B-GA-405-000/FP-001

DOCTRINE AÉROSPATIALE

DES FORCES CANADIENNES

PROTECTION

Défense nationale National Defence

Canada

Publié avec l'autorisation du Commandant de l'Aviation royale canadienne

Commandant 2e Division aérienne du Canada
Division de la doctrine et de l'instruction de la Force aérienne
Winnipeg, Manitoba
R3J 3Y5

ISBN: D2-297/2012F-PDF 978-1-100-98612-8

B-GA-405-000/FP-001

Cette publication est disponible en ligne sur le RID : http://trenton.mil.ca/lodger/CFAWC
et sur Internet : www.rcaf-arc.forces.gc.ca/cfawc/index_f.asp

Publié par la section de la production du
Centre de guerre aérospatiale des Forces canadiennes

1re édition, février 2012

DOCTRINE AÉROSPATIALE

DES FORCES CANADIENNES

PROTECTION

PRÉFACE

Le présent manuel présente la doctrine opérationnelle relative à la sous-fonction de Protection de l'Aviation royale canadienne (ARC). Bien qu'il soit surtout destiné aux militaires œuvrant au niveau opérationnel, il décrit également les fondements applicables aux niveaux stratégique et tactique. Le présent manuel a été produit à l'intention des utilisateurs suivants:

a. les écoles et académies des Forces canadiennes (FC) pour la formation, l'endoctrinement et le perfectionnement du personnel en matière de maintien en puissance et de soutien des opérations et activités aérospatiales;

b. les unités aérospatiales et postes de commandement des FC;

c. les autres éléments des FC qui se proposent de commander ou de soutenir les forces aérospatiales des FC.

Ce manuel se divise en trois chapitres :

a. **Chapitre 1 – Fondements**. Court historique et présentation de la fonction Protection comme une des principales fonctions de l'ARC.

b. **Chapitre 2 – Fonction Protection**. Explication des trois domaines de la fonction Protection et de leurs interdépendances avec les autres fonctions de l'ARC.

c. **Chapitre 3 – Application de la fonction Protection**. Description du fonctionnement général de la résolution de problèmes relatifs à la Protection.

Le présent manuel doit être consulté de concert avec les publications suivantes :

a. B-GA-400-000/FP-000, *Doctrine aérospatiale des Forces canadiennes*, 2e édition;

b. B-GA-401-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Commandement*;

c. B-GA-402-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Détection*;

d. B-GA-403-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Acquisition de l'avantage* (à être adoptée);

e. B-GA-404-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Projection*;

f. B-GA-405-001/FP-002 *Doctrine de protection des Forces aérospatiales*;

g. B-GA-406-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Maintien en puissance*;

h. B-GA-407-000/FP-001, *Doctrine aérospatiale des Forces canadiennes – Montée en puissance* (à être adoptée)

i. B-GJ-005-300/FP-001, *Publication interarmées des Forces canadiennes (PIFC) 3.0 Les opérations;*

j. B-GJ-005-314/FP-001, *Protection des forces interarmées des FC.*

k. B-GJ-005-500/FP-000 *PIFC 5.0 Le processus de planification opérationnelle des FC (PPO).*

Veuillez faire parvenir vos recommandations de modifications à apporter à la présente publication au Centre de guerre aérospatiale des Forces canadiennes (CGAFC), aux soins du Service de développement de la doctrine.

Le commandant de la 2e Division aérienne du Canada (2 DAC) est l'autorité de ratification de la présente doctrine.

PRINCIPES DOMINANTS

Les principes dominants de la doctrine de Protection reposent sur les idées centrales suivantes :

- La Protection est une fonction globale.
- La Protection est un catalyseur fondamental de la puissance aérospatiale, et tous les membres de l'ARC jouent un rôle crucial à cet égard.
- La Protection englobe des mesures actives, passives et réactives.
- La Protection est une responsabilité inhérente à la fonction Commandement.
- L'élaboration de politiques et de plans de Protection de haut niveau et le contrôle de ressources spécialisées doivent être centralisés. Pour garantir une protection efficace d'une force aérospatiale contre chaque menace et danger, la planification et l'exécution détaillées doivent être décentralisées.
- La Protection est une fonction dont doivent toujours tenir compte les fonctions Commandement, Détection, Maintien en puissance, Montée en puissance et Action (Acquisition de l'avantage et Projection) dans le cadre de leurs activités.

TABLE DES MATIÈRES

PRÉFACE ii
PRINCIPES DOMINANTS iv

CHAPITRE 1 FONDEMENTS
Introduction 1
Principes 2
Environnement de la Protection 8
Hypothèses de la Protection 11
Caractéristiques de la Protection 13
Protection dans le domaine de l'aérospatiale 15
Sommaire 16

CHAPITRE 2 FONCTION PROTECTION
Introduction 19
Composants de la Protection 20
Domaine physique 20
Domaine informationnel 23
Guerre électronique 23
Domaine moral 27
Capacités de la Protection 28
Interdépendances de la Protection dans les autres fonctions 31
Sommaire 35

CHAPITRE 3 APPLICATION DE LA FONCTION PROTECTION
Introduction 37
Fonctionnement de la Protection 37
Risque résiduel 37
Application continue de la Protection 39
Sommaire 40

GLOSSAIRE 42
LISTE DES ABRÉVIATIONS 44
DOCUMENTS DE RÉFÉRENCE 45

CHAPITRE 1

FONDEMENTS

Photo FC : Cpl Jasper Shwartz

INTRODUCTION

Les forces aériennes ont pour raison d'être l'exercice de la puissance aérospatiale au nom du pays auquel elles appartiennent. Elles s'acquittent de cette mission surtout en exploitant les environnements aérien et spatial de manière à réaliser les objectifs dont on les a chargées. Un siècle de guerre aérienne a démontré que toutes les forces aériennes efficaces, qu'elles soient grandes ou petites, sont capables d'exercer un certain nombre de fonctions données. Ces fonctions subissent l'influence des possibilités et limites physiques dont les encadrent leurs environnements et leurs pairs. L'une ne peut fonctionner avec efficience ni efficacité sans l'autre; ce sont toutefois les capacités exclusives à chaque fonction qui, une fois intégrées à celles des autres fonctions, garantissent l'application adéquate de la puissance aérospatiale. Conforme à la doctrine des Forces canadiennes (FC), la doctrine aérospatiale canadienne se constitue des six fonctions suivantes:

Protection

Fonction opérationnelle qui permet d'assurer la protection d'une force, de ses capacités et de sa liberté d'action

COMMANDEMENT - DÉTECTION - ACTION - MAINTIEN EN PUISSANCE – PROTECTION – MONTÉE EN PUISSANCE

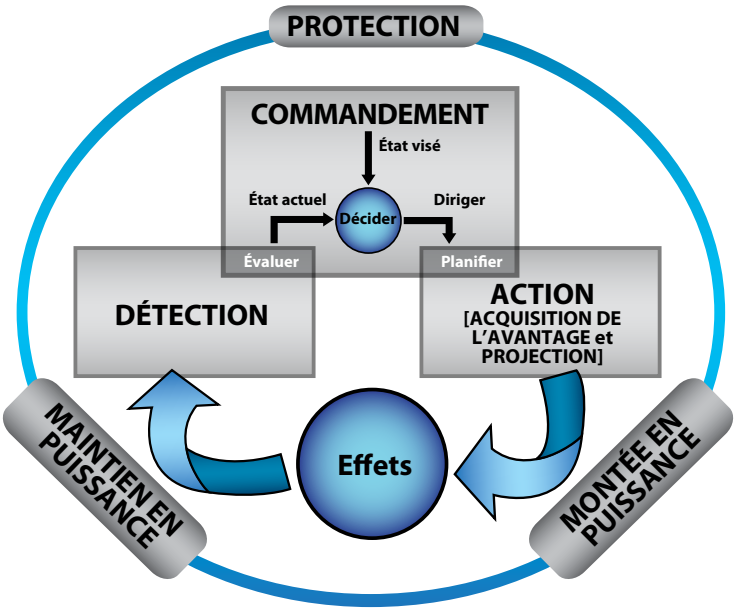

Figure 1-1. Les fonctions de l'Aviation royale canadienne[1, 2]

1 La fonction Action se divise en deux sous-fonctions : Acquisition de l'avantage et Projection.
2 Se reporter aux manuels clés de la doctrine aérospatiale des opérations, qui contiennent des examens détaillés des autres fonctions et sous-fonctions de l'ARC.

Dans l'exécution d'opérations et d'activités aérospatiales, les fonctions essentielles Commandement, Action et Détection se succèdent selon un cycle continu d'activité. Les produits des activités de la fonction Détection sont évalués lors des activités de la fonction Commandement; elles permettent d'établir l'état actuel. Après l'évaluation des états actuel et visé, les activités de la fonction Commandement ordonnent et planifient les actions. Les activités de la fonction Action créent des effets dont résulte l'état visé. Les activités de la fonction Détection évaluent les résultats de ces effets et le cycle reprend. Ce cycle d'activités influence les activités d'habilitation en cours des fonctions Maintien en puissance, Protection et Montée en puissance, ou il en subit l'influence.

Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites.

Sun Tzu,
général et stratège militaire chinois,
VIe siècle av. J.-C.

Les activités des fonctions Maintien en puissance, Protection et Montée en puissance doivent être exécutées en continu afin de maintenir en puissance, de protéger et de développer en continu les moyens et capacités de l'ARC. Les activités des fonctions Commandement, Action et Détection, si elles sont privées des activités des fonctions Maintien en puissance, Protection et Montée en puissance, risquent d'être compromises, voire éliminées. On le voit, la faiblesse ou l'échec de l'une des fonctions a des effets négatifs non seulement sur les cinq autres fonctions, mais aussi sur la capacité de la force d'atteindre l'état visé.

À partir de cette brève description des fonctions de l'ARC, ce manuel de doctrine sera consacré à la fonction Protection. Dans les FC, la fonction Protection protège une force, ses capacités et sa liberté d'action.

PRINCIPES

La Protection est un catalyseur qui aide les autres fonctions (Commandement, Action [Acquisition de l'avantage et Projection], Détection, Maintien en puissance et Montée en puissance) à jouer leurs rôles dans les escadres d'attache et durant les opérations déployées en facilitant la liberté d'action. La Protection n'est pas qu'une fonction, mais aussi un état d'esprit, une sorte de lentille qui sert à observer les autres fonctions en planifiant ses propres activités afin de déterminer les menaces réelles et possibles

pouvant avoir une incidence sur les opérations, d'évaluer l'éventuel effet de ces menaces et de choisir comment les gérer. La Protection ne doit pas entraver ni compromettre la capacité des forces déployées à exécuter des actions contribuant à la réussite de la mission. Elle doit mettre en place un ensemble de conditions qui améliorent l'efficacité opérationnelle et militaire tout en garantissant la sécurité du personnel déployé ou non. En d'autres termes, la Protection doit établir un équilibre entre évitement des risques et prise de risques.

En étudiant l'historique de la Protection, on constate une transition ferme de cette fonction d'une simple question de sécurité avec ses domaines d'intérêt unilatéraux vers une fonction bien plus dynamique et intégrée qui interagit avec tous les niveaux décisionnels et qui a des conséquences sur la planification et la réalisation des activités. Traditionnellement, la Protection était fondée sur les mesures de sécurité de la sécurité du périmètre, de l'évitement des risques, des pare-feu de l'information, de la masse, de la puissance de feu et de la protection passive ainsi que de l'analyse de la menace. Les principaux problèmes de ces types de mesures sont les suivantes :

a. « **Masse, puissance de feu et protection passive** : La masse et la puissance de feu ont été les principaux moyens permettant à des forces de défense de se protéger contre leurs adversaires. Les forces militaires d'aujourd'hui comptent sur des techniques de protection passive (p. ex., fortifications, blindage, vestes de protection balistique, bunkers, clôtures, etc.) comme approche de force brute pour absorber la force d'un choc et permettre la protection des forces (PF). Les adversaires d'aujourd'hui et ceux qui savent s'adapter ciblent les principales vulnérabilités ou utilisent des armes de destruction pour contrer les améliorations des forces qui s'opposent à eux.

Figure 1-2 . Protection des forces d'un aérodrome

b. « **Analyse de la menace** : Traditionnellement, l'évaluation de la menace portait essentiellement sur une petite partie des futurs environnements et scénarios de conflit. Aujourd'hui, elle est fondée sur les prévisions relatives à une menace existante (habituellement révélée par le personnel du renseignement) et l'évaluation des capacités et de l'intention d'adversaires reconnus (p. ex., engagement force contre force de forces combattantes). Elle comporte toutefois un inconvénient. En effet, l'analyse de la menace devrait être proactive par nécessité, mais elle est en fait réactive en raison des événements imprévus. Elle devient alors un processus linéaire très vulnérable aux perceptions changeantes et aux fausses interprétations à court terme. Dans la nouvelle réalité, les planificateurs de la défense doivent prévoir des opérations dans un environnement électronique complexe, urbain, anti-insurrectionnel et interrelié où le concept d'« adversaire » n'est pas clairement défini et où la probabilité d'une menace linéaire semblable à celle de la guerre froide est très faible.

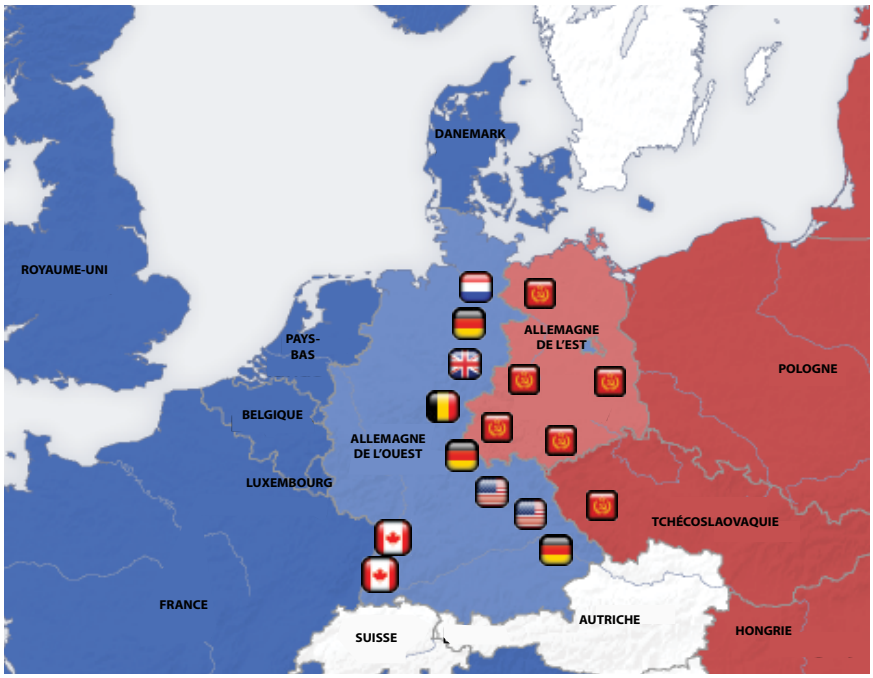

Figure 1-3. Guerre froide en bleu sur carte route

c. « **Évitement des risques** : Les forces de défense ont consacré beaucoup de temps, d'efforts et d'argent pour éviter les risques des vastes champs de bataille traditionnels (p. ex., attaque chimique, biologique, radiologique et nucléaire [CBRN]). L'évitement des

risques a toutefois mené à une stagnation et à une limitation de la capacité d'intervention efficace et rapide dans cette société réseautée et intégrée à l'échelle mondiale. Les techniques fondées sur le principe de l'évitement des risques peuvent convenir à des situations de combat conventionnel en terrain découvert, mais elles ne sont pas adaptées aux adversaires non étatiques ni aux types d'environnements de conflit en milieux urbains et littoraux.

Figure 1-4. Personnel de protection des forces dans un environnement CBRN

d. « **Pare-feu de l'information** : L'approche historique de la sécurité de l'information consistait à protéger des réseaux et des systèmes complets contre les menaces externes en mettant au point des pare-feu toujours plus vastes et perfectionnés. Il fallait donc un contrôle suffisant de l'accès et des autorisations des utilisateurs pour protéger le système. Cette approche a mené au développement de dépôts centralisés et de systèmes d'information cloisonnés qui ont nui au partage de renseignements. L'objectif est d'adopter une approche plus proactive et préventive qui met à contribution des outils militaires, commerciaux et civils dans le but de profiter au maximum des avantages, d'exploiter les renseignements plus rapidement que l'adversaire et de faciliter la redondance.

Figure 1-5. Logiciel pare-feu d'un système informatique

e. « **Sécurité du périmètre** : Au fil de l'évolution de la guerre, les fortifications de campagne ont presque toujours donné un faux sentiment de sécurité contre un adversaire rapide, agile et imprévisible. La stratégie de construction de fortifications de défense complexes ou de concentration des unités militaires sur de vastes bases impose une réflexion isolationniste insoutenable et incompatible avec les exigences de l'environnement opérationnel local, le phénomène de la mondialisation ou les systèmes adaptatifs complexes. Il est faux de croire qu'il est possible d'instaurer une zone de sécurité absolue, car cela ne limite pas la capacité de l'adversaire à mener une attaque asymétrique. Les mesures de sécurité d'un périmètre n'éliminent pas toutes les vulnérabilités, et on ne peut plus les considérer comme une panacée permettant d'éviter les menaces de l'avenir[3]. »

3 Centre d'analyse et de recherche opérationnelle de Recherche et développement pour la défense Canada du ministère de la Défense nationale (MDN). *Capability Domain Concept, Shield Capability Domain*, DRDC CORA TM 2009-005, janvier 2009, p. 7 et 8 (appelé ci-après « DRDC CORA TM 2009-005 »).

Figure 1-6. Force de protection d'un aérodrome (FPA)

Les forces militaires sont formées pour effectuer une gamme limitée d'opérations dont la fonction est limitée. Dans un environnement opérationnel, les forces armées modernes qui mettent en œuvre les mesures examinées précédemment, comme la masse et la puissance de feu, l'analyse de la menace et l'évitement des risques, peuvent subir l'effet des restrictions suivantes :

a. Les mesures peuvent être difficiles à gérer, car elles ne sont pas toujours intégrées aux autres fonctions (p. ex., Action et Détection). Ces mesures traditionnelles ne sont pas optimisées pour réagir à une vaste gamme d'éventuelles menaces traditionnelles et asymétriques.

b. L'utilisation exclusive de ces mesures peut limiter les options dont disposent les commandants, ce qui réduit la mobilité stratégique et opérationnelle.

c. Le but de ces méthodes axées sur la sécurité est particulièrement problématique pour les opérations anti-insurrectionnelles et de soutien de la paix, durant lesquelles les forces doivent interagir étroitement avec la population locale.

d. De telles méthodes de sécurité ne sont pas évolutives. Elles coûtent chères à entretenir et à réparer et elles peuvent être considérées comme excessivement agressives dans le cadre d'opérations anti-insurrectionnelles et de soutien de la paix.

e. Les méthodes axées sur la sécurité ont une applicabilité limitée dans un environnement de plus en plus caractérisé par la mondialisation et l'interdépendance ainsi que dans des environnements où l'on trouve des menaces mondiales omniprésentes, comme des pandémies ou des attaques visant des réseaux informatiques.

f. Les méthodes de sécurité de l'ère industrielle s'appliquent principalement au domaine physique et composent difficilement avec les domaines informationnel et moral.

g. Ces méthodes s'appliquent principalement aux capacités de Protection. Elles sont inutiles pour optimiser les capacités d'une approche complète intégrant d'autres forces militaires, des civils, d'autres ministères, d'autres organisations non gouvernementales (ONG) et beaucoup d'autres intervenants dans le but de maximiser les avantages.

Étant donné la transition obligatoire de situations de combat à des activités de stabilisation complexes dans une seule zone opérationnelle, il faut établir des liens entre la protection et une vaste gamme de missions potentielles. Cela a laissé un héritage en matière de sécurité pour lequel les systèmes de défense ont accaparé la plupart des ressources en laissant peu d'obligations ou d'incitatifs pour l'innovation proactive ou l'élaboration de solutions souples. Les FC atténuent les menaces et améliorent la surviabilité en construisant de meilleures structures, en évaluant les vulnérabilités et en modernisant le matériel existant avec des systèmes de défense améliorés. Jusqu'à présent, ce travail a été fortement influencé par le modèle traditionnel de l'ère industrielle et il a fini par se dérouler dans des éléments séparés du système Protection. Il n'est toutefois pas parvenu à regrouper tous les domaines de la Protection (p. ex., physique, informationnel et moral) dans un cadre général.

ENVIRONNEMENT DE LA PROTECTION

« Les effets de la mondialisation influent sur l'ordre mondial politique, militaire et économique de façon innovatrice, imprévisible et peut-être déstabilisante. Les types de conflits et leur résolution seront différents du modèle traditionnel Paix - Conflit - Reconstruction après le conflit. Dans certaines régions du monde, les États défaillants et les États en déroute deviendront omniprésents dans le contexte de sécurité d'ici la fin de notre vie et mettront la table pour l'effondrement complet de la société. Les États défaillants connaîtront des mouvements sécessionnistes violents, des guerres civiles et régionales, la famine, la maladie et des crimes contre les personnes qui entraîneront tous des réactions en chaîne. Les menaces internationales telles que celles posées par les acteurs non étatiques,

les réseaux criminels internationaux, ainsi que l'extrémisme et le terrorisme religieux, tribaux et ethniques créeront de plus en plus de nouvelles sources d'instabilité qui mineront de façon asymétrique les intérêts nationaux.

« Alimentés par le radicalisme et l'extrémisme, la compétition accrue pour les ressources, ainsi que les changements climatiques et démographiques, les futurs conflits seront probablement violents, prolongés et dévastateurs. La croissance démographique florissante dans les grands centres urbains, surtout dans le monde en développement, aura des répercussions sur les activités du secteur public et du secteur privé ainsi que des effets perturbateurs sur la capacité de soutien de l'économie et de l'environnement mondiaux. La compétition pour les ressources naturelles et l'appauvrissement environnemental à l'échelle mondiale déclencheront des catastrophes humaines et la migration massive de personnes et de réfugiés. Les changements climatiques intensifieront l'accumulation des pénuries d'énergie et provoqueront d'autres manques de ressources et de ressources environnementales ainsi qu'une concurrence pour les ressources naturelles, ce qui accroîtra les probabilités de défaillance des États et d'actes terroristes.

« La prolifération continue des armes de destruction massive (ADM), particulièrement dans les États « voyous » ou aux mains des acteurs non étatiques, sera particulièrement préoccupante. Grâce à de telles armes, les acteurs non étatiques et les petites organisations radicales pourront orchestrer des effets destructeurs et perturbateurs à grande échelle. Les acteurs non étatiques qui possèdent la technologie et les armes modernes menacent de saper la puissance traditionnelle et la supériorité numérique des forces militaires des États nations organisés. Ces acteurs non étatiques se mêlent à la population locale et s'y fondent, utilisent des tactiques non traditionnelles et peuvent abuser des libertés civiles dans des sociétés plus ouvertes. … De plus, l'accroissement de l'interdépendance des infrastructures critiques, plus précisément dans les secteurs de soutien clés comme les finances, les communications et l'énergie, sera de plus en plus préoccupant à mesure que les vulnérabilités seront exploitées par des cyberattaques ou des attaques en force qui perturberont ou détruiront les services et auront des conséquences en cascade inimaginables pour le bien-être national[4]. »

Une variété d'adversaires traditionnels et non traditionnels (p. ex., états, acteurs non étatiques, terroristes, mercenaires, rebelles, irréguliers, milices, groupes multinationaux, criminels organisés, etc.) peuvent exploiter des technologies, des systèmes de commandement et de contrôle et des technologies de l'information. Il peut s'avérer difficile d'identifier, de définir

4 Shaye K. Friesen et Andrew N. Gale, «Pourfendre le dragon : l'environnement de sécurité de l'avenir et les limites de la sécurité à l'âge industriel » *Revue militaire canadienne,* vol. 11, no.1, http://www.journal.forces.gc.ca/vo11/no1/07-friesen%20gale-fra.asp (consulté le 22 juillet 2011).

ou d'évaluer de tels adversaires, car ils fonctionnent de façon autonome, se mêlent à la population locale et possèdent des capacités de contrôle de l'accès très meurtrières (p. ex., mines marines, munitions volumétriques et fusées et missiles portatifs) contre lesquelles il est difficile de se défendre. Les plateformes traditionnelles peuvent être particulièrement vulnérables à ce type d'armes. «En côtoyant les habitants locaux, les adversaires auront l'occasion d'influencer leurs attitudes, leurs comportements, et ainsi, leurs allégeances [5]. » La Protection doit pouvoir contrer les capacités acquises à des fins particulières pouvant servir à cibler des vulnérabilités ou des lacunes et à provoquer les FC et les partenaires de coalition de façon asymétrique.

Les forces ont dû mener des opérations dans des environnements urbains, littoraux et électroniques très complexes où il n'existait aucune ligne de front clairement définie. Les forces ont joué de nombreux rôles (reliés au combat ou non) dans des environnements inhospitaliers, comme des terrains montagneux, des centres urbains très peuplés et des régions littorales encombrées. Les forces peuvent s'exposer à des attaques asymétriques (p. ex., embuscades, dispositifs explosifs de circonstance [IED]) en plus des risques ordinaires des champs de bataille. Elles doivent s'exposer à des risques découlant de différents dangers, comme des catastrophes causées par l'être humain ou des menaces indépendantes de toute intervention humaine. La fonction Protection devrait permettre aux forces d'entreprendre simultanément des opérations réparties et multidimensionnelles, c'est-à-dire de passer de situations de combat et d'activités de stabilisation complexes à des missions humanitaires et de reconstruction durant la mission. Les forces doivent donc être en mesure de résister aux chocs, aux conséquences et au stress observés dans les domaines physique et moral et de poursuivre leur initiative ou de se ressaisir rapidement.

Les opérations peuvent poser un certain nombre de défis relatifs à la surviabilité et à la protection. Les conditions physiques difficiles, ce qui comprend les températures, le bruit, l'isolement et la noirceur à des niveaux extrêmes, peuvent mettre à l'épreuve la résistance physique et psychologique des militaires. Si l'on y ajoute les contraintes de temps et les conditions de vie difficiles, alors ces facteurs peuvent accroître la nécessité de protéger les forces contre les blessures hors combat subies durant les opérations.

L'espace de combat conservera vraisemblablement son caractère interarmées, interorganisationnel, multinational et public (IIMP)[6]. La présence de neutres, d'ONG, d'autres ministères, de multinationales,

5 *Ibid.*

6 Peter Gizewski, Michael Rostek et Andrew Leslie, « Comprehensive Operations: Moving to a JIMP-capable Land Force », *Vanguard* (2006), http://www.vanguardcanada.com/ComprehensiveOperationsGizewskiRostekLeslie (consulté le 20 juillet 2011).

d'entrepreneurs, de chercheurs universitaires, de groupes de réflexion et d'habitants locaux continuera de complexifier la différentiation des adversaires et des non-combattants. Les attentes relatives aux dommages collatéraux et aux pertes « bleues » mettent en évidence l'importance de l'agilité et de la précision dans le système Protection. Les opérations qui exigent l'intégration d'autres organismes ou acteurs non étatiques dans le système Protection peuvent poser des risques propres aux relations entre les organismes, comme la possible manipulation plus efficace de l'information (médias, Internet) et la diffusion de renseignements erronés.

HYPOTHÈSES DE LA PROTECTION

Dans l'environnement opérationnel très meurtrier de l'avenir, un environnement intégrant tous les domaines et fondé sur les effets, la protection des capacités exige un réseau de Protection intégré, actif et stratifié. Il faudrait intégrer ce réseau aux capacités de protection des autres organismes et partenaires multinationaux, comme les forces de défense (nationale et alliées), les organismes du renseignement, les autres ministères, les ONG, les groupes de réflexion, le secteur privé et le milieu de la recherche, dans l'ensemble des domaines physique, informationnel et moral. Il faudrait intégrer ces composants à la Protection et offrir de nombreux niveaux de redondance superposés (p. ex., infrastructure, systèmes et services). Les capacités de ce réseau devraient fonctionner comme un système de défense complet qui absorbe, réduit et répartit les effets des dangers possibles.

La méthode de mise en application de la fonction Protection est dictée par les hypothèses suivantes :

a. Le gouvernement du Canada ne modifiera pas les missions fondamentales des FC[7].

b. La situation internationale devrait demeurer anarchique et instable en soi.

c. On demandera aux FC de participer à une gamme d'opérations militaires dans le cadre d'une coalition multinationale.

d. On ne peut pas écarter la tenue possible d'opérations indépendantes des FC pour protéger les intérêts vitaux.

e. Les déploiements des FC continueront de subir les effets de la politique, de l'économie, des budgets, des questions juridiques et des règles d'engagement, conformément aux lois et aux valeurs canadiennes.

7 Stratégie de défense *Le Canada d'abord*, 12 mars 2010, http://www.forces.gc.ca/site/pri/first-premier/defstra/summary-sommaire-fra.asp (consulté le 22 juillet 2011).

Ils éprouveront également la volonté de la population canadienne à accepter des engagements, des dépenses et des pertes à long terme.

f. On s'attend à une réduction des pertes et des dommages collatéraux au cours des futures opérations.

g. Le recrutement, dans le cadre de la fonction Montée en puissance, respectera les niveaux établis par le gouvernement fédéral, alors que l'attrition devrait suivre les tendances historiques.

h. Le ministère de la Défense nationale (MDN) et les FC maintiendront une capacité interne à suivre, à mettre en application et à exploiter rapidement les percées scientifiques et technologiques ainsi que les nouveaux savoirs et renseignements dans le but de garantir l'existence d'une capacité optimisée en mesure de composer avec les résultats des missions cruciales[8].

L'utilisation croissante de l'infrastructure, des systèmes et des services du réseau devrait accroître les capacités et la souplesse tout en réduisant globalement les risques et les vulnérabilités. La protection séparée de chaque composant ne permet pas de produire cet effet stratifié qui permet aux FC de tirer avantage des interdépendances communes, d'élever les niveaux de protection pour établir des contre-mesures (actives ou passives) et de développer plus de synergies grâce à une meilleure connaissance de la situation (CS), au partage de l'information et à la collaboration. Le système de Protection peut toujours fonctionner même si un ou des niveaux échouent, car les capacités, les systèmes et les réseaux sont interdépendants et se renforcent mutuellement. La considération et l'exploitation explicites des composants moraux du cadre de Protection peuvent changer la façon dont on partage les renseignements, collabore dans le réseau et coordonne les interventions en cas de dangers externes, ce qui jette les bases d'une agilité et d'une précision accrues.

La fonction Protection doit pouvoir régler le niveau de protection requis pour satisfaire aux exigences changeantes, et ce, en tout temps et selon les besoins. Elle choisit les éléments à protéger en premier et décide rapidement comment les protéger à l'aide d'une analyse fondée sur les risques et les vulnérabilités. Les forces devraient mettre en œuvre des opérations de prévention et de dissuasion pour éliminer ou interdire tout danger externe avant qu'il ne comporte un risque. En exploitant les renseignements et les biens, en mettant en œuvre une approche fondée sur l'analyse des risques et des vulnérabilités et en utilisant des outils intelligents et de prévision, on peut obtenir une fonction Protection mieux ciblée et adaptée à des dangers ou à des vulnérabilités précises. La reconnaissance de la dépendance des

8 DRDC CORA TM 2009-005, p. 14.

FC à l'égard d'autres organisations (p. ex., ONG, acteurs non étatiques) pour le renseignement, l'information et les capacités cruciales ainsi que du caractère fondamental de la sécurité et de la protection de ces organisations externes pour la réussite de la mission est une considération implicite de cette fonction. La fonction Protection devrait dépendre fortement de l'action offensive et elle devrait être étroitement synchronisée avec les domaines Action et Détection. Une orientation agressive et offensive dans les domaines physique, informationnel et moral peut réduire la nécessité de protéger les forces. Toutefois, le personnel doit demeurer vigilant, et la fonction Protection sera toujours présente et capable de s'adapter rapidement aux exigences de la mission.

CARACTÉRISTIQUES DE LA PROTECTION

Une Protection efficace qui relève les défis cruciaux de l'environnement de sécurité actuel possède les caractéristiques suivantes :

CARACTÉRISTIQUES
RÉSEAUTAGE
AGILITÉ
PRÉCISION
PERSISTANCE
ROBUSTESSE
ÉCHELONNABILITÉ
INTEROPÉRABILITÉ

a. « **Réseautage** : Elle doit être soutenue par une plus vaste communauté et elle doit pouvoir intégrer de nombreux niveaux de traitement et d'information pour mettre en place un réseau coopératif, souple et redondant capable d'interfacer ou de fonctionner dans le cadre de nombreuses opérations variées avec d'autres organismes, dont des forces alliées, des ONG et d'autres ministères. Le système de Protection doit être intégré de façon transparente, inclure tous les composants et comprendre les liens entre les partenaires et les connexions afin que les effets de protection soient produits à partir de sources multiples.

b. « **Agilité** : Un niveau de protection qui s'adapte rapidement en temps réel et qui peut modifier lui-même sa portée, son échelle et sa configuration en fonction d'un continuum de menaces possibles en constante évolution. La fonction Protection doit produire un effet dynamique, extensible et stratifié qui intègre une technologie modulaire et des renseignements récents et automatisés. L'agilité laisse entendre que la Protection est très réactive, simple et caractérisée par un niveau adéquat de protection pour permettre aux autres fonctions d'accomplir leurs propres missions. Pour devenir vraiment agile, la Protection doit être facilitée par une organisation apprenante efficace.

c. « **Précision** : La fonction Protection doit s'adapter avec rapidité et précision afin de garantir la réussite des missions et de réduire au minimum les pertes amies et neutres. Elle doit être capable

d'identifier, de cibler et de neutraliser presque immédiatement les effets des menaces. Ces activités doivent offrir un choix d'entrée dans la Protection ou de sortie de la Protection et être disponibles dans divers contextes conflictuels (p. ex., environnements urbains et littoraux). L'usage maximal de la technologie de pointe pour identifier précisément une menace et éliminer son éventuel effet peut réduire les faiblesses et les vulnérabilités, ce qui permet aux forces d'avoir confiance dans leur capacité d'opération.

d. « **Persistance** : Les menaces actuelles et futures peuvent être implacables. Un système stratifié avec une redondance intégrée doit pouvoir fonctionner presque en tout temps. La fonction Protection doit pouvoir résister à des attaques soutenues ou répétées et poursuivre sa mission malgré les dommages subis ou les compromis. Ce système doit utiliser de façon maximale la technologie de pointe pour produire un effet de Protection redondant, complet et stratifié.

e. « **Robustesse** : L'espace de combat actuel et futur exigera vraisemblablement des opérations dans un environnement urbain ou littoral où il faudra peut-être interagir de façon rapprochée avec des adversaires très meurtriers. Les vulnérabilités et les lacunes peuvent être ciblées particulièrement dans un tel environnement. La Protection doit pouvoir absorber ces attaques, atténuer leurs effets et les répartir dans différentes directions tout en contribuant de manière décisive à la liberté d'action. Elle doit être insensible aux stress externes et adopter des mesures de protection proactives, comme l'usage de leurres, la déception et la dissimulation pour protéger les forces rapprochées de l'adversaire.

f. « **Échelonnabilité** : Pour réussir les missions et protéger les forces déployées dans tous les environnements et les domaines, il faudra adapter les forces à ces missions. Il faut donc un système échelonnable en temps réel capable de produire un effet de protection adéquat et progressif en réponse à une éventuelle menace. Ce système doit produire une gamme de réponses grâce à l'utilisation de systèmes de contrôle logiques, éthiques et fondés sur les règles[9]. »

g. **Interopérabilité** : Il s'agit de la capacité des systèmes, des unités de l'ARC ou des forces terrestres et navales à fournir des services à d'autres systèmes, unités ou forces et à accepter ou à utiliser de tels services offerts par d'autres pour leur permettre de fonctionner effacement ensemble.

9 DRDC CORA TM 2009-005, p. 20 et 21.

PROTECTION DANS LE DOMAINE DE L'AÉROSPATIALE

L'environnement aérospatial est unique et il exige une approche particulière en ce qui concerne les opérations. Le document B-GA-400-000/FP-000, *Doctrine aérospatiale des Forces canadiennes* précise 11 caractéristiques de la puissance aérospatiale. Le tableau 1-1 montre que la Protection des forces est essentielle si on souhaite compenser les vulnérabilités que présentent 5 de ces caractéristiques.

Caractéristiques	Définition et vulnérabilité	Exemples de l'atténuation de la vulnérabilité par la Protection
Fragilité	Les véhicules aérospatiaux ont tendance à être plus fragiles que les véhicules de surface et, par le fait même, nécessitent un entretien spécial pour demeurer en bon état de marche.	La Protection offre une alerte en cas d'attaque, une sécurité physique ainsi que des abris situés à distance de sécurité et des abris renforcés pour les aéronefs.
Nature provisoire	Généralement, les plates-formes aérospatiales ne peuvent demeurer en place dans les airs indéfiniment, et ne peuvent par conséquent pas demeurer à un même poste de manière permanente. Cette difficulté peut être en partie contournée par l'engagement de plateformes aérospatiales en rotation afin d'assurer une certaine permanence, ou par la répétition des missions au besoin .	La Protection fournit des bases opérationnelles sûres.
Sensibilité aux conditions environ-nementales	La puissance aérospatiale est généralement très sensible aux conditions environnementales. Des mauvaises conditions météorologiques, par exemple, entraîneront des problèmes de décollage et d'atterrissage, de navigation, d'acquisition d'objectif et de tir aérien.	La Protection donne un avertissement au sujet des conditions environnementales défavorables et elle offre des abris pour les aéronefs.

Sensibilité à la technologie	Des innovations technologiques relativement peu importantes peuvent avoir des répercussions considérables sur l'efficacité de la puissance aérospatiale. Ces innovations nécessitent un engagement permanent quant à l'amélioration et au développement continu des forces aérospatiales.	La Protection identifie les capacités de l'ennemi qui sont axées sur la technologie au moment de l'évaluation de la menace du processus de planification.
Dépendance au soutien	La puissance aérospatiale nécessite un niveau élevé de soutien technique et logistique offert à partir d'une base d'opérations de soutien.	La Protection protège les ressources de soutien techniques et logistiques, y compris les entrepôts de carburant et de munitions et les pistes.

Tableau 1-1. Atténuation des vulnérabilités par la fonction Protection

SOMMAIRE

Ce chapitre constitue une introduction au manuel clé de doctrine portant sur la fonction Protection. Il faut en retenir que la Protection est un état d'esprit qui existe à l'intérieur de toutes les autres fonctions : Commandement, Action (Acquisition de l'avantage et Projection), Détection, Maintien en puissance et Montée en puissance. L'usage de la lentille de la Protection durant la planification et l'exécution des activités facilite la réussite de la mission. La Protection précise les lacunes des opérations fondées sur la masse, la puissance de feu et la protection passive, l'évaluation de la menace, l'évitement des risques, les pare-feux de l'information et la sécurité du périmètre. Pour concrétiser la Protection de façon optimale, il existe sept caractéristiques souhaitables à intégrer dans les phases de planification et d'exécution, soit le réseautage, l'agilité, la précision, la persistance, la robustesse, l'échelonnabilité et l'interopérabilité. La Protection a pour objectif de contrer les risques inhérents au domaine de l'aérospatiale, c'est-à-dire la fragilité, la nature provisoire, la sensibilité aux conditions environnementales, la sensibilité à la technologie et la dépendance au soutien.

Photo FC : Cpl Asko Karhunen

CHAPITRE 2

FONCTION PROTECTION

Photo FC : Cpl Jean-François Lauzé

INTRODUCTION

« Protection de quoi? La protection […] est une fonction opérationnelle stratifiée, intégrée et omnidimensionnelle qui vise à prévenir toute influence, dans les sphères physique, morale et informationnelle, qui pourrait nuire à la surviabilité ou à la liberté d'action des forces amies. Essentiellement, la protection […] comprend la nécessité de définir le centre de gravité des forces amies et ses points faibles critiques et de les protéger contre une attaque de l'ennemi. À l'avenir, la Protection sur le plan physique sera axée sur les concepts défensifs traditionnels, notamment la protection des soldats, des partenaires et non-combattants, des plateformes, des systèmes, de l'équipement et des installations. Sur le plan des informations, la Protection sera probablement axée sur la protection de l'information, des produits d'information et des systèmes d'information amis et des activités des forces amies. Il faut reconnaître qu'une force facilitée par réseau a l'avantage d'augmenter la capacité à échanger l'information, mais elle entraîne aussi un risque accru d'attaque de ce réseau par l'ennemi. Sur le plan moral, les ennemis chercheront à attaquer la légitimité de notre mission et de notre force. En termes simples, ils s'attaqueront à notre volonté de combattre. Pour contrer cette menace, il faudra une instruction plus poussée sur l'éthique, la légitimité des missions, la résistance aux menaces psychologiques, etc. [1] »

Figure 2-1. Protection d'un aérodrome

1 R. J. Hillier, Directeur – Concepts stratégiques (Opérations terrestres). *Omni-Dimensional Shield in Future Conflicts*, DLSC 2007-04-27, p. 3.

COMPOSANTS DE LA PROTECTION

On peut répartir les considérations relatives à la Protection entre les domaines physique, informationnel et moral. Dans le domaine physique, les éléments physiques fonctionnent et interagissent pour produire des effets cinétiques ou non cinétiques. Le domaine informationnel est caractérisé par l'usage de l'information, du spectre électromagnétique, de systèmes en réseau et de l'infrastructure connexe. Ces domaines sont également composés de plusieurs capacités importantes : préemption, détection, évaluation, alerte, défense (active et passive) et récupération. Le domaine moral, qui comprend des éléments tels que la volonté, la motivation, le leadership, la confiance, le courage, la peur et la fatigue, peut faciliter ou entraver la capacité des forces de défense à opérer et la capacité des éléments cognitifs à produire les résultats souhaités. Le personnel doit savoir que, si les menaces et les risques sont atténués dans un domaine, il est toujours possible de mener des attaques asymétriques et de subir des dommages dans un autre domaine. Seule une fonction Protection pleinement intégrée tenant compte de tous les domaines et faisant fait continuellement l'objet d'une surveillance, d'une adaptation et d'une mise en œuvre de la part du personnel de la force aérienne parviendra à concrétiser véritablement la fonction Protection.

DOMAINE PHYSIQUE

Dans le domaine physique, la Protection fait référence à l'espace de combat cinétique et non cinétique. Elle demande au personnel de considérer tous les problèmes du domaine physique pouvant avoir une incidence sur l'efficacité de la mission. Ce domaine physique peut comprendre tous les aspects de la PF, mais il doit toutefois tenir compte de l'incidence possible de ces aspects sur les autres domaines de la fonction Protection, soit les domaines informationnel et moral.

La technologie a établi des liens additionnels entre les mesures de protection physique et d'autres membres du personnel de la fonction Protection; cela peut accroître l'importance du processus d'évaluation ou d'atténuation des risques mis à la disposition des officiers supérieurs. Si le processus d'identification, d'évaluation et d'atténuation est suivi minutieusement, alors il devrait produire le plan détaillé d'une approche stratifiée et interactive du domaine physique avec une robustesse et une redondance améliorées. En outre, la mise en œuvre du processus peut améliorer la CS à l'intérieur du domaine physique, renforcer la capacité permettant de tirer avantage de l'information et du renseignement et instaurer une protection efficace dans le domaine physique.

Par le passé, le domaine physique s'occupait de la surveillance, surtout grâce à l'utilisation de personnel comme mesure cinétique ainsi qu'à

la diminution des empreintes, au camouflage, à la dissimulation et à la déception (CDD) et la consigne du silence comme mesures non cinétiques visant à concrétiser cette capacité. Aujourd'hui, on a grandement amélioré ces moyens en utilisant du matériel de haute technologie, comme des capteurs visuels et sonores et des réseaux d'alerte avancée tels que Big Voice de la Royal Air Force (RAF)[2]. La combinaison d'un ensemble de tactiques, techniques et procédures (TTP) et de matériel de haute technologie peut permettre au domaine physique d'offrir une surviabilité maximale tout en garantissant la liberté d'action (figure 2-2). Toutefois, pour permettre à la fonction Protection d'habiliter des forces mobiles et agiles, ces dernières doivent être conçues pour s'adapter et survivre aux défis géographiques du terrain, à l'environnement et aux conditions sociologiques. Cela peut engendrer des situations pour lesquelles les forces devront opérer à l'extérieur des limites de la Protection (p. ex., pour obtenir l'allégeance de la population locale lors d'opérations anti-insurrectionnelles). L'interaction entre les mesures de sécurité cinétiques et non cinétiques peut dépendre de systèmes et d'outils agiles d'aide à la décision qui soutiennent les interventions plus proactives. « L'aspect physique de la fonction Protection comprend ce qui suit :

a. Protection contre les effets balistiques, les explosions et les projectiles (y compris les attaques par missile et les attaques aériennes).

b. Protection contre l'éblouissement par le laser et contre l'aveuglement par la fumée.

c. Protection contre les opérations d'information de l'ennemi.

d. Protection contre les armes de destruction massive (p. ex. systèmes de détection/d'alerte rapides NBC, systèmes DNBC intégrés aux plateformes et combinaisons DNBC des soldats).

e. Protection contre les menaces à la santé (c.-à-d. après une blessure), une protection pouvant être améliorée par l'évacuation sanitaire et les traitements dans l'espace de combat.

f. Protection (y compris des traitements préventifs et correctifs) contre des menaces passives comme les rigueurs du climat (p. ex., chaleur/froid intenses, déshydratation) et l'environnement (p. ex., toxines, maladies, faune).

2 Un système de radiodiffusion d'aérodrome capable de diffuser des avertissements et des alertes à la grandeur de l'aérodrome et du campement. Il a été utilisé à l'aérodrome de Kandahar par l'élément de protection de la force du régiment de la RAF.

g. Protection contre les surprises. À cet effet, la CS est vitale à la survie dans l'ensemble de l'espace de combat. La CS améliore la capacité du soldat à agir de façon proactive, à éviter les surprises et, ainsi, à survivre. Lorsque la situation est confuse, la surprise peut venir autant des forces amies que de l'ennemi. Les pertes de vie dues au tir fratricide témoignent de mesures déficientes au chapitre de la fonction *protéger*… Les incidents de tir fratricide peuvent facilement saper le moral d'une force de combat pourtant très motivée.

h. Protection passive contre la détection (p. ex., furtivité — camouflage sophistiqué, mobilité, dispositifs de dissimulation (de type caméléon) et déception).

i. Habileté proactive consistant à agir de façon létale contre une menace potentielle avant qu'elle ne puisse entrer en action[3]. »

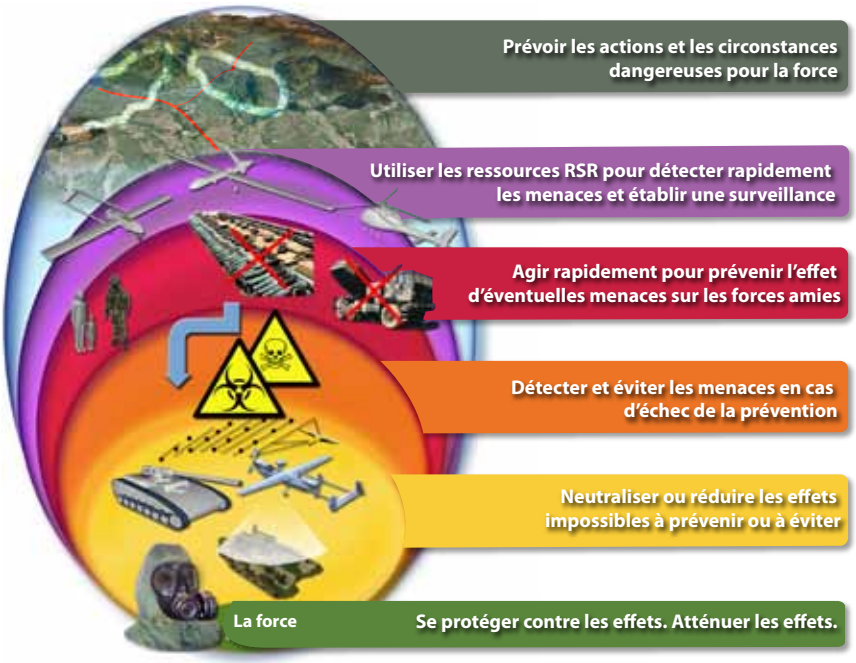

Figure 2-2. Domaine physique

3 MDN, Direction des concepts et schémas de la Force terrestre, *La force de demain : vision conceptuelle des capacités de l'Armée de terre,* Kingston, On, 2003, p. 150, http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/special/futureforce/FPAC_fre.pdf (consulté le 22 juillet 2011).

DOMAINE INFORMATIONNEL

La fonction Protection est liée à la protection du domaine informationnel. Elle doit donc veiller à ce que ce domaine fonctionne correctement, sans subir d'influences externes et même internes. Cela comprend également les domaines relatifs au transfert de données qui peuvent avoir des effets néfastes sur les autres fonctions et capacités. Plusieurs de ces domaines incluent la fonction Détection et le domaine de la guerre électronique (GE), appui de la fonction Commandement, et tout autre aspect des opérations pouvant subir l'incidence d'une quelconque sorte de transfert de données.

La Détection interagit pour atteindre la supériorité informationnelle avec la fonction Protection (par la protection) et la sous-fonction Acquisition de l'avantage (empêcher l'ennemi). La réussite des opérations militaires modernes dépend de plus des renseignements. On définit la supériorité informationnelle comme suit : « L'avantage opérationnel découlant de la capacité d'acquérir, d'exploiter, de protéger et de diffuser un flux ininterrompu d'informations tout en privant l'adversaire de la capacité de faire de même[4] . » La supériorité informationnelle est un objectif en soi, mais elle sert également de descripteur pour définir la relation causale entre les décisions prises par des forces amies et l'effet ultérieur de ces décisions sur la capacité des adversaires à influer sur l'environnement opérationnel. En définitive, elle aide à habiliter le commandant à prendre de meilleures décisions, mais aussi à prévoir les changements de l'environnement opérationnel et d'y réagir plus rapidement que l'adversaire. Si une force amie parvient à obtenir la supériorité informationnelle sur un adversaire, alors elle pourra vraisemblablement prendre de meilleures décisions plus rapidement que le temps de réaction de l'adversaire et elle possédera un avantage déterminant dans le domaine informationnel et des opérations. Pour la fonction Protection, il est essentiel de protéger le domaine informationnel pour habiliter tous les aspects des opérations.

GUERRE ÉLECTRONIQUE

La guerre électronique contribue à la fonction de protection grâce à ses trois composants : soutien de guerre électronique (SE), protection électronique (PE) et attaque électronique (AE). Pour protéger une force, des capteurs SE doivent d'abord détecter la présence de l'utilisation du spectre électromagnétique par un adversaire afin d'intercepter, de reconnaître et de localiser les sources d'émissions électromagnétiques. Lorsque des signaux ennemis sont détectés, les capteurs SE peuvent les enregistrer aux fins d'analyse détaillée pour permettre le développement et l'emploi de contre-mesures, lesquelles protégeront encore plus les ressources de l'ARC.

4 *Banque de terminologie de la Défense* (ci-après appelé BTD), fiche 41413, http://terminologie.mil.ca/term-fra.asp.

Bien que l'interception d'émissions électromagnétiques ennemies puisse être utilisée par les forces amies à des fins tactiques immédiates, comme le vol en dehors d'une zone de couverture radar d'un adversaire, toute transmission intentionnelle ou par inadvertance de signaux amis peut fournir des informations similaires à un adversaire et être utilisée pour détecter, localiser et, tôt ou tard, cibler des forces amies. Par conséquent, la transmission de signaux électroniques doit être perçue comme une activité qui peut être utilisée pour cibler des forces amies, et des mesures qui permettent de réduire ou d'éliminer complètement les émissions contribueront à protéger les forces amies.

Les mesures de protection électronique sont utilisées pour protéger des forces amies de la dégradation, de la neutralisation ou de la destruction de leurs propres systèmes électroniques et peuvent être de nature soit passive, soit active. Dans des plateformes aéroportées, on compte parmi les mesures passives la réduction des radiofréquences (RF) émises par les aéronefs et de la signature infrarouge (IR) des aéronefs; tandis que des mesures actives peuvent comprendre des manœuvres à l'extérieur des zones d'engagement d'arme, l'emploi du brouillage électronique actif, le recours à des systèmes de leurre qui diffuse de faux signaux ou l'utilisation de postes radio à saut de fréquence et de systèmes radar qui balaient un groupe de fréquences pseudo-aléatoires préprogrammées pour empêcher le brouillage efficace par un adversaire.

Des mesures de PE passives et actives servent aussi à protéger des systèmes électroniques basés au sol qui utilisent le spectre électromagnétique (EMS) [c.-à-d. postes radio tactiques, téléphones cellulaires et dispositifs informatiques sans fil], ou qui rayonnent des signaux dans l'EMS (c.-à-d. ordinateurs de bureau, imprimantes, télécopieurs, etc.). Cette protection est réalisée au moyen de mesures passives, comme le contrôle d'émission (CONEM) sur le matériel des systèmes de communication et d'information (SCI) [c.-à-d. zone de la sécurité des émissions (EMSEC) et TEMPEST], le renforcement électronique du matériel pendant la conception et la fabrication et l'utilisation de réserves du temps de la guerre. En raison de ces mesures, on ne peut pas utiliser de façon normale les capacités offensives et défensives d'un système électronique ami jusqu'à ce que celles-ci soient requises lors d'une guerre ou d'une urgence. Le brouillage RF actif et le masquage électronique des signaux électromagnétiques (EM) amis sont en outre utilisés pour protéger de manière proactive les systèmes électroniques au sol des capacités de GE d'un adversaire.

Bien que les mesures de PE visent à protéger l'emploi du spectre électromagnétique par l'utilisateur, les mesures d'AE utilisent des armes à énergie électromagnétique, à énergie dirigée ou à anti-rayonnement pour attaquer les troupes, les installations ou les équipements dans le but de

dégrader, de neutraliser ou de détruire le potentiel de combat de l'ennemi. Les missiles anti-rayonnement sont très efficaces pour protéger les aéronefs en vol, car ils sont conçus pour se diriger vers les signaux RF ennemis, puis soit détruire le site radar émetteur, soit forcer le site à cesser de rayonner sous la menace d'un missile en rapprochement qui pourrait les détruire.

D'autres informations sur les capacités de GE et leur emploi peuvent être trouvées dans le document B-GA-403-002/FP-001, *Doctrine de guerre électronique aérospatiale*.

L'ARC utilise un certain nombre de technologies en réseau; certaines sont mieux protégées que d'autres, et certaines sont accessibles à l'échelle mondiale. Cette accessibilité comporte des risques pour les systèmes. Ces systèmes se divisent en trois activités distinctes, soit la défense des réseaux informatiques (CND), l'exploitation non autorisée des réseaux informatiques (CNE) et l'attaque des réseaux informatiques (CNA). Ensemble, ces trois activités forment la base des opérations des réseaux informatiques (CNO) et elles tentent d'offrir au domaine des méthodes de détection, de protection et de riposte pour prévenir les tentatives de perturbation des opérations. Les attaques à l'intérieur de ce domaine peuvent être orchestrées par des personnes seules, des organisations ou des groupes parrainés par un État dans le but de perturber ou d'arrêter les opérations en exploitant des moyens détournés ou en utilisant des virus, des robots et ainsi de suite.

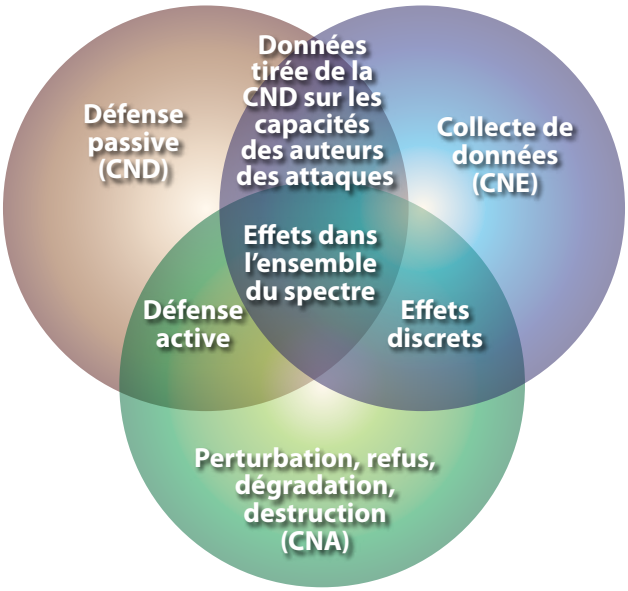

Figure 2-3. Interdépendances entre les disciplines des opérations des réseaux informatiques[5]

5 Centre d'analyse et de recherché opérationnelle de Recherche et développement pour la défense Canada du ministère de la Défense nationale (MDN). *CF Cyber Operations in the Future Cyber Environment Concept*, DRDC CORA TM 2009-058, décembre 2009, p. 22 (appelé ci-après « DRDC CORA TM 2009-058 »).

L'ARC a tenté d'implanter des réseaux protégés avec des mesures et des systèmes intégrés pour éliminer les attaques contre le domaine informationnel. Ces mesures et systèmes comprennent des sauvegardes, des protections contre les virus, des procédures d'utilisations et d'autres protocoles différents. Cela ne garantit toutefois pas un environnement opérationnel sûr. « Dès que l'on détecte ou soupçonne une menace, il faut mettre en œuvre au moins une des mesures suivantes :

a. débrancher physiquement l'appareil visé;

b. bloquer le trafic en question avec un pare-feu;

c. rediriger l'auteur de l'attaque vers un « pot de miel »[6] pour observer ses techniques et son intention;

d. effectuer une CNA pour mettre l'auteur de l'attaque hors d'état de nuire.

« Le processus de récupération peut inclure, au besoin :

e. la restauration d'un appareil à partir d'une image de sauvegarde intacte connue;

f. la décontamination d'un ou de plusieurs hôtes afin d'éliminer tout virus;

g. l'examen d'éventuels changements pour prévenir une deuxième attaque. Cela peut correspondre à l'« évaluation des dommages de combat » du domaine Détection, laquelle peut être une activité de renseignement[7]. »

L'un des composants de la défense contre les menaces consiste à informer les utilisateurs sur leur rôle dans la sécurité d'un réseau et les effets réels du non-respect des procédures de sécurité. Il faut seulement un utilisateur pour insérer une clé USB (bus série universel) dans un hôte interne et ainsi ouvrir une porte dérobée dans le réseau d'un ennemi. Ensuite, tout le réseau devient vulnérable aux fuites ou à la destruction de renseignements. On peut considérer que le domaine informationnel fait partie de la défense informatique.

6 En informatique, le terme « **pot de miel** » désigne un piège visant à détecter, à détourner et à contrer d'une quelconque manière les tentatives d'accès interdit aux systèmes d'information. Il est généralement composé d'un ordinateur, de données ou d'un site réseau qui semble faire partie d'un réseau et comprendre des ressources ou des renseignements précieux pour l'auteur de l'attaque, mais qui est en fait est isolé et surveillé. Wikipédia, http://fr.wikipedia.org/wiki/Honeypot (consulté le 20 juillet 2011).

7 DRDC CORA TM 2009-058, p. 20.

DOMAINE MORAL

D'éventuels adversaires tenteront de s'attaquer à notre volonté de combattre à l'aide de tous les éléments du domaine moral. Il s'agit là d'une attaque très rentable dont peuvent profiter les adversaires incapables de nous affronter dans le cadre d'opérations ordinaires sur un champ de bataille. Les méthodes d'attaque peuvent inclure, et incluront, des attaques ciblant notre patrie, des attaques visant à inciter nos forces à poser des gestes douteux ou à l'issue incertaine ainsi que des attaques pour miner notre légitimité et notre efficacité, tant à l'intérieur qu'à l'extérieur du théâtre. Ces types de menaces sont souvent difficiles à contrer, surtout quand ils sont fréquemment exposés à l'œil du public ou des médias. Les attaques énumérées ci-dessous sont des méthodes utilisées, mais elles n'incluent pas tous les éléments de ce domaine.

a. **Menaces psychologiques** : Ces menaces peuvent faire l'objet de démonstration et s'avérer efficaces de bien des manières, surtout avec le recours aux médias. Cela comprend les messages des forces militaires envoyés par l'entremise de leur personnel des affaires publiques. Ces messages sont transmis au personnel au pays, à l'étranger ou en déploiement par les médias ou les journalistes militaires ou civils. Si le public au pays ne reçoit pas le bon message, alors il peut limiter ou retirer l'appui qu'il accorde à la mission et au personnel déployé (figure 2-4), ce qui peut imposer des dilemmes éthiques importants au personnel en mission.

Figure 2-4. Manifestation contre la guerre à Toronto en 2008[8]

8 Miles Storey, « What Is It Good For? », photo tirée de *Torontoist*, 23 octobre 2008, http://torontoist.com/2008/10/phototo_what_is_it_good_for.php?gallery0Pic=37# (consultation le 20 juillet 2011).

b. **Moral et cohésion de l'unité** : L'opération ou la tâche peut subir un effet dévastateur si l'on ne prend pas dûment en considération cette facette de la Protection. Si le moral et la cohésion de l'unité ne sont pas maintenus, alors l'efficacité de l'unité et sa capacité à mettre en œuvre et à maintenir la fonction Protection seront grandement réduites.

c. **Attaques contre la patrie** : Le personnel déployé doit savoir que sa famille et ses amis sont en sécurité. Si le personnel ne peut pas avoir cette garantie, alors il ne se concentrera pas sur la mission.

d. **Maintien de la légitimité de la mission** : Le personnel doit croire en la légitimité de sa mission. Il faut que ses actions soient approuvées par des organisations internationales, comme l'Organisation des Nations Unies (ONU) ou l'Organisation du Traité de l'Atlantique Nord (OTAN).

e. **Règles d'engagement (RE)** : Elles doivent être claires, concises et valides. Elles ne laissent planer aucune interrogation quant aux actions acceptables et possibles. Une compréhension profonde des RE est nécessaire pour atténuer les dilemmes moraux.

f. **Peuples autochtones et menaces non militaires** : Cela comprend les activités hostiles des populations civiles, des criminels et des initiés. Un initié peut être un membre des FC, un civil canadien, un employé du MDN, un entrepreneur canadien, un civil employé localement (LEC) du pays hôte (PH) ou bien un employé ou un entrepreneur qui n'est ni canadien ni un citoyen du PH (citoyen d'un pays tiers) ayant accès aux ressources de l'ARC. Ces menaces peuvent être sans cohésion ou bien orchestrées et elles peuvent se manifester sous la forme de renseignements compromis, de manifestations, d'occupations d'immeubles, d'émeutes, d'agressions physiques ou d'enlèvements. Les initiés peuvent menacer les intérêts de l'ARC en divulguant des renseignements sensibles ou classifiés, en prenant des décisions favorables aux groupes dissidents ou en aidant les attaques asymétriques. L'activité criminelle peut donner un indice des futures actions ou fournir des indications et des avertissements sur des attaques à venir.

CAPACITÉS DE LA PROTECTION

« La fonction Protection fait partie d'un système conçu pour décourager, prévenir et écarter les dangers avant qu'ils ne posent un risque. Ce système sert aussi à détecter, à dévier et à contrer les éventuelles attaques visant

des points faibles cruciaux au moyen d'interventions actives, intégrées et stratifiées. La fonction Protection se déroule dans un cadre conçu pour offrir une protection agile, précise et échelonnable dans l'ensemble du spectre des activités de l'ARC. Nulle part ailleurs cela n'est plus apparent que dans le programme du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), qui comprend de nombreux aspects de la fonction Protection (de concert avec plusieurs autres fonctions).

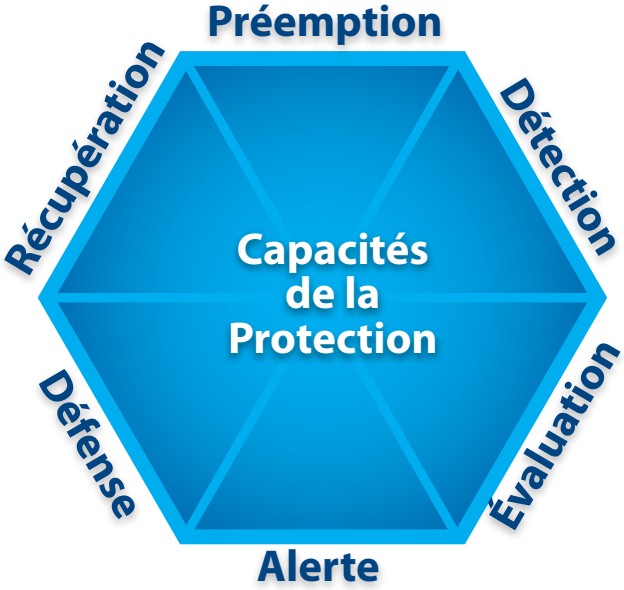

Figure 2-5. Capacités de la Protection

« Il y parvient en comprenant et en mettant en œuvre tous les domaines de la fonction Protection (physique, informationnel et moral) à l'aide d'une évaluation systématique des activités qui tient compte et qui applique les actions suivantes :

a. **Préemption** : Agir dans le but de perturber, d'interdire ou de détruire la capacité d'un adversaire à mener des actions contre des capacités, des plateformes ou des systèmes amis.

b. **Détection** : Surveiller les actions et les mouvements d'un adversaire grâce à la CS et permettre aux décideurs de comprendre qui est l'adversaire.

c. **Évaluation** : Évaluer tous les dangers que doit affronter la force déployée et permettre aux décideurs de recentrer les capacités de détection et d'identification ou parfaire la compréhension et prévoir les intentions de l'adversaire.

d. **Alerte** : Présenter des indicateurs et des avertissements aux décideurs de différents niveaux de l'administration, du secteur privé ou du public. L'utilisation d'outils de prévision permet de détecter des choses, de réagir directement aux dangers et de protéger les systèmes essentiels.

e. **Défense** : Défendre les forces à l'aide de mesures actives et passives et de moyens cinétiques et non cinétiques. Les mesures passives produisent un effet préventif et dissuasif. Les mesures actives utilisent des actions cinétiques et non cinétiques pour perturber et interdire les actions d'un adversaire tout en continuant de protéger les forces déployées et les partenaires multinationaux.

f. **Récupération** : Absorber un danger, favoriser la continuité et reprendre les fonctions opérationnelles en un temps minimal, et ce, malgré les pertes et les dommages subis[9]. »

Il faut considérer, intégrer, prévoir et, au besoin, atténuer ces capacités de la fonction Protection durant la planification des opérations et des missions. Par exemple, la fonction Action doit tenir compte de quelques-unes de ces capacités ou de toutes ces capacités pendant la planification d'une mission Acquisition de l'avantage exigeant une protection aérienne contre un grand nombre de facteurs, comme des missiles sol-air, une guerre électronique et d'autres facteurs semblables. La fonction Action doit prévoir des contre-mesures adéquates pour atténuer et éliminer les effets négatifs sur l'opération ou la mission. Cela s'applique également à toutes les autres fonctions. On peut contrer et atténuer ces effets négatifs et facteurs nuisibles grâce au processus d'évaluation et d'atténuation des risques.

Une approche analytique fondée sur les vulnérabilités et les risques permet de gérer les effets de tous les dangers à l'intérieur de la fonction Protection et de se concentrer sur la formulation du meilleur plan d'action dans tous les domaines. Dans le cadre de la fonction Protection, la protection est répartie et elle est formée de capacités superposées et de systèmes redondants, avec une exigence ultérieure relative à un processus d'évaluation des risques, ainsi que d'outils d'analyse à l'appui du remaniement de l'ordre de priorité des ressources. Cette analyse axée sur les vulnérabilités et les risques exige une synchronisation et des liens plus étroits entre les systèmes de détection, d'identification et d'alerte (c.-à-d. la fonction Détection) et le processus d'analyse des risques (c.-à-d. la fonction Protection) pour atténuer les vulnérabilités nationales.

Au centre de la fonction Protection se trouve une exigence plus vaste et plus profonde quant au partage de l'information. Une reconnaissance claire

9 DRDC CORA TM 2009-005, p. 10 et 11.

des liens et des capacités entre les différentes fonctions est essentielle aux activités de Protection. La fonction Protection devrait pouvoir réduire au minimum la dépendance à l'égard de la protection axée exclusivement sur les défenses de masse et la puissance de feu en augmentant l'importance de l'exigence relative à une meilleure CS. L'application de principes clés, l'agilité et la précision faciliteront l'atténuation des vulnérabilités de la fonction Protection. « Voici quelques-unes des capacités améliorées qui devraient résulter de cette application :

a. la capacité de faire converger et d'adapter les activités, l'expertise et les ressources en temps plus opportun;

b. la capacité de réagir rapidement et de façon préventive aux nouvelles menaces;

c. la capacité de lier les fonctions de Protection à une vaste gamme d'exigences des missions, de les adapter et de les personnaliser avec précision;

d. la capacité d'intégrer d'autres ministères (au besoin) et partenaires de sécurité, de coordonner leurs activités et d'établir des liens entre eux pour obtenir les effets désirés;

e. la capacité de profiter de nombreuses interdépendances de l'infrastructure cruciale;

f. la capacité de faciliter une convergence des capacités physiques, informationnelles et morales;

g. la capacité de synchroniser la fonction Protection avec les fonctions Action, Détection et Commandement à tous les niveaux;

h. la capacité de détecter et de diriger des interventions pour contrer des menaces ou protéger des systèmes essentiels;

i. la capacité de fournir une fonction Protection robuste, échelonnable et complète pour les environnements opérationnels complexes[10]. »

INTERDÉPENDANCES DE LA PROTECTION DANS LES AUTRES FONCTIONS

Une fonction Protection efficace devient un catalyseur pour les fonctions Détection, Commandement, Action, Montée en puissance et Maintien en puissance, mais elle en dépend également. À cet égard,

10 DRDC CORA TM 2009-005, p. 12.

la Protection possède un certain nombre d'interdépendances avec ces autres fonctions.

Dans bien des cas, les capacités d'une fonction ne peuvent pas exister sans la mise en place des capacités d'une autre fonction. Certaines de ces interdépendances exigent l'examen, l'atténuation, la planification et la mise en œuvre des activités de la fonction Protection pour atteindre l'objectif du commandant. En outre, les activités des autres fonctions doivent se dérouler en harmonie avec des éléments de la Protection pour offrir au commandant l'ensemble des activités requises pour accomplir la mission.

a. **Protection et Commandement** : Tout comme les autres fonctions, la fonction Commandement doit être intégrée pleinement. La fonction Protection dépend fortement de la fonction Commandement qui lui donne une orientation durant la configuration initiale et à mesure que change la situation opérationnelle. Dès que les fonctions Détection et Protection ont fourni les renseignements pertinents au commandant, la Protection attend une orientation rapide et adéquate de la part de la fonction Commandement. La fonction Protection utilise cette orientation pour éliminer, atténuer ou déplacer les menaces ou les risques. La fonction Commandement dépend de la Protection pour accomplir ses tâches dans un environnement raisonnablement sûr et, conséquemment, exécuter les fonctions Maintien en puissance, Action, Montée en puissance et Détection.

b. **Protection et Détection** : Lorsque les commandants examinent la fonction Protection, ils ont besoin de la fonction Détection pour obtenir continuellement des renseignements sur les capacités et les intentions des forces rouges et bleues. Ces renseignements permettent à la fonction Protection d'éliminer, d'atténuer ou de déplacer les menaces et les risques recensés selon la situation. Cela offre aux autres fonctions, dont la Détection, un endroit relativement sûr et stable à partir duquel accomplir leur mission ou leur opération. La fonction Protection dépend de la fonction Détection qui lui permet de prévoir, de détecter, d'identifier, de prévenir et de suivre une gamme complète de menaces. Les activités de détection et d'alerte doivent se dérouler avec beaucoup de rapidité et de précision pour permettre la mise en œuvre du processus d'analyse de l'évaluation des risques. Cela fournit à la fonction Commandement les options possibles quant à la défense ou aux contre-mesures adéquates. Par exemple, on peut envoyer un hélicoptère Sea King remplir simultanément une fonction de Protection (PF du domaine physique) et une mission

de Détection pour soutenir son navire ou le groupe opérationnel naval auquel il appartient. On peut aussi le rediriger pour remplir simultanément une fonction de Protection (« couverture » du domaine physique) et une fonction de Détection, c'est-à-dire protéger le groupe opérationnel naval en lançant des armes à l'appui de la fonction Protection ou Détection.

c. **Protection et Action** : Il faut tenir simultanément compte de la fonction Protection et de la fonction Action (Acquisition de l'avantage et Projection). On peut envoyer une escadrille de six chasseurs-bombardiers pour remplir une fonction de Détection à l'appui d'une opération. Durant cette opération, on peut désigner plusieurs de ces chasseurs-bombardiers comme escortes afin qu'ils accomplissent cette activité de la fonction Protection ou toute autre activité semblable en éliminant, en atténuant ou en déplaçant les menaces ou les risques durant le déroulement de leur mission ou du processus de planification opérationnelle. On peut ordonner à l'ARC de remplir une fonction de Protection (couverture ou tir de protection) pour soutenir des opérations d'Action ou de Manœuvre de l'Armée de terre ou lors d'affrontements avec des forces ennemies. Cette couverture serait considérée comme une fonction de Protection. Les forces de PF peuvent exiger le soutien de la fonction Montée en puissance, et ce type de fonction Montée en puissance à l'appui d'une activité de la fonction Protection (PF du domaine physique) peut être demandé par des éléments de la PF engagés à l'extérieur d'un campement, mais à l'intérieur de la zone de responsabilité (AOR) du commandement de la composante aérienne (ACC), qui peut s'étendre jusqu'à 15 km ou 20 km du périmètre du camp. La fonction Projection peut aussi s'avérer nécessaire pour remplacer les unités de PF qui soutiennent la fonction Protection par de nouvelles troupes et du nouveau personnel de la force aérienne.

d. **Protection et Maintien en puissance** : Le Maintien en puissance est l'une des principales fonctions ayant besoin de l'appui de la fonction Protection pour mener ses activités. La Protection offre un environnement dans lequel la fonction Maintien en puissance peut s'accomplir, et ce, tant sur le camp ou l'aérodrome que durant les opérations de maintien en puissance, y compris celles qui concernent les emplacements avancés d'opérations (EAO) et les missions de réapprovisionnement terrestre. L'ACC doit tenir compte des menaces et des risques recensés par la fonction Protection ainsi que les éliminer, les atténuer ou les déplacer pour permettre l'exécution

de la fonction Maintien en puissance, comme l'approvisionnement d'un EOA ou d'une base d'opérations avancée (BOA) (à l'aide d'un convoi logistique) durant lequel peut s'avérer nécessaire une couverture aérienne (fonction Protection sous Action). Les exigences relatives à la Protection peuvent également comprendre le soutien d'autres ministères ou d'opérations humanitaires ou nationales lors d'une inondation ou d'une tempête de verglas. La fonction Maintien en puissance est aussi nécessaire pour fournir à la fonction Protection (effort de PF du domaine physique) du matériel et du ravitaillement, surtout pour remplacer le matériel utilisé ou bien l'équipement et les pièces endommagés ou usés.

e. **Protection et Montée en puissance** : « La Montée en puissance développe et prépare une force aérospatiale pour qu'elle réponde aux exigences de son emploi. … La Montée en puissance de forces afin d'offrir une puissance aérospatiale est une activité permanente qui comprend trois éléments principaux : le développement des capacités de force nécessaires, l'exécution des activités de préparation des forces et l'établissement de programmes destinés à prévenir la perte accidentelle ou la détérioration de ces capacités[11]. » La fonction Protection offre l'environnement le plus sûr qui soit pour la conduite des activités de la fonction Montée en puissance. Les mesures mises en œuvre pour protéger les capacités de l'ARC ou prévenir les pertes ou la dégradation de ces capacités sont essentielles à la fonction Montée en puissance. La production et l'utilisation des ressources de la force aérienne comprennent un certain degré de risque, un risque qui peuvent causer des décès, de graves blessures, des dommages matériels, une dégradation des capacités ou des dommages à l'environnement. Les programmes de prévention des pertes organisationnelles sont donc intégrés au tout début du cycle de vie de tout système d'armement ou de tout autre matériel, soit de son introduction à son élimination en passant par son utilisation et son maintien. Les principaux programmes qui protègent l'ARC contre les pertes et les dommages sont le Programme de la sécurité des vols, le Programme de sécurité générale, le Programme de navigabilité et le Programme de gérance de l'environnement.

Toutes les fonctions (Commandement, Détection, Action [Acquisition de l'avantage et Projection], Maintien en puissance et Montée en puissance) possèdent des interdépendances et des ramifications particulières avec la

11 B-GA-400-000/FP-000, *Doctrine aérospatiale des Forces canadiennes*, 2e édition, décembre 2010, p. 53, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Strategic/B-GA-400/Edition_2/B-GA-400-000-FP-000-Edition_2_f.pdf, (consulté le 22 juillet 2011).

fonction Protection. Étant donné que la fonction Protection est davantage un état d'esprit qu'un groupe précis du personnel de l'ARC affecté à la fonction Protection, chaque fonction doit donner les grandes lignes et décrire précisément ses relations avec la Protection à l'intérieur de sa propre fonction et dans ses manuels de doctrine subordonnés.

SOMMAIRE

Ce chapitre a présenté les trois principaux composants de la fonction Protection, soit le domaine physique, le domaine informationnel et le domaine moral. Il a décrit les différentes facettes de chaque domaine et l'effet de chaque domaine sur les opérations de l'ARC. Il a expliqué les capacités des domaines et comment tenir compte de chacune d'entre elles durant l'application de la fonction Protection au moyen de la préemption, de la détection, de l'évaluation, de l'alerte, de la défense et de la récupération. Enfin, il a expliqué les relations et les interdépendances avec les autres fonctions. Il a précisé les documents de doctrine clés des fonctions de chaque composant afin d'y trouver d'autres conseils sur les relations avec la fonction Protection.

Photo FC

CHAPITRE 3

APPLICATION DE LA FONCTION PROTECTION

Photo FC : Cpl Owan Budge

INTRODUCTION

L'objectif fondamental de la fonction Protection consiste à renforcer les capacités opérationnelles et l'assurance de la mission, tout en réduisant au minimum les pertes dues aux menaces et aux risques. Pour y parvenir, elle a recours au processus de gestion des risques. Les secteurs de risque considérés qui se rapportent à la Protection englobent les risques qui ont des conséquences sur les domaines physique, informationnel et moral.

FONCTIONNEMENT DE LA PROTECTION

RISQUE RÉSIDUEL

« Bien que les menaces militaires traditionnelles ne vont pas disparaître [pour les FC], dans un avenir proche, les menaces non traditionnelles qui visent à tirer parti des faiblesses et à miner les forces semblent être les méthodes d'attaque les plus probables. Les accidents et l'environnement présentent également des dangers pour nos forces. Étant donné que l'ARC oeuvre souvent dans des régions où on retrouve des conditions environnementales malsaines et des infrastructures rudimentaires ou endommagées (notamment les aérodromes, les routes et les services d'hygiène et de santé publiques), des mesures s'avèrent nécessaires pour protéger le personnel contre les maladies endémiques, les catastrophes naturelles, les accidents, les disséminations accidentelles ou intentionnelles de [roduits chimiques industriels toxiques, [de substances biologiques dangereuses, de produits radioactifs,]e matières industrielles toxiques (MIT) ou bien d'autres [menaces] [1]. »

Les opérations de l'ARC, et par conséquent la fonction Protection, « sont intrinsèquement complexes, dynamiques, dangereuses et présupposent le consentement à prendre des risques. Le niveau de risque est dans bien des cas associé aux possibilités de gain, aussi les chefs doivent être en mesure de bien pondérer le coût estimatif de chaque opération en fonction des résultats escomptés. Il incombe au commandant de trouver un compromis entre le besoin de mener à bien sa mission et les risques qu'elle comporte de façon inhérente. Les chefs militaires prennent depuis toujours des décisions suivant les principes de gestion des risques; la façon d'aborder la gestion des risques et le degré de succès obtenu varient considérablement selon le niveau d'entraînement et d'expérience de chacun de ces chefs. Le processus de planification opérationnelle (PPO) des Forces Canadiennes est une méthode qui vise déjà à reconnaître et à gérer, dans une certaine mesure, les risques et permet aux commandants, par l'étude de chaque situation, de choisir le plan d'action le plus susceptible d'assurer le succès de la mission. Lorsque la gestion des risques est intégrée au PPO des FC, il en découle

1 B-GA-405-001/FP-002, *Doctrine de protection des forces aérospatiales*, août 2008, p. 1-7, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-002.pdf (consulté le 12 janvier 2012).

un processus qui garantit un examen adéquat de tous les risques, la mise en place des mesures nécessaires pour les réduire à un niveau acceptable ainsi qu'une parfaite connaissance des risques résiduels[2]. »

Les niveaux de risque et de menace sont établis en fonction de la valeur d'une ressource et de son incidence sur la mission si elle est disponible ou non. Voilà pourquoi la modélisation et l'analyse des risques rendent nécessaires les évaluations du caractère essentiel des ressources, des menaces et des vulnérabilités afin de comprendre le niveau total d'exposition au risque.

Dans le cadre de la fonction Protection, le risque comprend tout élément qui mine la capacité de protection des éléments tangibles et intangibles ou qui produit des effets négatifs sur ces éléments, ce qui comprend les éléments ayant un effet inévitable sur l'appui du public. Il faut indiquer que, dans un tel contexte, le risque ne fait pas référence au risque opérationnel d'échec inhérent à la conduite d'une mission donnée ni aux menaces que doit détecter et atténuer la fonction Protection ou contre lesquelles elle doit se défendre.

Photo FC : Cpl Shilo Adamson

2 B-GJ-005-502/FP-000, *Gestion des risques aux fins des opérations des FC*, novembre 2007, 103.3, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20Risk%20Management%20for%20CF%20Operations%20%20-%20FR.pdf (consulté le 22 juillet 2011).

APPLICATION CONTINUE DE LA PROTECTION

Les commandants doivent toutefois comprendre que certains facteurs de l'équation du risque résiduel ne peuvent pas être quantifiés et qu'ils découlent tant de l'exécution des missions opérationnelles et tactiques que de la science. On s'attend à ce que le personnel de l'ARC fasse preuve de diligence raisonnable dans le signalement de toute activité offensive ou défensive pouvant décourager, détecter, prévenir, atténuer ou annuler les intentions du commandant ou de toute menace visant les ressources et les opérations aérospatiales de l'ARC.

La fonction Protection doit être ancrée davantage dans la gestion des risques que dans l'élimination des risques. On ne peut pas développer une capacité de fonction Protection pour chaque scénario et tenir compte de tous les facteurs, de toutes les pièces d'équipement et de toutes les opérations. La gestion des risques doit servir à atténuer le plus de facteurs possible et se concentrer sur les éléments essentiels à la mission. L'un des objectifs de la Protection consiste à réduire les risques à un niveau gérable afin que le composant Commandement soit capable d'exécuter son opération ou sa mission. On y parvient en suivant le processus continu illustré à la figure 3-1.

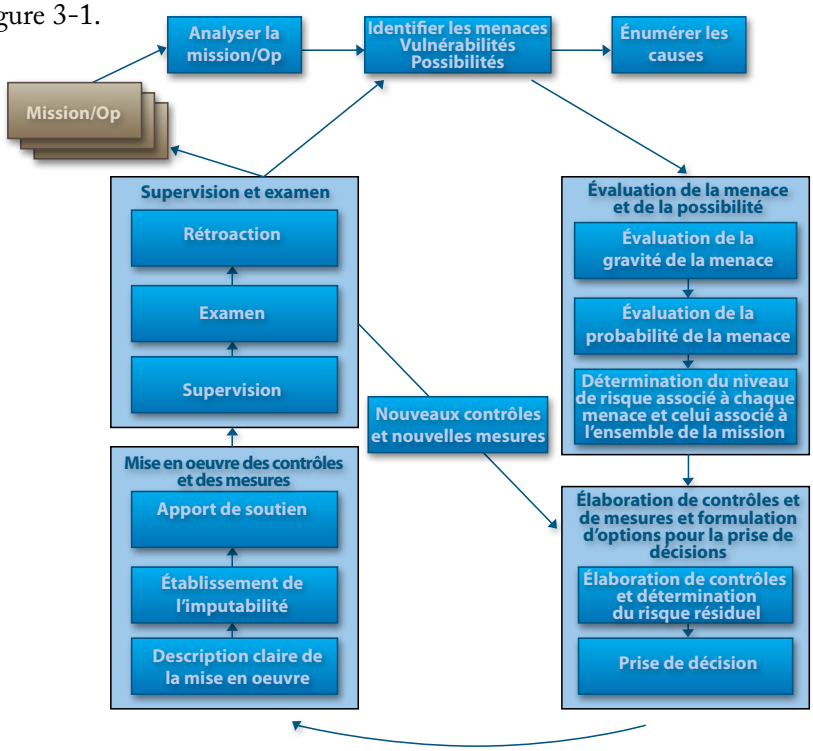

Figure 3-1. Application continue de la gestion des risques[3]

3 Adaptation du manuel B-GJ-005-502/FP-000, *Gestion des risques aux fins des opérations des FC*, novembre 2007, p. 2-4, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20Risk%20Management%20for%20CF%20Operations%20%20-%20FR.pdf (consulté le 22 juillet 2011).

Cette application continue de la fonction Protection est nécessaire pour produire, instruire, déployer et utiliser tout composant de l'ARC. La production, le déploiement et l'utilisation des ressources de l'ARC soulignent l'importance d'établir un équilibre entre le risque et les contraintes des ressources durant l'exécution de la fonction Protection.

« Toutes les opérations militaires comportent, de par leur nature même, une certaine mesure de risque. Il va de soi que l'utilisation de la violence expose les personnes et les ressources à des risques. Bon nombre de mécanismes sont déjà en place pour aider à contrôler et à atténuer les risques, notamment la doctrine, les instructions permanentes d'opération (IPO), les exercices et les normes de conception technique. Il faut que la planification militaire soit assortie d'un processus de gestion des risques clairement défini, afin qu'aucune menace n'échappe à un examen scrupuleux, que les mesures qui s'imposent soient adoptées pour limiter les effets de telles menaces et, qu'en matière de risque, toute décision soit prise de façon éclairée. La gestion des risques contribue à assurer un juste équilibre entre les moyens et les façons de réaliser l'état final escompté[4]. » Pour de plus amples renseignements sur la gestion des risques, veuillez consulter le document B-GJ-005-502/FP-000, Manuel de doctrine interarmées, *Gestion des risques aux fins des opérations des FC*.

SOMMAIRE

« En somme, la fonction [Protection] englobe toutes les actions et démarches visant à protéger la ressource la plus importante de l'espace de combat – les combattants — ainsi que les plates-formes et systèmes des forces amies qui sont nécessaires à la liberté d'action [et au succès d'une mission]. Idéalement, la fonction [Protection] doit s'étendre à tous les [domaines] physique, [informationnel et moral], dans l'ensemble de l'espace de combat … . Ainsi, la fonction [Protection] doit comprendre une combinaison de mesures actives et passives qui donnent la meilleure chance de survie possible contre les multiples menaces [physiques, informationnelles et morales] qui existeront probablement dans l'espace de combat de l'avenir. Après tout, pour réussir et vaincre en déploiement opérationnel, les [membres d'une force aérienne] doivent être sécurisés en sachant qu'ils sont protégés par les meilleurs systèmes …, les meilleures plateformes d'armes, les meilleurs soins de santé et les meilleurs systèmes d'évacuation sanitaire qui soient. De plus, ils doivent continuer à croire fermement que leur cause est juste, que leurs familles et êtres chers sont sains et saufs et que leur patrie les appuie. Finalement, le rôle de la fonction *protéger* est de s'assurer que ces questions complexes et étroitement liées sont prises en mains de manière efficace[5]. »

4 *Ibid*, par. 101.1.
5 *La force de demain : vision conceptuelle des capacités de l'Armée de terre*, 2003, p.154

Photo FC : Cpl Marilou Villeneuve

GLOSSAIRE

Les définitions qui figurent dans le présent glossaire sont tirées de diverses sources. Dans les cas où la présente publication est la source de la définition, aucune source n'est indiquée. Lorsqu'une définition provient d'une autre source, celle-ci est indiquée entre parenthèses après la définition. On emploie alors les abréviations suivantes :

a. B-GA-405-001 – B-GA-405-001/FP-002, *Doctrine de protection des Forces aérospatiales, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-002.pdf.*

b. B-GJ-005-314 – B-GJ-005-314/FP-001, Manuel de doctrine interarmées *Doctrine sur la Protection des Forces Interarmées des Forces canadiennes*, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J3%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-314%20FP-001%20-%20CF%20FP%20Doctrine%20-%20FR.pdf.

c. B-GJ-005-502 – B-GJ-005-502/FP-000, Manuel de doctrine interarmées *Gestion des risques aux fins des opérations des FC*, Modificatif 1, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20Risk%20Management%20for%20CF%20Operations%20%20-%20FR.pdf.

d. BTD – *Banque de terminologie de la Défense*, http://terminologie.mil.ca/term-fra.asp.

contrôles
Mesures prises pour atténuer les risques, normalement par la réduction de leur probabilité ou de leur gravité.

décision concernant le risque
Décision d'accepter ou non le ou les risques associés à une action. Elle est prise par le commandant ou le responsable de l'exécution de cette action.

domaine informationnel
Sphère à l'intérieur de laquelle résident l'information et les données. (BTD fiche 41414)

domaine moral
Sphère dans laquelle des gens interagissent sur le plan psychologique, éthique ou cognitif. (BTD fiche 41423)

domaine physique
Sphère à l'intérieur de laquelle les gens vivent et travaillent.

évaluation des risques
Méthode systématique de recensement et d'évaluation des dangers ou des menaces dont les résultats sont fondés sur la probabilité ou la gravité. (BTD fiche 43999)

gravité
Conséquence prévue et possible d'un incident, exprimée en termes de gravité des blessures, des dommages matériels ou d'autres facteurs d'entrave à l'opération ou à la mission (p. ex., perte de puissance de combat, mauvaise presse, etc.).

menace
Personne, groupe ou chose ayant la capacité ou l'intention de nuire à l'accomplissement de la mission. (BTD fiche 44002)
Nota : Les conditions pouvant compromettre l'exécution réussie de la mission sont la confidentialité, l'intégrité ou la disponibilité des moyens.

risque
Possibilité d'échec, de blessure ou de perte exprimée en fonction de la probabilité qu'un agent de la menace exploite une vulnérabilité et aussi en fonction de la gravité de cette éventualité. (B-GJ-005-314, définition modifiée)

risque résiduel
Degré de risque qui subsiste une fois toutes les mesures de contrôle définies et appliquées. (B-GJ-005-502)

supériorité de l'information
Avantage opérationnel découlant de la capacité d'acquérir, d'exploiter, de protéger et de diffuser un flux ininterrompu d'informations tout en privant l'adversaire de la capacité de faire de même. (BTD fiche 41413)

LISTE DES ABRÉVIATIONS

ARC	Aviation royale canadienne
BTD	Banque de terminologie de la Défense
CBRN	chimique, biologique, radiologique et nucléaire
CGAFC	Centre de guerre aérospatiale des Forces canadiennes
CNA	attaque des réseaux informatiques
CND	défense des réseaux informatiques
CNE	exploitation non autorisée des réseaux informatiques
CS	connaissance de la situation
EAO	emplacement avancé d'opérations
EMS	spectre électromagnétique
FC	Forces canadiennes
GE	guerre électronique
IIMP	interarmées, interorganisationnel, multinational et public
MDN	ministère de la Défense nationale
ONG	organisation non gouvernementale
PE	protection électronique
PF	protection des forces
PH	pays hôte
PIFC	Publication interarmées des Forces canadiennes
PPO	processus de planification opérationnelle
RAF	Royal Air Force
RE	règles d'engagement
RF	radiofréquence
RSR	renseignement, surveillance et reconnaissance
SE	soutien de guerre électronique

DOCUMENTS DE RÉFÉRENCE

B-GA-400-000/FP-000, *Doctrine aérospatiale des Forces canadiennes*, 2e édition, décembre 2010, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Strategic/B-GA-400/Edition_2/B-GA-400-000-FP-000-Edition_2_f.pdf (consulté le 22 juillet 2011).

B-GA-405-001/FP-002, Doctrine de protection des Forces aérospatiales, 8 août 2008, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-002.pdf (consulté le 22 juillet 2011).

B-GJ-005-500/FP-000, *Publication interarmées des Forces canadiennes (PIFC) 5.0 Le processus de planification opérationnelle des FC (PPO),* Modificatif 2, avril 2088, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J5%20Publications/CF%20Joint%20Doctrine%20B-GJ-005-5000%20FP-000%20Cf%20Operational%20Planning%20Process%20FR.pdf (consulté le 22 juillet 2011).

B-GJ-005-502/FP-000, *Manuel de doctrine interarmées Gestion des risques aux fins des opérations des FC*, Modificatif 1, http://cfd.mil.ca/cfwc-cgfc/Index/JD/Pub_Fre/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20Risk%20Management%20for%20CF%20Operations%20%20-%20FR.pdf (consulté le 22 juillet 2011).

Friesen, Shaye K. et Andrew N. Gale, « Pourfendre le dragon : L'environnement de sécurité de l'avenir et les limites de la sécurité à l'âge industriel », *Revue militaire canadienne*, Vol. 11, no 1. http://www.journal.forces.gc.ca/vo11/no1/07-friesen%20gale-fra.asp (consulté le 22 juillet 2011).

Gizewski, Peter, Michael Rostek, et Andrew Leslie. « Comprehensive Operations: Moving to a JIMP-capable Land Force », *Vanguard* (2006), http://www.vanguardcanada.com/ComprehensiveOperationsGizewskiRostekLeslie (consultation le 14 juillet 2011).

MDN. Stratégie de défense *Le Canada d'abord,* 12 March 2010, http://www.forces.gc.ca/site/pri/first-premier/defstra/summary-sommaire-fra.asp (consulté le 22 juillet 2011).

_____. Centre d'analyse et de recherche opérationnelle de Recherche et développement pour la défense Canada (CARO - RDDC). *Capability Domain Concept, Shield Capability Domain*, CARO TM 2009-005, RDDC, janvier 2009.

_____. CARO - RDDC. *CF Cyber Operations in the Future Cyber Environment Concept*, CARO TM 2009-058, RDDC, décembre 2009.

_____. Direction des concepts stratégiques (Opérations terrestres), *La force de demain : vision conceptuelle des capacités de l'Armée de terre*, Kingston, Ontario, 2003, 150, http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/special/futureforce/FPAC_fre.pdf (consultation le 14 juillet 2011).

R. J. Hillier, Directeur – Concepts stratégiques (Opérations terrestres). *Omni-Dimensional Shield in Future Conflicts*, DLSC 2007-04-27, MDN, Ottawa.