23 OCTOBRE 2009

Concept cadre intégré

Défense nationale National Defence

Canada

Concept cadre intégré

Chef du Développement des forces
Quartier général de la Défense nationale
101 Colonel By Drive
Ottawa (Ontario) K1A 0K2

Réalisé pour le Chef du Développement des forces
par le Bureau de publications de la 17e Escadre
WPO30558

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

Catalogage avant publication de Bibliothèque et Archives Canada

Concept cadre intégré.

Produit pour le Chef du développement des Forces par le Bureau de publications de la 17e Escadre.
Publ. aussi en anglais sous le titre : Integrated capstone concept.
Également disponible sur l'Internet.
Comprend des réf. bibliogr.
ISBN 978-1-100-95251-2
No de cat.: D2-265/2010F

1. Canada--Politique militaire. 2. Canada. Forces armées canadiennes. 3. Sécurité nationale--Canada.
I. Canada. Forces armées canadiennes. Escadre, 17e II. Canada. Chef du développement des Forces

UA600 I6214 2010 355'.033571 C2010-980201-2

Imprimé au Canada

1 3 5 7 9 10 8 6 4 2

AVANT-PROPOS

J'ai le plaisir de présenter le *Concept cadre intégré* (CCI) au ministère de la Défense nationale (MDN) et aux Forces canadiennes (FC) à titre de référence générale. Le présent document a pour objet de fournir à l'institution de la Défense un concept général, grâce à un ensemble de concepts opérationnels, intégrants et habilitants, qui préparera les FC à affronter les défis du contexte de sécurité futur. Il servira au développement des forces intégrées des FC et constituera une ressource pour l'évaluation des besoins en matière de perfectionnement professionnel des FC et des autres besoins du Ministère.

Comprendre les implications que la complexité du concept entraîne est essentiel à la réussite stratégique des FC. Il est également fondamental de comprendre la nature changeante de nos adversaires, les domaines dans lesquels nous agissons et les types d'opérations que les FC devront mener. Afin de relever ces défis, nous devrons former une force militaire intégrée, polyvalente et apte au combat qui devra être globale, intégrée, adaptative et réseautée en vue de réaliser l'intention du pays.

Les organisations responsables du développement de la force utiliseront le *Concept cadre intégré* qui leur servira de guide pour le développement des capacités intégrées dans toutes les fonctions des FC en vue de l'élargissement du nouvel environnement stratégique. On recommande également vivement aux commandements d'armée d'utiliser ce document comme point de départ pour l'élaboration et le développement des concepts et des capacités.

Les idées du CCI ont déjà donné naissance à l'élaboration du concept au sein des différentes organisations et ont généré des commentaires pour la prochaine version du CCI. La nouvelle version doit :

1. Inclure une « dimension » humaine afin de remplacer le domaine humain;
2. Clarifier l'intention, la présentation et l'explication de la conception du CCI;
3. Améliorer la description des concepts sur la fonction stratégique;
4. Approfondir les idées clés entendues par global, adaptatif, intégré et réseauté.

J'encourage tous les membres de l'équipe de la Défense à utiliser ce document pour maintenir un niveau élevé de connaissance au sujet du concept cadre et de ses incidences éventuelles sur notre capacité à rester pertinents sur le plan stratégique, réactifs sur le plan opérationnel et efficaces d'un point de vue tactique dans les années à venir.

Major-général S.A. Beare
Chef du Développement des forces

REMERCIEMENTS

Le Chef du Développement des forces (CDF) souhaite remercier toutes les organisations du niveau 1 du QGDN pour leur soutien et leur contribution ainsi que tous les intervenants du milieu du développement du concept pour leur importante participation au groupe de travail sur le concept intégré (GTCI).

Nous souhaitons remercier les membres du personnel suivants pour leur participation :

Bgén MD Kampman
Bgén P Matte
Col JK Tattersall
Capf KPL Hansen
Capf HJ Henderson
Capf NT Leak
Capf 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
Capc DJ Harnett
Capc JJ MacDonald
Capc MD McKinley
Capc PR Moller
Capc 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
Adjum CC Deroche
Adjum 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 DES MATIÈRES

LISTE DES FIGURES

1 INTRODUCTION

1.1 Défi

Le ministère de la Défense nationale (MDN) et les Forces canadiennes (FC) sont confrontés à de nombreux défis, tels que le vieillissement de la population, l'émergence d'acteurs non étatiques, l'accès à des technologies perturbatrices en raison de la mondialisation, etc. Conjointement, ces défis donnent lieu à une complexité accrue dans le contexte de sécurité moderne.

Les critiques diront que la complexité du contexte de sécurité a toujours existé et, d'une certaine façon, ils ont raison. Ce qui change, ce sont les différents niveaux de complexité qui caractérisent l'environnement de la sécurité et les interactions des systèmes complexes en jeu. Depuis le milieu des années 1970, l'étude de la complexité en tant que science a fait beaucoup de progrès dans le traitement des questions complexes. Le *Concept cadre intégré* (CCI) prétend que la complexité de l'environnement de la sécurité s'intensifiera en même temps que l'ampleur et la nature des stimuli stratégiques déterminant nos intérêts nationaux. C'est pourquoi, afin de rester pertinentes sur le plan stratégique, réactives sur le plan opérationnel et décisives du point de vue tactique dans le contexte de sécurité futur, les FC doivent relever les défis posés par la complexité accrue.

Une analyse des tendances actuelles et futures montre que la complexité accrue sera au cœur de la presque totalité des opérations. Le document *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations* examine les défis auxquels le personnel militaire fait face au cours des opérations actuelles. Grâce à un processus d'entrevue avec bon nombre de militaires[1] ayant différentes expériences et connaissances, l'équipe de projet de l'Institut de leadership des Forces canadiennes relève que la plupart des personnes interrogées « ont décrit avec exactitude un environnement opérationnel présentant un degré de complexité et d'imprévisibilité élevé »[2]. Les conclusions du document *Broadsword or Rapier*? montrent l'urgence du défi actuel. Si la complexité accrue est importante dans nos opérations actuelles, que nous réserve l'avenir?

Si la complexité accrue est importante dans nos opérations actuelles, que nous réserve l'avenir?

Le document *L'environnement de la sécurité future 2008-2030 : Tendances actuelles et émergentes* (ci-après nommé ESA) examine un large éventail de tendances

qui auront des répercussions sur les opérations du MDN/des FC. De manière plus précise, l'ESA examine les tendances économiques et sociales, les tendances relatives à l'environnement et aux ressources, les tendances géopolitiques, scientifiques et technologiques, et les tendances sur le plan militaire et de la sécurité; il conclut que le contexte de sécurité futur suivra indubitablement la tendance actuelle qui sera de plus en plus complexe[3]. C'est pourquoi, nous devrons connaître les répercussions de ce paradigme et déterminer comment agir dans cet environnement de la sécurité dynamique.

APERÇU 1

L'ENVIRONNEMENT STRATÉGIQUE A TOUJOURS ÉTÉ DOMINÉ PAR DES QUESTIONS DE COMPLEXITÉ. CEPENDANT, LE NOMBRE DE FACTEURS ET DE DÉFIS PRÉSENTS DANS LE CONTEXTE DE SÉCURITÉ FUTUR AUGMENTERA SENSIBLEMENT LES NIVEAUX DE COMPLEXITÉ.

1.2 Objectif

L'objectif du présent document est de décrire les considérations pertinentes sur le plan stratégique pour les Forces canadiennes dans le contexte de sécurité futur et de présenter la conception du cadre en vue du développement des capacités. La thèse principale est qu'avec un environnement de sécurité de plus en plus complexe, il faut mettre en place des approches globales, intégrées, adaptatives et réseautées en vue de réaliser l'intention du pays. Ces facteurs doivent devenir les principes régissant la nature des FC de l'avenir et du besoin d'être pertinentes sur le plan stratégique, réactives sur le plan opérationnel et décisives du point de vue tactique.

Étant donné la complexité grandissante de l'environnement de sécurité, il faut mettre en place des approches globales, intégrées, adaptatives et réseautées en vue de réaliser l'intention du pays.

Le CCI vise à :

- décrire les considérations pertinentes sur le plan stratégique pour le MDN/les FC;
- déterminer quatre attributs nécessaires (global, intégré, adaptatif, réseauté) que les concepts, les approches et le développement des capacités des FC de l'avenir doivent intégrer;
- approfondir la connaissance de l'environnement stratégique et des domaines terrestre, maritime, aérien, spatial, virtuel et humain;

- présenter la conception du cadre comme un outil d'aide en vue du développement du concept, des capacités et de la force pour le MDN/les FC.

1.3 Hypothèses

- Les trois objectifs persistants des FC tels qu'ils sont décrits dans la Stratégie de défense *Le Canada d'abord* (SDCA) demeureront inchangés : défendre le Canada et les Canadiens, défendre l'Amérique du Nord et contribuer à la paix et la sécurité à l'échelle internationale.
- Le Canada demeurera un allié stratégique des États-Unis et conservera un ensemble de partenariats multilatéraux en matière de sécurité.
- Le MDN et les FC continueront de servir les Canadiens, le gouvernement du Canada (GC) et les alliés du Canada et demeureront ainsi un instrument de puissance nationale.
- Le biais organisationnel, l'esprit de clocher et l'inertie institutionnelle constitueront toujours des obstacles à la transformation.

1.4 Contraintes

- Le potentiel militaire continuera de dépendre des niveaux de financement du gouvernement.
- Les opérations des FC continueront d'être dirigées conformément à la législation et aux directives du GC, aux principes régissant la profession des armes au Canada et aux attentes des Canadiens.
- La tolérance à l'égard des dommages collatéraux sera de moins en moins grande, imposant ainsi une plus grande précision et des défis de plus grande envergure en matière d'adaptabilité, de perspective globale et d'intégration.

1.5 Faits saillants de chaque section

La section 2 examine la théorie de la complexité et comment elle peut s'appliquer à l'étude du contexte de sécurité. Les tendances décrites dans l'ESA sont examinées et comparées avec la réalité stratégique d'aujourd'hui afin de formuler des hypothèses sur la réalité stratégique de l'avenir.

La section 3 propose une discussion concise sur l'importance d'adopter une approche globale, intégrée, adaptative et réseautée dans le contexte de sécurité complexe.

La section 4 aborde la nature des conflits futurs et propose un modèle afin de représenter l'application des éléments de puissance nationale dans un environnement stratégique complexe. La section examine également les missions de la SDCA en fonction des conditions dans le *Concept cadre intégré*.

La section 5 donne un aperçu de l'environnement stratégique futur. Elle préconise l'agrandissement de l'environnement stratégique afin d'y intégrer trois nouveaux domaines : spatial, virtuel et humain. La description du domaine humain comprend une discussion sur la façon dont la technologie et la mondialisation a permis à des éléments antagonistes (États et acteurs non étatiques) d'avoir accès à des instruments de puissance nationale et d'avoir une influence qu'il était auparavant impossible d'obtenir.

La section 6 examine les fonctions de commandement, de détection, d'action, de protection, de maintien en puissance et de mise sur pied des FC par rapport aux attributs visés : global, adaptatif, intégré et réseauté.

La section 7 présente la conception du cadre et en décrit l'objectif. Elle regroupe les renseignements des sections précédentes et examine d'un point de vue stratégique les relations entre les conditions, les domaines et les fonctions. Elle propose également une discussion sur l'utilisation de la conception du cadre comme un outil en vue du développement des capacités et de l'élaboration du concept.

La section 8 énonce les éléments stratégiques et les répercussions pour le MDN et les FC à la lumière de la thèse centrale selon laquelle l'environnement de sécurité de plus en plus complexe exige l'élaboration d'approches globales, intégrées, adaptatives et réseautées en vue de l'exécution de l'intention du pays.

RÉPERCUSSIONS STRATÉGIQUES

Les défis imposés par l'environnement de sécurité complexe de l'avenir exigent l'élaboration d'approches globales, intégrées, adaptatives et réseautées Ces attributs doivent ainsi devenir les principes régissant la nature des FC de l'avenir et la nécessité d'être pertinent sur le plan stratégique, réactif sur le plan opérationnel et décisif d'un point de vue tactique.

2 COMPLEXITÉ, LE CONTEXTE DE SÉCURITÉ FUTUR ET LA RÉALITÉ STRATÉGIQUE CANADIENNE

La présente section du CCI examine la théorie de la complexité et comment elle peut s'appliquer à l'étude du contexte de sécurité. Les tendances décrites dans l'ESA sont examinées et comparées avec la réalité stratégique d'aujourd'hui afin de formuler des hypothèses sur la réalité stratégique de l'avenir.

2.1 Complexité

La communauté internationale et les interconnexions entre les différentes sous communautés constituent manifestement un système complexe. Par conséquent, le CCI appuie le fait que l'étude sur la théorie de la complexité est fondamentale en vue de préparer le MDN/les FC aux défis qui les attendent lors des opérations dans l'environnement de sécurité complexe de l'avenir. Si on devait placer le terme « complexité », on le glisserait « entre les termes ordre et désordre »[4]. On associe également la complexité à « la science de la surprise »[5], élément qui à lui seul devrait recevoir l'attention du milieu militaire.

« Les systèmes complexes forment une nouvelle approche en matière de science qui étudie la façon dont les relations entre les composants créent des comportements collectifs dans un système et la façon dont les éléments du système interagissent et créent des liens avec leur environnement. »

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

Cette science étudie les systèmes complexes, leurs caractéristiques, leurs propriétés et leurs comportements. Un système complexe est une agrégation de composants en interaction[6]. Ces systèmes ne sont ni rigides ni fluides; il s'agit en réalité d'un enchevêtrement et d'une combinaison de comportements réguliers, prévisibles, aléatoires et chaotiques. Les composants qui constituent le système complexe sont connectés par l'intermédiaire d'interactions; les sous-systèmes sont simultanément autonomes et mutuellement dépendants. Des modèles de systèmes complexes considèrent les composants constituants comme des agents : « systèmes individuels qui agissent sur leur environnement à la suite d'événements dont ils font l'expérience ». On sous-entend ainsi que les agents sont motivés par un but et agissent de façon à tirer le maximum d'avantages. Les actions des agents ont un effet sur l'environnement, qui à son tour influence les actions d'autres agents.

Même si les interactions commencent localement, elles peuvent finalement entraîner des conséquences à l'échelle mondiale[7].

Les interactions des systèmes complexes sont rarement linéaires : il n'existe aucune relation directe de cause à effet proportionnelle et prévisible[8]. Cependant, les systèmes complexes ont tendance à s'auto-organiser : « un ensemble d'interactions locales permet de créer une coordination générale » et cette structure constitue ce qu'on appelle un réseau[9]. Les agents dans les systèmes complexes évoluent conjointement et s'adaptent en fonction des actions et des réactions des autres agents, mais en étant toujours à la poursuite d'une situation avantageuse ou stable[10]. Les propriétés des systèmes complexes ne peuvent pas être déduites en déterminant les propriétés de chaque composant. L'ensemble du système possède des propriétés émergentes qui proviennent de « motifs d'interactions ou de connexions entre chaque (composant) »[11]. Étant donné que des interactions non linéaires se produisent en permanence entre les agents dans les systèmes complexes, il est normal que ces systèmes soient imprévisibles et incontrôlables par nature et ils « ne pourront jamais être représentés sous la forme d'un modèle précis et déterministe »[12]. La connexion entre les composants peut créer des profils ou favoriser l'auto-organisation. Il s'agit des propriétés émergentes des systèmes adaptatifs. Les propriétés émergentes peuvent créer de nouvelles organisations ou les dissoudre, et peuvent être à l'origine de nouveaux comportements à un niveau local ou dans l'ensemble du système. Toute action dans les systèmes complexes adaptatifs peut également entraîner des effets secondaires non désirés[13].

Étant donné que l'environnement de la sécurité et des opérations est constitué d'une multitude de systèmes complexes, comprendre la théorie des systèmes complexes (au meilleur de nos capacités) est essentiel à la réussite stratégique du MDN/des FC dans l'environnement de sécurité de l'avenir. L'étude de la théorie de la complexité est également fondamentale pour que l'on soit conscient du nombre d'agents affectant la sécurité nationale et internationale, de la nature changeante de nos adversaires, des conséquences des interactions des différents groupes, de la nature imprévisible et non linéaire des actions et des comportements, des domaines dans lesquels nous agissons et du type d'opérations que les FC devront exécuter. Les outils linéaires existants et les concepts hérités que nous utilisons afin de résoudre les problèmes ne seraient peut-être pas adaptés aux défis imposés par les systèmes complexes futurs. Il serait peut-être plus approprié d'utiliser le processus de planification opérationnelle (PPO) afin d'intégrer des outils tels que la méthodologie douce des systèmes ou le génie technique évolutif de pointe en vue de traiter les problèmes complexes.

APERÇU 2

COMPRENDRE LES CONSÉQUENCES QUE LES SYSTÈMES COMPLEXES REPRÉSENTERONT DANS LE CONTEXTE DE SÉCURITÉ FUTUR EST ESSENTIEL À LA RÉUSSITE STRATÉGIQUE DES FC. L'ENVIRONNEMENT DE SÉCURITÉ DE L'AVENIR SERA INFLUENCÉ PAR UNE GAMME DE PLUS EN PLUS LARGE DE SYSTÈMES COMPLEXES DYNAMIQUES ET ADAPTATIFS.

2.2 L'environnement de la sécurité future

Le document ESA examine un ensemble de tendances qui auront des répercussions sur nos éventuelles opérations futures et qui les influenceront. Il expose les grandes lignes sur les tendances en étudiant les facteurs économiques, sociaux, environnementaux, géopolitiques, scientifiques, technologiques et militaires, ainsi que les facteurs liés aux ressources et à la sécurité. Il propose des hypothèses sur l'évolution de l'environnement stratégique d'ici 2030.

La mondialisation est une tendance prédominante ayant des répercussions sur le contexte de sécurité futur. La prolifération de nouvelles technologies facilite et permet l'élaboration de moyens créatifs et dynamiques permettant aux personnes et aux systèmes d'interagir. Ces interactions créent une interdépendance et des connexions et sont à la base de la complexité de l'environnement de sécurité de l'avenir.

Une grande partie des tendances décrites dans l'ESA pourraient être à l'origine d'effets indirects et donner lieu à des conflits[14]. Les tendances sociales et économiques peuvent créer des tensions et aggraver des hostilités et des problèmes existants dans des régions où règnent déjà un malaise, des inégalités ou le désespoir. De manière similaire, l'inégalité économique, le surpeuplement, les migrations, l'urbanisation, les maladies, la pauvreté et l'extrémisme peuvent tous produire des effets déstabilisants.

Les tendances de la population mondiale favorisent l'instabilité et les conflits. Les tendances liées à l'urbanisation dans les mégapoles augmentent la probabilité de désaccord et poussent des groupes autrefois disparates à interagir pour la défense d'intérêts communs. Il en est de même pour le partage des ressources stratégiques et des questions pandémiques et de santé évidentes découlant de l'urbanisation. Le changement climatique et la concurrence liée à l'acquisition de ressources sont également à l'origine d'autres désaccords et de mouvements de population.

La mondialisation, ou plus particulièrement l'interconnectivité et l'accès rendu possible grâce à la mondialisation, dotent un large ensemble d'acteurs de capacités qui

étaient auparavant réservées à des pays développés. L'accès général à la science et aux technologies (telles que les technologies spatiales et virtuelles et les technologies perturbatrices avancées) permet au plus rapide et au plus apte à acquérir et à exploiter ces nouvelles capacités d'obtenir l'avantage militaire, augmentant ainsi les capacités des acteurs non étatiques antagonistes à des niveaux qui rivalisent avec ceux des États. Ces tendances entraînent de graves conséquences pour la défense et la sécurité en matière de réalité stratégique au Canada.

APERÇU 3

L'ENVIRONNEMENT STRATÉGIQUE DYNAMIQUE ET COMPLEXE SERA DANS L'AVENIR INFLUENCÉ PAR UNE GAMME GRANDISSANTE D'ACTEURS TECHNOLOGIQUEMENT ET SOCIALEMENT HABILITÉS QUI SERONT MIEUX COORDONNÉS ET DE PLUS EN PLUS RÉSEAUTÉS, ET QUI AURONT LA MÊME INTENTION QUE L'ANTAGONISTE.

2.3 La réalité stratégique canadienne

La Stratégie de défense *Le Canada d'abord* (SDCA) décrit trois objectifs durables pour les Forces canadiennes[15] :

1) Défendre le Canada – Servir avec excellence au pays.
2) Défendre l'Amérique du Nord – Un partenaire solide et fiable.
3) Contribuer à la paix et à la sécurité à l'échelle internationale – Faire preuve de leadership à l'étranger.

La comparaison entre les tendances de l'ESA et les objectifs des FC annonce de manière évidente une activité future des FC particulièrement dynamique au pays et à l'étranger. Les antagonistes non étatiques, utilisant des technologies modernes et bénéficiant d'un financement provenant d'éventuelles activités criminelles, resteront sans doute un problème. Les conflits entre les États demeureront une réalité; cependant, ces conflits prennent de plus en plus d'ampleur.

La mondialisation continuera d'avoir un effet sur les relations intra-étatiques et de nouvelles interdépendances apparaîtront dans un contexte stratégique plus large.

FIGURE 1 : MISSIONS DE LA SDCA.

FIGURE 2 : IMPACT D'UN AVENIR INCERTAIN SUR LES MISSIONS DE LA SDCA.

L'environnement de la sécurité, tel que décrit dans l'ESA, sera en permanence dynamique et incertain. Cependant, les trois objectifs des FC (défendre le Canada, défendre l'Amérique du Nord, contribuer à la paix et la sécurité à l'échelle internationale) devraient demeurer inchangés. Les équipes des FC devront remplir ces objectifs dans le contexte de sécurité élargi et chaque objectif est régi par la nécessité d'être global, intégré, adaptatif et réseauté. La combinaison de ces objectifs et le contexte de sécurité forme ce qu'on désignera comme la *problématique*.

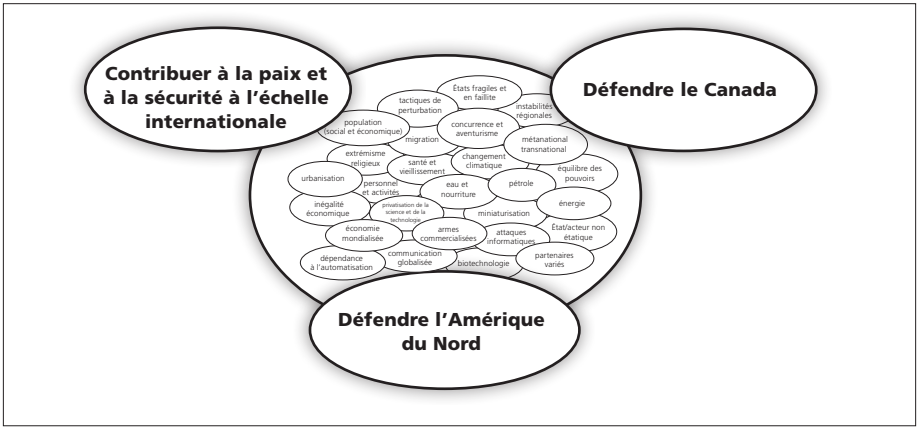

FIGURE 3 : INTERDÉPENDANCE DES OBJECTIFS DES FC ET DU CONTEXTE DE SÉCURITÉ FUTUR.

Les conditions entourant les missions de la SDCA et les attentes du GC auront la même importance. La combinaison de chaque mission de la SDCA et les attentes du GC sont référencées en tant que *conditions*. Chaque condition établie devra être pertinente sur le plan stratégique, réactive sur le plan opérationnel et efficace d'un point de vue tactique.

Avec l'objectif de permettre aux FC d'opérer avec succès dans la problématique, le CCI expliquera la relation entre la nature du conflit futur, l'environnement stratégique et les fonctions découlant des conditions. La réussite dans le contexte de sécurité futur exige l'élaboration d'approches globales, intégrées, adaptatives et réseautées.

RÉPERCUSSIONS STRATÉGIQUES

Il est essentiel de comprendre le nombre grandissant d'agents affectant la sécurité à l'échelle nationale et internationale, la nature changeante de nos adversaires, les conséquences des interactions des différents groupes, la nature imprévisible et non linéaire des actions et des comportements, les domaines dans lesquels nous mènerons nos opérations et les types d'opérations que les FC devront mener.

Les outils linéaires existants et les concepts hérités que nous utilisons afin de résoudre les problèmes ne seraient peut-être pas adaptés aux défis imposés par les systèmes complexes futurs.

L'accès général à la science et aux technologies (tel que les technologies spatiales et virtuelles et les technologies perturbatrices avancées) permet au plus rapide et au plus apte à acquérir et à exploiter ces nouvelles capacités d'obtenir l'avantage militaire, augmentant ainsi les capacités des antagonistes non étatiques à des niveaux qui rivalisent ceux des États.

3 LA NOUVELLE APPROCHE ET LES FC DE L'AVENIR

Cette section propose une discussion concise sur l'importance d'adopter une approche globale, intégrée, adaptative et réseautée dans l'environnement de sécurité complexe.

Il existe des méthodes aidant la direction des FC dans l'élaboration d'un meilleur cadre, qui nous incite à utiliser l'ensemble de nos capacités face à un défi complexe. Afin de bien comprendre la thèse, l'idée de complexité externe et interne doit être clairement comprise.

« L'environnement externe d'une organisation peut varier en passant d'un état stable à un état dynamique et complexe. Si la complexité de l'environnement devient supérieure à la complexité interne de l'organisation, les risques d'échec seront plus élevés sauf si l'organisation augmente suffisamment sa complexité interne afin d'intervenir efficacement face aux exigences de l'environnement. »

John Verdon *et al.*, *The Last Mile of the Market*, p. 54.

Notre capacité à réagir face aux problèmes de complexité externe dépend totalement de notre capacité à résoudre nos problèmes de complexité institutionnelle interne. Tout au long de la transformation des FC, nous gérons l'incertitude et nous optimisons la capacité totale de tous les composants du MDN de manière intégrée. Cependant, les institutions de la défense peuvent améliorer leur rendement dans les environnements complexes en résolvant également les questions de complexité internes par des interventions globales, intégrées, adaptatives et réseautées. Les cloisonnements actuels ne seraient peut-être pas la solution la plus adaptée.

3.1 Global

Le terme « global » comprend trois aspects différents :

- Une parfaite compréhension de l'environnement stratégique;
- Une définition précise du ou des problèmes et des objectifs adaptés;
- Une capacité à appliquer une approche pluridisciplinaire.

Le terme « global » doit décrire l'environnement stratégique dans son ensemble incluant tous les domaines envisagés. Il faut porter une attention particulière aux aspects physiques tels que la température, le terrain et le lieu. Cependant, il est d'autant plus important de prendre en compte les aspects humains tels que les systèmes culturels, politiques et de croyance sociale afin de comprendre l'espace d'opération. De plus, si l'adversaire peut agir à l'extérieur des domaines traditionnels (maritime, terrestre et aérien), les FC doivent alors être prêtes elles aussi à assumer leurs fonctions. C'est en tenant compte de tous ces aspects qu'il sera possible de bien comprendre l'environnement stratégique.

Deuxièmement, afin de comprendre ce que le terme « global » implique, il faut savoir définir les problèmes et les objectifs. Certains aspects de la problématique ne sont pas toujours évidents et, par conséquent, la problématique doit sans cesse être redéfinie. Il se peut que les objectifs ne soient pas toujours réalisables et aient été, au départ, minorés ou mal définis. Toutes les actions en vue de réaliser les objectifs doivent être sans arrêt contrôlées et, au besoin, les chefs et les planificateurs doivent examiner à nouveau les problèmes, les objectifs et des démarches. En raison de la nature imprévisible de la problématique, les systèmes d'aide à la prise de décision et les processus de planification opérationnelle ne peuvent pas être linéaires.

En raison de la nature imprévisible du problème, les systèmes d'aide à la prise de décision et les processus de planification opérationnelle ne peuvent pas être linéaires.

Enfin, cette perspective globale[16] doit constituer en une approche pluridisciplinaire afin de relever les défis envisagés dans le document ESA qui dépassent de loin la portée et les capacités des FC seules. Les FC constituent l'un des instruments de puissance nationale et d'influence à la disposition du GC. De plus, des organismes non gouvernementaux peuvent travailler simultanément au sein de l'espace complexe afin de résoudre d'autres problèmes liés à une crise et peuvent ou non avoir les mêmes objectifs que le GC. Afin de résoudre ou gérer au mieux des situations complexes, il faut élaborer un cadre global.

Le MDN et les FC doivent connaître parfaitement l'environnement stratégique commun, afin d'établir et de modifier les objectifs en faisant en sorte qu'ils soient adaptés et pertinents en vue de réaliser l'intention stratégique du GC et de travailler dans un cadre d'équipe pluridisciplinaire.

APERÇU 4

CETTE PERSPECTIVE GLOBALE DOIT CONSTITUER EN UNE APPROCHE PLURI-DISCIPLINAIRE AFIN DE RELEVER LES DÉFIS ENVISAGÉS DANS LE DOCUMENT ESA QUI DÉPASSENT DE LOIN LA PORTÉE ET LES CAPACITÉS DES FC SEULES.

3.2 Intégré

Le terme « intégré » est normalement utilisé afin d'étendre la signification des termes « interarmées » et « interalliés » afin d'intégrer d'autres acteurs et organisations dans l'approche pangouvernementale. Dans le CCI, le terme renferme trois significations distinctes :

- La coordination des efforts entre le MDN et les FC, et à l'intérieur de ces organisations, pour le développement de la force, la mise sur pied de la force et l'emploi de la force.
- La collaboration d'au moins deux organisations différentes.
- Le niveau d'interopérabilité.

La première définition du terme « intégration » concerne le MDN et les FC. Afin de résoudre les problèmes ayant trait au développement de la force, à la mise sur pied de la force et à l'emploi de la force dans le cadre du soutien à la politique nationale, le MDN et les FC doivent endosser le rôle de développeur et de responsable de la mise sur pied de la force, de telle sorte que les FC puissent assumer leur rôle d'utilisateur de la force. Il ne s'agit pas d'intégration organisationnelle; il s'agit plutôt d'intégrer les effets nécessaires permettant d'atteindre des états de disponibilité équilibrés et gérés. Intégrer les efforts du MDN et des FC est un processus clé qui permettra à l'ensemble de l'institution de la Défense de surmonter l'inertie existante et l'esprit de clocher organisationnel.

La seconde définition du terme « intégration » va au-delà des définitions données aux termes militaires « interarmées » et « interalliés ». Le terme décrit les relations entre le MDN/les FC et les organisations externes, telles que les ministères gouvernementaux et les alliés. Cette intégration permet d'appliquer une approche pluridisciplinaire dans le cadre des situations complexes. Les relations les plus importantes pour le MDN/les FC sont celles entretenues avec les autres ministères du gouvernement concernant la sécurité et la souveraineté du Canada. Parmi les acteurs transitoires, on

trouve les organisations non gouvernementales, les entreprises de haute technologie et les entrepreneurs militaires privés. L'équipe ou la force est intégrée durant la durée nécessaire à la réalisation de l'objectif; la question dominante concernant tous les partenaires intégrés est de travailler en vue d'atteindre un objectif commun. On présume que le MDN/les FC font toujours partie d'une équipe intégrée ou d'une force intégrée. Cependant, il ne faut pas absolument être intégré d'un point de vue organisationnel afin de produire des effets intégrés.

La troisième définition se rapporte au niveau d'interopérabilité entre les organisations concernées nécessaire en vue d'atteindre un objectif. Le niveau d'interopérabilité (ou d'intégration), ou le niveau minimum auquel l'interopérabilité est un facteur critique, dépend de la mission. Les problèmes et les situations extrêmement complexes peuvent imposer des niveaux d'intégration plus élevés permettant d'atteindre l'objectif à atteindre. La culture, la langue, les procédures, le matériel et les aspects légaux institutionnels font partie des contraintes de l'intégration.

Peindre la situation maritime générale permet de situer le besoin d'intégration afin de favoriser une meilleure connaissance situationnelle. Beaucoup d'atouts, dont les détecteurs aériens et les détecteurs spatiaux, appartenant au MDN/aux FC ou à d'autres ministères, peuvent être intégrés en vue d'obtenir de l'information. À l'inverse, la nécessité de mener une opération expéditionnaire contre un adversaire motivé dans une zone littorale urbaine et densément peuplée exigerait un niveau d'intégration bien plus élevé à tous les niveaux, allant du niveau tactique au niveau stratégique, et dans toutes les activités entre la conception et l'exécution.

Le MDN et les FC devront modifier leur structure organisationnelle verticale et adopter des processus, des réseaux de connexions et des capacités rendant possibles des opérations intégrées. De plus, l'ensemble de l'institution devra s'intégrer au besoin avec les autres organismes et les autres acteurs. L'objectif est d'obtenir un effet synergétique en exploitant la puissance de l'ensemble de l'institution plutôt que de compter sur l'addition de toutes les parties.

APERÇU 5

L'INTÉGRATION DANS LE CADRE D'UNE APPROCHE PLURIDISCIPLINAIRE GARANTIRA DES MEILLEURES CHANCES DE RÉSOUDRE LES QUESTIONS COMPLEXES LIÉES AU CONTEXTE DE SÉCURITÉ FUTUR QUE DE TRAVAILLER DE MANIÈRE INDÉPENDANTE.

3.3 Adaptatif

L'adaptation est nécessaire pour réagir au changement et aux défis de manière positive et est essentielle afin de comparer avec la complexité et les systèmes complexes. Comprendre que les situations complexes et les relations sont imprévisibles ou incertaines oblige les acteurs confrontés à la complexité à s'adapter pour éviter l'échec. Dans le milieu militaire, on illustre cette idée par l'expression « aucun plan ne survit au premier contact avec l'ennemi ».

L'adaptation a une dimension temporaire. Les systèmes évoluent continuellement. Le changement peut être lent et passer inaperçu, ou bien il peut être très radical et prononcé. Les changements plus lents sont habituellement évolutionnaires, alors que les changements plus rapides sont révolutionnaires. L'adaptation évolutionnaire est la capacité d'une organisation ou d'une personne à apprendre. L'adaptation révolutionnaire est rapide et innovante. Alors que l'apprentissage reste un atout essentiel pour une organisation ou une personne, lors de l'adaptation révolutionnaire, l'accent sera mis sur la réactivité, la flexibilité et l'agilité, ce qui historiquement s'est avéré être la condition de la réussite de l'adaptation militaire.

L'adaptation comprend une autre caractéristique connue sous le nom coévolution. Cette notion fait référence à un système n'évoluant pas de façon isolée, mais plutôt à un ensemble de systèmes évolutionnaires pouvant être interdépendants. Chaque système, ou agent, en plus d'interagir avec les agents du même niveau, interagit également avec les agents supérieurs ou subordonnés en évolution.

CARACTÉRISTIQUES DE L'ADAPTATION17[17]	
Intelligent	Comportement/décision adapté au contexte, découverte et utilisation des avantages.
Résilient	Être capable de se remettre des effets d'un choc, d'une surprise, d'un dommage ou d'un malheur, ou de s'y adapter.
Robuste	Efficace dans un éventail de conditions.
Souple	Être capable de se restructurer.
Agile	Être capable de se rediriger rapidement.
Créatif	Processus d'élaboration de concepts, de solutions et de produits nouveaux et utiles.
Réactif	Être capable de reconnaître une situation rapidement et d'agir.
Endurant	Être capable de résister à un effort prolongé.

Les FC ont besoin de chefs capables de reconnaître les conséquences des tendances nouvelles et de réagir à des chocs stratégiques. Les FC ont également besoin de

commandants qui n'ont pas peur d'adopter des solutions innovantes et non conventionnelles. Les FC ont besoin de personnes qui, comme nos adversaires, projettent d'utiliser du matériel et des capacités avec de nouveaux moyens innovateurs. Nous avons besoin de personnes capables de déceler un changement dans le plan d'action de l'adversaire et de l'exploiter au profit de la mission. Si nous ne créons pas cette capacité parmi nos gens et dans notre institution, nous serons pénalisés, et ce, au profit de l'adversaire. En un mot, les FC doivent être adaptatives au risque d'échouer.

APERÇU 6

L'ADAPTATION EST PRIMORDIALE AFIN DE FAIRE FACE AUX DÉFIS, AUX SITUATIONS ET AUX RELATIONS IMPRÉVISIBLES, INCERTAINES ET COMPLEXES. LES FC DOIVENT ÊTRE ADAPTATIVES AU RISQUE D'ÉCHOUER.

3.4 Réseauté

Les réseaux portent sur les relations et l'interconnectivité. L'existence de réseaux nationaux, la nature des réseaux sociaux, l'importance des réseaux organisationnels et l'impact de la technologie sur les réseaux sont d'une grande pertinence pour les FC.

Il existe deux types de réseaux : les réseaux humains (sociaux) et les réseaux liés à la technologie. Ces deux types de réseaux sont très importants et ne sont pas mutuellement exclusifs. Les réseaux technologiques ont créé des réseaux sociaux virtuels où la distance n'est pas un facteur et où la limite entre un réseau social et un réseau technique est, à certains égards, non pertinente.

Le conflit n'existe pas uniquement entre les États; il s'étend également parmi les réseaux interconnectés sous-jacents de puissance nationale. Traditionnellement, il s'agit de réseaux diplomatiques, économiques et militaires. Dans un environnement de sécurité complexe, il se peut que d'autres éléments de l'infrastructure et des ressources nationales tels que l'information, le domaine financier, le renseignement, l'application de la loi[18] soient utilisés à cet effet. Ces réseaux nationaux peuvent également collaborer avec les acteurs étatiques, non étatiques, provinciaux, locaux et avec d'autres acteurs.

Les réseaux sociaux sont déterminés par la relation existante entre les groupes, les institutions et les personnes au sein d'une société. Les réseaux culturels se sont développés afin d'accueillir des identités, des croyances, des valeurs, des coutumes

et des comportements[19]. À l'avenir, les réseaux des acteurs étatiques et non étatiques qui ont des intérêts communs pourraient donner lieu à des partenariats, créer des collaborations et se disperser lorsqu'ils n'ont plus leur raison d'être. Une discussion sur les réseaux humains et sociaux est proposée ultérieurement dans la section sur le domaine humain (section 5.2.3).

La structure d'une organisation ou d'un réseau est également un élément important. Il existe trois structures qui sont particulièrement pertinentes pour les FC. Dans les relations hiérarchiques, l'information circule vers le haut ou vers le bas et les décisions sont prises au niveau hiérarchique supérieur. Ce type d'organisation est appelé réseau « faible », car il peut être facilement surchargé d'information et sa capacité de gestion de la complexité est limitée. Surtout, les organisations hiérarchiques deviennent facilement des cibles.

Les réseaux intégrés sont bien connectés et l'information est diffusée à tous les niveaux, de telle sorte que chaque nœud peut prendre des décisions. Ces structures peuvent être très complexes, mais sont également idéales pour la gestion de la complexité à des degrés élevés. Un réseau intégré est plus flexible qu'un réseau hiérarchique.

Les réseaux hybrides sont une combinaison des deux types de réseaux mentionnés ci-dessus. Il existe un élément hiérarchique, mais le pouvoir de prendre des décisions est réparti à différents niveaux et la communication est à la fois latérale et verticale. Un réseau hybride est utile pour un ensemble de tâches qu'elles soient simples ou compliquées. Cette structure hybride a des fondements militaires historiques décrits comme « commandement centralisé, contrôle décentralisé ». Une telle structure prendra de plus en plus d'importance dans l'environnement de sécurité complexe de l'avenir; c'est pourquoi les FC devraient privilégier les réseaux intégrés ou hybrides plutôt que les réseaux hiérarchiques.

La technologie des réseaux a pris une place importante dans la vie moderne et dans le lieu de travail. Le réseau technologique nécessite des ordinateurs et des technologies de l'information nécessaires pour la connectivité interne dans toutes les fonctions au sein de l'environnement stratégique. On a recours à la connectivité externe dans le cadre de la défense et de la sécurité des organisations, des autres ministères, des alliés et des partenaires dans la mesure nécessaire, et ce, dans le but d'atteindre les objectifs.

La technologie des réseaux fait déjà partie de chaque domaine et de chaque fonction. Les réseaux sont essentiels à l'intégration de ces deux groupes. En d'autres termes, « réseautez vos réseaux ».

Il ne faut pas oublier que le réseautage a des limites et des contraintes.

- Même si un réseau hautement intégré peut éventuellement permettre l'échange d'information et améliorer la connaissance de la situation, il ne permet pas l'accès à l'ensemble de l'information nécessaire à une prise de décision parfaite.
- La diffusion est fortement limitée pour des raisons de protection et de sauvegarde nécessaires. Ces mesures sont applicables aux FC, aux ministères du GC et dans le cadre des partenariats.
- La création de réseaux techniques *ad hoc* et la création de réseaux sociaux *ad hoc* ont le même problème : les réseaux reposent principalement sur la confiance et les relations.
- Par conséquent, bien que l'objectif de l'avenir soit de trouver des solutions idéales en matière de réseaux technologiques, il faudra se contenter de trouver au mieux des solutions « suffisamment bonnes ».

Cependant, il est primordial que les FC continuent à exploiter les progrès technologiques et méthodologiques en matière de réseautage. Les adversaires ont des moyens technologiques de plus en plus avancés et seront totalement aptes à exploiter la moindre faiblesse hiérarchique. C'est pourquoi les réseaux sociaux et techniques adaptatifs joueront un rôle clé dans l'objectif d'instaurer une force globale et intégrée dans l'environnement de sécurité complexe.

APERÇU 7

LES FC DOIVENT EXPLOITER LES RÉSEAUX SOCIAUX ET TECHNIQUES DANS L'ENVIRONNEMENT STRATÉGIQUE ET DANS TOUS LES DOMAINES FACE AUX MOYENS TECHNIQUES ET SOCIAUX DE PLUS EN PLUS NOMBREUX UTILISÉS PAR LES ANTAGONISTES.

3.5 La nouvelle approche – Synergies et interconnexions

La nouvelle approche exige que l'organisation des FC soit globale, intégrée, adaptative et réseautée afin de garantir la réussite dans l'environnement de sécurité complexe. Ces éléments distincts de la nouvelle approche se chevauchent dans une certaine mesure : les approches globales voient la création d'équipes pluridisciplinaires qui sont en réalité des réseaux humains. Ces équipes et ces réseaux fonctionnent

efficacement s'ils sont intégrés et, en formant la meilleure équipe possible pour une solution donnée à partir d'un grand bassin de partenaires, on peut ainsi mieux s'adapter. Ces approches fournissent également une aide mutuelle afin de créer un effet synergétique conformément à toutes les conditions dans l'environnement stratégique et en matière de fonctions stratégiques.

Trouver des solutions aux problèmes dans l'environnement de sécurité complexe représentera un défi. Les relations de cause à effet seront peut-être problématiques étant donné que chaque action entraînera des effets désirés et non désirés. Les effets inconnus et indésirés sont particulièrement difficiles. C'est pourquoi, afin de mieux évaluer les solutions dans un environnement complexe, un portrait global des effets intermédiaires devra être contrôlé continuellement et les objectifs devront être adaptés en conséquence[20]. Ces efforts permettront la synchronisation des effets tactiques permettant de produire l'effet stratégique désiré.

Il faut bien comprendre les relations de cause à effet si les FC veulent être pertinentes sur le plan stratégique, réactives sur le plan opérationnel et efficaces d'un point de vue tactique.

RÉPERCUSSIONS STRATÉGIQUES

Les FC constituent l'un des instruments de puissance nationale et d'influence à la disposition du GC.

Les organismes non gouvernementaux peuvent également travailler dans un espace complexe afin de résoudre d'autres aspects d'une crise et peuvent ou non avoir les mêmes objectifs que le GC.

Il faut élaborer un cadre global afin de résoudre au mieux les situations complexes ou de les gérer.

Le MDN et les FC devront modifier leur structure organisationnelle verticale et adopter des processus, des réseaux, des relations et des capacités permettant des opérations intégrées.

L'ensemble de l'institution devra intégrer au besoin d'autres organismes ou d'autres acteurs.

Afin d'être adaptatives, les FC ont besoin :

- *De chefs capables de reconnaître les conséquences des tendances nouvelles et de réagir aux chocs stratégiques;*

- *De commandants qui n'ont pas peur d'adopter des solutions innovantes et non conventionnelles;*

- *De personnes qui, comme nos adversaires, projettent d'utiliser du matériel et des capacités avec de nouveaux moyens innovateurs;*

- *De soldats, de marins et de personnel aérien capables de déceler un changement dans le plan d'action de l'adversaire et de l'exploiter au profit de la mission.*

Nos réseaux hiérarchiques actuels ne sont peut-être pas suffisants afin de garantir la réussite dans l'environnement de sécurité complexe de l'avenir.

Les FC devraient privilégier les réseaux intégrés ou hybrides plutôt que les réseaux hiérarchiques.

On a recours à la connectivité externe avec des organismes de défense et de sécurité d'autres ministères, des alliés et des partenaires dans la mesure nécessaire en fonction des objectifs à atteindre.

Les réseaux sociaux et les réseaux techniques fournissent les moyens nécessaires aux FC afin d'être globales, intégrées et adaptatives en vue de relever les défis imposés par l'environnement de sécurité complexe.

---

4 LA NATURE DES CONFLITS FUTURS ET LES CONDITIONS FUTURES

Cette section porte sur la nature des conflits futurs et propose un modèle afin de représenter l'application des éléments de la puissance nationale dans un environnement stratégique complexe. La section examine également les missions de la SDCA en tant que conditions de la conception du CCI.

4.1 La nature des conflits futurs

La conduite d'une guerre se caractérise par deux aspects dominants contraires; elle est soit régulière, soit irrégulière (y compris terroriste). Aujourd'hui, on utilise les mots symétrique et asymétrique. »

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

La mondialisation a joué un rôle important dans l'évolution de la conduite de la guerre. Elle a laissé entrer des acteurs étatiques et non étatiques antagonistes, avec des ressources standards telles que les télécommunications mondiales, le positionnement mondial, l'information, le renseignement, le système de cryptographie, les systèmes d'imagerie télédétectée et les armes. Même si de telles ressources ne permettraient pas d'être aussi résistants et efficaces que les forces militaires des pays occidentaux, elles demeurent des ressources de poids sur le plan stratégique..

Des conflits récents ont montré un changement : la guerre qui était surtout conventionnelle est devenue asymétrique ou irrégulière, où on retrouve des tactiques terroristes et de guérilla (figure 4). Même si le nombre de conflits interétatiques reste presque inchangé, une analyse montre que les conflits nationaux sont plus nombreux et durent plus longtemps. Les FC doivent être capables d'intervenir efficacement (de manière proactive et réactive) dans toute la gamme des conflits, que ce soit d'une manière conventionnelle ou non conventionnelle.

Lors des conflits nationaux, une des parties concernées est un acteur non étatique inférieur. Cette asymétrie oblige l'acteur non étatique inférieur à avoir recours à la guerre irrégulière. Les acteurs non étatiques adaptent continuellement leurs opérations en fonction des nouvelles situations, que ce soit pour obtenir un avantage ou pour réduire les avantages de l'adversaire supérieur avec de ressources conventionnelles.

L'efficacité accrue de ce type de guerre s'est renforcée grâce au fossé toujours plus étroit entre le matériel militaire extrêmement sophistiqué et la technologie disponible sur le marché.

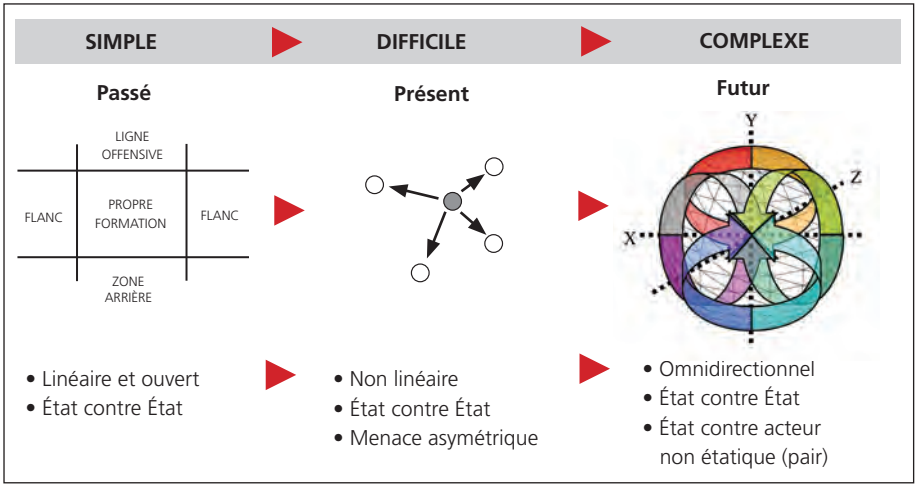

FIGURE 4 : ÉVOLUTION DU CONFLIT.

Nous devons adopter une vision omnidirectionnelle au lieu d'une vision complexe étant donné que le nombre de fronts potentiels formés par un adversaire représente une menace omnidirectionnelle. Les conflits futurs impliquant des États en faillite nécessiteront peut-être l'intervention prolongée d'une force d'intervention afin d'atteindre les résultats désirés. Les tactiques et la doctrine devront sûrement être adaptées selon ces conditions. Lorsque les FC sont déployées dans le cadre d'un conflit, elles devront agir dans un environnement complexe où évoluent un ensemble d'acteurs. La nature du conflit futur doit comprendre une analyse globale de l'évolution des opérations futures, des différents États et acteurs non étatiques, des éléments de puissance et d'influence nationale de plus en plus accessibles à tous les acteurs. Les différences entre les nationalités, les langues, les cultures et les motivations doivent être comprises afin de mener les opérations avec efficacité dans cet environnement. De plus, le début et la fin de ces conflits ne sont pas souvent très clairs.

À l'avenir, une intervention canadienne visant à gérer des situations complexes dans des environnements difficiles nécessitera certainement la participation d'un large ensemble d'organisations gouvernementales et non gouvernementales. Étant donné que la nature du conflit est de plus en plus dynamique, la gamme des acteurs et de solutions s'agrandit proportionnellement et pourrait nécessiter la mise en place de mesures qui ne relèvent plus uniquement des forces militaires.

4.2 Modèle de conflit

La figure 5 est un schéma représentant un modèle traditionnel d'un conflit où les périodes de paix, de conflit et de guerre sont trois conditions distinctes. Ce type de modèle montre également que le conflit est un élément délimité et distinct et que les trois conditions sont reliées par une transition.

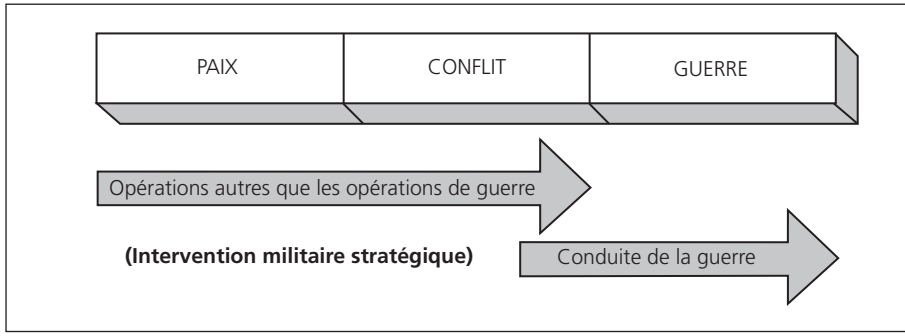

FIGURE 5 : MODÈLE LINÉAIRE TRADITIONNEL D'UN CONFLIT.

L'histoire a démontré que le conflit ne suit pas un processus linéaire et ne fait pas exclusivement partie du domaine militaire. La figure 6 propose un aperçu plus général d'un conflit et illustre l'application des trois éléments traditionnels de puissance nationale, à savoir les éléments diplomatiques, militaires et économiques. Il indique les périodes où beaucoup d'interventions, à différents degrés d'intensité, sont nécessaires afin de gérer un conflit.

Le conflit ne doit pas forcément être violent et des éléments de puissance nationale autres que des éléments militaires peuvent être utilisés afin de résoudre des situations conflictuelles. Un conflit violent devrait toujours être considéré, pas comme une nécessité, mais comme un résultat potentiel de l'intensification du conflit.

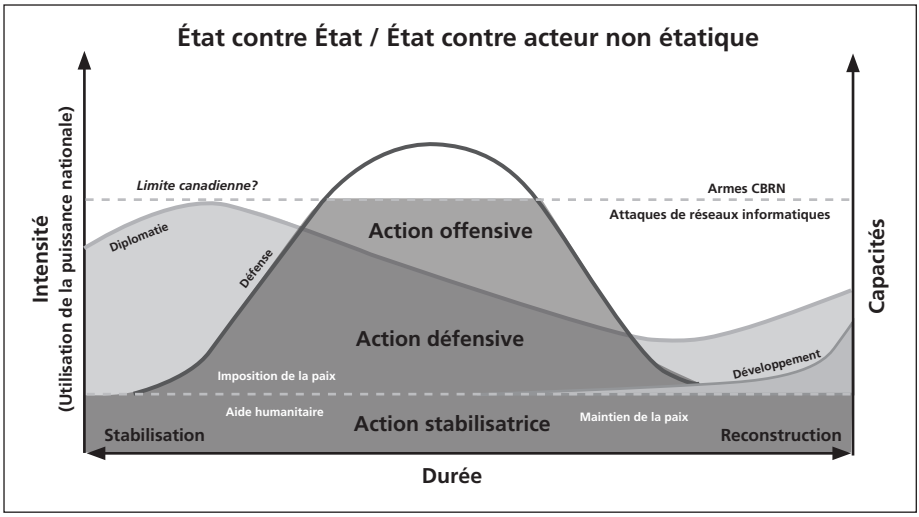

FIGURE 6 : APERÇU GLOBAL D'UN CONFLIT.

Les changements dynamiques illustrés à chaque ligne n'ont pas pu être représentés. Il faut garder à l'esprit que ces courbes évolueront certainement selon la nature de la mission (voir les figures 7 et 8).

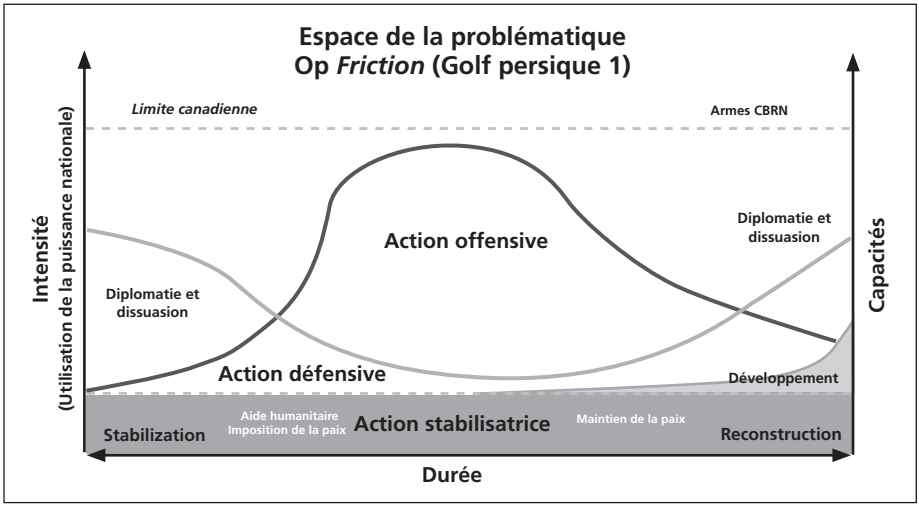

FIGURE 7 : APERÇU GLOBAL DE L'OP *FRICTION.*

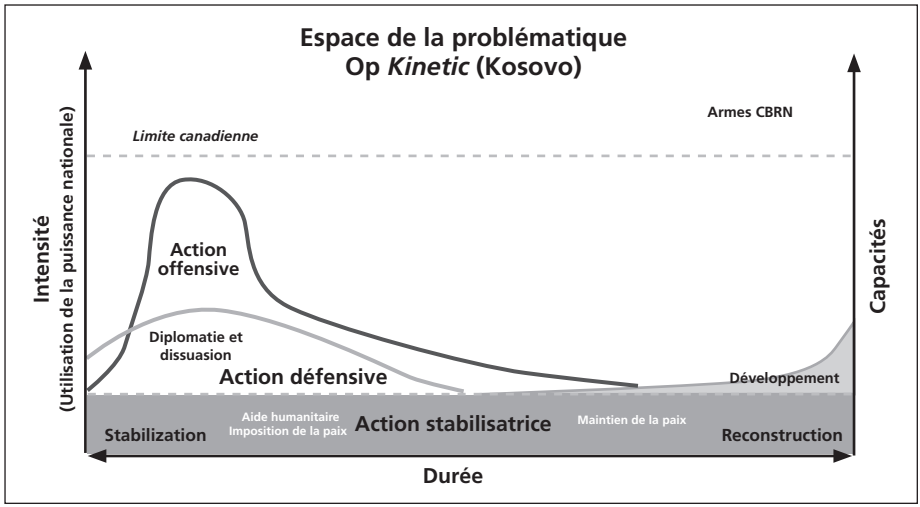

FIGURE 8 : APERÇU GLOBAL DE L'OP ***KINETIC***.

APERÇU 8

LA GAMME DES CONFLITS FUTURS NE SE RÉDUIT PLUS À UNE CONNAISSANCE LINÉAIRE DE LA PAIX, DES OPÉRATIONS AUTRES QUE LA GUERRE ET DE LA GUERRE.

4.3 Missions de la SDCA – Ensembles de conditions

Les conditions comprennent toutes les variables que les FC doivent gérer dans le cadre de leurs fonctions et leurs missions. Au niveau stratégique, les variables peuvent être regroupées dans de larges catégories, c'est-à-dire géographique, climatique et sociopolitique. Les conditions ne seront presque jamais les mêmes pour deux missions. Les techniques, les tactiques et les procédures utilisées dans des opérations similaires, ou même plus tôt lors de la même opération, obtiendront rarement les mêmes résultats et peuvent en fait devenir contre productives.

Aux fins du CCI, les six missions de la SDCA serviront de base pour l'ensemble des conditions. Chacune de ces missions devra répondre à des exigences afin d'être globales, intégrées, adaptatives et réseautées afin de faire en sorte que les FC restent pertinentes sur le plan stratégique, réactives sur le plan opérationnel et efficaces d'un point de vue tactique.

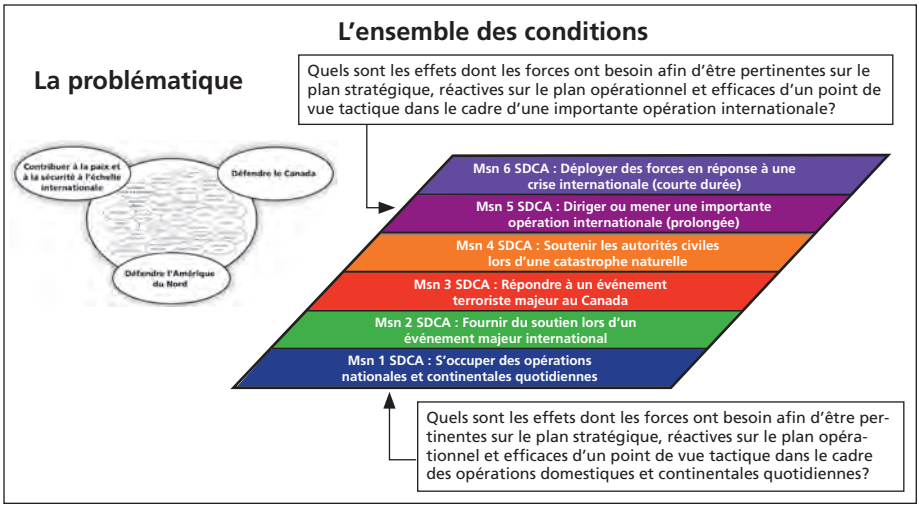

FIGURE 9 : L'ENSEMBLE DES CONDITIONS.

RÉPERCUSSIONS STRATÉGIQUES

Les FC doivent être capables d'intervenir efficacement (de manière proactive et réactive) dans toute la gamme des conflits, que ce soit d'une manière conventionnelle ou non conventionnelle.

Étant donné que la nature du conflit est de plus en plus dynamique, la gamme des acteurs et des solutions s'agrandit proportionnellement et pourrait nécessiter la mise en place de mesures qui ne relèvent plus uniquement des forces militaires.

5 LA NATURE DE L'ENVIRONNEMENT STRATÉGIQUE FUTUR

Cette partie donne un aperçu de l'environnement stratégique futur. Elle préconise l'élargissement de l'environnement stratégique, constitué des domaines maritime, terrestre et aérien, afin d'y intégrer trois nouveaux domaines : spatial, virtuel et humain. La description du domaine humain comprend une discussion sur la façon dont la technologie et la mondialisation ont permis à des éléments antagonistes (États et acteurs non étatiques) d'avoir accès à des instruments de puissance nationale et d'avoir une influence qu'il était auparavant impossible d'obtenir.

5.1 Description de l'environnement stratégique

L'environnement stratégique est défini comme le lieu où les éléments de pouvoir et d'influence s'exercent. Les éléments traditionnels de puissance nationale et d'influence sont les capacités militaires, économiques et diplomatiques[21] du niveau national visant éventuellement à changer la condition humaine dans le cadre de la politique et de l'intention nationales. La politique et l'intention nationales sont ces conditions, attentes et désirs établis par la politique gouvernementale qui ordonnent le recours aux éléments de puissance nationale.

L'environnement stratégique est défini comme le lieu où les éléments de pouvoir et d'influence s'exercent.

Les antagonistes non étatiques opèrent de plus en plus dans le même environnement stratégique que le MDN/les FC. Historiquement, les éléments traditionnels de puissance et d'influence ont été limités à l'État. Dans l'environnement de sécurité moderne, les éléments de puissance et d'influence ne sont plus l'apanage de l'État et les États ne dominent plus de manière exclusive les domaines de l'environnement stratégique. Les antagonistes actuels et futurs, qu'ils soient étatiques ou non, ont le pouvoir de créer des effets stratégiques dirigés contre les intérêts nationaux canadiens. Nous devons être conscients qu'au sein des États, de nouveaux éléments de puissance et d'influence voient le jour et défient les perspectives classiques.

Les États ne dominent plus de manière exclusive les domaines de l'environnement stratégique.

5.2 Trois nouveaux domaines

Bien que les domaines maritime, terrestre et aérien sont considérés comme traditionnels, ils n'ont pas toujours été trois. Ce nombre est susceptible d'augmenter ou de diminuer à l'avenir. L'accès à chacun des domaines traditionnels de l'environnement stratégique s'explique par les développements technologiques. Avec la création des voiliers, les forces armées ont pu mener la guerre sur terre et en mer. L'avènement de l'avion et les améliorations technologiques qui ont suivi signifiaient que le conflit s'étendait aussi dans les airs.

Dans la mesure où ces développements technologiques ont évolué, les forces armées ont été capables de concevoir des utilisations stratégiques de la technologie et d'exercer ensuite leur puissance et leur influence depuis leurs navires et leurs aéronefs. Les domaines maritime et aérien sont devenus partie intégrante de l'environnement stratégique lorsque des gens ont développé la capacité de générer de la puissance nationale et de l'influence en y accédant.

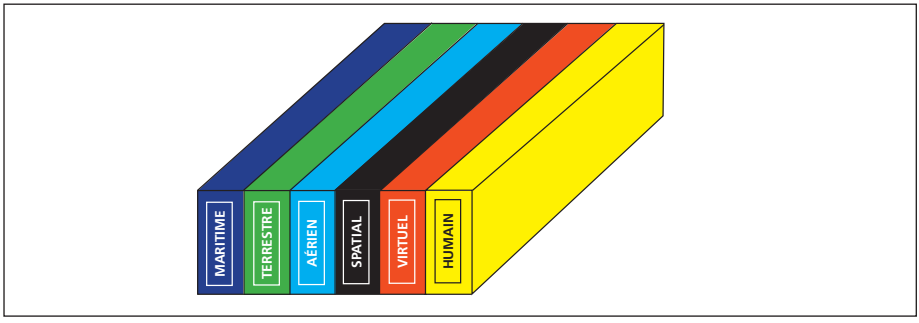

FIGURE 10 : AXE DE L'ENVIRONNEMENT STRATÉGIQUE (DOMAINES) DE LA CONCEPTION DU CADRE.

Les récents progrès des astronefs, des communications, des technologies informatiques, des médias et des sciences du comportement élargissent l'environnement stratégique et créent de nouveaux domaines, soit les domaines spatial, virtuel et humain. Les acteurs étatiques et non étatiques prouvent déjà qu'ils peuvent exercer et qu'ils exerceront les éléments de puissance et d'influence dans les domaines en évolution.

5.2.1 Domaine spatial

L'espace doit être considéré comme un domaine de l'environnement stratégique. La technologie continue à soutenir le développement spatial, permettant un plus grand accès à l'espace, et ce, pour des périodes plus longues. Les biens spatiaux

ainsi que leurs éléments terrestres respectifs, font partie de l'infrastructure nationale du Canada[22]. L'espace est le support d'un certain nombre de moyens de communication et de nombreuses capacités civiles et militaires.

L'espace n'est la propriété de personne[23], ce qui le rend accessible aussi bien aux acteurs étatiques que non étatiques qui sont capables et désirent projeter des capacités dans ce domaine. De plus, dans la conduite des opérations militaires mondiales, la disponibilité des services par satellite pour le MDN/les FC sera vital. À l'appui de la réalisation des objectifs stratégiques canadiens tels que l'exercice de la souveraineté dans l'Arctique, les biens spatiaux sont des catalyseurs de missions essentiels. Les FC devront étendre leur rôle dans l'espace en vue de protéger et d'exploiter des sources de communication et d'information essentielles.

L'espace va continuer de croître dans la mesure où le recours à la technologie spatiale continue de croître. Cependant, comme les récents exemples ont pu montrer, ces systèmes spatiaux sont de plus en plus vulnérables aux attaques provenant de diverses plates-formes d'armes[24]. Cette capacité à détruire ou à mettre hors d'état des satellites est actuellement limitée à un certain nombre d'États, mais la technologie qui perturbe, détruit ou met hors d'état les satellites sera probablement accessible aux acteurs non étatiques ou aux États voyous à court terme.

De nombreuses forces aériennes ont défendu le domaine spatial, mais ont considéré l'espace comme une partie subordonnée à l'aérospatial[25]. Ce lien de subordination ne met pas suffisamment l'accent sur l'importance croissante de l'espace. L'espace est devenu un domaine commun et doit être considéré à tous les niveaux d'opérations. L'espace est un domaine unique et indépendant dans lequel les éléments de puissance nationale et d'influence s'exercent.

5.2.2 Domaine virtuel

Le cyberespace permet des réseaux à la fois techniques et sociaux. Les technologies de communication et de l'information sont des éléments essentiels des infrastructures nationales et constituent les fondements de la puissance économique et financière. La capacité de défense, aujourd'hui et à l'avenir, dépend des réseaux de systèmes d'information et de communications qui lient les capteurs, les plates-formes d'armes, les opérateurs et les décideurs.

Le domaine virtuel[26] est également le monde virtuel dans lequel les gens se rencontrent, interagissent, échangent des idées et « réseautent » sans un espace physique défini. Des « communautés de praticiens » et « communautés d'intérêts » militaires

existent déjà et collaborent en ligne et échangent de l'information. La collaboration avec d'autres ministères et d'autres organismes de sécurité et de défense est également possible sur le plan technique. Cet accès aux données et à l'information facilite la compréhension et la connaissance de la situation qui, couplées à l'intuition humaine, mènent à une connaissance approfondie et à la créativité.

Le marché stimule l'innovation et la technologie dans le cyberespace. Tous les aspects de ce domaine – dont Internet, les réseaux de télécommunications, les systèmes informatiques et les logiciels – sont en perpétuelle évolution. Les tendances telles que la convergence des médias (radio, télévision et journaux) avec Internet ne font que s'ajouter au contexte changeant. L'émergence d'une nouvelle technologie ou tendance s'accompagne de nouveaux concepts, d'une nouvelle terminologie et d'un nouveau jargon. Suivre le rythme des cycles d'innovation rapides et se tenir au courant des principaux concepts de pointe qui sont rapidement écartés ou remplacés par de nouveaux concepts représentera un défi pour les FC.

Le domaine virtuel sera un mécanisme d'intégration de tous les domaines au niveau stratégique qui aboutira à une approche opérationnelle commune. Cette fonctionnalité sera complétée par l'installation du domaine virtuel en vue de fusionner les fonctions stratégiques, produisant des effets intégrés. Le cyberespace peut également être l'endroit où le moyen et le message sont pratiquement inséparables.

Le cyberespace présente des vulnérabilités particulières. La technologie accessible et abordable a fait de ce domaine le plus facile à exploiter par les antagonistes. Dans ce domaine, la distinction entre l'activité criminelle et la menace pour la sécurité nationale peut être difficile à établir. Le cyberespace n'a pas de limites; des serveurs hébergés dans des pays neutres ou amis peuvent être utilisés par un antagoniste en vue de mener des cyberattaques. Les aspects temporels nécessaires pour mener la cyberdéfense sont extrêmement condensés. Le défi constant consistera à veiller à ce que notre politique et notre doctrine suivent le rythme des avancées dans le domaine virtuel.

Indépendamment des technologies et des méthodes employées, les effets sur la puissance et l'influence nationales sont régis par la nature des opérations de réseau informatique (CNO) qui peuvent être menées dans le domaine virtuel. La plupart des pays les classent comme l'exploitation non autorisée de réseaux informatiques (CNE), comme l'attaque de réseaux informatiques (CNA) et comme la défense des réseaux informatiques (CND) (figure 11). Ces opérations peuvent être menées à tous les niveaux de conduite de guerre et le MDN/les FC doivent se concentrer sur les effets produits plutôt que sur les moyens avec lesquels les opérations sont menées.

En attaquant ou en désactivant nos réseaux, un antagoniste peut facilement porter préjudice à nos capacités de commandement, de contrôle, de communication, d'informatique, de renseignement, de surveillance et de reconnaissance dans les domaines maritime, terrestre, aérien et spatial. De plus, un antagoniste peut attaquer au cœur de nos infrastructures et de nos systèmes de soutien nationaux.

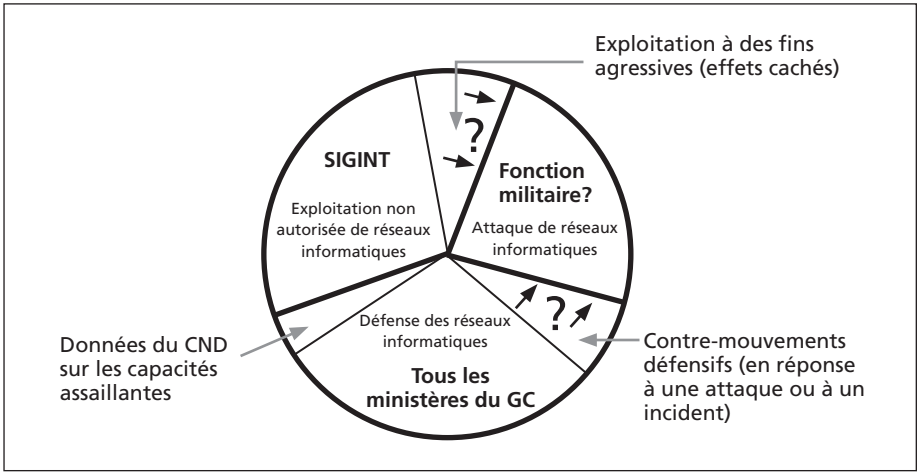

FIGURE 11 : OPÉRATIONS DE RÉSEAU INFORMATIQUE.

Le cyberspace, domaine particulier, représente des défis. La définition et le concept militaires actuels de ce domaine sont en train d'être établis, mais ce travail est axé sur des concepts existants fondés sur un « contexte de l'information ». Ce concept existant n'a pas été bien compris et a été mal appliqué aux opérations psychologiques. Une plus grande confusion découle du fait que la définition militaire du cyberespace se limite aux communications physiques et à la technologie de l'information alors que l'usage dans le domaine public comprend également un élément du réseautage social virtuel.

Le monde virtuel du cyberespace peut-il créer des effets physiques? Oui, la majeure partie de tous les pouvoirs économiques (instruments financiers) est transmise par voie électronique et les infrastructures critiques reposent sur le cyberespace. Par conséquent, il faut aussi reconnaître que le cyberespace devient le moyen prédominant d'influencer le domaine humain.

La nouvelle question devrait être, « Le monde réel peut-il créer des effets dans le cyberespace (par exemple détruire de l'information)? » La réponse est certainement « oui » car les nœuds individuels, les capteurs et les composants matériels peuvent être effectivement détruits; cependant, une fois la vidéo, les images, les données,

l'information et la désinformation situées dans le cyberespace, il devient impossible de les enlever. Pour ces raisons, le cyberspace est un domaine distinct dans lequel les éléments de puissance nationale et d'influence s'exercent clairement.

5.2.3 Domaine humain

Dans le domaine humain, il y a les personnes, les groupes de personnes et tous les aspects découlant de l'entreprise humaine. Une autre méthode pour décrire ce domaine est d'adopter une perspective conflictuelle : des antagonistes, des acteurs neutres ou des acteurs amis. Pour que les FC atteignent leurs objectifs dans l'environnement de sécurité complexe de l'avenir, il faut prendre en ligne de compte les motivations des personnes et des groupes, la technologie en tant qu'instrument favorisant les réseaux humains, et l'intention de l'adversaire.

Dans l'univers individuel (psychologique), la perception, la prise de décision et le comportement sont les résultats d'une démarche cognitive (réflexion, connaissance, perception), d'une démarche émotive et affective (affection, émotion, humeur), et d'une démarche conative (volonté, efforts, motivation); voir figure 12[27]. Il faut comprendre ces éléments et ces émotions afin de réduire les capacités de l'adversaire en matière de prise de décision et de renforcer sa propre résistance[28].

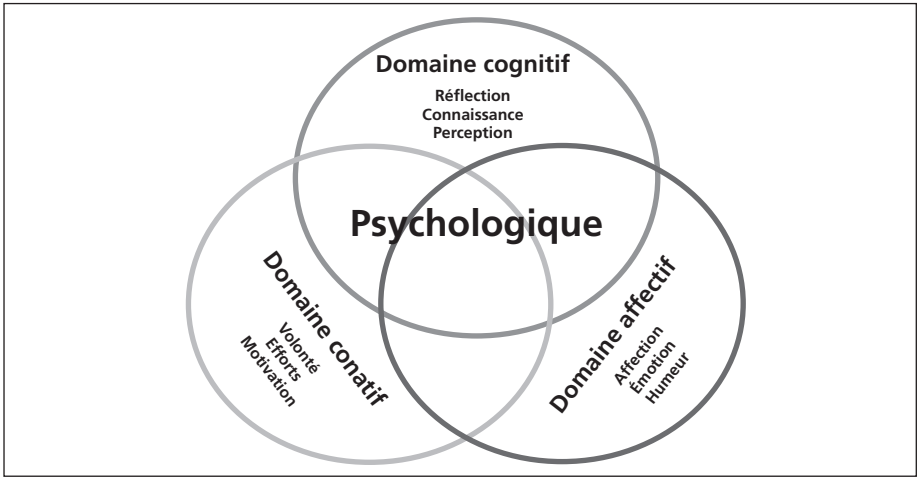

FIGURE 12 : ASPECTS PSYCHOLOGIQUES DU DOMAINE HUMAIN.

Peut-on utiliser les éléments physiques et non physiques de puissance nationale afin d'influencer ces aspects?

Oui, comme on le fait depuis toujours!

De plus, est-ce que ces trois éléments psychologiques sont pertinents pour la puissance nationale et l'influence? Oui, absolument, étant donné que ces éléments

jouent un rôle fondamental dans les « affrontements de volontés » ou dans un conflit. Des technologies sociales habilitantes dans l'avenir donneront accès à l'univers psychologique de la personne.

Dans l'univers socioculturel, il existe plusieurs aspects pertinents pour les FC en matière de réseaux : leur nature (analyse du réseau), leur capacité à apprendre et s'adapter, leurs différentes catégories (p. ex. crime organisé) et la nature des réseaux culturels et sociaux pertinents.

Dans le domaine humain des FC, il existe trois aspects essentiels : l'aspect humain institutionnel où sont générées les capacités militaires, l'aspect humain physique qui endure les difficultés et les dangers dans le théâtre des opérations et qui est soutenu afin de maintenir en puissance la capacité opérationnelle, et le guerrier qui détecte, agit et protège. Le domaine humain des FC devra être global, intégré, adaptatif et réseauté et sera indispensable afin d'obtenir les effets des projets dans tous les domaines de l'environnement stratégique.

Les réseaux sociologiques et culturels (ou les groupes) formés présentent un intérêt particulier, car ils constituent la base pour ce qui est des « autres visions du monde ». En plus de connaître les antagonistes, il faut connaître les acteurs neutres et les amis potentiels dans le domaine afin d'être efficace sur le plan stratégique. Voici les réseaux sociaux et culturels présentant un intérêt particulier :

- Affiliations familiales ou tribales.
- Culture et langue : identités, religions, croyances, valeurs, habitudes, comportements communs.
- Autres catégories : influence politique, criminelle et économique.
- Catégories organisationnelles : militaire, autres ministères, commerciale.

Tous les antagonistes, les acteurs neutres ou les amis peuvent servir de lentilles distinctes pour observer l'ensemble du domaine humain. Par exemple, l'étude des économies locales et nationales est un moyen d'élargir les perspectives sur le comportement humain correspondant. Chaque lentille éventuelle représente des systèmes complexes différents constituant le domaine humain.

Voici les principales inquiétudes associées à ce domaine :

- Comment l'antagoniste en créant des effets influence-t-il les citoyens canadiens, les FC, les acteurs neutres, les combattants ou les non-combattants?

- À l'inverse, comment les FC pourraient créer des effets influençant les antagonistes, les non-combattants antagonistes, les acteurs neutres et nos propres citoyens?
- Que faut-il changer à l'intérieur du domaine humain des FC afin d'être capable de mener les opérations dans le cadre des conditions prévalentes, dans l'environnement stratégique et en exécutant les fonctions? Il faut noter que ce domaine est la source ultime de puissance militaire.

L'objectif cible ultime en ce qui concerne les éléments de puissance et d'influence a toujours fait partie du domaine humain. La nouveauté réside dans la capacité de communiquer les idées à l'échelle mondiale, grâce à des mots et des idées puissantes, dans un temps presque réel en vue de créer une influence stratégique. Ces capacités visant à influencer les personnes et les groupes se sont extrêmement accrues. Les technologies habilitantes fournissent aux personnes la capacité de former et d'influencer un public large à l'échelle mondiale par de la propagande et de l'information erronée. L'utilisation de tels moyens était auparavant limitée aux États et aux médias de masse.

EXEMPLES DE TECHNOLOGIES HABILITANTES SOCIALES	
Imagerie numérique	Photographies et vidéo
Télévision (cycle de nouvelles sur 24 h)	CNN et Al Jazeera
Technologies des communications	Téléphone cellulaire, téléphone Web
Activités rendues possibles par Internet	Messagerie électronique, services bancaires en ligne, approvisionnement, jeux, accès aux technologies.
Web 2.0 (Réseautage social)	Twitter, Blogues, MySpace, YouTube

Les images et les mots puissants qui franchissent les frontières internationales afin d'atteindre des audiences mondiales ont le pouvoir d'élargir les conflits au-delà des acteurs directement impliqués. Le conflit peut attirer plus d'États et d'acteurs non étatiques non combattants. De plus, l'opinion publique mondiale pourrait se transformer en influences politiques au sein d'organismes multinationaux tels que les Nations Unies et l'OTAN. Sur le plan tactique, l'utilisation par les antagonistes de la propagande pourrait influencer les acteurs non combattants et créer ainsi un effet stratégique. Par exemple, les décès et l'élimination des acteurs non combattants, provoqués par des acteurs antagonistes ou par les FC, peuvent être un avantage pour l'antagoniste.

Le domaine humain constitue les fondations vitales dans l'environnement stratégique.

Le domaine humain constitue les fondations vitales dans l'environnement stratégique. Les FC doivent connaître les antagonistes, les amis et les acteurs neutres ainsi que les facteurs sous-jacents dictant le comportement humain. Les FC doivent se servir des connaissances disponibles découlant des sciences humaines et comportementales afin de mieux se positionner en vue de gérer et de limiter l'ampleur du conflit, de faciliter la collaboration entre tous les acteurs, de comprendre comment fonctionnent, s'adaptent et évoluent les réseaux entre les personnes, et de faciliter l'évaluation de la menace et la réduire.

Les FC doivent également comprendre les facteurs sous-jacents qui dictent le comportement d'une personne et d'un groupe, et en particulier mieux connaître les antagonistes, les amis et les acteurs neutres. De plus, nous devons comprendre la nature adaptative des réseaux humains antagonistes, ainsi que l'effet stratégique des opérations d'influence antagonistes combinées aux réseaux humains rendus possibles grâce à la technologie.

Par conséquent, le domaine humain est un domaine distinct, où les éléments de puissance nationale et d'influence sont utilisés en vue de générer un effet stratégique. De plus, un échec dans le domaine humain, indépendamment du degré de réussite dans le reste de l'environnement stratégique, pourrait être à l'origine d'un échec stratégique national.

APERÇU 9

L'ENVIRONNEMENT STRATÉGIQUE S'EST ÉTENDU AU-DELÀ DES DOMAINES TRADITIONNELS (MARITIME, TERRESTRE ET AÉRIEN) ET DOIT MAINTENANT COMPRENDRE LES DOMAINES SPATIAL, VIRTUEL ET HUMAIN. L'ENVIRONNEMENT STRATÉGIQUE CONTINUERA DE S'ÉLARGIR, CE QUI INTENSIFIERA LES QUESTIONS DE COMPLEXITÉ ET SOULIGNERA LA NÉCESSITÉ POUR LES FC D'ÊTRE GLOBALES, INTÉGRÉES, ADAPTATIVES ET RÉSEAUTÉES.

5.3 Relations entre les domaines

La figure 13 schématise les relations entre les composants de l'environnement stratégique. L'élément humain est central. Les domaines physiques (maritime, terrestre, aérien et spatial) entourent l'humain. De plus en plus, le domaine virtuel peut affecter notre perception du monde physique; c'est pourquoi dans cette représentation, le domaine virtuel est en lien direct avec le domaine humain. Les limites sont incertaines et la technologie peut confirmer ou déformer une perception. Le domaine virtuel rend également possible la mise en place de réseaux séparés physiquement dans l'espace; il existe donc une relation directe avec le domaine humain.

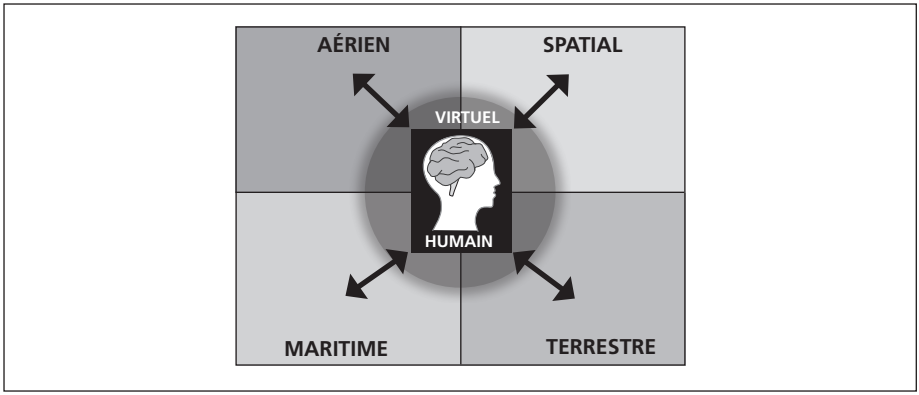

FIGURE 13 : RELATIONS ENTRE LES DOMAINES.

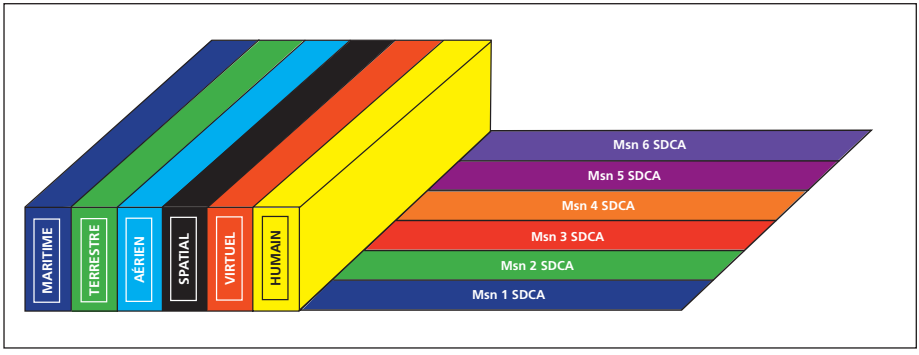

FIGURE 14 : AXES DES CONDITIONS ET DES DOMAINES DE LA CONCEPTION DU CADRE.

Les composants organisationnels des FC (Marine, Armée de terre, Force aérienne et Forces spéciales) continueront à fournir de l'expertise et à mener des opérations dans les domaines traditionnels, et ils contribueront à la réalisation des objectifs dans tout l'environnement stratégique. Les nouveaux domaines ne suggèrent pas d'assumer la responsabilité, mais ils exigent le leadership. Intégrer les nouvelles capacités d'un large ensemble d'organisations fournira un panel d'outils plus adaptatifs afin de faire face aux problèmes complexes de l'avenir.

Les nouveaux domaines ne suggèrent pas d'assumer la responsabilité, mais ils exigent le leadership.

Alors que nous nous dirigeons vers l'avenir, nous devons conserver une attitude progressiste en ce qui concerne les domaines qui restent à découvrir où les éléments de puissance nationale et d'influence pourront être appliqués. Les nanosciences et la notion de quantum pourraient certainement faire partie des futurs domaines.

Nos capacités à être pertinents sur le plan stratégique, réactifs sur le plan opérationnel et efficaces d'un point de vue tactique dans toute la gamme des conflits futurs dépendent essentiellement de nos capacités à se projeter et à contrer les effets dans tous ces domaines. Les commandants à tous les niveaux doivent être prêts à gérer les effets infligés par les acteurs antagonistes faisant partie des six domaines, peut-être simultanément. En fonction de la nature de la mission, les commandants à tous les niveaux devront également être prêts à créer des effets relevant des six domaines simultanément et d'une manière intégrée et globale.

Nos capacités à être pertinents sur le plan stratégique, réactifs sur le plan opérationnel et efficaces d'un point de vue tactique dans toute la gamme des conflits futurs dépendent essentiellement de nos capacités à se projeter et à contrer les effets dans tous ces domaines.

RÉPERCUSSIONS STRATÉGIQUES

Les États ne dominent plus de manière exclusive les domaines de l'environnement stratégique.

Les antagonistes actuels et futurs, qu'ils soient étatiques ou non, ont le pouvoir de créer des effets stratégiques dirigés contre les intérêts nationaux canadiens.

En attaquant ou en désactivant nos réseaux, un antagoniste peut facilement porter préjudice à nos capacités de commandement, de contrôle, de communications, d'informatique, de renseignement, de surveillance et de reconnaissance dans les domaines maritime, terrestre, aérien, et spatial. De plus, un antagoniste peut attaquer au cœur de nos infrastructures et de nos systèmes de soutien nationaux.

Un échec stratégique dans n'importe quel domaine pourrait entraîner un échec stratégique à l'échelle nationale.

Un échec dans le domaine humain, indépendamment du degré de réussite dans le reste de l'environnement stratégique, pourrait entraîner un échec stratégique à l'échelle nationale.

Les FC doivent connaître les acteurs amis, antagonistes et neutres ainsi que les facteurs sous-jacents dictant les comportements humains.

En utilisant les sciences humaines et comportementales, les FC peuvent mieux se positionner en vue de gérer et de limiter l'ampleur du conflit, de faciliter la collaboration entre tous les acteurs, de comprendre comment fonctionnent, s'adaptent et évoluent les réseaux entre les personnes, et de faciliter l'évaluation de la menace et la réduire.

Les FC doivent comprendre la nature adaptative des réseaux humains antagonistes, ainsi que l'effet stratégique des opérations d'influence antagonistes combinées aux réseaux humains rendus possibles grâce à la technologie.

Les nouveaux domaines ne suggèrent pas d'assumer la responsabilité, mais ils exigent le leadership.

Les commandants à tous les niveaux doivent être prêts à gérer les effets infligés par les acteurs antagonistes faisant partie des six domaines, peut-être simultanément.

Les commandants à tous les niveaux, en fonction de la nature de la mission, devront également être prêts à créer des effets relevant des six domaines simultanément et d'une manière intégrée et globale.

Les domaines spatial, virtuel et humain sont trois domaines distincts où il est possible de mettre en application les instruments de puissance nationale et d'influence au même titre que les domaines traditionnels.

Nos capacités à être pertinents sur le plan stratégique, réactifs sur le plan opérationnel et efficaces d'un point de vue tactique dans toute la gamme des conflits futurs dépendent essentiellement de nos capacités à se projeter et à contrer les effets dans tous ces domaines.

6 LA NATURE DES FONCTIONS FUTURES

Cette section examine les fonctions des FC, soit le commandement, la détection, l'action, le maintien en puissance, la protection et la mise sur pied, par rapport aux attributs visés : global, adapté, intégré et réseauté.

Les six fonctions décrivent ce que les FC font au quotidien et lors des opérations de contingence. Un manquement à l'une des fonctions dans l'environnement stratégique peut conduire à un échec stratégique. Notre vision actuelle des fonctions stratégiques est régie par nos expériences historiques ainsi que nos connaissances des domaines traditionnels terrestre, maritime et aérien. Cette planification en vue de batailles traditionnelles peut nous donner une vision stéréotypée de ces fonctions, une vision qui ne fait pas nécessairement référence à l'avenir. Au mieux, elle peut nous limiter dans la mesure où nos idées sur les opérations futures sont régies exclusivement par la connaissance des opérations en cours. Dans le pire des cas, cette vision peut nous contraindre à planifier le conflit d'hier. Pour mener à bien l'orientation du GC dans un contexte de sécurité de plus en plus complexe, des approches globales, intégrées, adaptées et réseautées doivent être appliquées aux fonctions futures.

Le tableau suivant dresse la liste des futures propositions de définitions pour les fonctions des FC[29].

Fonction	Définition
Commandement	L'exercice créatif et délibéré d'autorité légitime en vue d'accomplir la mission légalement, avec professionnalisme et de façon éthique.
Détection	L'acquisition et le traitement de l'information pour permettre aux commandants et aux autorités de comprendre les caractéristiques et les conditions de l'environnement opérationnel pertinentes pour la prise de décisions militaires.
Action	L'utilisation militaire des capacités en vue d'atteindre les résultats voulus à l'appui de la politique nationale.
Maintien en puissance	La fourniture de tous les services de soutien nécessaires au maintien des opérations courantes et de contingence – nationales, continentales et expéditionnaires – y compris les opérations prolongées.
Protection	L'approche globale de la protection des éléments matériels et immatériels par le biais des activités d'intégration de détection, d'évaluation, d'avertissement, de défense (active et passive) et de récupération.
Mise sur pied	La méthode par laquelle le MDN et les FC recrutent, instruisent et forment le personnel, acquièrent du matériel, des infrastructures et des services, et font en sorte que l'ensemble des ressources soit prêt à répondre à la mission de défense.

Notre vision actuelle des fonctions stratégiques (commandement, détection, action, maintien en puissance, protection et mise sur pied) est régie par nos expériences historiques ainsi que nos connaissances des domaines traditionnels terrestre, maritime et aérien. Dans le pire des cas, cette vision peut nous contraindre à planifier le conflit d'hier.

6.1 Commandement

La fonction future de commandement est définie comme « l'exercice créatif et délibéré d'autorité légitime en vue d'accomplir la mission légalement, avec professionnalisme et de façon éthique »[30].

Le commandement adaptatif comprend la boîte à outils qui permet aux postes de commandement, à tous les niveaux, d'exercer le commandement de mission.

Le commandement adaptatif est l'évolution logique de la façon dont cette fonction doit être exercée au sein des FC afin d'appuyer le concept de commandement de mission. Si le commandement de mission est un prolongement des intentions du commandement par la compréhension implicite de ces intentions, alors le commandement adaptatif comprend la boîte à outils qui permet aux postes de commandement, à tous les niveaux, d'exercer le commandement de mission. Un antagoniste ingénieux et organisé peut atteindre des niveaux de surprise en prenant des mesures contraires à ce qui était prévu. Inversement, la créativité des antagonistes peut être atténuée et contrée par les personnes aux postes de commandement qui peuvent anticiper, adapter et répondre rapidement à une action contradictoire imprévisible. Le commandement adaptatif comporte les caractéristiques de l'adaptation[31].

Le concept futur de commandement doit décrire les facteurs globaux qui aident cette fonction. Comprendre l'ensemble des conditions et l'environnement stratégique aidera les commandants à définir le problème et à fixer (ou réévaluer) des objectifs appropriés. Le concept futur de commandement devrait conduire à l'adoption d'une approche pluridisciplinaire afin d'intégrer les forces dans une structure organisationnelle plus large en vue de résoudre, de gérer ou de contenir les nombreux défis posés par l'environnement de sécurité complexe.

6.2 Détection

La fonction future de détection est décrite comme « l'acquisition et le traitement de l'information pour permettre aux commandants et aux autorités de comprendre les caractéristiques et les conditions de l'environnement opérationnel liées à la prise de décisions militaires ».

Les capacités futures de détection doivent permettre aux décideurs de bien comprendre l'information et les renseignements requis. Il est nécessaire d'examiner le domaine humain et de comprendre les nombreux réseaux que forme l'environnement stratégique.

Cette fonction doit être intégrée à un niveau élevé pour permettre aux décideurs d'obtenir les meilleurs résultats. L'information provenant de diverses sources – réseaux civils et militaires – doit être fusionnée afin de fournir une connaissance de la situation. Les capacités de détection doivent être en mesure d'atténuer les défis que représentent le climat et les conditions météorologiques, le terrain, la langue, les croyances et les différences culturelles. Néanmoins, même en tenant compte de tous les acteurs, une connaissance parfaite de la situation est pratiquement impossible.

Le concept futur de détection devrait utiliser des réseaux hautement intégrés afin de partager l'information en temps opportun, mais la fonction doit également être capable d'utiliser des réseaux *ad hoc* ou propres à la mission. Déterminer les organismes qui forment des réseaux humains amicaux, neutres et contradictoires au sein de l'environnement stratégique sera difficile, mais est essentiel à l'efficacité stratégique.

6.3 Action

La fonction future d'action est définie comme « l'utilisation militaire de la/des capacité(s) en vue d'atteindre les résultats voulus à l'appui de la politique nationale ».

Dans l'environnement de sécurité de l'avenir, les FC doivent être en mesure d'agir de façon globale comme un des instruments nationaux du pouvoir. Les actions engendreront une multitude d'effets, certains prévus, d'autres imprévus et parfois indésirables. Dans le cadre d'une approche pluridisciplinaire, nos propres actions, mais également celles de tous les autres organismes, doivent être prises en compte. Une bonne compréhension de l'environnement stratégique, de l'ensemble des conditions, de nos actions et des actions des autres permettra d'atteindre les objectifs souhaités et d'atténuer les effets secondaires.

Le concept futur d'action doit englober la notion d'intégration dans la mesure où les FC seront incapables de résoudre des problèmes complexes de façon isolée. Il est très probable que les futures FC devront agir de concert avec d'autres pays, d'autres ministères et des organisations non gouvernementales. L'intégration de tous les participants, au niveau approprié, produira des effets convergents.

Les forces mandatées pour agir doivent s'adapter. En montrant leur capacité à se restructurer face à une nouvelle menace (flexibilité), à rediriger les effets rapidement (agilité), à faire tout cela rapidement (réactivité) et de manière soutenue pendant une période prolongée (endurance), les forces seront en mesure de contrecarrer toute action d'opposition imprévisible.

6.4 Maintien en puissance

La fonction future de maintien en puissance est définie comme « la fourniture de tous les services de soutien nécessaires au maintien des opérations courantes et de contingence – nationales, continentales et expéditionnaires – y compris les opérations prolongées ».

Pour relever le défi de maintien en puissance des FC, que ce soit au pays ou à l'étranger, les décideurs doivent bien comprendre l'ensemble des conditions, l'évolution des besoins des FC et les obstacles en ce qui concerne les besoins du maintien en puissance. Les capacités de maintien en puissance nécessiteront également la coopération de tous les collaborateurs éventuels : FC, alliés, organismes, industrie, universités et ONG – à l'échelle nationale et internationale. Le maintien en puissance global comprendra du matériel, du personnel et de l'information.

Le maintien en puissance global permettra de tirer parti des organismes, des capacités, des systèmes et des processus du monde entier et d'établir volontairement des partenariats. Réunir les capacités au sein du gouvernement (fédéral, provincial, municipal), de l'industrie, des ONG, des universités et entre les alliés nécessitera une approche soigneusement intégrée afin de travailler de la manière la plus efficace et la plus transparente possible.

Ces partenariats de personnes et d'organismes de partout au pays et dans le monde devront être rassemblés par le biais des réseaux de l'ère de l'information. Une fois ces réseaux de collaborateurs établis et autorisés, les FC peuvent, au besoin, remonter le réseau pour accéder directement à partir de la source d'origine aux capacités de maintien en puissance.

Dans la mesure où les menaces évoluent et changent, les capacités (et dispositions) de maintien en puissance des FC devront être en mesure de se restructurer, de se réorganiser et d'établir de nouvelles priorités afin de répondre aux besoins. Afin d'accélérer l'apport précis du maintien en puissance, les décideurs doivent trouver des solutions en créant des outils d'anticipation et de prévision et en établissant des conventions collectives entre le gouvernement du Canada et les partenaires nationaux et internationaux. En raison de la grande diversité des partenaires disponibles pour répondre aux besoins de la fonction de maintien en puissance, ces réseaux peuvent s'adapter plus facilement en réunissant des partenaires selon les besoins et pour aussi longtemps qu'il le faudra.

6.5 Protection

La fonction future de protection est définie comme « l'approche globale de la protection des éléments matériels et immatériels par le biais des activités d'intégration de détection, d'évaluation, d'avertissement, de défense (active et passive) et de récupération.

Afin de protéger efficacement les FC à l'avenir, une bonne compréhension de l'environnement stratégique, de l'ensemble des conditions (circonstances particulières) et en particulier des menaces est nécessaire. Les FC doivent bien comprendre ce qui doit être protégé : les ressources de défense corporelles (capacités, plate-formes, personnes et télécommunications nationales, entreprises, transports et infrastructures énergétiques) et incorporelles (intérêts culture, valeurs et volonté du pays; bien-être économique; opinion publique) devraient être incluses. Il faut aussi évaluer les meilleurs acteurs avec lesquels établir des partenariats en vue d'optimiser les capacités de protection.

Une réponse de protection multidimensionnelle nécessitera l'intégration transparente des acteurs compétents militaires, civils, alliés, issus d'autres ministères et d'ONG. Les partenaires devront dépendre les uns des autres en matière de renseignement, d'information et de capacité critique. Pour faciliter une telle intégration, il faut créer des réseaux entre la défense nationale et internationale et les organismes de sécurité. Ces réseaux humains pourront exister en reliant les capacités des partenaires par le biais des réseaux de l'ère de l'information.

La capacité future de protection doit être plus souple. La réponse doit non seulement être rapide, mais doit également pouvoir être rééchelonnée, restructurée dans n'importe quelle condition et, en cas de nouvelle menace ou de l'évolution d'une

menace et de sa portée, doit pouvoir être revue. Le niveau de protection doit s'adapter aux besoins du nœud critique afin de fournir le nécessaire à l'endroit et au moment où le besoin se fait sentir. Une partie de l'adaptation consiste en la capacité de la protection à adopter l'approche nécessaire à un moment donné : dissuader, empêcher, prévenir ou détecter, détourner, contrebalancer.

L'environnement de sécurité complexe a conduit à une augmentation des menaces contre lesquelles le Canada doit se protéger : certaines personnes ont accès à des capacités qui étaient autrefois du seul ressort des États, et les États les moins développés ont obtenu l'accès à des capacités que seuls les pays riches pouvaient se procurer autrefois. La complexité de l'environnement de sécurité a également révélé de nouvelles vulnérabilités, dont le domaine humain et le bien-être national, l'identité et l'unité. Une question clé demeure : comment pouvons-nous protéger le cyberespace dans une société transparente?

6.6 Mise sur pied

La fonction future de mise sur pied est « la méthode par laquelle le MDN et les FC recrutent, instruisent et forment le personnel, acquièrent du matériel, des infrastructures et des services, et font en sorte que l'ensemble des ressources soit prêt à répondre à la mission de défense ». La mise sur pied est une fonction institutionnelle. Le concept futur de mise sur pied doit décrire des capacités adaptatives et intégrées.

L'environnement stratégique de plus en plus complexe souligne le besoin de capacités de mise sur pied très adaptatives. Les FC doivent être en mesure de s'adapter, de se restructurer, de se réorganiser et de redéfinir la priorité d'une capacité de mise sur pied limitée afin de répondre aux besoins en constante évolution en matière de défense. Cet objectif sera atteint grâce à la mise en place progressive d'une technologie de l'ère de l'information et à des changements organisationnels et de procédés.

Afin de mieux s'adapter, le MDN et les FC doivent être capables de reconnaître le personnel apte à opérer dans un environnement exigeant sur le plan technique dans lequel plusieurs réseaux, à la fois humain et technique, sont omniprésents. Ces personnes – qu'il s'agisse membres de la Force régulière ou de la Force de réserve des FC ou de civils – auront besoin d'instruction, d'éducation et de perfectionnement professionnel pour leur permettre d'employer les caractéristiques de l'adaptation. Cela permettra au personnel nécessaire de répondre aux attentes du gouvernement du Canada, comme en témoigne la SDCA.

« Pour exécuter ces missions, les Forces canadiennes devront être entièrement intégrées, souples, polyvalentes et aptes au combat, et elles devront travailler de concert avec le personnel civil compétent et réactif du ministère de la Défense nationale. »

Stratégie de défense *Le Canada d'abord,* p. 3.

La pratique future pourrait voir tous les membres du MDN et des FC employés et rapidement affectés à des postes fondés sur une adéquation des compétences qui va au-delà des étiquettes Force régulière, Force de réserve et civil. L'intégration devient un élément essentiel. La mise en place d'un poste civil de professionnel de la sécurité et de la défense est une idée qui met en évidence l'intégration potentielle du personnel civil du MDN, de la Gendarmerie royale du Canada, du Service canadien du renseignement de sécurité et de l'Agence des services frontaliers du Canada.

Il est également nécessaire d'avoir recours à une approche plus intégrée pour la création et le développement de la capacité qui s'adaptera aux nouvelles menaces dans un avenir dynamique et incertain. Il faut intégrer de manière stratégique l'emploi, la mise sur pied et le développement d'une force dans un système global de gestion de l'état de préparation qui traite de la complexité de tous les ensembles de conditions, domaines et fonctions.

APERÇU 10

NOTRE VISION ACTUELLE DES FONCTIONS STRATÉGIQUES EST RÉGIE PAR NOS EXPÉRIENCES HISTORIQUES AINSI QUE NOS CONNAISSANCES DES DOMAINES TRADITIONNELS. LA VISION FUTURE DES FONCTIONS STRATÉGIQUES DOIT ÊTRE RÉGIE DE MANIÈRE GLOBALE, INTÉGRÉE, ADAPTATIVE ET RÉSEAUTÉE DANS TOUS LES DOMAINES.

6.7 Perspectives de la vision future des fonctions stratégiques

Afin d'éviter l'écueil de la planification du conflit d'hier, les développeurs de concepts et les planificateurs doivent sortir de notre schéma de pensée traditionnel dans les domaines maritime, terrestre et aérien. La vision future des fonctions stratégiques doit être régie de manière globale, intégrée, adaptée et réseautée. De plus, afin de rester pertinent sur le plan stratégique, réactif sur le plan opérationnel et ferme sur le plan tactique dans l'environnement stratégique complexe, une bonne compréhension des effets requis par chacune de ces fonctions pour chaque condition et domaine distincts est essentielle. Néanmoins, des questions fondamentales

demeurent sans réponses, comme « En quoi les trois nouveaux domaines vont-ils changer les fonctions des FC? ».

RÉPERCUSSIONS STRATÉGIQUES

L'incapacité à comprendre les similitudes et les différences des fonctions liées aux domaines en expansion et aux conditions dynamiques se traduira par la « planification des conflits d'hier ».

Les concepts futurs des fonctions (commandement, détection, action, maintien en puissance, protection, mise sur pied) doivent décrire des capacités globales, intégrées, adaptatives et réseautées.

Le concept futur de commandement doit comprendre l'efficacité d'une approche pluridisciplinaire afin de résoudre, de gérer et de contenir de nombreux types de problèmes et en vue d'intégrer les forces dans l'organisme global plus large.

Le concept futur de détection devrait utiliser des réseaux hautement intégrés afin de partager l'information en temps opportun, mais la fonction devrait également être capable d'utiliser des réseaux ad hoc ou propres à la mission.

Dans le cadre du concept futur d'action, les forces doivent s'adapter. Les FC seront plus en mesure de contrecarrer une action contradictoire imprévisible si elles peuvent se restructurer face à une nouvelle menace (flexibilité), rediriger les effets rapidement (agilité), faire tout cela rapidement (réactivité) et de manière soutenue pendant une période prolongée (endurance).

Dans le cadre du concept futur de maintien en puissance, un réseau de la grande diversité des partenaires disponibles doit plus facilement s'adapter et être rassemblé au besoin et pour aussi longtemps que nécessaire afin de répondre aux besoins.

En ce qui concerne le concept futur de protection, les FC doivent avoir une vision globale des vulnérabilités du Canada : les ressources de défense corporelles (capacités, plate-formes, personnes, télécommunications nationales, entreprises, transports et infrastructures énergétiques) et incorporelles (intérêts nationaux, culture, valeurs et volonté, bien-être économique; opinion publique) devraient être incluses.

En ce qui concerne le concept futur de mise sur pied, il est nécessaire d'intégrer de manière stratégique l'emploi, la mise sur pied et le développement d'une force dans un système global de gestion de l'état de préparation qui traite de la complexité de tous les ensembles de conditions, domaines et fonctions.

Afin de s'intégrer et de s'adapter, le MDN et les FC devront mettre en place un personnel compétent, capable d'agir dans des situations complexes, ce qui implique la création d'un poste civil de « professionnel de la défense » et la possibilité d'un poste identique de« professionnel de la sécurité » pour le GC.

Afin de rester pertinent sur le plan stratégique, réactif sur le plan opérationnel et ferme sur le plan tactique dans les environnements stratégiques complexes, une bonne compréhension des effets requis par chacune de ces fonctions pour chaque condition et domaine distincts est essentielle.

7 CONCEPTION DU CADRE

Cette partie présente la conception du cadre et décrit son but. L'information contenue dans les parties précédentes est regroupée et les liens entre les conditions, les domaines et les fonctions sont examinés au niveau stratégique. L'utilisation de la conception du cadre comme outil pour la mise au point de la capacité et du concept est également abordée.

7.1 Conception du cadre et systèmes complexes

Un concept unique et partagé qui régit la relation entre les ensembles de conditions, les domaines et les fonctions est essentiel pour partager la vision, le but et l'action visant l'emploi, la mise sur pied et le développement d'une force intégrée.

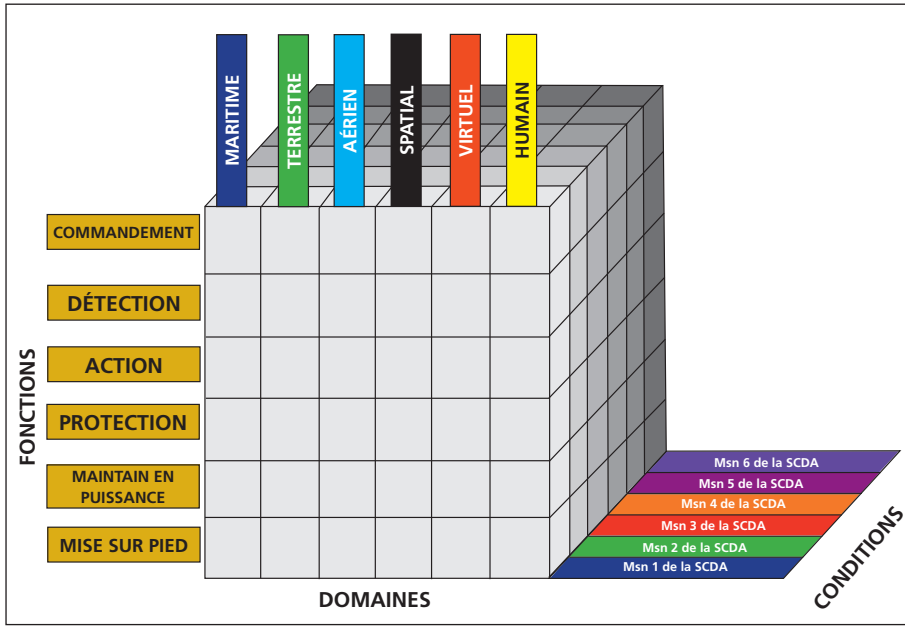

FIGURE 15: LA CONCEPTION DU CADRE.

La conception du cadre ne représente ni une tentative de modélisation du contexte de sécurité futur et des FC, ni une tentative de déconstruction de sa complexité inhérente. Un véritable système complexe ne peut, par définition, être défini, déconstruit et délimité.

Toutefois, il est nécessaire de déterminer l'éventail des conditions à examiner ainsi que les rapports au sein des systèmes complexes. Il faut également bien comprendre et représenter les interdépendances et les rapports mutuels entre les

ensembles de conditions, les domaines et les fonctions. Il pourrait également y avoir des domaines où nous pourrions établir les limites. Si nous pouvons, nous devons le faire. La conception du cadre répond à ces besoins.

7.2 Relations entre les ensembles de conditions, les domaines et les fonctions

La conception du cadre se fonde sur l'analyse des ensembles de conditions, des domaines et des fonctions futures afin de comprendre les interactions entre ces trois axes. Dans le cas d'un ensemble de conditions particulier, chacune des six fonctions des FC peut être analysée dans chacun des domaines de l'environnement stratégique. Chaque bloc de la conception peut être utilisé pour décrire une fonction particulière dans un domaine particulier pour une condition particulière en vue de déterminer quels effets sont nécessaires pour être pertinent sur le plan stratégique, réactif sur le plan opérationnel et ferme sur le plan tactique. La conception sert également de cadre à la comparaison des similitudes et des différences.

Ce qui se vérifie dans un bloc ne se vérifiera probablement pas pour un autre ensemble de conditions, tout simplement parce que les conditions sont de nature complexe.

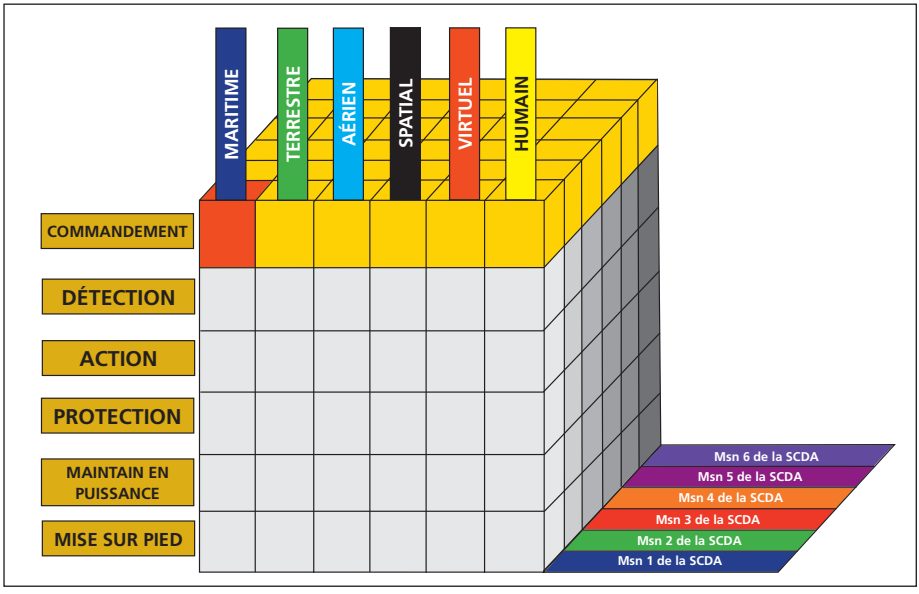

FIGURE 16 : ANALYSER LE COMMANDEMENT DANS LE DOMAINE MARITIME DANS LE CADRE DE LA MISSION 1 DE LA SDCA.

Comme l'illustre la figure 16, une fois les besoins de la fonction de commandement déterminés pour les opérations quotidiennes nationales et continentales, ceux-ci peuvent être comparés aux besoins de commandement correspondants dans les autres domaines, pour la même mission. Par ailleurs, les besoins de la fonction de commandement dans le domaine maritime peuvent être comparés à un large éventail d'ensembles de conditions (missions de la SDCA), permettant ainsi d'avoir une vision d'ensemble des besoins en capacités du commandement maritime. Ce processus peut être reproduit pour un large éventail d'interactions entre les fonctions et les domaines. Par exemple, en quoi le commandement, dans le cadre de la mission 1 de la SDCA, diffère des domaines maritime et aérien?

En utilisant la conception du cadre, les besoins communs ainsi que les différences fondamentales qui sous-tendent un effort collectif peuvent être déterminés, tout comme les éléments communs et les besoins particuliers des ensembles de conditions, des domaines et des fonctions particuliers. Cette analyse comparative démontrera ce qui est commun à tous et ce qui est unique, et indiquera la nature des besoins collectifs pour produire des effets intégrés.

En utilisant la conception du cadre, les besoins communs ainsi que les différences fondamentales qui sous-tendent un effort collectif peuvent être déterminés, tout comme les éléments communs et les besoins particuliers des ensembles de conditions, des domaines et des fonctions particuliers.

La conception du cadre fournit un cadre analytique commun aux développeurs de capacités et de concepts ainsi qu'aux planificateurs stratégiques. Un développeur de concept peut utiliser la conception du cadre en vue de déterminer les besoins de la fonction de détection dans le domaine aérien nécessaire pour faire face à un événement terroriste majeur au Canada. En utilisant la même conception, le développeur de capacités peut étudier quelles capacités, autorités, structures et quels procédés sont nécessaires à la fonction de détection dans le domaine virtuel pour la même mission. Le planificateur stratégique peut utiliser la conception du cadre afin de déterminer les besoins d'intégration, de commandement et de contrôle de la fonction de détection dans les missions.

7.3 Cadre conceptuel – Concepts d'intégration, concepts opérationnels et concepts habilitants

La conception du cadre fournit également un cadre pour la création de concepts et la compréhension d'une hiérarchie de concepts. C'est en examinant la conception de trois points de vue différents que les concepts d'intégration, les concepts opérationnels et les concepts habilitants peuvent être systématiquement mis au point.

APERÇU 11

CE N'EST QU'EN AYANT UNE VISION D'ENSEMBLE DES RELATIONS ENTRE LES ENSEMBLES DE CONDITIONS, LES DOMAINES ET LES FONCTIONS QUE NOUS POUVONS DÉTERMINER LE BESOIN D'ÊTRE GLOBAL, INTÉGRÉ, ADAPTATIF ET RÉSEAUTÉ.

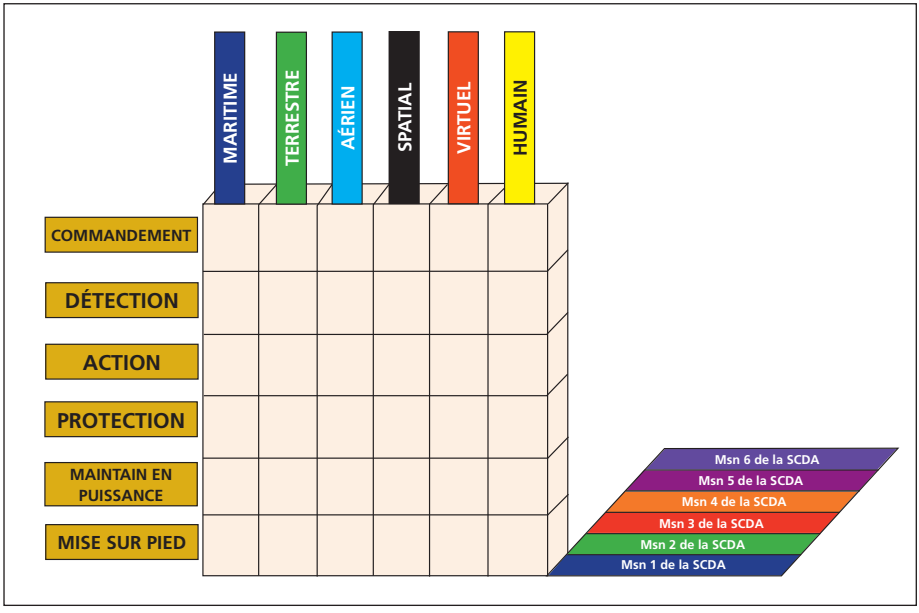

FIGURE 17 : CONCEPTS D'INTÉGRATION.

Des concepts d'intégration peuvent être mis au point en tenant compte des relations collectives d'une application globale, intégrée, adaptative et réseautée de l'intérêt national dans un ensemble de conditions particulier.

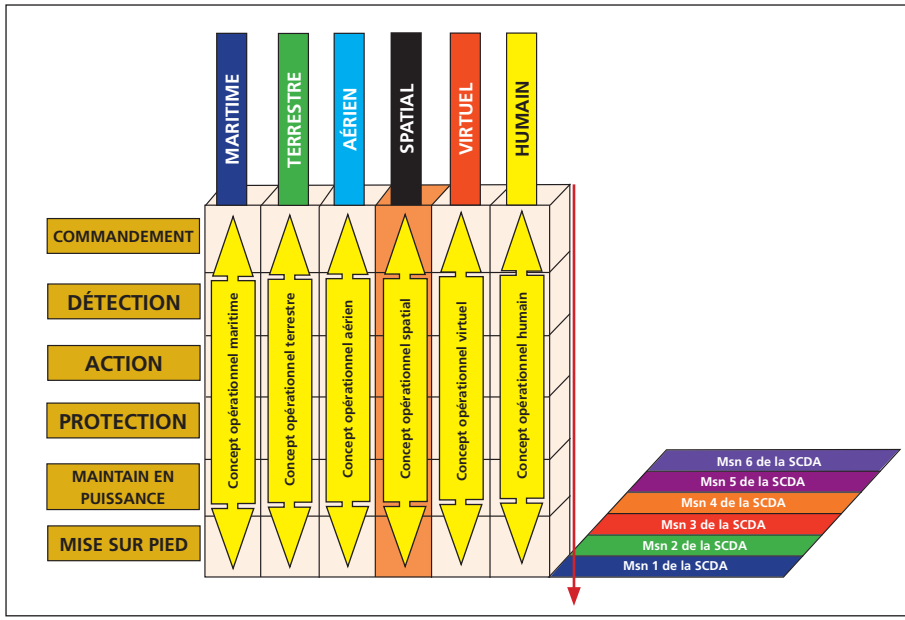

FIGURE 18 : CONCEPTS OPÉRATIONNELS.

Des concepts opérationnels peuvent être mis au point en vue de décrire les besoins (fondés sur les six fonctions) d'un environnement particulier dans le cadre d'une mission particulière. Ces concepts comprennent la relation collective d'une application globale, intégrée, adaptative et réseautée de l'intérêt national dans un domaine particulier et un ensemble de conditions particulier. (p. ex. concept opérationnel spatial dans le cadre de la mission 1 de la SDCA).

La conception du cadre peut également être utilisé afin de développer des outils habilitants méthodologiques ou technologiques (concepts habilitants) qui couvrent une grande variété de missions, de domaines et de fonctions. À titre d'exemple, l'approche exhaustive est un concept habilitant méthodologique. L'intelligence artificielle, d'autre part, serait un concept habilitant technologique qui pourrait entraîner une nouvelle gamme de répercussions en étant pertinentes sur le plan stratégique, réactives sur le plan opérationnel et décisives sur le plan tactique.

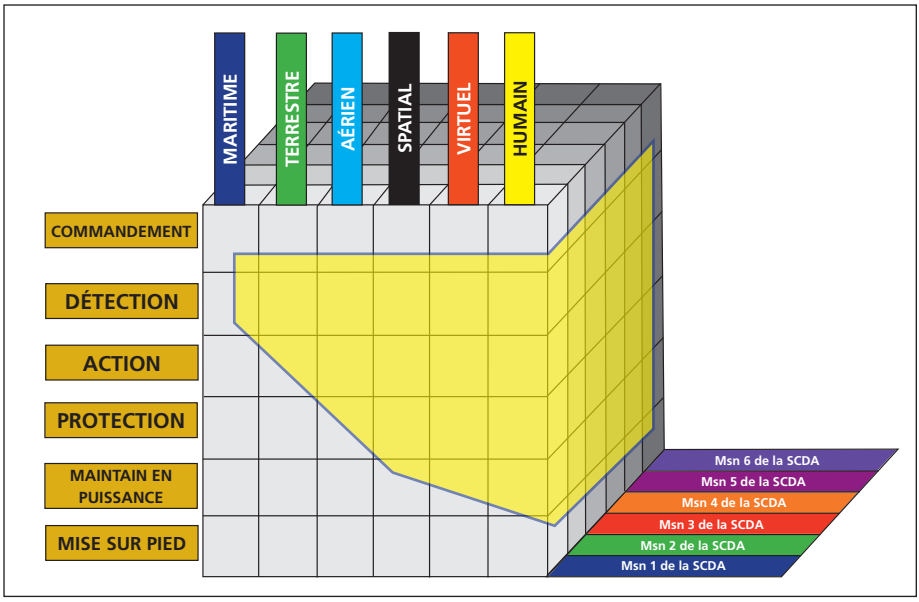

FIGURE 19 : CONCEPTS HABILITANTS.

La conception du cadre est un outil destiné aux développeurs de concepts, aux gestionnaires des capacités et aux planificateurs stratégiques et qui a pour but de les aider à établir des niveaux d'ambition et à analyser le risque.

À l'avenir, la conception du cadre se développera dans la mesure où le nombre de facteurs et de défis présents dans le contexte de sécurité futur augmentera le niveau de complexité. Ainsi, dans la mesure où l'environnement stratégique continuera de se développer à l'avenir, davantage de domaines seront susceptibles de voir le jour. La même perspective d'expansion existe pour les ensembles de conditions et les fonctions.

RÉPERCUSSIONS STRATÉGIQUES

Un concept unique et partagé qui régit la relation entre les ensembles de conditions, les domaines et les fonctions est essentiel pour partager la vision, le but et l'action visant l'emploi, la mise sur pied et le développement d'une force intégrée.

La conception du cadre aide les décideurs à établir des niveaux d'ambition et à analyser le risque.

À l'avenir, la conception du cadre se développera. Dans la mesure où l'environnement stratégique continuera de se développer à l'avenir, davantage de domaines seront susceptibles de voir le jour. La même perspective d'expansion existe pour les ensembles de conditions et les fonctions.

8 RÉSUMÉ DES APERÇUS ET DES RÉPERCUSSIONS STRATÉGIQUES

Comprendre les implications que la complexité du concept entraîne est essentiel à la réussite stratégique des FC. Il est également fondamental de comprendre la nature changeante de nos adversaires, les domaines dans lesquels nous agissons et les types d'opérations que les FC devront mener. Afin de relever ces défis, nous devrons former une force militaire intégrée, polyvalente et apte au combat qui devra être globale, intégrée, adaptative et réseautée en vue de réaliser l'intention du pays.

APERÇUS	RÉPERCUSSIONS STRATÉGIQUES
Aperçu 1 : L'environnement stratégique a toujours été dominé par des questions de complexité. Cependant, le nombre de facteurs et de défis présents dans le contexte de sécurité futur augmentera sensiblement les niveaux de complexité.	• Les défis imposés par l'environnement de sécurité complexe de l'avenir exigent l'élaboration d'approches globales, intégrées, adaptatives et réseautées. Ces attributs doivent ainsi devenir les principes régissant la nature des FC de l'avenir et la nécessité d'être pertinent sur le plan stratégique, réactif sur le plan opérationnel et décisif d'un point de vue tactique.
Aperçu 2 : Comprendre les conséquences que les systèmes complexes représenteront dans le contexte de sécurité futur est essentiel à la réussite stratégique des FC. L'environnement de sécurité de l'avenir sera influencé par une gamme de plus en plus large de systèmes complexes dynamiques et adaptatifs.	• Il est essentiel de comprendre le nombre grandissant d'agents affectant la sécurité à l'échelle nationale et internationale, la nature changeante de nos adversaires, les conséquences des interactions des différents groupes, la nature imprévisible et non linéaire des actions et des comportements, les domaines dans lesquels nous mènerons nos opérations et les types d'opérations que les FC devront mener. • Les outils linéaires existants et les concepts hérités que nous utilisons afin de résoudre les problèmes ne seraient peut-être pas adaptés aux défis imposés par les systèmes complexes futurs.
Aperçu 3 : L'environnement stratégique dynamique et complexe sera dans l'avenir influencé par une gamme grandissante d'acteurs technologiquement et socialement habilités qui seront mieux coordonnés et de plus en plus réseautés, et qui auront la même intention que l'antagoniste.	• L'accès général à la science et aux technologies (tel que les technologies spatiales et virtuelles et les technologies perturbatrices avancées) permet au plus rapide et au plus apte à acquérir et à exploiter ces nouvelles capacités d'obtenir l'avantage militaire, augmentant ainsi les capacités des antagonistes non étatiques à des niveaux qui rivalisent ceux des États.

APERÇUS	RÉPERCUSSIONS STRATÉGIQUES
Aperçu 4 : Cette perspective globale doit constituer en une approche pluridisciplinaire afin de relever les défis envisagés dans le document ESA qui dépassent de loin la portée et les capacités des FC seules.	• Les FC constituent l'un des instruments de puissance nationale et d'influence à la disposition du GC. • Les organismes non gouvernementaux peuvent également travailler dans un espace complexe afin de résoudre d'autres aspects d'une crise et peuvent ou non avoir les mêmes objectifs que le GC. • Il faut élaborer un cadre global afin de résoudre au mieux les situations complexes ou de les gérer.
Aperçu 5 : L'intégration dans le cadre d'une approche pluridisciplinaire garantira des meilleures chances de résoudre les questions complexes liées au contexte de sécurité futur que de travailler de manière indépendante.	• Le MDN et les FC devront modifier leur structure organisationnelle verticale et adopter des processus, des réseaux, des relations et des capacités permettant des opérations intégrées. • L'ensemble de l'institution devra intégrer au besoin d'autres organismes ou d'autres acteurs.

Aperçu 6 : L'adaptation est primordiale afin de faire face aux défis, aux situations et aux relations imprévisibles, incertaines et complexes. Les FC doivent être adaptatives au risque d'échouer.	• Afin d'être adaptatives, les FC ont besoin :
	  • De chefs capables de reconnaître les conséquences des tendances nouvelles et de réagir aux chocs stratégiques.
	  • De commandants qui n'ont pas peur d'adopter des solutions innovantes et non conventionnelles.
	  • De personnes qui, comme nos adversaires, projettent d'utiliser du matériel et des capacités avec de nouveaux moyens innovateurs.
	  • De soldats, de marins et de personnel aérien capables de déceler un changement dans le plan d'action de l'adversaire et de l'exploiter au profit de la mission.

Aperçu 7 : Les FC doivent exploiter les réseaux sociaux et techniques dans l'environnement stratégique et dans tous les domaines face aux moyens techniques et sociaux de plus en plus nombreux utilisés par les antagonistes.	• Nos réseaux hiérarchiques actuels ne sont peut-être pas suffisants afin de garantir la réussite dans l'environnement de sécurité complexe de l'avenir. • Les FC devraient privilégier les réseaux intégrés ou hybrides plutôt que les réseaux hiérarchiques. • On a recours à la connectivité externe avec des organismes de défense et de sécurité

APERÇU	RÉPERCUSSIONS STRATÉGIQUES
	d'autres ministères, des alliés et des partenaires dans la mesure nécessaire en fonction des objectifs à atteindre. • Les réseaux sociaux et les réseaux techniques fournissent les moyens nécessaires aux FC afin d'être globales, intégrées et adaptatives en vue de relever les défis imposés par l'environnement de sécurité complexe.
Aperçu 8 : La gamme des conflits futurs ne se réduit plus à une connaissance linéaire de la paix, des opérations autres que la guerre et de la guerre.	• Les FC doivent être capables d'intervenir efficacement (de manière proactive et réactive) dans toute la gamme des conflits, que ce soit d'une manière conventionnelle ou non conventionnelle. • Étant donné que la nature du conflit est de plus en plus dynamique, la gamme des acteurs et des solutions s'agrandit proportionnellement et pourrait nécessiter la mise en place de mesures qui ne relèvent plus uniquement des forces militaires.
Aperçu 9 : L'environnement stratégique s'est étendu au-delà des domaines traditionnels (maritime, terrestre et aérien) et doit maintenant comprendre les domaines spatial, virtuel et humain. L'environnement stratégique continuera de s'élargir, ce qui intensifiera les questions de complexité et soulignera la nécessité pour les FC d'être globales, adaptatives et réseautées.	• Les États ne dominent plus de manière exclusive les domaines de l'environnement stratégique. • Les antagonistes actuels et futurs, qu'ils soient étatiques ou non, ont le pouvoir de créer des effets stratégiques dirigés contre les intérêts nationaux canadiens. • En attaquant ou en désactivant nos réseaux, un antagoniste peut facilement porter préjudice à nos capacités de commandement, de contrôle, de communications, d'informatique, de renseignement, de surveillance et de reconnaissance dans les domaines maritime, terrestre, aérien, et spatial. De plus, un antagoniste peut attaquer au cœur de nos infrastructures et de nos systèmes de soutien nationaux. • Un échec stratégique dans n'importe quel domaine pourrait entraîner un échec stratégique à l'échelle nationale. • Un échec dans le domaine humain, indépendamment du degré de réussite dans le reste de l'environnement stratégique, pourrait entraîner un échec stratégique à l'échelle nationale.

APERÇUS

RÉPERCUSSIONS STRATÉGIQUES

- Les FC doivent connaître les acteurs amis, antagonistes et neutres ainsi que les facteurs sous-jacents dictant les comportements humains.
- En utilisant les sciences humaines et comportementales, les FC peuvent mieux se positionner en vue de gérer et de limiter l'ampleur du conflit, de faciliter la collaboration entre tous les acteurs, de comprendre comment fonctionnent, s'adaptent et évoluent les réseaux entre les personnes, et de faciliter l'évaluation de la menace et la réduire.
- Les FC doivent comprendre la nature adaptative des réseaux humains antagonistes, ainsi que l'effet stratégique des opérations d'influence antagonistes combinées aux réseaux humains rendus possibles grâce à la technologie.
- Les nouveaux domaines ne suggèrent pas d'assumer la responsabilité, mais ils exigent le leadership.
- Les commandants à tous les niveaux doivent être prêts à gérer les effets infligés par les acteurs antagonistes faisant partie des six domaines, peut-être simultanément.
- Les commandants à tous les niveaux, en fonction de la nature de la mission, devront également être prêts à créer des effets relevant des six domaines simultanément et d'une manière intégrée et globale.
- Les domaines spatial, virtuel et humain sont trois domaines distincts où il est possible de mettre en application les instruments de puissance nationale et d'influence au même titre que les domaines traditionnels.
- Nos capacités à être pertinents sur le plan stratégique, réactifs sur le plan opérationnel et efficaces d'un point de vue tactique dans toute la gamme des conflits futurs dépendent essentiellement de nos capacités à se projeter et à contrer les effets dans tous ces domaines.

APERÇUS

Aperçu 10 : Notre vision actuelle des fonctions stratégiques est régie par nos expériences historiques ainsi que nos connaissances des domaines traditionnels. La vision future des fonctions stratégiques doit être régie de manière globale, intégrée, adaptative et réseautée dans tous les domaines.

RÉPERCUSSIONS STRATÉGIQUES

- L'incapacité à comprendre les similitudes et les différences entre les fonctions liées aux domaines en expansion et les conditions dynamiques se traduira par la « planification des conflits d'hier ».
- Les concepts futurs des fonctions (commandement, détection, action, maintien en puissance, protection, mise sur pied) doivent décrire des capacités globales, intégrées, adaptatives et réseautées.
- Le concept futur de commandement doit comprendre l'efficacité d'une approche pluridisciplinaire afin de résoudre, de gérer et de contenir de nombreux types de problèmes et en vue d'intégrer les forces dans l'organisme global plus large.
- Le concept futur de détection devrait utiliser des réseaux hautement intégrés afin de partager l'information en temps opportun, mais la fonction devrait également être capable d'utiliser des réseaux ad hoc ou propres à la mission.
- Dans le cadre du concept futur d'action, les forces doivent s'adapter. Les FC seront plus en mesure de contrecarrer une action contradictoire imprévisible si elles peuvent se restructurer face à une nouvelle menace (flexibilité), rediriger les effets rapidement (agilité), faire tout cela rapidement (réactivité) et de manière soutenue pendant une période prolongée (endurance).
- Dans le cadre du concept futur de maintien en puissance, un réseau de la grande diversité des partenaires disponibles doit plus facilement s'adapter et être rassemblé au besoin et pour aussi longtemps que nécessaire afin de répondre aux besoins.
- En ce qui concerne le concept futur de protection, les FC doivent avoir une vision globale des vulnérabilités du Canada : les ressources de défense corporelles (capacités, plate-formes, personnes, télécommunications nationales, entreprises, transports et infrastructures énergétiques) et incorporelles (intérêts nationaux, culture, valeurs et volonté, bien-être économique; opinion publique) devraient être incluses.

APERÇUS	RÉPERCUSSIONS STRATÉGIQUES
	• En ce qui concerne le concept futur de mise sur pied, il faut intégrer de manière stratégique l'emploi, la mise sur pied et le développement d'une force dans un système global de gestion de l'état de préparation qui traite de la complexité de tous les ensembles de conditions, domaines et fonctions. • Afin de s'intégrer et de s'adapter, le MDN et les FC devront mettre en place du personnel compétent, capable d'agir dans des situations complexes, ce qui implique la création d'un poste civil de « professionnel de la défense » et la possibilité d'un poste identique de« professionnel de la sécurité » pour le GC. • Afin de rester pertinent sur le plan stratégique, réactif sur le plan opérationnel et ferme sur le plan tactique dans les environnements stratégiques complexes, une bonne compréhension des effets requis par chacune de ces fonctions pour chaque condition et domaine distincts est essentielle.
Aperçu 11 : Ce n'est qu'en ayant une vision d'ensemble des relations entre les ensembles de conditions, les domaines et les fonctions que nous pouvons déterminer le besoin d'être global, intégré, adptatif et réseauté.	• Un concept unique et partagé qui régit la relation entre les ensembles de conditions, les domaines et les fonctions est essentiel pour partager la vision, le but et l'action visant l'emploi, la mise sur pied et le développement d'une force intégrée. • La conception du cadre aide les décideurs à établir des niveaux d'ambition et à analyser le risque. • À l'avenir, la conception du cadre se développera. Dans la mesure où l'environnement stratégique continuera de se développer à l'avenir, davantage de domaines seront susceptibles de voir le jour. La même perspective d'expansion existe pour les ensembles de conditions et les fonctions.

9 BIBLIOGRAPHIE

Documents du ministère de la Défense nationales

Ministère de la Défense nationale. *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations*, Kingston, Académie canadienne de la Défense – Institut sur le leadership des Forces canadiennes, 2008.

--- Doctrine B-GG-005-004/AF-101 *Opérations d'information des FC*, Ottawa, Ministère de la Défense nationale, 1998.

--- *Loi sur la défense nationale* (R.S., 1985, c. N-5) disponible sur le site Web du ministère de la Justice, 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 [consulté le 23 juin 2009].

--- *Manuel des abréviations des Forces canadiennes/de la Défense nationale*, Ottawa, Chef d'état-major de l'Armée de terre.

--- *Servir avec honneur : la profession des armes au Canada*, Kingston, Académie canadienne de la Défense – Institut sur le leadership des Forces canadiennes, 2003. http://www. cda.forces.gc.ca/cfli-ilfc/doc/dwh-eng.pdf [consulté le 31 mars 2009].

--- *Stratégie de défense Le Canada d'abord*, Ottawa, Ministère de la Défense nationale, 2008.

Documents d'analyse de la sécurité future

Ministère de la Défense nationale. « Concept du domaine de capacité : Action », Ottawa, Chef – Développement des forces, 2008.

--- « Concept du domaine de capacité : Commandement », Ottawa, Chef – Développement des forces, 2008.

--- « Concept du domaine de capacité : Détection », Ottawa, Chef – Développement des forces, 2008.

--- « Concept du domaine de capacité : Maintien en puissance », Ottawa, Chef – Développement des forces, 2008.

--- « Concept du domaine de capacité : Mise sur pied », Ottawa, Chef – Développement des forces, 2008.

--- « Concept du domaine de capacité : Protection », Ottawa, Chef – Développement des forces, 2008.

--- « Document de travail sur le Concept cadre intégré, août 2008 », Ottawa, Chef – Développement des forces, 2008.

--- « Document de travail sur la nature des conflits futurs », Ottawa, Chef – Développement des forces, 2009.

--- « Document de travail sur la nature des environnements futurs », Ottawa, Chef – Développement des forces, 2008.

--- « Document de travail sur la nature des fonctions futures », Ottawa, Chef – Développement des forces, 2009.

--- *L'environnement de la sécurité future 2008-2030. Partie 1 : Tendances actuelles et émergentes*, Ottawa, Chef – Développement des forces, 2009.

--- « Nature des futurs environnements : environnement virtuel », Ottawa, Chef – Développement des forces, 2009.

Théorie de la complexité

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*, traduit par Rita et Robert Kimber, New York, Metropolitan Books, 1996.

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

Nouveaux domaines

Domaine virtuel

Air University. « Qu'est-ce que les opérations d'information? » sur le site Web du Centre d'études sur les opérations d'information et sur le cyberespace, http://www.au.af.mil.info-ops/what.htm [consulté le 13 mars 2009].

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

--- John J. Gastka and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2e Édition (révisée), Washington D.C., DoD Command and Control Research Program, août 1999.

« America Prepares for Cyber War », http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/06/1 5/wcyber1 1 5.xml [consulté le 9 avril 2008].

« Analysis: DHS Stages Cyber War Exercise 10 Mar 2008 », sur le site Web Space War : Your World at War http://www.spacewar.com/reports/Analysis D HS stages cyberwar exercise 999.html [consulté le 9 avril 2008].

Arquilla, John. et David Ronfeldt. *Cyberwar is Coming: Comparative Strategy 12.2*, Spny 1993, p. 141-165.

Bowie, Christopher J., Robert P. Haffa Jr et Robert E. Mullins. « Trends in Future Warfare », *Joint Force Quarterly*, été 2003, http://findarticles.com/p/articles/mim0KNN/is 35/ai n8563330 [consulté le 23 avril 2008].

« C4ISR Strategy 2028 », Ébauche de la nouvelle version C4ISR OC 2.0 (24 novembre 2008).

Chuka, Neil S. « Confusion et désaccord : la doctrine des opérations d'information des États-Unis, du Royaume-Uni, de l'Australie, du Canada et de l'OTAN », Kingston : Mémoire de maîtrise du CMR, septembre 2007.

Cordray, Robert et Marc J. Romanych. « Mapping the Information Environment », *IO Sphere – La Revue professionnelle des opérations d'information interarmées*, été 2005, http://www.au.af.mil/info-ops/iosphere/iosphere_summer05_cordray.pdf [consulté le 18 février 2009].

Département américain de la Défense. *C4ISR Architecture Framework*, Version 2, Washington D.C., Département de la Défense, 18 décembre 1997, http://www.afcea.org/ education/courses/archfwk2 .pdf [consulté le 31 mars 2009].

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

--- *Effects-based Operations White Paper*, Version 1.0, Norfolk, Département J9 des concepts de commandement des forces interarmées, 2001.

--- *Information Operations Roadmap*, Washington D.C., Département de la Défense, 30 octobre 2003, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info ops roadmap.pdf [consulté le 8 avril 2008].

---- *Joint Communication System* (US), Joint Publication 6-0, Washington D.C., Département de la Défense, 6 mars 2006.

--- *Joint Doctrine for Information Operation*, Joint Publications 3-13, Washington, D.C., Département de la Défense, 9 octobre 1998.

--- Site Web du Command and Control Research Program, http://www.dodccrp.org/ [consulté le 31 mars 2000].

Federman, Mark. « On Reading McLuhan », http://individual.utoronto.ca/markfederman/On ReadingMcLuhan.pdf [consulté le 11 mars 2009].

--- « What is the Meaning of the Medium is the Message? », http://individual.utoronto. ca/markfederman/article mediumisthemessage.htm [consulté le 11 mars 2009].

Grande Bretagne. *Doctrine de la Défense britannique*, PDI 0-01, publication de doctrine interarmée 0-01 (PDI-0-01),3e Édition, Londres, Ministère de la Défense, août 2008.

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, juin 2008. http://se1.isn.ch/serviceengine/FileContent?serviceID=47&fileid=8463B1AA-EA8C¬D652-FD34-3450CA2B7FC5&lng=en [consulté le 31 mars 2009].

« Groupe de gestion de l'information : politiques et directives », sur le site Web du SMA(GI), http://img.mil.ca/poldir/index e.asp [consulté le 31 mars 2009].

Leiner, Barry M. « A Brief History of the Internet », http://www.isoc.org/internet/history/brief.shtml#Commercialization [consulté le 27 mars 2009].

Mattis, James N. « USJFCOM Commander's Guidance for Effects-based Operations », Joint Force Quarterly, 51 (4e trimestre 2008), http://www.dtic.mil/doctrine/jel/jfq pubs/ [consulté le 9 février 2009].

Melnick, John. « The Cyber War Against the United States », *Boston Globe*, 19 août 2007, httpi/www.boston.com/news/globe/editorial opin ion/oped/articles/2007/08/19/the cyberwar against the united states/ [consulté le 9 avril 2008].

Ministère de la Défense nationale. « Document de conception et feuille de route du MDN/des FC sur les opérations facilitées par réseaux », document de travail du MDN/des FC sur les opérations facilitées par réseaux, R et D pour la défense Canada, Rapport technique RDDC RT 2006-001, janvier 2006. http://esquimalt.mil.ca/cfp/f3ops/F3%20CNCIOP/C4ISR%20References/NEW%20CONC EPTS/NEOps.pdf [consulté le 18 mars 2009].

--- « Opérations facilitées par réseaux : réponse du MDN/des FC face au nouvel environnement de sécurité », Groupe de travail sur les OFR, 5 novembre 2004.

Romanych, Marc J. « A Theory Based View of IO », in *IO Sphere – La Revue professionnelle des opérations d'information interarmées*, printemps 2005, http://www.au.af.mil/info¬ops/iosphere/iosphere spring05 romanych.pdf, [consulté le 16 mars 2009].

Schramm, LCol Kent. « Cyberespace : opérations des réseaux informatiques », Présentation au groupe de travail sur le concept intégré, 25 février 2009, Ministère de la Défense nationale, Canada.

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

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

Weiss, Geoffrey F. « Exposing the Information Domain Myth: A New Concept for Air Force and Information Operations Doctrine », *Air and Space Power Journal*, printemps 2008, http://www.airpower.maxwell.af.mil/airchron icles/apj/apj08/spr08/ weiss.html [consulté le 31 mars 2009].

Weatherbee, T.G. *Remote Leadership*, Kingston, Académie canadienne de la Défense – Institut sur le leadership des Forces canadiennes, 2003.

Domaine humain

Alberts, David S. « Key Concepts for Information Superiority », présenté au bureau du secrétaire adjoint à la Défense, DoD américain, Washington, D.C., 28 mai 2001.

---. *Understanding Information Age Warfare*, Washington D.C., bureau du secrétaire adjoint à la Défense, 2001.

Chery, Sandra and Philip S.E. Farrell. « A Look At Behaviourism and Perceptual Control Theory in Interface Design », Ministère de la Défence nationale – Institut militaire et civil de médecine environnementale, 1998.

Comeau, Paul. Présentation à la Direction d'analyse et de recherche opérationnelle (Recherche et développement pour la défense Canada), 14 mai 2008.

« Control Systems Group – Studying, Understanding, Applying Perceptual Control Theory », http://www.perceptualcontroltheory.org/ [consultée le 3 novembre 2008].

Dahl, Arden B. « Command Dysfunction: Minding the Cognitive War », thèse présentée à la School of Advanced Airpower Studies, Alabama, Air University Maxwell AFB, juin 1996, http://www.au.af.mil/au/awc/awcgate/saas/dahl ab.pdf [consultée le 27 mars 2009].

Endsley, M. R. « Situation Awareness Measurement », *Human Factors*, 37 (1995), p. 65-84.

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

--- « Discussion Paper: Can Perceptual Control Theory Be Applied To Organization Information Processing », présenté lors de la conférence de 2007 du groupe des systèmes de contrôle (GSC), Université de Manchester, Royaume-Uni, http://www.psych-sci.manchester.ac.uk/aboutus/events/csgconference/proceedings.pdf [consulté le 31 mars2009].

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, sur le site Web du Center for the Study of Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence/csipublications/books-and-monographs/psychology-of-intelligenceanalysis/PsychofIntelNew.pdf [consulté le 27 mars 2009].

Huitt, W. « The Mind », in *Educational Psychology Interactive*, Valdosta, GA, Valdosta State University, mai 2001, http://chiron.valdosta.edu/whuitt/col/summary/ mind.html [consulté le 5 mai 2009].

Ministère de la Défence nationale. *Cultural Intelligence, Emotional Intelligence and the Canadian Forces Leader Development Concepts, Relationships and Measures*, ILFC TM 2007-01, décembre 2007.

Nicholson, Peter. *Effects-Based Strategy: Operations in the Cognitive Domain*, Volume 2 Numéro 1 (2006), http://www.securitychallenges.org.au/ArticlePDFs/vol2no1 Nicholson.pdf [consulté le 27 mars 2009].

Pigeau, Ross and Carol McCann. « Analysing Command Challenges using the Command and Control Framework », Rapport technique 2003-034, 2003 de RDDC.

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

---. *The Nature of PCT*, document présenté à l'American Educational Research Association, San Francisco, avril 1995.

Romanych, Marc. « Applying the Domains of Conflict to Information Operations », document présenté lors du 10e Congrès international de technologie et de recherche Commandement et contrôle, JB Management, Inc., Alexandria, VA.

Triandis, H.C. « Cultural Intelligence in Organizations » *Group and Organization Management*, 31.1 (février 2006), p. 20-26.

Autres

Agence OTAN de normalisation. *Glossaire OTAN de termes et définitions* (AAP-6), Bruxelles, OTAN, 1998.

Département américain de la Défense. *Doctrine for Joint Operations 3-0*, Washington, D.C., instance collégiale des chefs d'état-major, 2001.

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

---. « How has War Changed Since the End of the Cold War? », *Paramètres*, printemps 2005.

Pugliese, David. « Military Zeroes in on Taliban Bombers », *Ottawa Citizen*, 20 mai 2008, httpi/www.canada.com/ottawacitizen/news/story.html?id+32a2fe5c-7fab¬4fed-859f-d90466953618.

Verdon, John, LCdr Bruce C. Forrester et Zhingang Wang. *The Last Mile of the Market: How Networks, Participation and Responsible Autonomy Support Mission Command and Transform Personnel Management*, Ottawa, ébauche d'un document technique du DGRAPM, 2009.

10 LEXIQUE

10.1 Terminologie

Le CCI a défini le terme *environnement stratégique* comme « le lieu où s'exercent les éléments du pouvoir et de l'influence ». Le CCI a également préconisé un élargissement de la conception traditionnelle de l'environnement stratégique dans la mesure où les éléments du pouvoir et de l'influence peuvent s'exercer dans l'espace, le cyberespace et dans les aspects cognitifs, connectifs et affectifs de la condition humaine – ainsi que dans un environnement terrestre, maritime et aérien.

Ces six divisions ne sont pas désignées *environnements* dans le présent document parce que ce terme fait déjà référence aux forces aériennes, terrestres et maritimes (qui, au Canada, portent respectivement les noms de commandement maritime, commandement de la force terrestre et commandement aérien). De plus, ce terme implique des qualités organisationnelles particulières. Il y a également un débat quant à la la nature différente des divisions humaines et virtuelles du pouvoir et de l'influence, c'est-à-dire qu'elles ne sont pas de la même nature physique que les divisions terrestres, maritimes, aériennes et spatiales. Nous soutenons que d'un point de vue stratégique, la présence physique d'un environnement n'est qu'une des manières pour délimiter les divisions majeures du pouvoir et de l'influence.

Le terme *domaine* est défini par Webster comme un « domaine de pensée »[32]. L'*Oxford Concise Dictionary* définit le mot domaine comme une « sphère de contrôle ou d'influence »[33]. Ces définitions constituent la base de l'utilisation du terme *domaine* dans le CCI pour décrire l'environnement stratégique élargi comme étant composé des domaines terrestre, maritime, aérien, spatial, virtuel et humain.

Les six fonctions stratégiques des FC (commandement, détection, action, maintien en puissance, protection et mise sur pied) sont largement comprises et forment le deuxième des trois axes du CCI.

10.2 Glossaire

TERME	USAGE	ORIGINE
Action	L'utilisation militaire des capacités en vue d'atteindre les résultats voulus à l'appui de la politique nationale.	Canada (Ébauche du CDF)[34]
Adaptatif	Capable de répondre aux changements et aux défis de manière positive; requiert intelligence, résilience, robustesse, souplesse, agilité, créativité, réactivité et endurance.	CCI

TERM	USAGE	ORIGIN
Art opérationnel	L'emploi de forces pour atteindre des objectifs stratégiques et/ou opérationnels par la conception, l'organisation, l'intégration et la mise en place de stratégies, de campagnes, d'opérations majeures et de batailles. Habileté à employer des forces militaires pour atteindre des objectifs stratégiques dans un théâtre de guerre ou un théâtre d'opérations par la conception, l'organisation et l'exécution de campagnes et d'opérations majeures.	Canada[35]
Commandement	L'exercice créatif et délibéré d'autorité légitime en vue d'accomplir la mission légalement, avec professionnalisme et de façon éthique.	Canada (Ébauche du CDF)[36]
Complexité	« Les systèmes complexes forment une nouvelle approche en matière de science qui étudie la façon dont les relations entre les composants créent des comportements collectifs dans un système et la façon dont les éléments du système interagissent et créent des liens avec leur environnement. »	Yaneer Bar-Yam[37]
Concept habilitant	Concepts qui développent des outils habilitants méthodologiques ou technologiques et couvrent une grande variété de missions, de domaines et de fonctions.	CCI
Concept d'intégration	Concepts mis au point en tenant compte des relations collectives dans le cas d'une condition particulière.	CCI
Concept opérationnel	Concepts mis au point en vue de décrire les besoins (fondés sur les six fonctions) d'un domaine particulier dans le cadre d'une mission particulier.	CCI
Contexte de sécurité futur, ou Environnement de sécurité de l'avenir	La projection des tendances et des chocs dans le futur. Les tendances sont économiques et sociales, environnementales et associées aux ressources, géopolitiques, scientifiques et technologiques, militaires et associées à la sécurité.	Canada (CDF)
Cyberespace	Désigne le matériel et les interactions sociales qui se produisent dans le monde virtuel.	CCI
Détection	L'acquisition et le traitement de l'information pour permettre aux commandants et aux autorités de comprendre les caractéristiques et les conditions de l'environnement opérationnel liées à la prise de décision militaire.	Canada (Ébauche du CDF)[38]
Domaine	Divisions principales au sein de l'environnement stratégique dans lesquelles s'exercent les éléments du pouvoir national et de l'influence : maritime, terrestre, aérien, spatial, virtuel et humain.	CCI
Ensemble de conditions	Conditions (circonstances) résultant de la combinaison des missions assignées dans le cadre de la SDCA et des attentes du gouvernement du Canada.	CCI

TERM	USAGE	ORIGIN
Environnement stratégique	Endroit où s'exercent les éléments du pouvoir et de l'influence.	CCI
Fonctions	Manière dont les FC mènent leurs opérations par le commandement, l'action, la détection, le maintien en puissance, la protection et la mise sur pied.	CCI
Global	Bien comprendre l'environnement stratégique; avoir une définition précise du problème et avoir fixé des objectifs adaptés; avoir la capacité d'appliquer une approche pluridisciplinaire.	CCI
Intégré	Élargissement des termes interarmées ou combiné afin d'inclure d'autres acteurs et organismes du gouvernement du Canada autre que le MDN.	CCI
Interopérabilité	La capacité des systèmes à fournir de l'information et des services à d'autres systèmes et à recevoir de l'information et des services d'autres systèmes et leur capacité à utiliser l'information et les services ainsi échangés.	Canada et OTAN
Maintien en puissance	La fourniture de tous les services de soutien nécessaires aux opérations courantes et de contingence – nationales, continentales et expéditionnaires – y compris les opérations prolongées.	Canada (Ébauche du CDF)[39]
Mise sur pied	La méthode par laquelle le MDN et les FC recrutent, instruisent et forment le personnel, acquièrent du matériel, des infrastructures et des services, et font en sorte que l'ensemble des ressources est prêt à répondre à la mission de défense.	Canada (Ébauche du CDF)[40]
Problème	La combinaison des trois rôles des FC (défendre le Canada, défendre l'Amérique du Nord, contribuer à la paix et à la sécurité internationales) et les défis du contexte de sécurité futur.	CCI
Protection	L'approche globale de la protection des éléments matériels et immatériels par les activités d'intégration de détection, d'évaluation, d'avertissement, de défense (active et passive) et de récupération.	Canada (Ébauche du CDF)[41]
Réseauté	Relations et interconnectivité entre les humains et/ou la technologie	CCI
Stratégique	Niveau auquel un pays ou un groupe de pays, fixe des objectifs de sécurité à l'échelle nationale ou multinationale et déploie des ressources nationales, notamment militaires, pour les atteindre. Le niveau stratégique correspond à ce niveau de guerre auquel une nation, souvent en tant que membre d'un groupe de nations, détermine des objectifs et des orientations stratégiques nationaux ou multinationaux (alliance ou coalition) et développe et emploie des ressources nationales pour réaliser ces objectifs.	OTAN[42] Opérations interarmées 3-0[43]

TERM	USAGE	ORIGIN
Tactique	Le niveau tactique porte sur la planification et l'exécution des batailles, des engagements et des activités pour atteindre les objectifs militaires assignés aux unités tactiques ou aux forces opérationnelles (FO).	Opérations interarmées 3-0[44]
Tactique	La menace ou le recours à n'importe quelles forces armées. Une action ou une stratégie soigneusement planifiée en vue d'atteindre un but spécifique. L'art de disposer les forces armées en ordre de bataille et d'organiser des opérations, en particulier en contact avec un ennemi. L'art de disposer des forces navales, terrestres et aériennes en contact immédiat avec l'ennemi.	Dictionnaire Oxford [45] Canada[46]

11 LISTE D'ACRONYMES

ACRONYME	SIGNIFICATION
ADM	Armes de destruction massive
AE	Approche exhaustive
AM	Autres ministères
ASAT	Antisatellite
ASFC	Agence des services frontaliers du Canada
CCI	*Concept cadre intégré*
CDF	Chef – Développement des Forces
CNA	Attaque de réseaux informatiques
CND	Défense des réseaux informatiques
CNE	Exploitation non autorisée de réseaux informatiques
CNO	Opérations de réseaux informatiques
CST	Centre de la sécurité des télécommunications
DASF	Directeur – Analyse de la sécurité future
DIMEFIL	Diplomatie, information, militaire, économie, finance, renseignement et application de la loi
ESA	*L'environnement de la sécurité future*
FC	Forces canadiennes
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
IED	Dispositif explosif de circonstance
ILFC	Institut sur le leadership des Forces canadiennes
MDN	Ministère de la Défense nationale
ONG	Organisation non gouvernementale
OTAN	Organisation du Traité de l'Atlantique Nord
PE	Protocole d'entente
PPOFC	Processus de planification opérationnelle des Forces canadiennes
RDDC	Recherche et développement pour la défense Canada
S et T	Sciences et technologie
SAC	Systèmes adaptatifs complexes
SCRS	Service canadien du renseignement de sécurité
SDCA	Stratégie de Défense *Le Canada d'abord*
SP	Sécurité publique Canada

12 NOTES

1 Ministère de la Défense nationale, *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations*, Kingston : Institut sur le leadership des Forces canadiennes, 2008. Le personnel interrogé avait de l'expérience dans divers domaines et représentait le personnel civil canadien et militaire étranger doté d'une vaste expérience des opérations des 15 dernières années à tous les niveaux – tactique, opérationnel, stratégique et politico-stratégique.

2 *Broadsword or Rapier*, p. 21.

3 Ministère de la Défense nationale, *L'environnement de la sécurité future 2008-2030 Partie 1 : Tendances actuelles et émergentes*, Ottawa, Chef – Développement des forces, 2009, p. 91.

4 Francis Heylighen, rubrique « Complexity and Self-Organization » de l'*Encyclopaedia of Library and Information Sciences*, Taylor et Francis, 2008, p. 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? », dans *Discover* (février 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 », p. 1, 4.

9 Heylighen, « Complexity and Self-Organization », p. 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 L'interdépendance fait partie de l'étude des systèmes complexes qui nous aide à reconnaître et comprendre les effets indirects. Yaneer Bar-Yam. *Making Things Work: Solving Complex Problems in a Complex World*, Cambridge, MA, NECSI/Knowledge Press, 2004, p. 27-29.

14 *L'environnement de la sécurité future*, p. 5-9.

15 Gouvernement du Canada, Stratégie de Défense *Le Canada d'abord*, Ottawa, Ministère de la Défense nationale, 2008, p. 7.

16 Ne pas confondre la perspective globale avec « l'approche exhaustive » (AE); l'AE fait référence à un autre concept mis au point conjointement par les organismes gouvernementaux (pas encore paru).

17 Paul Comeau, débat sur la présentation le 14 mai 2008.

18 La liste des éléments nationaux du pouvoir a été élargie à certains milieux afin d'inclure DIMEFIL : diplomatie, information, militaire, économie, finance, renseignement et application de la loi.

19 Jonathan Hearn, *Rethinking Nationalism: A Critical Introduction*, New York, Palgrave Macmillan, 2006, p. 230-232.

20 Dietrich Dorner, *The Logic of Failure, Recognizing and Avoiding Error in Complex Situations*, traduit par Rita et Robert Kimber, New York, Metropolitan Books, 1996, p. 49-70.

21 Certains arguments suggèrent que d'autres capacités peuvent être incluses comme éléments nationaux du pouvoir telles que « l'information » et « le juridique ». En fait, un élargissement à sept éléments du pouvoir national a été suggéré : DIMEFIL (diplomatie, information, militaire, économie, finance, renseignement, application de la loi).

22 Les dix éléments des infrastructures essentielles sont l'énergie et les services publics; les communications et technologies de l'information; la finance; les soins de santé; l'alimentation; l'eau; les transports; la sécurité; le gouvernement; et la fabrication.

23 Le droit spatial fait partie du droit international, fondé sur les traités; les traités deviennent légaux une fois ratifiés par les 200 États membres des Nations Unies.

24 Le 13 septembre 1985, la première et seule destruction d'un satellite par un missile aéroporté américain s'est produite lorsqu'un F-15A a lancé une arme antisatellite (ASAT) contre le satellite d'observation solaire P78-1 dans une orbite de 600 km (375 miles). Le 11 janvier 2007, le gouvernement chinois a détruit un de ses satellites, à 537 miles dans l'espace à l'aide d'un système terrestre de défense contre les missiles balistiques à moyenne portée. Le 20 février 2008, les États-Unis ont tiré un missile SM-3 de l'USS Lake Erie en vue de détruire un satellite à la dérive du National Reconnaissance Office à 133 milles marins au-dessus de l'océan Pacifique.

25 Les défis que représentent les opérations dans l'espace sont bien différents des défis que représentent les opérations aériennes. Par exemple, l'espace est un environnement hostile à la présence humaine. Le vol spatial n'est en fait pas un vol spatial, mais un vol balistique par nature : la trajectoire d'un satellite est gérée par la mécanique orbitale. La rotation de la terre, associée à une trajectoire de vol prévisible, signifie que toute activité spatiale où qu'elle ait lieu peut toucher n'importe quel pays. Les véhicules spatiaux doivent être conçus de telle sorte qu'ils tolèrent les conditions difficiles de l'espace pour une longue période sans avoir besoin de réparation ou d'un réapprovisionnement de matières consommables.

26 La définition ad hoc de cyberespace fournie par le SMA(GI) J6 est la suivante : « Un domaine global dans l'environnement de l'information comprenant des infrastructures

interdépendantes de technologies de l'information de réseau parmi lesquelles Internet, des réseaux de télécommunications, des systèmes informatiques ainsi que des processeurs et des contrôleurs intégrés ». Lcol Kent Schramm, « Cyberespace : Opérations de réseau informatique », groupe de travail sur le concept intégré, 25 février 2009. L'environnement de l'information est « l'ensemble des personnes, des organismes et des systèmes qui collectent, traitent, diffusent ou agissent sur l'information ». Une explication complémentaire consiste à dire que l'environnement de l'information se compose de trois dimensions interdépendantes : physique, informationnelle et cognitive. Gouvernement des États-Unis d'Amérique, glossaire 3-13 de la publication interarmées, opérations d'information interarmées (É.-U), Washington. Department of Defense.

27 W. Huitt, "The Mind », *Educational Psychology Interactive*, Valdosta, GA, Valdosta State University, mai 2001, sur http://chiron.valdosta.edu/whuitt/col/summary/mind.html [consulté le 5 mai 2009].

28 Le biais perceptuel comprend : l'attente, la résistance au changement, l'impact de l'ambiguïté, une direction centralisée. Le biais cognitif comprend : l'évaluation de la probabilité, l'attribution de la causalité, l'évaluation des preuves. Richards J. Heuer. *Psychology of Intelligence Analysis*, Washington , Center for the Study of Intelligence, Central Intelligence Agency 1999.

29 Directeur – Analyse de la sécurité future (DASF), document de conception du CDF « Concept du domaine de capacité : Commandement », 29 février 2008; DASF, document de conception du CDF « Concept du domaine de capacité : Détection », 15 avril 2008; DASF, document de conception du CDF « Concept du domaine de capacité : Action », 27 mai 2008; DASF, document de conception du CDF « Concept du domaine de capacité : Maintien en puissance », 30 novembre 2008; DASF, document de conception du CDF « Concept du domaine de capacité : Protection », 17 avril 2008; DASF, document de conception du CDF « Concept du domaine de capacité : Mise sur pied », 23 janvier 2009.

30 Ross Pigeau et Carol McCann, « Analysing Command Challenges using the Command and Control Framework », Rapport technique RDDC 2003-034, 2003.

31 Voir Les caractéristiques de l'adaptation, p. 15.

32 « Domaine » *Webster's English Dictionary Concise Edition*, Toronto, Strathearn Books Limited, 2005, p. 84.

33 « Domaine » *Oxford Concise Dictionary*, 8e édition, Oxford, Oxford University Press, 1990, p. 347.

34 DASF, document de conception du CDF, « Concept du domaine de capacité : Action », 27 mai 2008.

35 Banque de terminologie de la Défense.

36 DASF, document de conception du CDF, « Concept du domaine de capacité : Commandement », 29 février 2008.

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

38 DASF, document de conception du CDF, « Concept du domaine de capacité : Détection », 15 avril 2008.

39 DASF, document de conception du CDF, « Concept du domaine de capacité : Maintien en puissance », 30 novembre 2008.

40 DASF, document de conception du CDF, « Concept du domaine de capacité : Mise sur pied », 23 janvier 2009.

41 DASF, document de conception du CDF, « Concept du domaine de capacité : Protection », 17 avril 2008.

42 AAP-6.

43 Gouvernement des États-Unis d'Amérique, *Doctrine des opérations interarmées 3-0*, (Washington, D.C. : Instance collégiale des chefs d'état-major, 2001).

44 *Joint Operations 3.0*, Chapitre 2, Section 2, niveaux de guerre.

45 *Concise Oxford Dictionary*.

46 Gouvernement du Canada, *Manuel des abréviations des Forces canadiennes/de la Défense nationale*, Ottawa, Chef d'état-major de l'Armée de terre.

CHIEF OF FORCE DEVELOPMENT
CHEF DU DÉVELOPPEMENT DES FORCES