptive, both DND and the CF will need to generate appropriate personnel capable of operating in complex situations; this implies the creation of the civilian "Defence Professional" and the possibility of an equivalent "Security Professional" for the GoC.

In order to remain strategically relevant, operationally responsive, and tactically decisive in the complex strategic environments, a fundamental understanding of the effects required by each of these functions in each discrete condition set and domain is essential.

7 CAPSTONE CONSTRUCT

This section introduces the capstone construct and describes its purpose. The information in the preceding sections is brought together, and the relationships between condition sets, domains, and functions are examined at a strategic level. The use of the capstone construct as a tool for capability and concept development is also discussed.

7.1 Capstone Construct and Complex Systems

A singular and shared construct that governs the relationship between condition sets, domains, and functions is fundamental to unity of thought, purpose, and action for integrated force development, force generation, and force employment.

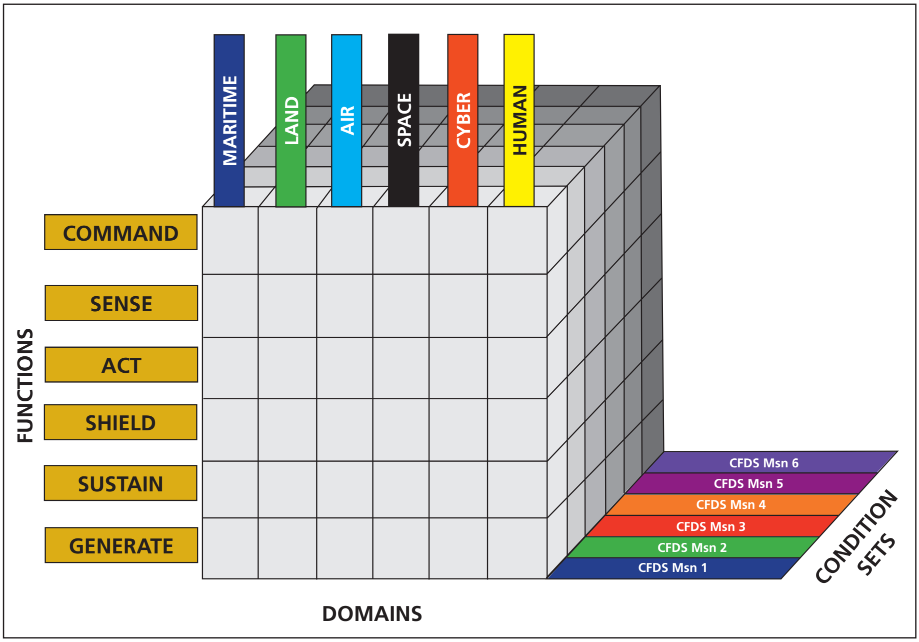


FIGURE 15: THE CAPSTONE CONSTRUCT.

The capstone construct is not an attempt to model the future security environment and the CF, nor is it an attempt to deconstruct the inherent complexity. A true complex system, by definition, refuses to be defined, deconstructed, and bounded.

However, there is a need to identify the range of conditions to be examined and the relationships in complex systems. There is also the need to provide a comprehensive understanding and representation of interactions and inter-relationships of the condition sets, domains, and functions. There could also be areas where we may be able to define the boundaries. If we can, we should do so. The capstone construct fulfills these needs.

7.2 Relationship Amongst Condition Sets, Domains, and Functions

The capstone construct builds upon the analysis of condition sets, domains, and future functions to provide an understanding of the interactions between these three axes. For a particular condition set, each of the six CF functions can be analyzed in each of the domains within the strategic environment. Each block of the construct can be used to describe a specific function within a specific domain for a specific condition set to identify what effects are necessary in order to be strategically relevant, operationally responsive, and tactically decisive. The construct also serves as a framework for comparing similarities and differences.

What is found to be the case in one block will probably be different for an alternative condition set, simply because condition sets have complex natures.

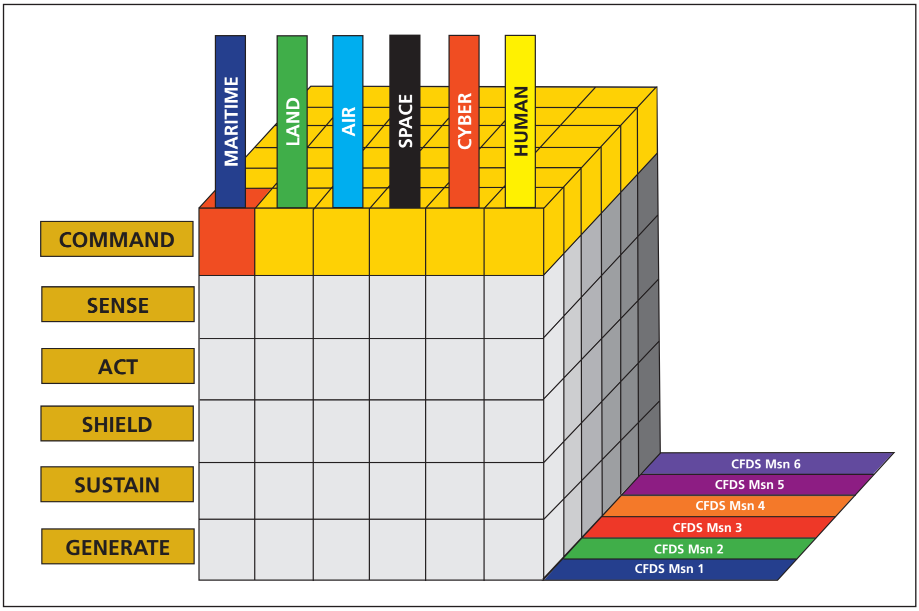


FIGURE 16: ANALYZING COMMAND IN THE MARITIME DOMAIN FOR CFDS MISSION 1.

As illustrated in Figure 16, once the requirements for the Command function in the maritime domain have been identified for daily domestic and continental operations, they can then be compared to the corresponding command requirements in the other domains, for the same mission. Alternatively, the requirements for the Command function in the maritime domain can be compared against a wide array of condition sets (CFDS missions), thereby allowing a comprehensive view of maritime Command capability requirements. This process can be replicated across an extensive range of function and domain interactions. For example, how does command differ in CFDS Mission 1 between the maritime and space domains?

By using the capstone construct, the joint requirements, as well as the fundamental differences underlying a collective effort, can be identified, as can the common elements and the unique requirements for specific condition sets, domains, and functions. Such comparative analysis will demonstrate what is common to all, what is unique, and what the collective requirements are for delivery of integrated effects.

By using the capstone construct, the joint requirements, as well as the fundamental differences underlying a collective effort, can be identified, as can the common elements and the unique requirements for specific condition sets, domains, and functions.

The capstone construct provides a common analytical framework for concept and capability developers and strategic planners. A concept developer can use the capstone construct to determine the requirements for the Sense function in the space domain needed when responding to a major terrorist event in Canada. Using the same construct, the capability developer can study what capabilities, authorities, structures, and processes are required for the Sense function in the cyberspace domain for the same mission. The strategic planner can use the capstone construct to identify the requirements for integration and command and control for the Sense function across the missions.

7.3 Conceptual Framework – Integrating, Operating, and Enabling Concepts

The capstone construct also provides a framework for creating concepts and understanding a concept hierarchy. By looking at the construct in three different ways, integrating, operating, and enabling concepts can be systematically developed.

INSIGHT 11

ONLY BY HAVING A COMPREHENSIVE VIEW OF THE RELATIONSHIPS BETWEEN THE CONDITION SETS, DOMAINS, AND FUNCTIONS CAN WE DETERMINE THE REQUIREMENTS FOR BEING COMPREHENSIVE, INTEGRATED, ADAPTIVE, AND NETWORKED.

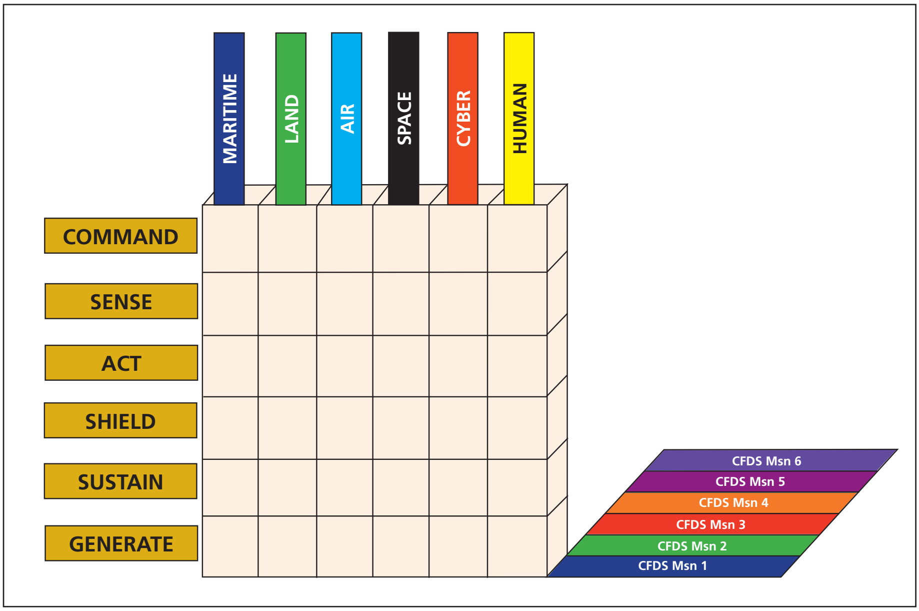


FIGURE 17: INTEGRATING CONCEPTS.

Integrating concepts can be developed by considering the collective relationships for a comprehensive, integrated, adaptive, and networked application of national intent within a particular condition set.

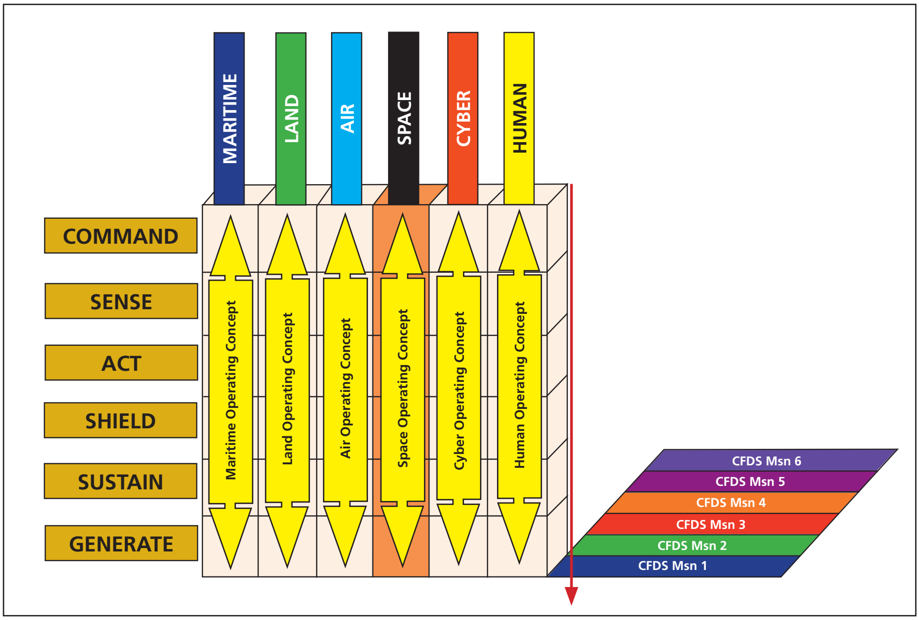


FIGURE 18: OPERATING CONCEPTS.

Operating concepts can be developed to describe the requirements (based on the six functions) for a specific environment within a specific mission. It comprises the collective relationship for a comprehensive, integrated, adaptive, and networked application of national interest within a particular domain and a particular condition set (ex: space operating concept for CFDS Mission 1).

The capstone construct can also be used to amplify methodological or technological enablers (enabling concepts) that cover a wide variety of missions, domains, and functions. As an example, the Comprehensive Approach is a methodological enabling concept. Artificial Intelligence, on the other hand, would be a technological enabling concept that could result in a new range of impacts on being strategically relevant, operationally responsive, and tactically decisive.

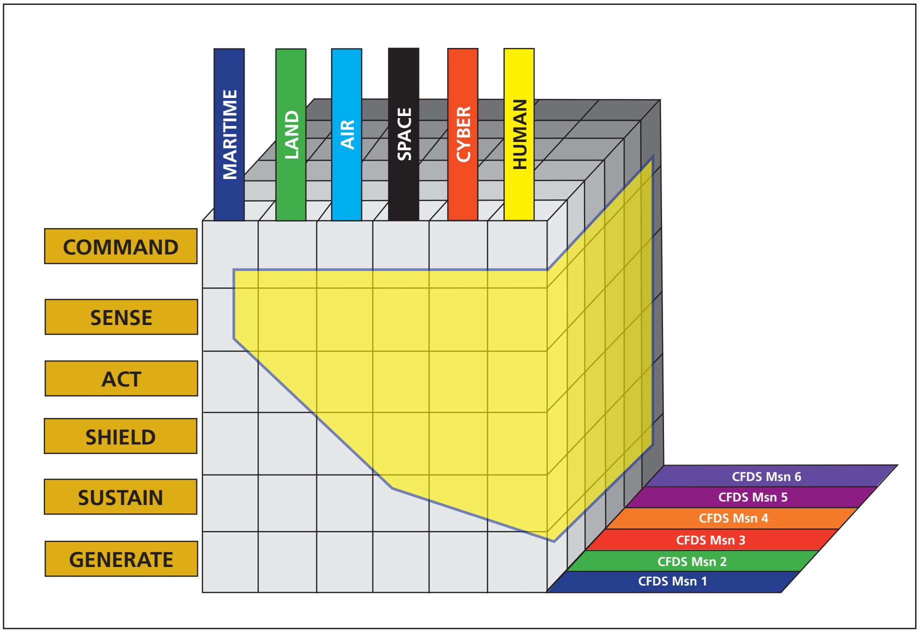


FIGURE 19: ENABLING CONCEPTS.

The capstone construct provides the tool for concept developers, capability mangers, and strategic planners to help set levels of ambition and assist in the analysis of risk.

In the future, the capstone construct will expand, as the number of factors and challenges resident in the future security environment will elevate the level of complexity. Hence, as the strategic environment continues to expand in the future, more domains are likely to come into existence. The same possibility of expansion exists for condition sets and functions.

STRATEGIC IMPACTS

A singular and shared construct governing the relationship amongst condition sets, domains, and functions is fundamental to unity of thought, purpose, and action for integrated force development, force generation, and force employment.

The capstone construct allows decision-makers to set levels of ambition and to conduct risk analysis.

In the future, the capstone construct will expand. As the strategic environment continues to expand in the future, more domains are likely to come into existence. The same possibility of expansion also exists for condition sets and functions.

8 SUMMARY OF INSIGHTS AND STRATEGIC IMPACTS

Understanding the implications that complexity will present is essential to strategic success for the CF. It is also fundamental to understanding the changing nature of our adversaries, the domains in which we will operate, and the types of operations that the CF will be tasked to perform. In order to meet these challenges, we will need to create an integrated, multi-role, and combat capable military force that will be comprehensive, integrated, adaptive, and networked in the execution of national intent.

INSIGHTS	**STRATEGIC IMPACTS**
Insight 1: The strategic environment has always been dominated by issues of complexity. However, the number of factors and challenges resident in the future security environment will significantly increase the levels of complexity.	• Complex future security challenges demand approaches that are comprehensive, integrated, adaptive, and networked. Therefore, these attributes must become the tenets that govern the nature of the future force and the requirements for being strategically relevant, operationally responsive, and tactically decisive.
Insight 2: Understanding the implications that complex systems will present in the future security environment is essential to strategic success for the CF. The future security environment will be influenced by an ever-expanding spectrum of dynamic complex and adaptive systems.	• It is fundamental to understand the growing number of agents affecting national and international security, the changing nature of our adversaries, the consequences of various groups' interactions, the unpredictable and non-linear nature of actions and behaviour, the domains in which we will operate, and the types of operations that the CF will be tasked to perform. • The linear tools and legacy constructs that we currently use for problem solving may be inadequate for the challenges provided by future complex systems.
Insight 3: The dynamic and complex strategic environment will be further influenced by an ever-expanding spectrum of technically and socially enabled actors who will be more co-ordinated, increasingly networked, and who share adversarial intent.	• Global access to science and technology (such as space, cyberspace, and advanced disruptive technologies) means military advantage can belong to whomever is quickest and best able to acquire and exploit new capabilities, thus increasing the adversarial capability of non-state actors to levels that rival those of nation states.

INSIGHTS	STRATEGIC IMPACTS
Insight 4: Comprehensiveness must describe a multi-disciplinary approach to resolve those challenges forecasted in the future security environment which are well beyond the scope and the capacity of the CF alone.	• The CF is but one instrument of national power and influence available to the GoC. • Non-governmental agencies may simultaneously be working in the complex space to solve other portions of a crisis and may or may not share the goals of the GoC. • To best resolve or manage complex situations, a comprehensive framework is needed.
Insight 5: Integration within a multi-disciplinary approach will provide a greater chance of resolving the complex issues of the future security environment than will working independently.	• Integration of DND and the CF must evolve from organizational silos to processes, networks, relationships, and capabilities that enable integrated operations. • The entire institution will need to integrate as required with other agencies or actors.
Insight 6: Adaptation is imperative to coping with unpredictable and uncertain complex challenges, situations, and relationships. The CF must be adaptive or risk failure.	• To be adaptive, the CF needs: • Leaders who can discern the consequences of emerging trends and react to strategic shocks; • Commanders who are not afraid to pursue innovative and unconventional solutions; • Individuals who, like our adversaries, can envision the use of equipment in new and innovative ways; and • Soldiers, sailors, and air personnel who can sense a change in the adversary's course of action and exploit it to the benefit of the mission.
Insight 7: Both social and technical networks must be exploited by the CF across the strategic environment and within all domains in response to adversaries' increased technically and socially enabled capabilities.	• Our current hierarchical networks may not be conducive to succeeding in a future complex security environment. • The CF should explore more integrated or hybrid networks as opposed to hierarchical ones. • Based on goals to be achieved, external connectivity with defence and security organizations, OGDs, allies, and partners will be required to the extent necessary. • Both social and technical networks provide the means to be comprehensive, integrated, and adaptive so that the CF can meet the challenges of the complex security environment.

INSIGHTS	**STRATEGIC IMPACTS**
Insight 8: The spectrum of future conflict is no longer a linear understanding of peace, operations other than war, and war.	• The CF must be able to adaptively operate (proactively and reactively) throughout the spectrum of conflict, whether in a conventional or irregular manner. • As the nature of conflict becomes increasingly dynamic, the spectrum of actors and solutions also increases and may necessitate actions that are no longer the exclusive realm of military forces.
Insight 9: The strategic environment has expanded beyond the traditional domains (maritime, land, and air) and now must include space, cyberspace, and human. The strategic environment will continue to expand, which will place an even greater emphasis on issues of complexity and the need for being comprehensive, integrated, adaptive, and networked.	• States no longer have exclusive dominion over the domains in the strategic environment. • Current and future adversaries, whether state or non-state, have the power to create strategic effects directed against Canadian national interests. • By attacking or disabling our networks, an adversary can readily affect command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities in the maritime, land, air, and space domains. An adversary can also attack the core of our national infrastructure and support systems. • Strategic failure in any particular domain could result in national strategic failure. • Failure in the human domain, regardless of the level of success in the remainder of the strategic environment, could result in national strategic failure. • The CF must understand friendly, adversarial, and neutral actors as well as the underlying factors motivating human behaviour. • By drawing from human and behavioural sciences, the CF can better position itself to counter and mitigate conflict, to facilitate collaboration amongst all actors, to understand how human networks form, adapt, and evolve, and to facilitate threat assessment and threat reduction. • The CF must understand the adaptive nature of adversarial human networks, as well as the strategic effect of adversarial influence operations when combined with new technology-enabled human networks.

INSIGHTS	**STRATEGIC IMPACTS**
	• These new domains do not imply ownership, but they rather demand leadership. • Commanders at all levels must be prepared to have adversarial effects projected at them from all six domains, perhaps simultaneously. • Commanders at all levels, depending upon the nature of the mission, will have to be prepared to generate effects in all six domains simultaneously, in an integrated and comprehensive manner. • Space, cyberspace, and human are all separate domains where the instruments of national power and influence can be exercised, with equal importance to the traditional domains. • Our ability to be strategically relevant, operationally responsive, and tactically decisive within the entire spectrum of future conflict is fundamentally dependent upon our ability to project or to deny effects in all these domains.
Insight 10: The current view of the strategic functions is governed by our historical experiences and knowledge of the traditional domains. The future view of the strategic functions must be governed by the attributes of being comprehensive, adaptive, integrated, and networked across all domains.	• Failure to understand the similarities and differences of the functions in relation to the expanding domains and dynamic condition sets will result in "planning for yesterday's conflicts." • Future function concepts (Command, Sense, Act, Sustain, Shield, and Generate) should describe comprehensive, integrated, adaptive, and networked capabilities. • The future Command concept must understand the effectiveness of a multi-disciplined approach to solve, manage, or contain many types of problems and to integrate forces into the larger comprehensive organization. • The future Sense concept should employ highly integrated networks to share information in a timely manner, but the function should also be capable of employing *ad hoc* or mission-specific networks.

INSIGHTS	**STRATEGIC IMPACTS**
	• In the future Act concept, the forces must be adaptive. The CF will be better able to thwart unpredictable adversarial action if it can reconfigure to a new threat (flexibility), redirect effects swiftly (agility), do all this quickly (responsiveness) and in a manner that can be sustained over a prolonged period (endurance). • In the future Sustain concept, the network of the wide variety of partners must be more easily adaptive and brought together as needed, when needed, and for only as long as needed to meet sustain requirements. • For the future Shield concept, the CF must have a comprehensive understanding of Canada's vulnerabilities: this should encompass tangible defence assets (capabilities, platforms, people, national telecommunications, business, transportation, and energy infrastructure) and intangible defence assets (national interests, culture, values, and will; economic well-being; public opinion). • In the future Generate concept, there must be strategic integration of force employment, force generation, and force development within a comprehensive managed readiness system that speaks to the complexity of all the condition sets, domains, and functions. • To be integrated and adaptive, both DND and CF will need to generate appropriate personnel capable of operating in complex situations; this implies the creation of the civilian "Defence Professional" and the possibility of an equivalent "Security Professional" for the GoC. • In order to remain strategically relevant, operationally responsive, and tactically decisive in the complex strategic environment, a fundamental understanding of the effects required by each of these functions in each discrete condition set and domain is essential.

INSIGHTS

Insight 11: Only by having a comprehensive view of the relationships between the condition sets, domains, and functions can we determine the requirements for being comprehensive, integrated, adaptive, and networked.

STRATEGIC IMPACTS

- A singular and shared construct governing the relationship amongst condition sets, domains, and functions is fundamental to unity of thought, purpose, and action for integrated force development, force generation, and force employment.
- The capstone construct allows decision-makers to set levels of ambition and to conduct risk analysis.
- In the future, the capstone construct will expand. As the strategic environment continues to expand in the future, more domains are likely to come into existence. The same possibility of expansion also exists for condition sets and functions.

9 REFERENCES

Department of National Defence Documents

Department of National Defence. *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations*. Kingston: Canadian Defence Academy – Canadian Force Leadership Institute, 2008.

---. *Canada First* Defence Strategy. Ottawa: Department of National Defence, 2008.

---. *CF Information Operations* Doctrine B-GG-005-004/AF-101. Ottawa: Department of National Defence, 1998.

---. *DND/CF Manual of Abbreviations*. Ottawa: Chief of the Land Staff.

---. *Duty With Honour: The Profession of Arms in Canada*. Kingston: Canadian Defence Academy – Canadian Forces Leadership Institute, 2003. http://www.cda.forces.gc.ca/cfli-ilfc/doc/dwh-eng.pdf [accessed 31 March 2009].

---. *National Defence Act*, (R.S., 1985, c. N-5) available on Department of Justice website, http://laws.justice.gc.ca/en/showdoc/cs/N-5/bo-ga:l_II-gb:s_14/20090623/ en#anchorbo-ga:l_II-gb:s_14 [accessed 23 June 2009].

Directorate of Future Security Analysis Documents

Department of National Defence. "Capability Domain Concept: Act." Ottawa: Chief of Force Development, 2008.

---. "Capability Domain Concept: Command." Ottawa: Chief of Force Development, 2008.

---. "Capability Domain Concept: Generate." Ottawa: Chief of Force Development, 2008.

---. "Capability Domain Concept: Sense." Ottawa: Chief of Force Development, 2008.

---. "Capability Domain Concept: Shield." Ottawa: Chief of Force Development, 2008.

---. "Capability Domain Concept: Sustain." Ottawa: Chief of Force Development, 2008.

---. *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*. Ottawa: Chief of Force Development, 2009.

---. "Integrated Capstone Concept Discussion Paper August 2008." Ottawa: Chief of Force Development, 2008.

---. "Nature of Future Conflicts Discussion Paper." Ottawa: Chief of Force Development, 2009.

---. "Nature of Future Environments: Cyberspace Environment." Ottawa: Chief of Force Development, 2009.

---. "Nature of Future Environments Discussion Paper." Ottawa: Chief of Force Development, 2008.

---. "Nature of Future Functions Discussion Paper." Ottawa: Chief of Force Development, 2009.

Complexity Theory

Bar-Yam, Yaneer. *Dynamics of a Complex System*. Addison-Wesley, 1997.

---. *Making Things Work: Solving Complex Problems in a Complex World*. Cambridge, MA: NECSI /Knowledge Press, 2004.

Dorner, Dietrich. *The Logic of Failure, Recognizing and Avoiding Error in Complex Situations.* Translated by Rita and Robert Kimber (New York: Metropolitan Books, 1996).

Maxfield, Robert R., David S. Alberts, and Thomas J. Czerwinski, eds. *Complexity, Global Politics, and National Security.* Washington D.C.: National Defense University, 1997.

New Domains

Cyberspace Domain

Air University. "What are Information Operations?" on Cyberspace and Information Operations Study Center website, http://www.au.af.mil.info-ops/what.htm [accessed 13 March 2009].

Alberts, David S. John J. Garstka, Richard E. Hayes, and David A. Signori. "Understanding the Information Age Warfare." Washington D.C.: DoD Command and Control Research Program, August 2001.

---., John J. Gastka and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised). Washington D.C.: DoD Command and Control Research Program, August 1999.

"America Prepares for Cyber War." http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/06/15/wcyber115.xml [accessed 9 April 2008].

"Analysis: DHS Stages Cyber War Exercise 10 Mar 2008," on Space War: Your World at War website. http://www.spacewar.com/reports/Analysis_DHS_stages_cyberwar_exercise_999.html [accessed 9 April 2008].

Arquilla, John. and David Ronfeldt. *Cyberwar is Coming: Comparative Strategy 12.2* (Spny 1993), pp. 141-165.

Bowie, Christopher J., Robert P. Haffa Jr, and Robert E. Mullins. "Trends in Future Warfare," *Joint Force Quarterly*, Summer, 2003. http://findarticles.com/p/articles/mi_m0KNN/is_35/ai_n8563330 [accessed 23 April 2008].

"C4ISR Strategy 2028." Draft for C4ISR OC Review Version 2.0 (24 Nov 2008).

Chuka, Neil S. "Confusion and Disagreement: The Information Operations Doctrine of the United States, The United Kingdom, Australia, Canada, and NATO." Kingston: RMC Masters Thesis, September 2007.

Cordray, Robert and Marc J. Romanych. "Mapping the Information Environment" *IO Sphere – The Professional Journal of Joint Information Operations*, Summer 2005. http://www.au.af.mil/info-ops/iosphere/iosphere_summer05_cordray.pdf [accessed 18 Feb 2009].

Department of National Defence. "A DND/CF Concept Paper and Roadmap for Network Enabled Operations," DND/CF Network Enabled Operations Working Paper, Defence R&D Canada, Technical Report DRDC TR 2006-001, January 2006. http://esquimalt.mil.ca/cfp/f3ops/F3%20CNCIOP/C4ISR%20References/NEW%20CONCEPTS/NEOps.pdf [accessed 18 March 2009].

---. "Network Enabled Operations: DND/CF Responding to the New Security Environment." NEOps Symposium Working Group, 5 November 2004.

Federman, Mark Federman. "On Reading McLuhan." http://individual.utoronto.ca/markfederman/OnReadingMcLuhan.pdf [accessed 11 March 2009].

---. "What is the Meaning of the Medium is the Message?" http://individual.utoronto.ca/markfederman/article_mediumisthemessage.htm [accessed 11 March 2009].

Groh, Jeffrey L. "Network-Centric Warfare: Leveraging the Power of Information" *US Army War College Guide to National Security Issues, Volume 1: Theory of War and Strategy*, 3rd Ed. Washington DC: US Army War College, June 2008. http://se1.isn.ch/serviceengine/FileContent?serviceID=47&fileid=8463B1AA-EA8C-D652-FD34-3450CA2B7FC5&lng=en [accessed 31 March 2009].

"Information Management Group: Policies and Directives" on ADM(IM) website. http://img.mil.ca/poldir/index_e.asp [accessed 31 March 2009].

Leiner, Barry M. "A Brief History of the Internet." http://www.isoc.org/internet/history/brief.shtml#Commercialization [accessed 27 March 2009].

Mattis, James N. "USJFCOM Commander's Guidance for Effects-based Operations," *Joint Force Quarterly*, 51 (4th Quarter 2008). http://www.dtic.mil/doctrine/jel/jfq_pubs/ [accessed 9 February 2009].

Melnick, John. "The Cyber War Against the United States" *Boston Globe*, 19 Aug 2007. http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/19/the_cyberwar_against_the_united_states/ [accessed 9 April 2008].

Romanych, Marc J."A Theory Based View of IO" in *IO Sphere – The Professional Journal of Joint Information Operations*, Spring 2005. http://www.au.af.mil/info-ops/iosphere/iosphere_spring05_romanych.pdf, [accessed 16 March 2009].

Schramm, LCol Kent. "Cyberspace: Computer Network Operations." Presentation to Integrated Concept Working Group, 25 February 2009 (Department of National Defence, Canada).

Thrasher, Roger Dean. *Information Warfare Delphi: Raw Results*. Monterey: Naval Postgraduate School, June 1996. http://all.net/books/iw/iwdelphi/index.html [accessed 26 September 2006].

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

United Kingdom. *British Defence Doctrine* JDP 0-01. Joint Doctrine Publication 0-01 (JDP-0-01) (3rd Edition), London: Ministry of Defence, August 2008.

US Department of Defense. *C4ISR Architecture Framework* Version 2. Washington D.C.: Department of Defense, 18 December 1997. http://www.afcea.org/education/courses/archfwk2.pdf [accessed 31 March 2009].

---. Command and Control Research Program website http://www.dodccrp.org/ [accessed 31 March 2000].

---. *Effect-Based Approach to Military Operations*, No 05-19. Fort Leavenworth, KS: Center for Army Lessons Learned, May 2005.

---. *Effects-based Operations White Paper* Version 1.0. Norfolk: Joint Forces Command Concepts Department J9, 2001.

---. *Information Operations Roadmap*. Washington D.C.: Department of Defense, 30 October 2003. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf [accessed 8 April 2008].

----. *Joint Communication System* (US), Joint Publication 6-0. Washington D.C.: Department of Defense, 6 March 2006.

---. *Joint Doctrine for Information Operation*, Joint Publications 3-13. Washington, D.C.: Department of Defense, 9 October 1998.

Weiss, Geoffrey F. "Exposing the Information Domain Myth: A New Concept for Air Force and Information Operations Doctrine" *Air and Space Power Journal*, Spring 2008. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj08/spr08/weiss.html [accessed 31 March 2009].

Weatherbee, T.G. *Remote Leadership*. Kingston: Canadian Defence Academy – Canadian Forces Leadership Institute, 2003.

Human Domain

Alberts, David S. "Key Concepts for Information Superiority." Presented to Office of the Assistant Secretary of Defense, United States DOD. Washington, D.C., 28 May 2001.

---. *Understanding Information Age Warfare*. Washington D.C.: Office of the Assistant Secretary of Defense, 2001.

Chery, Sandra and Philip S.E. Farrell. "A Look At Behaviourism and Perceptual Control Theory in Interface Design." Department of National Defence-Defence and Civil Institute of Environmental Medicine, 1998.

Comeau, Paul. Presentation to Centre for Operational Research and Analysis (Defence Research and Development Canada), 14 May 2008.

"Control Systems Group – Studying, Understanding, Applying Perceptual Control Theory." http://www.perceptualcontroltheory.org/ [accessed 3 November 2008].

Dahl, Arden B. "Command Dysfunction: Minding the Cognitive War." Thesis presented to the School of Advanced Airpower Studies. Alabama: Air University Maxwell AFB, June 1996, http://www.au.af.mil/au/awc/awcgate/saas/dahl_ab.pdf [accessed 27 Mar 2009].

Department of National Defence. *Cultural Intelligence, Emotional Intelligence and the Canadian Forces Leader Development Concepts, Relationships and Measures* CFLI TM 2007-01, December 2007.

Endsley, M. R. "Situation Awareness Measurement," *Human Factors*, 37 (1995), pp. 65-84.

Farrell, Philip S.E. *Control Theory Perspective of Effects Based Thinking and Operations* DRDC Ottawa TR 2007-168, November 2007.

---. "Discussion Paper: Can Perpetual Control Theory Be Applied To Organization Information Processing." Presented to the Control Systems Group (CSG) Conference 2007, University of Manchester, UK. http://www.psych-sci.manchester.ac.uk/aboutus/events/csgconference/proceedings.pdf [accessed 31 March 2009].

Hearn, Jonathan. *Rethinking Nationalism: A Critical Introduction*. New York: Palgrave Macmillan, 2006.

Heuer, Richards J. *Psychology of Intelligence Analysis*. Washington D.C.: Central Intelligence Agency, 1999 on Center for the Study of Intelligence website. https://www. cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf [accessed 27 March 2009].

Huitt, W. “The Mind” in *Educational Psychology Interactive*. Valdosta, GA: Valdosta State University, May 2001. http://chiron.valdosta.edu/whuitt/col/summary/mind.html [accessed 5 May 2009].

Nicholson, Peter. *Effects-Based Strategy: Operations in the Cognitive Domain* Volume 2 Number 1 (2006). http://www.securitychallenges.org.au/ArticlePDFs/vol2no1Nicholson.pdf [accessed 27 March 2009].

Pigeau, Ross and Carol McCann. “Analysing Command Challenges using the Command and Control Framework.” DRDC Technical Report 2003-034, 2003.

Powers, William T. *Behavior: The Control of Perception*. Chicago: Aldine Press, 1973.

---. *The Nature of PCT*. Paper presented to American Educational Research Association, San Francisco, April 1995.

Romanych, Marc. “Applying the Domains of Conflict to Information Operations.” Paper presented at 10th International Command and Control Research and Technology Symposium, JB Management, Inc., Alexandria, VA.

Triandis, H.C. “Cultural Intelligence in Organizations,” *Group and Organization Management* 31.1 (February 2006), pp. 20-26.

Other

Gray, Colin S. *Another Bloody Century – Future Warfare*. London: Phoenix, 2005.

---. “How has War Changed Since the End of the Cold War?” *Parameters,* Spring 2005.

NATO Military Agency for Standardization. *NATO Glossary of Terms and Definitions* (AAP-6). Brussels: NATO, 1998.

Pugliese, David. “Military Zeroes in on Taliban Bombers,” *Ottawa Citizen*, 20 May 2008, http://www.canada.com/ottawacitizen/news/story.html?id+32a2fe5c- 7fab-4fed-859f-d90466953618.

US Department of Defense. *Doctrine for Joint Operations 3-0*. Washington, D.C.: Joint Chiefs of Staff, 2001.

Verdon, John, LCdr Bruce C. Forrester, and Zhingang Wang. *The Last Mile of the Market: How Networks, Participation and Responsible Autonomy Support Mission Command and Transform Personnel Management.* Ottawa: DGMPRA Draft Technical Memorandum, 2009.

10 LEXICON

10.1 Terminology

The ICC defined the term *strategic environment* as "where the elements of power and influence are exercised." The ICC also advocated an expansion of the how the strategic environment is traditionally understood since the elements of power and influence can be exercised in space, cyberspace, and the cognitive, connective, and affective aspects of the human condition – as well as on land, sea, and air.

These six divisions are not called *environments* in the present work because the term *environmental command* already refers to the navy, army and air force (in Canada styled Maritime Command, Land Force Command, and Air Command respectively.) Additionally, these terms have particular organizational qualities. There is also debate as to whether or not cyberspace and human divisions of power and influence are of the same physical nature as land, maritime, air, and space. We contend that from a strategic perspective, the physicality of an environment may be only one way to identify major divisions of power and influence.

The term *domain* is defined by Webster as a "field of thought."[32] The Oxford Concise Dictionary defines domain as "sphere of control or influence."[33] Together, these definitions form the basis for using the term *domain* in the ICC to describe the expanded strategic environment as being comprised of the land, maritime, air, space, cyberspace, and human domains. These six domains form the first of the three axes of the ICC.

The six CF strategic functions (Command, Sense, Act, Sustain, Shield, and Generate) are widely understood and form the second of the three axes of the ICC.

10.2 Glossary

TERM	USAGE	ORIGIN
Act	The military use of capabilities to achieve desired effects in support of national policy.	Canada (CFD draft)[34]
Adaptive	Able to respond to change and challenges in a positive manner; includes the hallmarks of being intelligent, resilient, robust, flexible, agile, creative, responsive, and enduring.	ICC
Command	The creative and purposeful exercise of legitimate authority to accomplish the mission legally, professionally, and ethically.	Canada (CFD draft)[35]

TERM	USAGE	ORIGIN
Complexity	"Complex Systems is a new approach to science, which studies how the relationships between parts give rise to the collective behaviours of a system and how the system interacts and forms relationships with its environment."	Yaneer Bar-Yam[36]
Comprehensive	Having a complete and broad understanding of the strategic environment; having an accurate definition of the problem and having set appropriate goals; having the ability to apply a multi-disciplinary approach.	ICC
Condition Set	Conditions (circumstances) resulting from the combination of the assigned missions in CFDS and the of expectations of GoC.	ICC
Cyberspace	Refers to hardware and social interactions that occur through the virtual world.	ICC
Domain	Major divisions within the strategic environment where the elements of national power and influence are exercised: maritime, land, air, space, cyberspace, and human	ICC
Enabling Concept	Concepts that amplify methodological or technological enablers and cover a wide variety of missions, domains, and functions.	ICC
Functions	How the CF carries out its operations through Command, Act, Sense, Sustain, Shield, and Generate.	ICC
Future Security Environment	The projection of trends and shocks out into the future. Trends include economic/social, environmental/resource, geopolitical, science/technology, and military/security.	Canada (CFD)
Generate	The method by which DND and CF recruit, train, and develop personnel, procure equipment, infrastructure, and services, and all are made ready in order to meet the defence mission.	Canada (CFD draft)[37]
Integrated	Expansion of the terms joint or combined to include other actors and organizations of the GoC beyond DND.	ICC
Integrating Concept	Concepts developed by considering the collective relationships within a particular condition set.	ICC
Interoperability	The ability of systems to provide information and services to, and accept information and services from, other systems and to use the information and services so exchanged.	Canada and NATO
Networked	Relationships and interconnectivity of humans and/or technology.	ICC

TERM	USAGE	ORIGIN
Operational Art	The employment of forces to attain strategic and/or operational objectives through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles. The skill of employing military forces to attain strategic objectives in a theatre of war or theatre of operations through the design, organization, and conduct of campaigns and major operations.	Canada[38]
Operating Concept	Concepts developed to describe the requirements (based on the six functions) for a specific domain within a specific mission.	ICC
Problem Set	The combination of the three roles of the CF (defend Canada, defend North America, contribute to international peace and security) and the challenges of the future security environment.	ICC
Sense	The acquisition and processing of information to enable commanders and authorities to understand the characteristics and conditions of the operating environment pertinent to military decision-making.	Canada (CFD draft)[39]
Shield	The comprehensive approach to the protection of tangible and intangible elements through the integrating activities of detection, assessment, warning, defence (active and passive), and recovery.	Canada (CFD draft)[40]
Strategic	The level at which a nation or group of nations determine national or multinational security objectives and deploy national, including military, resources to achieve them. The strategic level is that level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic objectives and guidance and develops and uses national resources to achieve these objectives.	NATO[41] Joint Operations 3-0[42]
Strategic Environment	Where the elements of power and influence are exercised.	ICC
Sustain	The provisioning of all support services required to maintain routine and contingency operations – domestic, continental, and expeditionary – including prolonged operations.	Canada (CFD draft)[43]
Tactical	The tactical level focuses on planning and executing battles, engagements and activities to achieve military objectives assigned to tactical units or task forces (TFs).	Joint Operations 3-0[44]
Tactics	The threat or use of any kind of armed forces. An action or strategy carefully planned to achieve a specific end. The art of disposing armed forces in order of battle and of organizing operations, especially in contact with an enemy. The art of disposing naval, land, and air forces in actual contact with the enemy.	Oxford Dictionary[45] Canada[46]

11 LIST OF ACRONYMS

ACRONYM	MEANING
ASAT	Anti-Satellite
CA	Comprehensive Approach
CAS	Complex Adaptive Systems
CBSA	Canada Border Services Agency
CF	Canadian Forces
CF OPP	Canadian Forces Operational Planning Process
CFD	Chief of Force Development
CFDS	*Canada First* Defence Strategy
CFLI	Canadian Forces Leadership Institute
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DFSA	Directorate of Future Security Analysis
DIMEFIL	Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement
DND	Department of National Defence
DRDC	Defence Research and Development Canada
ICC	Integrated Capstone Concept
IED	Improvised Explosive Device
FSE	Future Security Environment
GoC	Government of Canada
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
OGD	Other Government Department
PSC	Public Safety Canada
RCMP	Royal Canadian Mounted Police
S&T	Science and Technology
WMD	Weapons of Mass Destruction

12 ENDNOTES

1 Department of National Defence, *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations* (Kingston: Canadian Force Leadership Institute, 2008). The personnel interviewed were from a diverse background and represented Canadian and foreign military and civilian personnel with extensive experience on operations over the past 15 years at all levels – tactical, operational, strategic, and politico-strategic.

2 *Broadsword or Rapier*, p. 21.

3 Department of National Defence, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends* (Ottawa: Chief of Force Development, 2009), p. 91.

4 Francis Heylighen, "Complexity and Self-Organization" entry for *Encyclopaedia of Library and Information Sciences* (Taylor and Francis, 2008), pp. 1-2, http://pespmc1.vub.ac.be/Papers/ELIS-Complexity.pdf.

5 Dana Mackenzie, "The Science of Surprise: Can Complexity Theory Help Us Understand the Real Consequences of a Convoluted Event Like September 11?" in *Discover* (February 2002), http://discovermaganize.com/2002/feb/featsurprise.

6 Heylighen, "Complexity and Self-Organization," p. 1.

7 Heylighen, "Complexity and Self-Organization," p. 4.

8 Heylighen, "Complexity and Self-Organization," pp. 1, 4.

9 Heylighen, "Complexity and Self-Organization," pp. 1, 6, 10.

10 Heylighen, "Complexity and Self-Organization," p. 8.

11 Heylighen, "Complexity and Self-Organization," p. 9.

12 Heylighen, "Complexity and Self-Organization," p. 16.

13 Interdependence is part of the study of complex systems that helps us recognize and understand indirect effects. Yaneer Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World* (Cambridge, MA: NECSI/Knowledge Press, 2004), pp. 27-29.

14 *Future Security Environment*, pp. 5-9.

15 Government of Canada, *Canada First* Defence Strategy (Ottawa: Department of National Defence, 2008), p. 7.

16 Comprehensiveness is not to be confused with the "Comprehensive Approach" (CA); CA relates to another concept being co-developed amongst government agencies (not yet published).

17 Paul Comeau, presentation discussion on 14 May 2008.

18 The list of national elements of power has been expanded in some circles to include DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement.

19 Jonathan Hearn, *Rethinking Nationalism: A Critical Introduction* (New York: Palgrave Macmillan, 2006), pp. 230, 231, 232.

20 Dietrich Dorner, *The Logic of Failure, Recognizing and Avoiding Error in Complex Situations*. Translated by Rita and Robert Kimber (New York: Metropolitan Books, 1996). pp. 49-70.

21 There have been some arguments that suggest that other capabilities can be included as an element of national power such as "information" and "legal." In fact, an expansion to seven elements of national power has been suggested: DIMEFIL (diplomacy, information, military, economic, financial, intelligence, law enforcement).

22 The ten elements of critical infrastructure are Energy and Utilities; Communications and Information Technology; Finance; Healthcare; Food; Water; Transportation; Safety; Government and Manufacturing.

23 Space Law is a component of International Law, which is based upon treaties; this means they are not considered law until ratified by the 200 member states of the United Nations.

24 On 13 September 1985, the first and only destruction of a satellite by an American air-launched missile occurred when an F-15A launched an *ASAT* against the solar observatory satellite "P78-1" in a 600 km (375 mile) orbit. On 11 January 2007, the Chinese government destroyed one of its own satellites 537 miles in space using a ground-based medium range ballistic missile system. On 20 February 2008, the US shot an SM-3 missile from the USS Lake Erie to destroy a defunct US National Reconnaissance satellite at 133 nautical miles over the Pacific Ocean.

25 The challenges of operating in space are far different than the challenges of operating in the air environment. For example, space is extremely hostile to human habitation. Space flight is not, in fact, flight but rather ballistic in nature: a satellite's path is governed by orbital mechanics. The rotation of the earth, coupled with a predictable flight path, means that any space activity anywhere can affect any country. Space vehicles must be designed to endure the harsh conditions of space for a considerable period without repair or replenishment of consumables.

26 The working definition of Cyberspace provided by ADM(IM) J6 is "A global domain within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers." LCol Kent Schramm, "Cyberspace: Computer Network Operations" Integrated Concept Working Group, 25 Feb 2009. Information Environment is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." Additional explanation is that the information environment is made

up of three interrelated dimensions: physical, informational, and cognitive. Government of United States of America, Joint Information Operations (US) Joint Publication 3-13 Glossary (Washington: Department of Defense).

27 W. Huitt, "The Mind," *Educational Psychology Interactive*. (Valdosta, GA: Valdosta State University, May 2001) at http://chiron.valdosta.edu/whuitt/col/summary/mind.html [accessed 5 May 2009].

28 Perceptual bias includes: expectation, resistance to change, impact of ambiguity, centralized direction. Cognitive bias includes: evaluation of probability, attribution of causality, evaluation of evidence. Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington: Center for the Study of Intelligence, Central Intelligence Agency 1999).

29 Directorate of Future Security Analysis (DFSA), "Capability Domain Concept: Command," CFD Concept Paper, 29 February 2008; DFSA, Capability Domain Concept: Sense," CFD Concept Paper, 15 April 2008; DFSA, "Capability Domain Concept: Act," CFD Concept Paper, 27 May 2008; DFSA, "Capability Domain Concept: Sustain," CFD Concept Paper, 30 November 2008; DFSA, "Capability Domain Concept: Shield," CFD Concept Paper, 17 April 2008; DFSA, "Capability Domain Concept: Generate," CFD Concept Paper, 23 January 2009.

30 Ross Pigeau and Carol McCann, "Analysing Command Challenges using the Command and Control Framework." DRDC Technical Report 2003-034, 2003.

31 See Hallmarks of Adaptation, p. 15.

32 "Domain." *Webster's English Dictionary Concise Edition*. Toronto: Strathearn Books Limited, 2005, p. 84.

33 "Domain." *Oxford Concise Dictionary*, 8th edition. Oxford: Oxford University Press, 1990, p. 347.

34 DFSA, "Capability Domain Concept: Act," CFD Concept Paper, 27 May 2008.

35 DFSA, "Capability Domain Concept: Command," CFD Concept Paper, 29 February 2008.

36 Bar-Yam, *Making Things Work*, p. 24.

37 DFSA, "Capability Domain Concept: Generate," CFD Concept Paper, 23 January 2009.

38 Defence Terminology Bank.

39 DFSA, "Capability Domain Concept: Sense," CFD Concept Paper, 15 April 2008.

40 DFSA, "Capability Domain Concept: Shield," CFD Concept Paper, 17 April 2008.

41 AAP-6.

42 Government of United States of America, *Doctrine for Joint Operations 3-0*, (Washington, D.C.: Joint Chiefs of Staff, 2001).

43 DFSA, "Capability Domain Concept: Sustain," CFD Concept Paper, 30 November 2008.

44 *Joint Operations 3.0*, Chapter 2, Section 2, Levels of War.

45 *Concise Oxford Dictionary.*

46 Government of Canada, *DND/CF Manual of Abbreviations* (Ottawa: Chief of the Land Staff).

CHIEF OF FORCE DEVELOPMENT
CHEF DU DÉVELOPPEMENT DES FORCES

A-FD-005-002/AF-001