National Defence / Défense nationale

B-GG-005-004/AF-010

OPÉRATIONS D'INFORMATION DES FC

Publiée avec l'autorisation du Chef d'état-major de la Défense

BPR: Opérations d'information du J6 **1998-04-15**

Canada

PRÉFACE

1. PORTÉE. Cette publication est un document subordonné au *Manuel des opérations des Forces canadiennes, B-GG-005-004/AF-OOO*, chapitre 32, Opérations d'information. Cette publication fournit l'orientation des opérations d'information (IO) par les FC dans la gamme complète des opérations militaires. Cela traite des principes des opérations d'information reliés aux opérations d'information offensives et défensives et décrit les responsabilités concernant la planification, la coordination, l'intégration et les opérations d'information des FC de résolution de conflit. L'orientation concernant le soutien du renseignement aux opérations d'information, les liens avec la Défense et interinstitutions et les opérations d'information en instruction et exercices aussi sont fournis.

2. But. Cette publication a été préparée sous la direction de l'Orientation de planification de la Défense (DPG) et par l'autorité du Chef d'état-major de la Défense. Elle met en valeur la doctrine pour gérer les activités et le rendement des Forces canadiennes dans les opérations interarmées ainsi que la base de doctrine pour l'implication militaire canadienne dans les opérations interministérielles ou interinstitutions. Cela fournit une orientation militaire à l'exercice de l'autorité par les commandants et prescrit la doctrine des opérations interarmées et l'instruction. Cela fournit une orientation militaire pour que les Services puissent préparer leurs plans appropriés. Cette publication n'a pas pour objectif de limiter le pouvoir du Commandant d'organiser la force et d'exécuter la mission de façon que le Commandant juge la plus appropriée pour assurer une unité d'effort dans l'accomplissement de toute la mission.

3. APPLICATION. Cette publication qui fait autorité n'est pas une directive. Les commandants devront exercer leur jugement en appliquant cette orientation présentée pour accomplir leur mission. S'il y a un conflit entre le contenu de cette publication et le contenu des publications des éléments des Forces canadiennes, cette publication aura préséance sur les activités des forces interarmées à moins que le Chef de l'état-major de la Défense, normalement en coordination avec les Chefs d'état-major des éléments fournisse une orientation plus actuelle et plus spécifique. Les commandants des forces en opérations comme partie d'un commandement militaire multinational (alliance ou coalition) devraient suivre la doctrine multinationale et l'orientation ratifiées par le MDN et les FC. En ce qui concerne la doctrine et les procédures non ratifiées par le Canada, les commandants devraient évaluer et suivre la doctrine et les procédures du commandement multinational si applicables non conflictuels avec les politiques et les procédures du MDN/FC, les commandants devraient demander à des pouvoirs de plus haut niveau une orientation selon le cas.

TABLE DES MATIÈRES

PAGE

LISTE DES TABLEAUX

PAGE

CHAPITRE 1

INTRODUCTION

«Généralement, dans une bataille, il faut utiliser la force normale [approche directe] dans un engagement; il faut utiliser la force extraordinaire [approche indirecte] pour gagner»

Sun Tzu, L'art de la guerre, tr. Griffith

101. POLITIQUE

1. La directive de politique des opérations d'information du QGDN souligne la politique des opérations d'information du MDN/FC et délimite le pouvoir des opérations d'information précises, les principes des opérations et les responsabilités.

a. Généralités

(1) Les buts stratégiques des opérations d'information sont d'assurer les objectifs de sécurité nationale en temps de paix, d'empêcher le conflit, de protéger le MDN et l'information des FC et les systèmes d'information et de former l'environnement de l'information. Si la dissuasion échoue, les opérations d'information cherchent à atteindre la supériorité de l'information canadienne pour atteindre ses objectifs contre des adversaires potentiels en temps de crise et/ou de conflit. Les opérations d'information cherchent à persuader les décideurs à tous les niveaux d'accepter dans le calme ou avec le moins de résistance possible une réponse à l'avantage des intérêts canadiens au moyen de l'utilisation d'information. Les opérations d'information peuvent être utilisées pour influencer les décideurs à tous les niveaux des chefs d'État aux troupes en contact sur les lignes de front de la populace générale sur l'un ou les deux côtés d'un conflit. L'information est le moyen; les décideurs sont l'objectif.

(2) Le paradigme des opérations d'information s'appliquant à tous ceux qui s'engagent dans la prise de décision de la Défense des niveaux stratégique à tactique est présenté au Tableau 1-1.

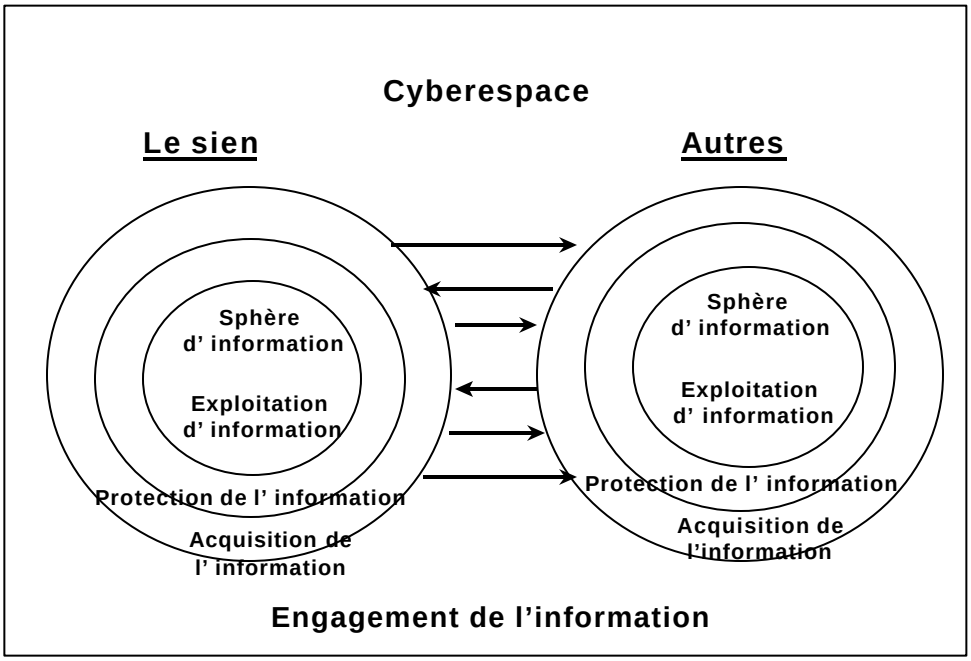


Tableau 1-1 Un paradigme des opérations de l'information

L'information qui a toujours été la clé de la prise de décision est décrite comme une sphère d'information (ressource importante ou avoir) et représente la somme totale de l.information disponible de toutes les sources (médias, météo, information émanant d'une source non secrète, etc.). L'acquisition de l'information est le processus par lequel notre sphère d'information sera pleine d'information amie et adversaire. La protection de l'information est le processus par lequel cet environnement sera assuré par nos adversaires et nous-mêmes (manipulation involontaire, destruction, etc.). L'exploitation de l'information est le processus par lequel l'information est présentée au décideur pour son usage en quantité, qualité, forme, localité et temps de son choix. Finalement, l'engagement de l'information est le processus par lequel tout cycle de décision de l'adversaire peut être lésé au moyen de lui nier la capacité d'acquisition de l'information, nullifiant ses mesures de protection, neutralisant ses outils d'exploitation, viciant son information ou détruisant ses systèmes de C2. Le changement en tant que poussée sur le monde par la révolution de l'information est le catalyseur du paradigme des opérations d'information ci-haut.

(3) L'information elle-même devient une ressource stratégique importante pour la sécurité nationale. L'information et sa circulation sont importantes pour la souveraineté d'une nation. Les sociétés modernes dépendent d'une infrastructure d'information civilo-militaire haut de gamme étayant chaque aspect de la société dans la plupart des pays développés. La défense, le commerce, le transport et les communications ne sont seulement que quelques exemples des secteurs clés dépendant grandement de la technologie de l'information pour fonctionner efficacement. Toutefois, cette dépendance et sa vulnérabilité consécutive ont créé une arme à double tranchant. Avec l'arme d'un moyen efficace d'acquisition, d'exploitation et d'influencer une autre information d'un pays, les avantages peuvent être obtenus s'échelonnant de politique, industriel, commercial à la défense. Tel que démontré dans la guerre du Golfe, les commandants militaires peuvent minimiser les pertes des deux côtés en employant les techniques de neutralisation par déroutement interdisant et interrompant les réseaux du renseignement civils et militaires importants incapacitant ainsi l'opposition. La partie capable d'atteindre un degré de Supériorité d'information en protégeant son propre potentiel tout en exploitant celui d'un adversaire actuel ou potentiel aura la plus grande chance de survie ou de succès. En outre, la vulnérabilité des systèmes d'information combinée au potentiel de dommage de grande portée fait aussi de ceci une cible attrayante pour de petits groupes ou d'individus (p. ex. terroristes). Il est donc implicite que la protection du potentiel d'information de quelqu'un et l'exploitation de toute capacité d'information de l'adversaire potentiel sont devenues un principe fondamental de la sécurité d'une nation.

(4) À travers le continuum de conflit, le MDN/FC doit être capable de maximiser les capacités et la sécurité de nos propres forces au moyen d'une utilisation efficace des opérations d'information en sauvegardant tout effort des opérations d'information adversaire contre nous ou nos alliés. Le but des opérations d'information est d'influencer les preneurs de décision en affectant l'information adversaire tout en exploitant et protégeant sa propre information. La doctrine des opérations d'information proactive et les procédures doivent être mises en oeuvre dans toute la portée du cycle de prise de décision de commandement et non limitée seulement à ces zones impliquant des systèmes automatisés. Cela forcera des examens fondamentaux sur la façon dont l'information est traitée et par qui où et quand cette information est diffusée et par quels moyens. En conséquence, l'impact des opérations d'information inévitablement sera de grande portée et profond.

(5) Les opérations d'information sont définies comme des actions prises en soutien des objectifs politiques et militaires influençant les décideurs en affectant l'information d'un autre en exploitant (entière utilisation) et en protégeant sa propre information. Cela comprend aussi des opérations d'information menées dans le continuum des opérations pour atteindre ou promouvoir des objectifs militaires spécifiques contre un adversaire ou des adversaires précis. Les activités des opérations d'information défensives sont menées sur une base continue en temps de paix et de guerre et sont une partie inhérente du processus d'emploi de la force dans toute la gamme des opérations

militaires. Les opérations d'information peuvent impliquer des questions juridiques complexes et de politique demandant un examen minutieux, une coordination de niveau national et une approbation.

(6) Comme stratégie intégrée, les opérations d'information se concentrent sur les vulnérabilités et les opportunités présentées par la dépendance croissante sur l'information et les systèmes d'information par les forces armées du Canada, nos alliés ainsi que tout potentiel adversaire. À cause de cela, l'emploi des opérations d'information est devenu essentiel à l'atteinte de nos objectifs militaires en appui au plan du commandant. Au MDN, le but stratégique ultime des opérations d'information offensives est d'influencer un décideur humain à un tel point qu'un adversaire cessera des actions menaçant les intérêts de sécurité nationale canadiens. Aux niveaux tactique et opérationnel, les opérations d'information ciblent et protègent l'information, les liaisons de transfert de l'information, le rassemblement d'information, les noeuds de traitement et l'interaction décisionnelle humaine avec des systèmes du renseignement. Les opérations d'information peuvent avoir le plus grand impact en temps de paix et les stages initiaux de crise. Finalement, les opérations d'information ne sont pas seulement essentielles à atteindre des buts et assurer des intérêts nationaux mais sont aussi des moyens clés par lesquels les forces peuvent être utilisées avec plus d'effet et minimiser les pertes. Voir Tableau 1-2.

OPÉRATIONS D'INFORMATION COMME APPROCHE

Les opérations d'information intègrent toutes les ressources disponibles pour influencer le décideur

Tableau 1-2. Opérations d'information comme approche

(7) Les opérations d'information ne sont pas un concept exclusif aux militaires. Elles doivent être comprises plutôt comme une stratégie à l'échelle de l'administration fédérale. Toutefois, une forte capacité des opérations d'information est un des nombreux éléments offerts par les militaires canadiens. Les opérations d'information peuvent appuyer la politique d'engagement stratégique du gouvernement canadien globale dans une gamme d'opérations militaires. L'efficacité de la dissuasion, la projection de l'influence nationale et d'autres concepts stratégiques est grandement facilitée par la capacité du Canada d'influencer les perceptions et la prise de décision des autres. En temps de crise, les opérations d'information peuvent aider à dissuader les adversaires d'initier des actions préjudiciables aux intérêts du Canada ou de ses alliés ou la conduite des opérations militaires amies. Si conçues soigneusement, coordonnées et exécutées, les opérations d'information peuvent être une contribution importante à désamorcer les crises; réduisant la période de confrontation et améliorant l'impact des efforts informationnels, diplomatiques,

économiques et militaires et anticipant ou éliminant le besoin d'employer des forces dans une situation de combat. Donc, les opérations d'information en temps de paix, de crise et de conflit aux niveaux stratégique national et stratégique dans le théâtre exigent une collaboration étroite parmi une grande variété d'éléments du gouvernement canadien incluant le MDN. Voir Tableau 1-3.

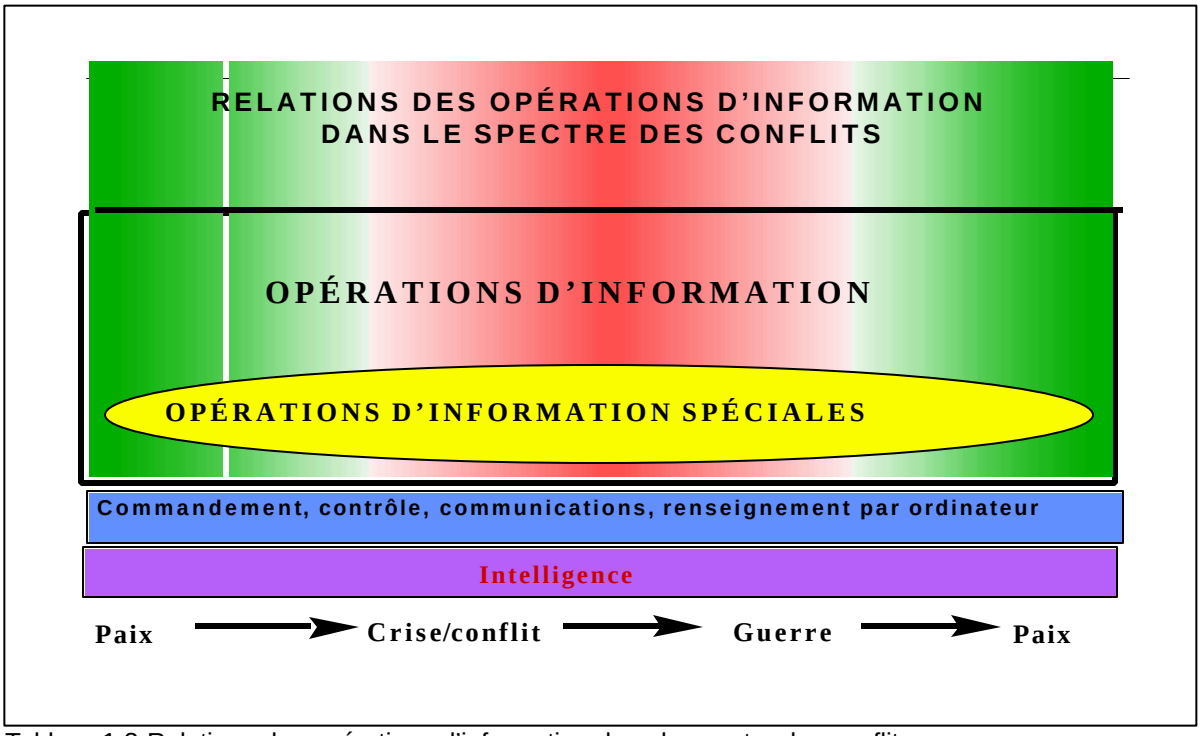


Tableau 1-3 Relations des opérations d'information dans le spectre des conflit

(8) Les opérations d'information peuvent être payées en temps de guerre à l'intérieur et au delà du champ de bataille militaire traditionnel. Comme un sous-ensemble des opérations d'information, la guerre de commandement et de contrôle (C2W) est une application des opérations d'information dans les opérations militaires spécifiques d'attaque et de défense de la gamme de cibles de commandement et contrôle (C2). La gamme de cibles de C2 inclut les cibles concernant la capacité de l'adversaire à exercer le commandement et le contrôle sur ses forces militaires. Toutefois, les capacités et les disciplines employées dans la GCC (opérations psychologiques (OPSPSY), la déception, la sécurité des opérations (SECOP), la guerre électronique (GE) et la destruction physique) ainsi que d'autres méthodes traditionnelles centrées sur des systèmes d'information pouvant être employés pour atteindre les objectifs hors de la gamme de cibles. (Voir le chapitre 2, para 201 pour de plus amples renseignements sur la GCC)

(9) Une orientation de politique des opérations d'information spécifiques est énoncée dans la directive de politique du QGDN des opérations d'information comme suit:

(a) évaluer les implications des opérations d'information dans la planification et l'exécution des opérations, le développement de la politique et la validation de nouveaux besoins menant la recherche et le développement et/ou par l'acquisition de nouveaux systèmes pour atteindre un résultat favorable rapidement et de façon concluante en minimisant les pertes et les effets préjudiciables collatéraux;

(b) harmoniser les plans et activités des opérations d'information du MDN/FC avec les objectifs nationaux globaux et stratégies ainsi que les objectifs militaires spécifiques pour avoir un effet délibéré, logique sur tout décideur;

(c) intégrer, durant la planification et l'exécution des opérations, les capacités des opérations d'information offensives et défensives et les activités;

(d) coordonner toutes les opérations d'information offensives entre les disciplines impliquées. Ces disciplines peuvent comprendre les opérations psychologiques (OPSPSY), la déception (OPDEC), la guerre électronique (GE), le renseignement, l'attaque du réseau informatique (CNA), la destruction et les opérations d'information spéciales (SIO);

(e) coordonner toutes les opérations d'information entre les disciplines impliquées. Les disciplines des opérations d'information défensives peuvent comprendre la sécurité de l'information (INFOSEC), la sécurité matérielle, la sécurité des opérations (SECOP), la contre déception, les opérations contre psychologiques, la contre-ingérence, la guerre électronique (GE) et les SIO;

(f) coordonner les plans des opérations d'information et les capacités incluant le développement de nouvelles tactiques, techniques, procédures et technologie avec d'autres ministères du gouvernement ou organismes;

(g) inclure les affaires publiques (AP) comme une partie intégrale des opérations d'information. Les activités des AP sont régies par les statuts existants, les lois, les politiques et les principes et ne devraient pas faire de compromis ni être compromises par les ordres ou directives des opérations d'information;

(h) inclure les Affaires civiles (CA) comme élément intégral des opérations d'information. Les activités des CA sont importantes aux opérations d'information à cause de leur capacité de faire la jonction avec les organisations clés et les individus dans un environnement d'information;

(i) poursuivre vigoureusement les activités de protection d'information pour protéger l'information du MDN/FC, les informations et les systèmes d'information.

"Nous devrons dire que dans toute cause le rôle décisif n'appartient pas à la technologie - derrière la technologie il y a toujours une personne agissant sans laquelle la technologie est inutile."

Mikhail Frunze, cité dans Gareyev, Frunze, Military Theorist, 1985

b. Responsabilités. Référer à la directive de politique concernant les opérations d'information du QGDN pour une liste des autorités spécifiques, des principes directeurs et des responsabilités d'individus des opérations d'information clés ou des organisations. Les individus, les commandements ou les organisations non spécifiquement traités dans les documents ci-dessus avec une influence substantielle ou une participation dans les opérations d'information sont énumérés ci-dessous:

(1) Commandants

(a) Planifier, exercer et conduire des opérations d'information en soutien des buts nationaux et objectifs.
(b) Intégrer les capacités des opérations d'information dans une planification d'action délibérée à délai de livraison critique selon une politique appropriée et une doctrine pour accomplir leurs missions assignées.

(c) Intégrer les capacités des opérations d'information dans tous les niveaux de planification et les opérations pour influencer un pouvoir de combat disponible au moyen du groupement des effets physiques et psychologiques.

(d) Utiliser le module de coordination des opérations d'information (IOCC) ou un concept semblable dans les quartiers généraux de niveau opérationnel et les états-majors subordonnés pour intégrer efficacement les activités reliées aux opérations d'information par les éléments variés.

(e) Incorporer les tactiques des opérations d'information, les techniques et les procédures dans les exercices et les événements d'instruction.

(f) Identifier les besoins de capacité des opérations d'information et soumettre les déclarations des manques de capacités au CEMA ou au SCEMD/MDN comme approprié pour validation.

(g) Capturer les leçons retenues des opérations d'information des examens après actions et les soumettre aux leçons retenues des BPR comme partie du rapport après action.

(2) Module de coordination des opérations d'information (IOCC)

(a) Tel que demandé, fournir un soutien direct aux commandants.

(3) À travers les états-majors de recherche opérationnelle:

(a) assurer que les efforts de modélisation et la simulation (M&S) sont coordonnés pour éliminer le chevauchement de l'effort et aider à se concentrer sur le développement des systèmes qui concrétisent l'instruction des opérations d'information des commandants et de l'environnement et des besoins d'exercice.

(b) Soyez prévenus de tous les efforts de M et S d'autre organisme pouvant soutenir les besoins des opérations d'information des commandants et des trois armes.

(c) Coordonne et assiste l'état-major interarmées et les états-majors des trois armes dans le développement de la doctrine des opérations d'information.

(4) Tous les éléments du MDN/FC. Adopter une approche de gestion du risque à la protection de leur information, des systèmes d'information et des processus basés sur l'information basés sur la vulnérabilité potentielle des opérations d'information.

102. TERMINOLOGIE

1. Les termes énumérés ci-dessous et les autres termes sélectionnés utilisés dans cette publication ainsi que des abréviations utilisées sont énumérées dans le glossaire. **Les définitions de base et les concepts dans ce chapitre sont importants pour la compréhension du reste de cette publication.**

a. L'information est définie comme ce qui informe ou a le potentiel d'informer. L'information est une combinaison du contenu et de la signification communiquée ou reçue, représentée par des symboles et les médias ou un conduit, utilisés ou utilisables dans un contexte particulier. (Source: Burk and Horton, Infomap). La même information peut avoir plusieurs significations et être interprétée différemment par différents destinataires. En outre, elle doit aussi être utilisée pour différents usages par les glaneurs d'information et les utilisateurs incluant les opérations et les milieux du renseignement.

b. Un système d'information est l'ensemble d'équipement, de méthodes et de procédures et si nécessaire de personnel, organisé pour accomplir des fonctions de traitement d'information spécifique. (Source: OTAN ADatP-2)

c. Des processus basés sur l'information sont des processus de collecte, d'analyse et de diffusion d'information utilisant toute formule. Ces processus peuvent être des processus autonomes ou sous-processus qui pris ensemble comprennent un plus grand système ou des systèmes de processus. (Source: US DoD JP 1-02) Des processus basés sur l'information sont trouvés dans toutes les facettes des opérations militaires et dans tout le spectre des opérations et dans les autres éléments du pouvoir national. Les processus basés sur l'information sont inclus dans tous les systèmes et les composantes de cela demandant des faits, des données ou des instructions de tout moyen, donnée ou instruction ou formule pour accomplir des fonctions désignées ou fournir des services anticipés.

d. Les opérations d'information signifient des actions prises en soutien des objectifs nationaux influençant les décideurs en influant sur l'information d'un autre en exploitant et protégeant ses propres informations. Cela comprend aussi les opérations d'information menées par le continuum des opérations pour atteindre ou promouvoir des objectifs spécifiques sur un adversaire ou des adversaires précis. (Source: Directive de politique pour les opérations d'information du QGDN)

   (1) Les opérations d'information demandent l'intégration étroite des capacités offensives et défensives et des activités ainsi qu'une conception efficace, l'intégration et l'interaction du C2 avec le soutien d'information. La pleine valeur des opérations d'information peut seulement être atteinte au moyen de l'intégration efficace de plusieurs disciplines. Voir Tableau 1-4. Il y a deux subdivisions importantes à l'intérieur des opérations d'information: les opérations d'information offensives et les opérations d'information défensives.

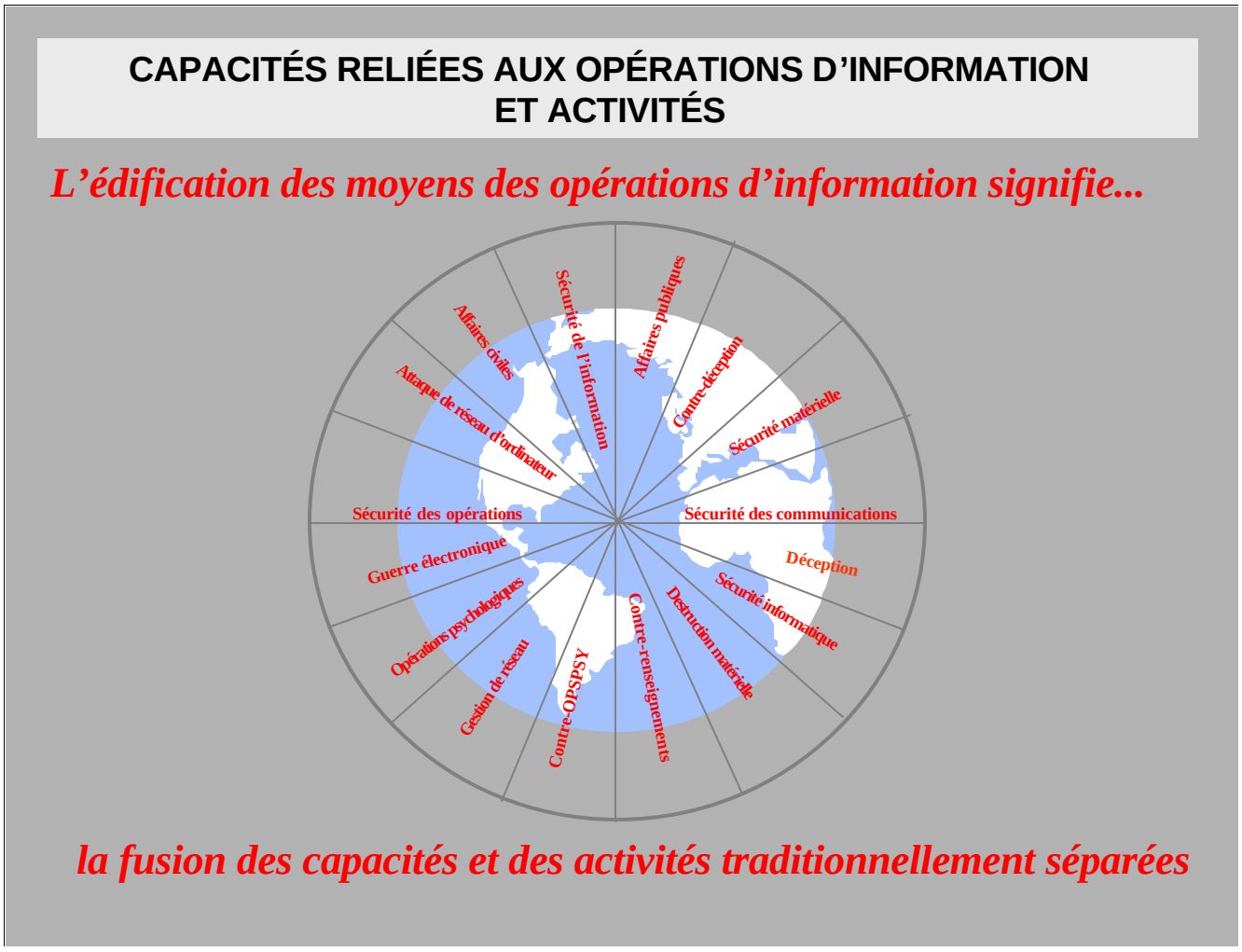


Tableau 1-4. Disciplines reliées aux opérations d'information

(2) Des opérations d'information offensives incluent des actions prises pour influencer des décideurs adversaires actuels ou potentiels. Cela peut être fait en affectant l'utilisation ou l'accès à l'information et des systèmes d'information d adversaire ou de l'adversaire potentiel. Des opérations d'information offensives peuvent comprendre l'utilisation des OPSPSY, la déception, la GE, le renseignement, l'attaque de réseau informatique, la destruction matérielle et des opérations d'information spéciales (SIO).

(3) Des opérations d'information défensives incluent des actions prises pour protéger ses propres informations et assurer que les décideurs amis ont un accès opportun à des informations nécessaires, pertinentes et précises. Des opérations d'information défensives assurent aussi que des décideurs amis sont protégés de tout effort des opérations d'information offensives adversaires. Des opérations d'information défensives s'efforcent de s'assurer que le processus de décision ami est protégé de tous les effets nuisibles, délibérés, par inadvertance ou accidentels. Les opérations d'information défensives sont un processus intégrant et coordonnant les politiques, les procédures, les opérations, le renseignement, le droit et la technologie.

e. La «supériorité de l'information» est la capacité d'acquérir, d'exploiter et de diffuser une circulation interrompue d'informations en niant la capacité à l'ennemi de faire la même chose. (Source: directive de politique sur les opérations d'information du QGDN). La supériorité de l'information peut être tout

envahissante dans la zone d'opérations (AO) ou elle peut être fonction ou avoir un aspect spécifique, localisé et temporel.

f. Des opérations d'information spéciales (SIO) sont des opérations d'information de nature délicate dues à leur effet potentiel ou impact, les besoins de sécurité ou le risque à la sécurité nationale du Canada demandent un examen spécial et un processus d'approbation. (Source: directive de politique sur les opérations d'information du QGDN)

> ***"La force n'a pas sa place où il y a un manque de compétence."***
> **Herodotus, *The Histories of Herodotus***

103. PRINCIPES DES OPÉRATIONS D'INFORMATION

1. Généralités

a. Des systèmes d'information complexes croissants sont intégrés dans les opérations militaires comme le commandement, le transport; la logistique et le renseignement. Plusieurs de ces systèmes sont conçus et employés avec des vulnérabilités inhérentes qui sont dans plusieurs cas les conséquences inévitables de fonctionnalité améliorée, d'efficacité et d'avantage aux utilisateurs. Le bas coût associé à une telle technologie le rend efficace et rentable pour étendre les capacités (et les vulnérabilités) à un nombre sans précédent d'utilisateurs. Le grand accès et l'usage de ces systèmes d'information améliore les opérations militaires. Toutefois, ces capacités utiles provoquent de la dépendance et cette dépendance crée des vulnérabilités. Ces vulnérabilités sont une arme à deux tranchants représentant des zones que les composantes peuvent protéger en créant d'un autre côté de nouvelles occasions pouvant être exploitées contre les adversaires. Voir Tableau 1-5.

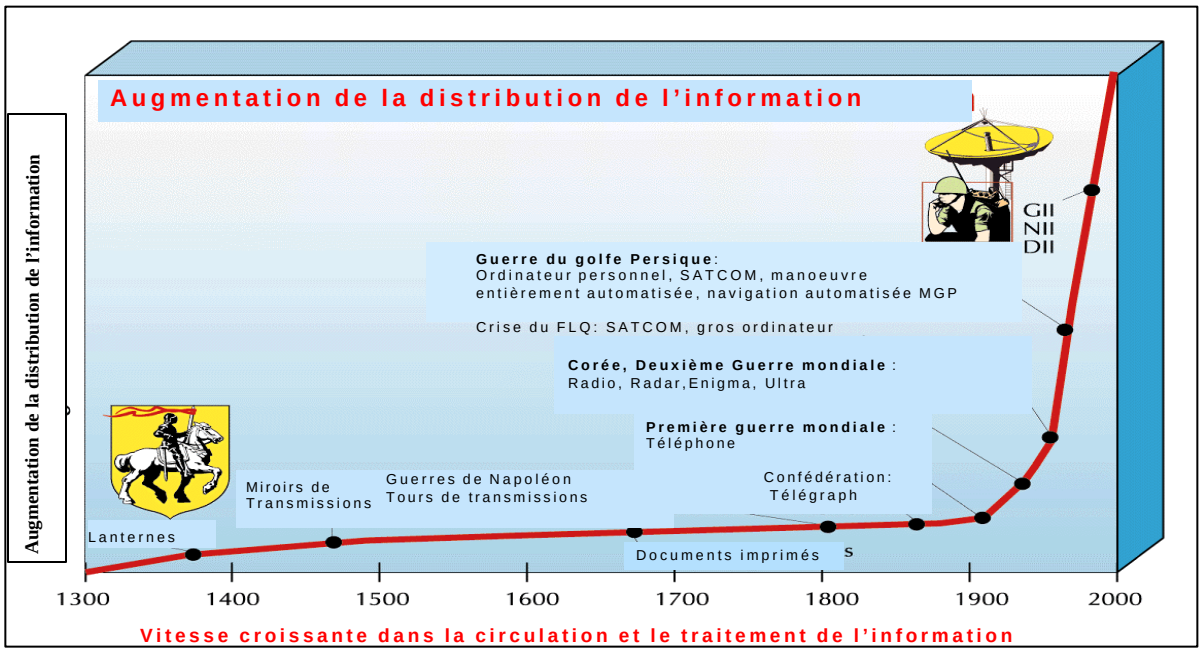


Tableau 1-5 Augmentation de l'accès à l'information

b. En conservant l'accent sur influer le décideur, les opérations d'information peuvent aussi être capables de capitaliser sur une sophistication croissante, la connectivité et la fiabilité sur la technologie de l'information. Un ensemble cible des opérations d'information peut être l'information ou les systèmes d'information de façon à influencer le processus dépendant de l'information soit humain ou automatisé.

Des processus dépendants de telle information s'étendent de la prise de décision de niveau du Cabinet au contrôle automatisé d'infrastructures commerciales clés comme le transport et l'énergie électrique.

c. Plusieurs systèmes différents, disciplines et techniques doivent être intégrés pour réussir une stratégie des opérations d'information logiques. Le soutien du renseignement et des communications est important pour la conduite offensive et défensive des opérations d'information. La conception réfléchie et l'utilisation correcte des systèmes d'information sont fondamentales pour la conduite réussie des opérations d'information en général mais des opérations d'information principalement.

d. La stratégie des opérations d'information doit soutenir la stratégie militaire nationale et devra demander de la coordination, de la participation et du soutien des autres ministères canadiens et organismes ainsi que de l'industrie commerciale. Même si la circulation de l'information du MDN stratégique et opérationnelle dépend des infrastructures commerciales, la protection de ces infrastructures n'est pas sous l'autorité et la responsabilité du MDN. Le MDN doit assister dans la démonstration aux fournisseurs de services le besoin péremptoire d'une approche collaboratrice, d'équipe en ébauchant des solutions--non seulement pour soutenir le MDN et pour protéger la sécurité nationale canadienne mais de protéger leurs propres intérêts de propriété aussi. Des actions des opérations d'information offensives peuvent aussi demander une résolution de conflit interinstitution et une coopération. Voir Tableau 1-6

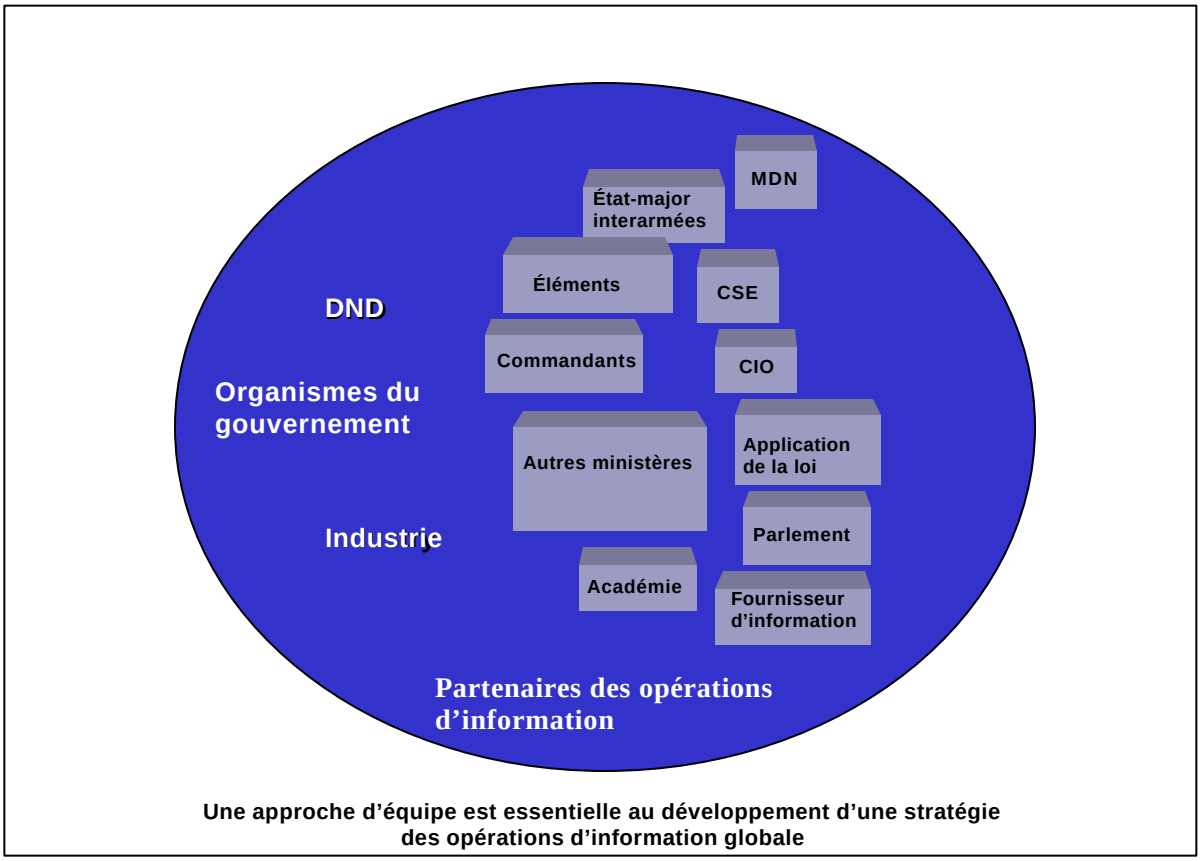


Tableau 1-6 Partenaires des opérations d'information

2. Environnement de l'information. La poussée continue des systèmes d'information et les technologies offrent un potentiel presque illimité d'exploitation du pouvoir de l'information dans la guerre interarmées. Les étiquettes placées sur les systèmes d'information et associés aux réseaux peuvent être trompeuses comme il n'y a pas de limites fixes dans l'environnement de l'information. Des systèmes ouverts et jumelés sont coalescents dans une infrastructure d'information globale (GII) enveloppant l'infrastructure d'information nationale (NII) et l'infrastructure d'information de la défense (DII).

a. L'infrastructure d'information de la Défense est enchâssée à l'intérieur et profondément intégrée dans le NII. Leurs relations sans coutures rendent la distinction entre eux impossible. Les deux partagent les réseaux de télécommunications terrestres, une variété de bases de données d'information et le réseau de télécommunications par satellite. Ces infrastructures connectent géographiquement les forces séparées et mesurent les frontières internationales. Voir Tableau 1-7.

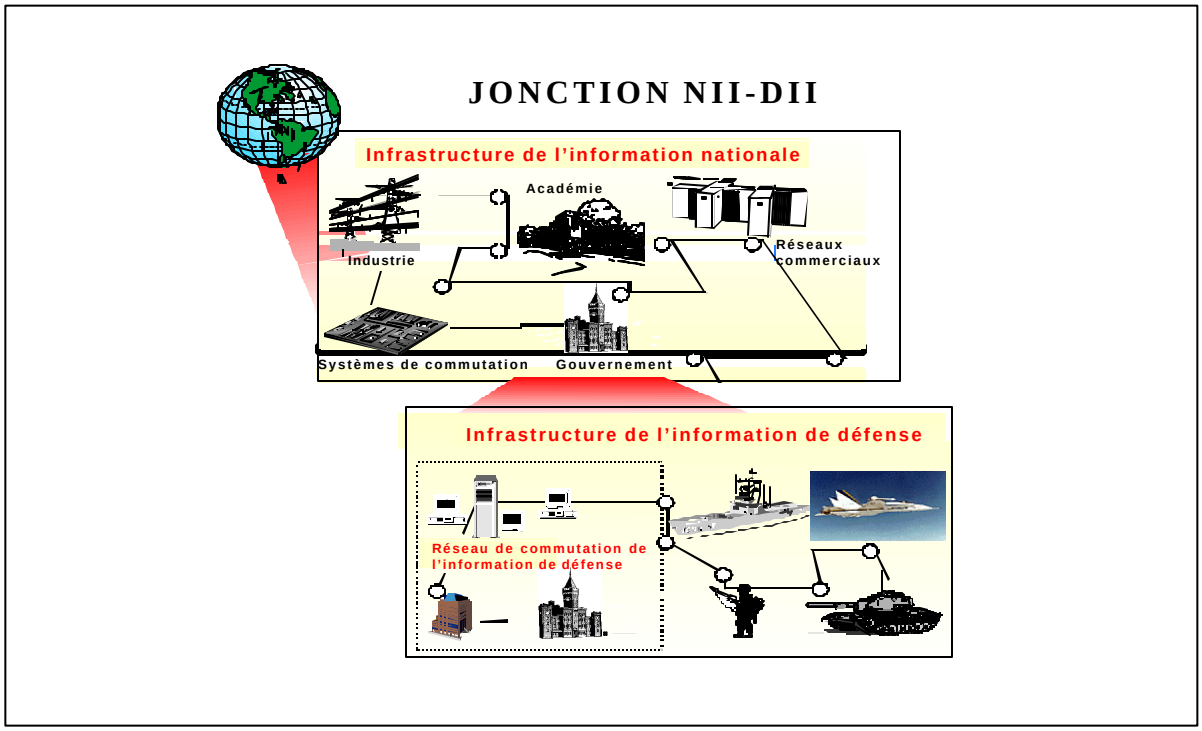


Tableau 1-7 Jonction NII-DII

b. L'infrastructure d'information globale est l'interconnexion à l'échelle mondiale des réseaux de communications, d'ordinateurs, de bases de données et d'électronique de grande consommation rendant de grands montants d'information disponibles aux usagers. Cela comprendra une vaste gamme d'équipement, incluant des caméras, des balayeurs, des claviers, des bélinographes, des ordinateurs, des commutations, des disques optiques compacts, des bandes vidéos et des bandes sonores, des câbles, des fils, des satellites, des lignes de transmission à fibres optiques, des réseaux de tous types, des télévisions, des moniteurs, des imprimantes et davantage. L'infrastructure nationale globale (GII) inclut plus que seulement les facilités matérielles utilisées pour emmagasiner, traiter et présenter l'information. Le personnel qui traitera l'information transmise constitue un élément important de l'infrastructure nationale globale.

c. L'infrastructure d'information nationale est semblable en nature et but à l'infrastructure d'information nationale mais est reliée quant à la portée seulement à un environnement d'information national.

d. L'infrastructure d'information de la défense est le système partagé ou étroitement lié d'ordinateurs, de communications, d'applications de données, de sécurité, de personnes, d'instruction et d'autres structures de soutien servant les besoins d'information du MDN locaux, nationaux et à l'échelle mondiale. L'infrastructure d'information de la défense connecte le soutien de la mission du MDN, C2 et les ordinateurs de renseignement avec la voix, les télécommunications, l'imagerie, le vidéo et les services multimédias. Il fournit le traitement d'information et les services aux souscripteurs au SNICC. Il inclut les systèmes du C2, tactiques, de renseignement et de communications commerciales utilisées pour transmettre l'information au MDN.

3. Les extensions du Système d'information de commandement et contrôle national. Les commandants à tous les niveaux devraient comprendre la nature, les complexités et les dépendances que les GII, NII et DII ont durant les diverses phases d'une opération, de l'avertissement, de la préparation, de déploiement, de l'emploi et du redéploiement dans la gamme des opérations militaires.

a. La conduite réussie de la guerre à l'âge de l'information demande un accès à l'information disponible à l'extérieur du théâtre des opérations. Les infrastructures de l'information n'équivalent plus aux lignes de commandement traditionnelles et les combattants ont besoin d'un accès à l'information fréquent, urgent et fiable aux localités dans le Canada ainsi que dans le théâtre. Cela peut demander l'extension de notre infrastructure d'information au delà de l'environnement d'information établi en temps de paix. Par exemple, le transport et le soutien des forces dépendent grandement des infrastructures de secours commerciales incluant les télécommunications internationales, le réseau public commuté, les réseaux de transport et les grilles d'énergie électrique commerciales. Les forces interarmées demandent une vidéo téléconférence sécuritaire, une imagerie détaillée des sources nationales et/ou alliées, le renseignement, la logistique et d'autres données de soutien à partir de diverses localités. Les forces interarmées doivent avoir l'assurance que cette infrastructure élaborée peut atteindre le niveau de protection requis pour assurer le succès de la mission. La nature de ces infrastructures d'information complique la capacité du commandant de contrôler la circulation de l'information ou de gérer de façon dynamique l'information disponible et les ressources de télécommunications. Pour soutenir des opérations offensives, les commandants peuvent recourir à employer de l'information, engager des capacités et techniques fournissant un avantage d'information dans leur zone d'opérations.

b. La dépendance des FC sur l'infrastructure d'information nationale et internationale et l'exposition subséquente à une gamme complète de menaces provenant de pirates informatiques avec des criminels, vandales et terroristes aux États-nations ont apporté un éclairage et une pertinence convaincante aux concepts des opérations d'information émergentes. Le pouvoir de mettre en place un niveau de protection pour ces infrastructures peut résider en dehors du MDN et du gouvernement canadien. Donc, le MDN/FC doit travailler dans des forums interinstitutionnels pour démontrer aux fournisseurs de service le besoin convaincant d'une approche de collaboration, d'équipe pour assurer que les forces amies ont accès à une information ponctuelle et pertinente au lieu et moment requis.

c. Les caractéristiques uniques des technologies basées sur de l'information de pointe ont mis en jeu les capacités révolutionnaires qui amélioreront et soutiendront les opérations militaires dans le prochain siècle. Voir le Tableau 1-8.

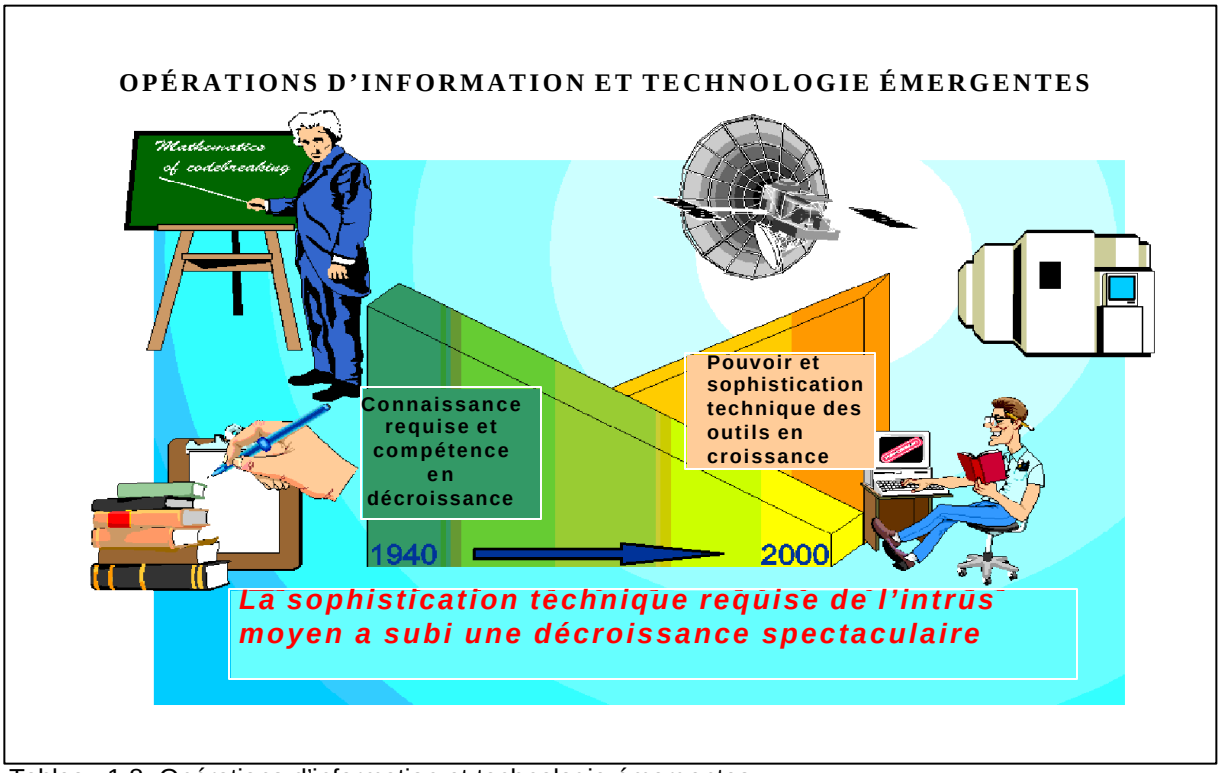


Tableau 1-8 Opérations d'information et technologie émergentes

4. Gamme cible des opérations d'information. Les cibles des opérations d'information sont déterminées par les objectifs globaux des commandants et sont influencés grandement par une analyse du renseignement approfondie. Le soutien du renseignement au commandant devrait inclure le développement des bases de données et gabarit pour déterminer les vulnérabilités d'une information adversaire, des processus basés sur l'information et des systèmes d'information. Inversement, le module de coordination des opérations d'information devrait identifier les vulnérabilités des informations amies, des processus basés sur de l'information et des systèmes d'information qu'un adversaire est normalement ciblé. Des exemples des cibles des opérations d'information sont montrés au Tableau 1-9.

a. Tel que montré au Tableau 1-9 il y a plusieurs types de cibles des opérations d'information. Une identification précoce des éléments importants concernant des cibles des opérations d'information spécifiques est essentielle à une offensive réussie des opérations d'information et défensive. Des opérations d'information offensives peuvent cibler seulement un élément clé d'un ensemble cible des opérations d'information adversaires importantes spécifiques et atteindre un grand succès. Inversement, la compréhension de la nature de la menace aidera la défense contre les capacités des opérations d'information offensives adversaires.

Tableau 1-9 Exemples de cibles des opérations d'information

b. Dans le but ultime d'influencer le décideur, le C2 demeure une cible substantielle des opérations d'information. Des systèmes de communications commerciaux liés aux systèmes C2 amis et ennemis offrent des défis uniques au ciblage offensif et à la protection défensive.

c. Des exemples de zones clés du soutien de guerre comprenant des gammes de cible potentielles et offensives et exigeant de la protection comprennent, jusques y compris, la logistique, le renseignement et les systèmes de communications non C2. Une infrastructure commerciale amie aussi peut être ciblée par des capacités offensives d'un adversaire; dans la même veine, une infrastructure commerciale adversaire est aussi la cible potentielle pour des capacités offensives amies.

5. Guerre de commandement et de contrôle (C2W)

a. Le C2W est une application des opérations dinformation dans les opérations militaires et un sous-ensemble des opérations d'information. Le C2W attaque spécifiquement les cibles du C2 adversaires en défendant l'ensemble cible du C2 ami. L'ensemble cible C2 inclut des cibles pouvant affecter la capacité de l'adversaire à exercer le commandement et le contrôle sur ses forces militaires.

b. Le C2W est l'utilisation intégrée de toutes les capacités militaires incluant la SECOP, la déception, les OPSPSY, la GE et la destruction matérielle soutenue par toute source du renseignement et des Systèmes d'information et de communications (CIS), pour nier l'information, influencer, dégrader ou détruire des capacités du C2 adversaires en protégeant les capacités du C2 amies contre des actions semblables.

c. Le C2W s'applique à toute la gamme des opérations militaires et à tous les niveaux de conflit. Le C2W est à la fois offensif et défensif.

(1) Attaque C2. Empêcher un C2 efficace des forces adversaires en niant de l'information ou influençant, dégradant ou détruisant le système C2 adversaire.

(2) Protection C2. Maintient un C2 efficace de nos propres forces en retournant à l'avantage ami ou reniant les efforts de l'ennemi pour nier l'information d'influencer, de dégrader ou de détruire le système C2 ami.

6. Autres éléments intégraux des opérations d'information

a. Les Affaires publiques (AP) cherchent une circulation de l'information dans les audiences externes et internes. La coordination des plans des AP et des opérations d'information est requise pour assurer que les initiatives des AP soutiennent les objectifs généraux du commandant. Les efforts des affaires publiques et des opérations d'information seront compatibles avec la limite de politique ou statutaire.

b. Les activités des Affaires civiles (CA) sont importantes aux opérations d'information à cause de leur capacité de joindre les organisations clés et les individus dans l'environnement d'information. Les CA peuvent soutenir et assister les objectifs des opérations d'information par la coordination, l'influence, le développement ou le contrôle des infrastructures indigènes dans des zones opérationnelles étrangères.

7. Soutien du renseignement

a. Le soutien du renseignement est important pour la planification, l'exécution et l'évaluation des opérations d'information. Le représentant (J-2) du renseignement d'état-major interarmées assigné pour soutenir les opérations d'information devrait être la liaison du soutien du renseignement pour toute la planification des opérations d'information.

b. Le renseignement doit être facilement accessible, opportun, précis et suffisamment détaillé pour soutenir une série de besoins des opérations d'information du MDN, incluant la recherche, le développement, l'acquisition et le soutien opérationnel.

c. La conduite des opérations d'information sophistiquées demande des renseignements uniques et détaillés jamais demandés auparavant des organismes de renseignement et des activités. La préparation du renseignement de l'espace de bataille (IPB) est importante aux opérations d'information.

d. Les produits du renseignement doivent soutenir la planification des opérations d'information, fournir l'analyse d'un adversaire potentiel des vulnérabilités des opérations d'information, permettre la détermination des capacités et des intentions d'un adversaire potentiel des opérations d'information, fournir des indications et avertissements (I&W) de toute menace potentielle et contribuer directement au Système de mesures de précaution.

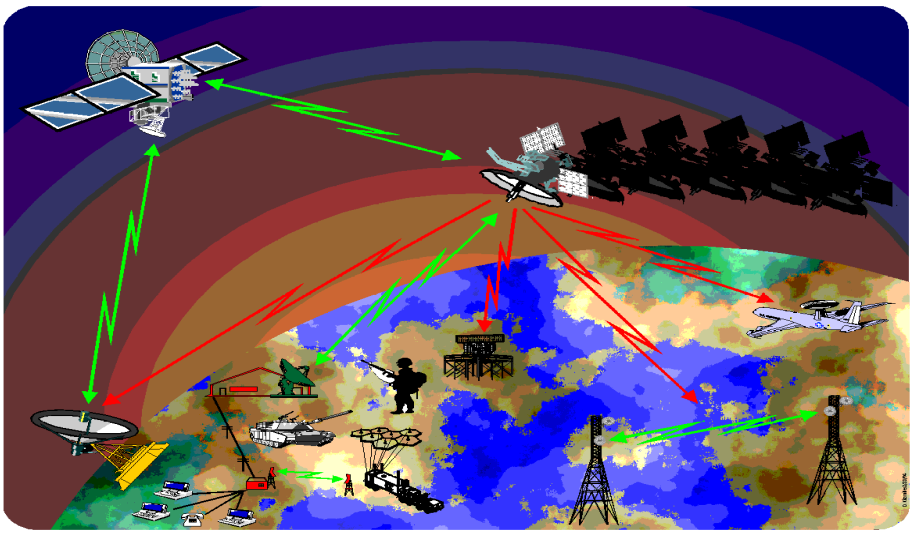
e. L'orientation du soutien du renseignement spécifique requis pour des opérations d'information offensives et défensives est fourni aux chapitres II, «Opérations d'information offensives» et III «Opérations d'information défensives,» respectivement.

«Rien n'a plus d'importance pour un bon général que la tentative de pénétrer les desseins de l'ennemi.»
Niccolo Machiavelli, Discours

8. Les opérations d'information servant d'outil aux commandants

a. Des technologies basées sur de l'information développée rapidement et un environnement global compétitif croissant ont de l'information importante dans l'étape du centre de la société, le gouvernement et la guerre du 21e siècle. L'information et les technologies basées sur l'information sont pénétrantes et elles affectent chaque facette d'une crise ou d'un conflit à partir des phases de l'avertissement, de la préparation, l'emploi et le redéploiement des opérations des FC à la pléthore des forces et systèmes d'armes employés par les commandants. Voir Tableau 1-10.

TECHNOLOGIE COMME OUTIL DES OPÉRATIONS D'INFORMATION



Technologies basée sur de l'information avancée…
l'outil clé du commandant pour les opérations d'information

Tableau 1-10. Technologie comme outil des opérations d'information

b. Les changements révolutionnaires dans les technologies de l'information présentent aux commandants les opportunités uniques utilisant les opérations d'information pour affecter les actions des autres au moyen de l'utilisation intégrée de toutes les capacités. Il est maintenant possible aux commandants de masser l'effet physique et l'effet psychologique au bon moment et au bon endroit pour miser sur leur puissance de combat et décideurs ayant de l'influence en utilisant les opérations d'information et ses technologies d'information de soutien.

c. Les opérations militaires et l'application précise de puissance de combat dépendent largement sur plusieurs activités simultanées et intégrées, en retour, dépendent de l'information et des systèmes d'information, spécialement ces activités associées aux processus de C2 importants. Certaines de ces activités incluent le déploiement stratégique de direction, les forces dans le théâtre de soutien, assurant la protection de la force--dans la garnison et des zones d'intervention lointaine, préservant le C2 stratégique dans le théâtre et développant le renseignement stratégique et dans le théâtre.

d. L'information elle-même devient une ressource stratégique importante pour la sécurité nationale. Cette réalité s'étend à travers le continuum du conflit. Des systèmes d'information complexes accrus sont intégrés dans des disciplines traditionnelles comme le transport, la logistique et le renseignement.

e. Les opérations d'information peuvent être utilisées pour renforcer des intérêts communs et des objectifs de partenaires multinationaux et empêcher les adversaires d'initier des actions préjudiciables aux intérêts du Canada, des partenaires ou à la conduite des opérations militaires amies.

f. Si soigneusement conçues, coordonnées et exécutées, les opérations d'information apporteront une importante contribution aux efforts des commandants opérationnels pour désamorcer les crises et retourner à la paix, réduire les périodes de confrontation, améliorer l'impact d'autres éléments du pouvoir national et prendre les devants ou éliminer le besoin d'employer les forces de combat. Toutefois, les opérations d'information doivent simultanément préparer aussi l'espace de bataille en vue du conflit.

Durant la guerre du golfe Persique, les opérations d'information défensives assuraient que la Coalition défasse solidement la stratégie politique de Saddam Hussein visant à influencer le leadership de la nation de la coalition dans la prise de décision. L'Irak a commencé une campagne de soutien public immédiatement après l'invasion du Koweit. Cet effort incluait la diffamation de la famille dirigeante du Koweit et faisait le portrait de l'Irak comme le champion de l'anticolonialisme, de la justice sociale, de l'unité arabe, de la cause palestinienne et de l'Islam. Dans un mouvement apparent pour désamorcer la condamnation internationale initiale de son invasion du Koweit, Saddam a faussement annoncé que les troupes irakiennes commenceraient à se retirer du Koweit le 6 août 1990. En dépit des efforts d'Hussein pour influencer les actions de la Coalition, la stratégie d'information de la Coalition a assuré que la guerre était faite dans des conditions favorables prenant l'avantage entier des forces de la Coalition et des faiblesses des Irakiens assurant que la stratégie politique et militaire de Saddam était solidement défaite. En dépit des essais d'Hussein d'intimider ses voisins, les États du Golfe demandaient de l'aide extérieure et la formation d'une Coalition. La «rue» arabe ne s'est pas révoltée en son nom et la contrainte israélienne à la face des attaques de Scud a ébranlé son plan de changer la guerre en un conflit arabe-israélien. Le leadership de coalition a agressivement riposté aux menaces largement rendues publiques des pertes massives et de ses prises d'otages, aucune d'elles n'a empêché la résolution de la Coalition. Les tentatives de Saddam de prendre l'offensive en utilisant les Scud et l'attaque sur la ville saoudienne de Al-Khafji n'ont pas atteint leur but stratégique de réduire la volonté de combattre de la Coalition. Sur tous les fronts de l'information, l'emploi efficace des informations d'opérations par la Coalition de défense contre la stratégie d'information de Saddam assurait que l'Iraq n'était pas seulement battu mais a aussi échoué à prendre même l'initiative.

Source: Conduite de la guerre du golfe Persique
Premier rapport au Congrès, avril 1992

CHAPITRE 2

OPÉRATIONS D'INFORMATION OFFENSIVES

> ***"Frappez en premier! Continuez de frapper!"***
> **Admiral Sir John Fisher, *Mémoires*, 1919**

201. PRINCIPES ET CAPACITÉS

1. Il y a les aspects offensif et défensif des opérations d'information. Les ensembles de cible impliqués dans les opérations d'information sont un lien commun entre les deux aspects. Les capacités des opérations d'information offensives seront employées à chaque niveau de guerre, dans la gamme des opérations militaires pour atteindre les objectifs de la mission. L'emploi d'une stratégie des opérations d'information d'influencer un décideur peut donner un avantage énorme aux Forces canadiennes en temps de guerre et de conflit. En conséquence, les commandants doivent soigneusement étudier le potentiel des opérations d'information pour empêcher et réduire les crises.

a. Principles. Les principes des opérations d'information offensives comprennent ce qui suit:

(1) Le décideur à tous les niveaux et processus de prise de décision associés est la cible absolue pour des opérations d'information offensives. Les opérations d'information offensives sont employées comme stratégie d'intégration orchestrant des disciplines variées et des capacités dans un plan cohérent, sans couture pour atteindre des objectifs spécifiques.

(2) Les objectifs des opérations d'information offensives doivent être clairement établis, soutenir des objectifs nationaux globaux et militaires, et inclure des indicateurs identifiables de succès.

(3) La sélection et l'emploi de capacités offensives spécifiques contre un adversaire devraient être adaptés à la situation et conformes aux conventions internationales applicables et règles d'engagement permanentes.

(4) Des opérations d'information offensives peuvent être l'élément principal ou de soutien d'une campagne du commandant ou opération.

(5) Des opérations d'information offensives en soutien d'une campagne du commandant ou opération peuvent comprendre la planification et l'exécution par les forces en dehors du MDN, des organismes ou organisations et doivent être tout à fait synchronisées et coordonnées avec tous les autres aspects de la campagne de soutien ou l'opération.

(6) De façon à attaquer suffisamment l'information et les systèmes d'information, il est nécessaire d'être capable de faire ce qui suit:

(a) Déterminer la valeur de l'adversaire, l'utilisation et la circulation de l'information.

(b) Identifier et cibler les parties discontinues de l'information de l'adversaire ou de systèmes d'information.

(c) Prédire les conséquences d'emploi des capacités offensives spécifiques avec un niveau prédéterminé de confiance.

(d) Évaluer la portée des attaques des opérations d'information spécifiques avec confiance.

b. Capacités. Vues comme stratégie d'intégration, les opérations d'information entremêlent les disciplines reliées et les capacités envers la satisfaction d'un objectif énoncé. Les opérations d'information s'appliquent aux disciplines de gestion de perception traditionnelle comme les OPSPSY et l'attaque du système d'information pour produire un effet synergique contre les éléments restants de systèmes d'information de l'adversaire. Il y a plusieurs capacités et disciplines exigeant l'intégration défensive et offensive pour mener des opérations d'information réussies. Certaines de ces capacités ou disciplines paraissent plus offensives ou défensives en nature mais c'est leur intégration et leur synergie potentielle qui assurent des opérations d'information offensives et défensives. Les capacités et les disciplines pouvant mener des opérations d'information offensives comprennent ce qui suit:

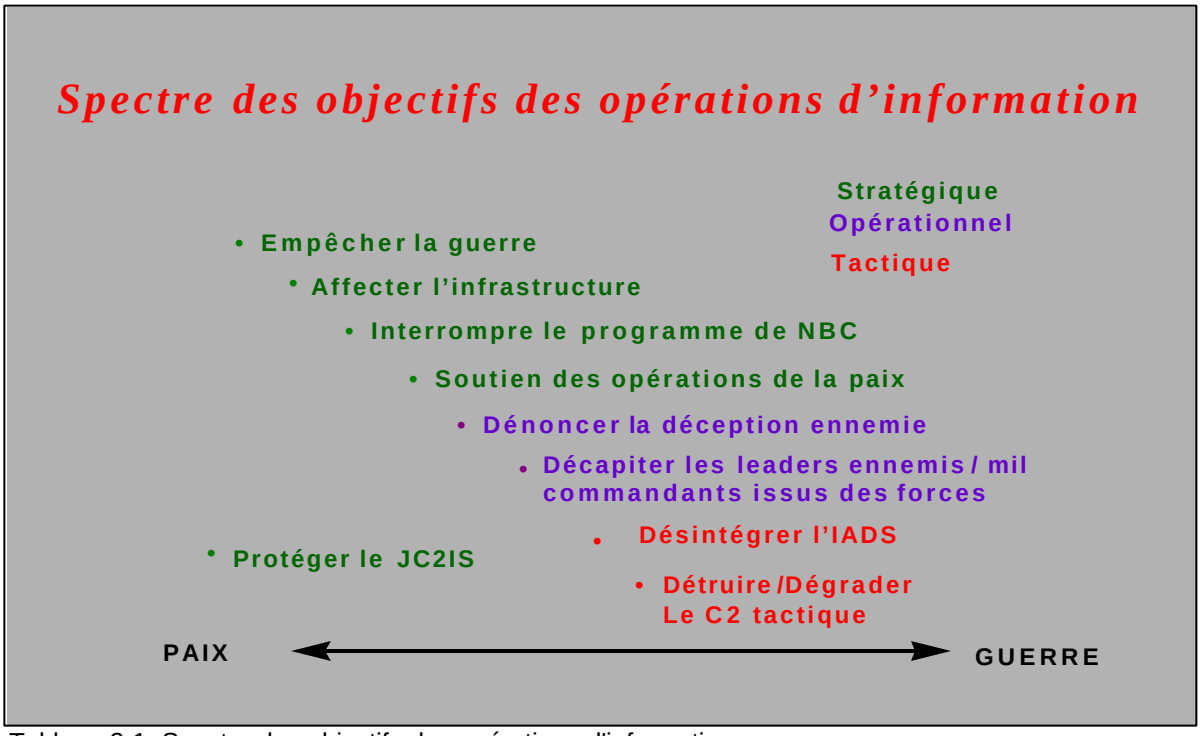


Tableau 2-1. Spectre des objectifs des opérations d'information

(1) C2W: Les mêmes éléments qui soutiennent traditionnellement le C2W -- la SECOP, les OPSPSY, la déception militaire, la GE et la destruction matérielle - peuvent être utilisés pour mener des opérations d'information offensives.

(a) SECOP

1. La SECOP est un processus d'identification d'information importante et par la suite d'analyse des actions amies au service des opérations militaires et autres activités pour:

a. Identifier ces actions pouvant être observées par des systèmes de renseignement adversaires.

b. Déterminer les indicateurs que les systèmes de renseignement adversaires peuvent obtenir pouvant être interprétés ou rassemblés pour tirer de l'information critique en temps utile.

c. Sélectionner et exécuter des mesures éliminant ou réduisant à un niveau acceptable les vulnérabilités des actions amies exploitées par l'adversaire.

2. L'histoire a démontré la valeur et le besoin de renseignement fiable, adéquat et opportun et le tort résultant de ses imprécisions et absence. Il est donc vital et avantageux de nier aux commandants adversaires l'information importante dont ils ont besoin et les obliger à dériver des appréciations imprécises, opportunes influençant leurs actions.

3. La plus importante caractéristique de la SECOP est que c'est un processus. La SECOP n'est pas un rassemblement de règles spécifiques et d'instructions pouvant être appliquées à chaque opération. C'est une méthodologie pouvant être appliquée à toute opération ou activité dans le but de nier cette information importante à l'ennemi. La SECOP s'applique à toutes les activités militaires à tous les niveaux de commandement. Le CFO devrait fournir une orientation de planification de la SECOP à l'état-major au temps voulu par le commandant et par la suite aux commandants de soutien dans la chaîne de commandement. En maintenant la liaison et coordonnant l'orientation de planification de la SECOP, le CFO assurera l'unité d'effort en gagnant et maintenant le secret essentiel considéré nécessaire au succès.

"Aucune entreprise n'a le plus de chances d'avoir du succès qu'une entreprise cachée de l'ennemi jusqu'à ce qu'elle soit prête à exécution."

Niccolo Machievelli, *L'art de la guerre*, 1521

(b) OPSPSY. Pendant que l'on se rend compte que les FC ne possèdent pas actuellement une capacité formelle des OPSPSY, plusieurs partenaires alliés potentiels n'ont pas cette capacité. Donc, les OPSPSY doivent être étudiées pour avoir une intégration efficace de toutes les capacités des opérations d'information.

1. Les OPSPSY sont des actions pour transmettre l'information choisie et des indicateurs aux destinataires étrangers. Elles sont conçues pour influencer les émotions, les motifs, le raisonnement et finalement, le comportement de gouvernements étrangers, d'organisations, de groupes et d'individus. Les OPSPSY ont des applications stratégiques, opérationnelles et tactiques incluant le soutien à des opérations de déception.

2. Au niveau stratégique, les OPSPSY peuvent prendre la forme de positions politiques ou diplomatiques, d'annonces ou de communiqués. Au niveau opérationnel, les OPSPSY peuvent comprendre la distribution de prospectus, d'émissions radio ou de télévision et d'autres moyens de transmission d'information pouvant encourager les forces de l'ennemi à faire défection, déserter, s'enfuir ou se rendre. Des attaques persistantes peuvent avoir un effet synergique avec les OPSPSY, accélérant la dégradation de la morale et encourageant davantage la désertion. Au niveau tactique, les OPSPSY incluent les mesures de promotion de la crainte ou de la dissension dans les rangs de l'ennemi.

3. Les OPSPSY peuvent contribuer de façon significative à tous les aspects des opérations interarmées. Le *Manuel des opérations des Forces canadiennes B-GG-005-004/AF-000*, Chapitre 34, "Opérations psychologiques" fournit de l'information supplémentaire.

"La vraie cible est l'esprit du commandant ennemi, non les corps de ses troupes."

Capitaine Sir Basil Liddell Hart, *Pensées sur la guerre*, 1944

(c) Déception

1. Ces mesures constituant la déception sont conçues pour induire l'ennemi en erreur par la manipulation, la distortion ou la falsification de la preuve pour l'amener à réagir de façon à nuire à ses intérêts.

2. La déception militaire, telle qu'exécutée par le CFO, cible les décideurs ennemis au moyen de leurs systèmes de collecte de renseignement, d'analyse et de diffusion. Cette déception demande une connaissance approfondie d'opposants et de processus de décision. L'anticipation est la clé. Durant la formulation du concept de commandant, une attention particulière est placée à définir la façon dont le CFO aimerait que l'ennemi agisse aux points critiques de la bataille. Ces actions ennemies désirées deviennent alors le but des opérations de déception. La déception se centre sur le comportement désiré, non pas simplement en fonction d'induire en erreur. Le but est d'amener les commandants adversaires à former les impressions imprécises sur les capacités de force amies ou d'intentions, de détourner les avoirs de la collecte du renseignement ou de manquer d'employer les unités de combat ou de soutien dans le meilleur intérêt.

3. Les opérations de déception sont un élément intégral des opérations interarmées. La planification des opérations de déception est descendante dans le sens que les plans de déception subordonnés soutiennent le plan de niveau supérieur.

4. Les commandants à tous les niveaux peuvent planifier des opérations de déception. Les plans peuvent inclure l'emploi d'unités de niveau inférieur même si les commandants subordonnés peuvent ne pas connaître l'effort de déception global. Il est donc essentiel pour les commandants de coordonner leurs plans de déception avec leur commandant principal pour assurer une unité globale d'effort.

5. Les opérations de déception dépendent des opérations du renseignement pour identifier les cibles de déception appropriées, pour aider à développer une histoire crédible pour identifier le destinataire de l'effort de déception et évaluer l'efficacité du plan de déception.

6. Les opérations de déception ne sont pas sans rien coûter mais un outil puissant dans les opérations à pleines dimensions. Les forces et les ressources doivent être engagées envers l'effort de déception pour le rendre crédible peut-être au détriment à court terme de certains aspects de la campagne. Les SECOP des opérations de déception peuvent dicter que seulement un groupe sélectionné de commandants principaux et d'officiers d'état-major dans la force interarmées connaissent quelles actions sont simplement trompeuses en nature. Cette situation peut provoquer de la confusion à l'intérieur de la force et doit être surveillée de près par les CFO et leur état-major.

> ***"Toute la guerre est basée sur la déception."***
>
> **Sun Tzu, *L'art de la guerre*, c. 500 BC, tr. Griffith**

(d) GE

1. La GE est une action militaire exploitant le spectre électromagnétique incluant l'interception et l'identification des émissions électromagnétiques, l'emploi de l'énergie électromagnétique incluant l'énergie dirigée pour réduire ou empêcher une utilisation hostile du spectre électromagnétique et des actions pour assurer son utilisation efficace par les forces amies. Les trois subdivisions majeures de la GE sont les mesures de soutien de guerre électronique (MSGE), les contre-mesures électroniques (CME) et les mesures de

protection électronique (MPE). La GE est une capacité des opérations d'information pouvant appuyer des opérations d'information offensives et défensives. Toutes les trois subdivisions de GE contribuent à un effort des opérations d'information.

2. La MSGE fournit une source d'information requise pour des décisions immédiates impliquant des CME, des MPE et d'autres actions tactiques. Les CME empêchent ou réduisent l'utilisation efficace de l'adversaire du spectre électromagnétique au moyen de l'usage de l'énergie électromatique. Les MPE assurent une utilisation efficace du spectre électromagnétique en dépit de l'emploi adversaire de l'énergie électromagnétique.

3. Toutes les subdivisions de GE devraient être employées pour affecter l'ensemble de cible comme approprié et selon des principes établis de guerre. La décision d'employer la GE devrait être basée non seulement sur les objectifs de mission interarmées globaux mais aussi sur les risques de réponses adversaires possibles et d'autres effets sur la mission.

4. Le CFO devrait assurer une coordination maximum parmi la GE et les autres activités de soutien du renseignement et des communications des opérations d'information pour un effet maximum. La coordination est nécessaire pour avoir un échange d'information efficace, éliminer le chevauchement d'effort indésirable et fournir un soutien mutuel ainsi que de réduire les probabilités de fratricide électronique. Voir le *Manuel des opérations des Forces canadiennes, B-GG-005-004/AF-000,* chapitre 33, "Guerre électronique" pour des informations supplémentaires.

(e) La destruction physique réfère à l'utilisation d'armes de "destruction" contre des cibles désignées comme élément d'un effort des opérations d'information intégré. Même si des hiérarchies C2 de l'adversaire seront des cibles de grande valeur, un avantage à long terme venant de leur destruction ne peut être assumé depuis que l'opposition peut normalement s'appliquer également à haute priorité à leur reconstitution. Le moment pour l'application de la destruction matérielle est important pour assurer que les opérations ultérieures exploitent tout effet à court terme. La destruction matérielle peut être le seul choix disponible pour attaquer un adversaire C2 incluant les quartiers généraux et le SIC pouvant être localisé à l'intérieur d'installations fortifiées.

(2) AP: les AP sont un élément important des opérations d'information pouvant appuyer des opérations d'information offensives au moyen de la création d'un sens des objectifs militaires durant une opération ou une mission.

(a) les activités des AP accélèrent la circulation d'information précise et opportune à des destinataires internes (leur propre organisation) et externe (le public).

(b) les activités des AP satisfont les désirs des destinataires internes et externes à informer au sujet de l'opération ou de la mission.

(c) les activités des AP encouragent une attitude favorable envers l'opération ou la mission.

(d) les activités des AP informent les destinataires internes et externes de développements importants les touchant.

(e) les activités des AP permettent au CFO d'influencer la perception d'un adversaire (ou un adversaire potentiel) sur l'intention de la force amie, de la capacité et de la vulnérabilité. Au même moment, les activités des AP ne seront pas utilisées comme capacité de déception militaire ou de fournir de la désinformation à des destinataires internes ou externes. Les activités des AP seront compatibles avec les efforts de la SECOP continus. Voir *Le manuel des Forces canadiennes*, B-GG-*005-004/AF-000*, Chapitre 29, "Affaires publiques" pour de plus amples renseignements.

> ***"Une fois que le respect de la vérité n'est plus le même ou même est le moindrement ébranlé, rien n'est hors de doute."***
>
> **Saint-Augustin, *"Sur le mensonge"***

(3) CA : les CA (affaires civiles) sont un élément important des opérations d'information pouvant soutenir les opérations d'information au moyen de la création d'une attitude positive parmi les factions belliqueuses, les non belligérants et/ou la populace générale dans la zone de tension ou de conflit.

(a) les activités des CA sont ces activités militaires interreliées incluant la relation entre les forces militaires et les autorités civiles et les populations.

(b) les activités des CA sont caractérisées par l'application des spécialités fonctionnelles, dont deux sont les communications publiques et les renseignements civils.

(c) les activités des CA sont menées par des forces (unités et personnel) possédant une compréhension en profondeur des aspects politico-militaires, économiques et sociaux des pays ou zones régionales où des forces militaires sont employées.

(d) les activités des CA améliorent et influencent la planification et l'exécution opérationnelle civilo-militaire par le MDN, en dehors du MDN, multinationales et non gouvernementales ou les organisations volontaires privées et d'autres organismes au moyen de budgets d'impacts opérationnels sur la populace civile, les ressources et les institutions dans les zones où les forces militaires sont employées.

(e) les activités des CA incluent le concept fondamental de contrôle de la politique au plus haut niveau pratique ajouté à l'intégration des efforts militaires et civils au plus bas échelon faisable.

(f) les activités des CA incluent le besoin de négocier et de soumettre à la médiation avec les belligérants durant les opérations d'imposition de la paix. Voir *Le manuel des opérations des Forces canadiennes, B-GG-005-004/AF-000,* Chap 30, "Coopération civilo-militaire" (COCIM) pour de plus amples renseignements.

202. GAMME DES OPÉRATIONS MILITAIRES

1. Des opérations d'information offensives peuvent être menées dans une variété de situations et de circonstances dans toute la gamme des opérations militaires. Les opérations militaires offensives peuvent avoir leur plus grand impact en temps de paix et dans les stages initiaux d'une crise. L'impact des opérations d'information dans la gestion de la perception ou de l'influence de la prise de décision d'un adversaire est le plus élevé en temps de paix et des opérations hors guerre (OOTW). Le but des opérations d'information initiales est de désamorcer la crise et prévenir le conflit. Comme dans une situation ou la circonstance se déplace vers le conflit, la capacité de cibler et d'engager de l'information adversaire importante et des systèmes d'information décroît. Comme un adversaire se prépare en vue d'un conflit, les systèmes de renseignement deviennent importants aux opérations de l'adversaire. Voir Tableau 2-2.

a. Opération hors guerre

(1) Certains des éléments des plans des opérations d'information offensives et de leurs capacités associées peuvent être employés en temps de paix pour empêcher la crise, contrôler l'escalade de la crise, projeter le pouvoir ou promouvoir la paix. L'emploi des capacités des opérations d'information offensives dans ces circonstances peut demander l'approbation du Cabinet avec le soutien, la coordination, la résolution de conflit, la coopération et/ou la participation par les autres ministères et les organismes. Les efforts des opérations d'information offensives militaires doivent être synchronisés avec d'autres efforts des opérations d'information du gouvernement canadien pour éviter des chances gaspillées et de rendre capable la capacité des opérations d'information si nécessaire et pour empêcher la confusion. Pour synchroniser les efforts offensifs, un agent responsable devrait être identifié, des objectifs désirés devraient être déterminés et des mesures de succès des opérations d'information devraient être établies.

(2) L'agent responsable des opérations d'information, les objectifs et les mesures d'efficacité changeront basés sur la situation ou les circonstances--influençant un adversaire potentiel en temps de paix ou en conduisant diverses opérations hors guerre. Selon l'objectif militaire et une capacité croissante de cibler précisément et engager des systèmes d'information adversaires, des opérations d'information offensives peuvent être utilisées pour prévenir l'emploi de la force du plan d'action adversaire ou détériorer la capacité de réponse donc d'influencer l'objectif global de retour à la paix.

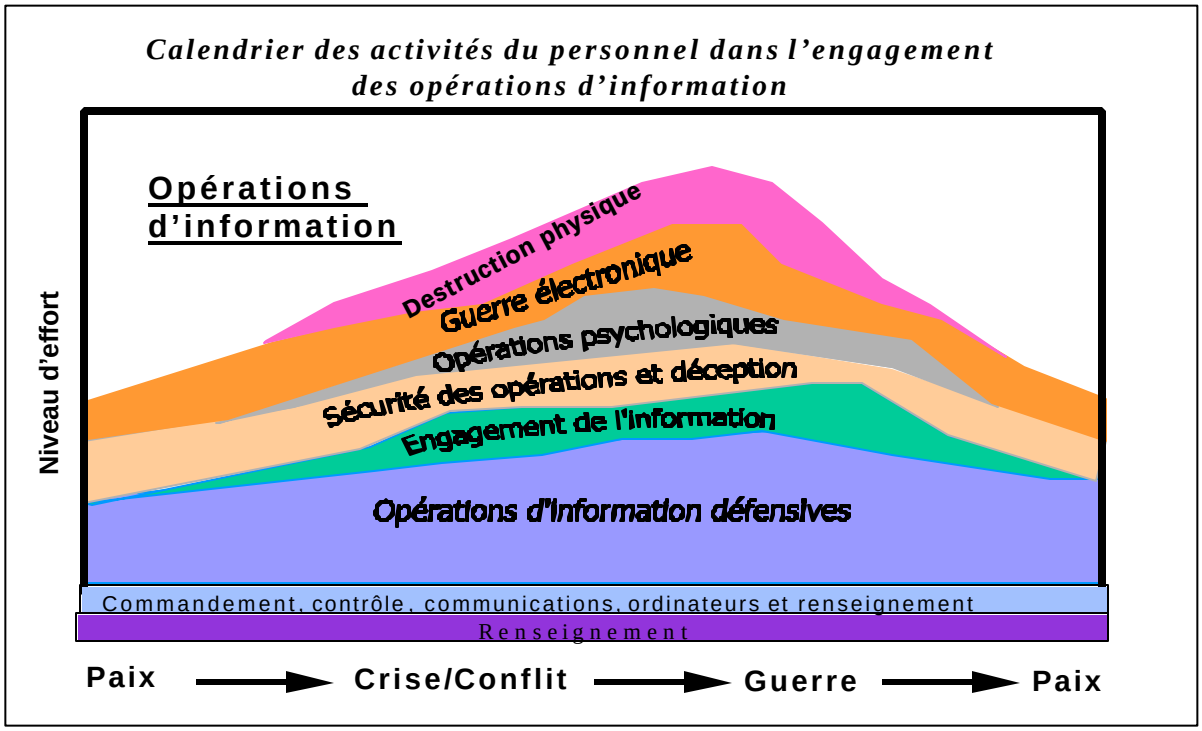


Tableau 2-2. Calendrier des activités du personnel dans l'engagement des opérations d'information

(3) Les opérations d'information offensives peuvent être menées dans tous les types des opérations hors guerre. Par exemple, mener des OPSPSY contre des alliés potentiels d'un belligérant dans le but d'interrompre les sources de soutien militaire, politique et économique. Dans certains cas, une telle aide humanitaire ou un soutien militaire aux autorités civiles, les opérations d'information peuvent être totalement non belliqueuses et axer sur les OPSPSY et les activités reliées aux CA ou AP.

(4) La planification des opérations d'information des objectifs de paix et les opérations hors guerre doivent aussi considérer et préparer l'espace de bataille et établir les conditions pour le succès de l'exécution des opérations contre un adversaire en conflit.

b. Conflit et guerre

(1) Au delà du seuil de la crise, les opérations d'information peuvent être un outil de force critique pour le combat antimissile interarmées. En plus de protéger l'information vitale aux militaires canadiens, l'emploi des capacités des opérations d'information offensives peut affecter chaque aspect du cycle de décision d'un adversaire en affectant ses décideurs clés, liens, hiérarchies et information. Les opérations d'information offensives deviennent un multiplicateur de force pour soutenir les opérations de combat. La détérioration ou la destruction de systèmes d'information adversaires et leur (élément humain) volonté de combattre sont les buts premiers des opérations d'information offensives en temps de guerre.

(2) Les opérations d'information offensives contre des systèmes d'information adversaires et leur (élément humain) volonté de combattre ne devrait pas prendre place dans le même espace de bataille ou être conduites dans le même délai que les opérations de combat qu'elles soutiennent mais doivent être synchronisées à fond avec les opérations de combat soutenues.

(3) Même si elles ne sont pas le principal effort en temps de guerre, les opérations d'information offensives devraient aider à dominer les opérations de combat et influencer l'adversaire à terminer les hostilités à des conditions favorables pour le Canada.

203. OPÉRATIONS D'INFORMATION OFFENSIVES EN TEMPS DE GUERRE

1. Des opérations d'information offensives peuvent être menées à tous les niveaux de guerre dans et hors de l'espace de bataille militaire traditionnel. Le niveau de guerre stratégique, opérationnelle et/ou tactique auquel les opérations d'information sont normalement menées variera avec la portée des opérations et objectifs militaires. Les opérations d'information se produisent dans le spectre des opérations; la guerre n'est qu'une partie de ce spectre. Les résultats attendus du commandant constituent le concept clé pour déterminer le niveau des opérations d'information à employer. Tout niveau des opérations d'information peut inclure les opérations d'information offensives ou SIO (opérations d'information spéciales) et peuvent nécessiter une approbation de haut niveau. Toutes les opérations d'information, spécialement les opérations d'information stratégiques doivent être planifiées et menées en coordination avec les autres ministères, autres organisations et organismes en dehors du MDN, selon le cas. Les opérations d'information peuvent aussi demander la coordination avec les alliés ou autres organisations non gouvernementales. Les opérations d'information stratégiques cherchent souvent à engager l'adversaire ou le leadership adversaire potentiel pour empêcher une crise ou terminer les hostilités une fois qu'elles se produisent. Ces opérations peuvent être menées pour influencer ou affecter tous les éléments (politique, militaire, économique, informationnel) d'un pouvoir national adversaire. Voir chapitre 5 Planification des opérations d'information pour de plus amples renseignements.

204. RENSEIGNEMENT ET SOUTIEN DES SYSTÈMES D'INFORMATION

1. Soutien du renseignement aux opérations d'information offensives.

a. Généralités. Les opérations d'information offensives demandent un soutien de renseignements généralisé, spécialisé. Parce que l'efficacité de plusieurs capacités des opérations d'information offensives est améliorée d'une façon significative par l'emploi précoce, des sources de collecte de renseignements potentielle et l'accès devraient être développées aussitôt que possible. Un délai important sera d'habitude exigé pour satisfaire les besoins des opérations d'information adéquatement. Les procédures appropriées d'évaluation de dommage de bataille (BDA) des opérations d'information de soutien doivent être établies et mises en oeuvre. Le Tableau 2-3 fournit un aperçu séquentiel de la relation entre des opérations d'information offensives et le soutien du renseignement requis.

b. Sources. Pour planifier et exécuter des opérations d'information offensives, le renseignement doit être ramassé, emmagasiné et facilement extrait, spécialement pour les contingents à court préavis de soutien des opérations d'information. La recherche du renseignement pour les opérations d'information offensives inclut toutes les sources possibles à partir des opérations secrètes de niveau national avec des sources ouvertes locales comme les médias de nouvelles, les contacts du monde commercial, académiques et locaux nationaux. Une grande étendue de sources du renseignement incluant le HUMINT comme celles de nature moins traditionnelle devrait être développée et employée pour soutenir les besoins en renseignements des opérations d'information de soutien.

c. La préparation du renseignement du champ de bataille (IPB). Pour les opérations d'information offensives, l'IPB est le processus continu utilisé pour développer et maintenir une connaissance détaillée de l'usage d'information de l'adversaire et des systèmes d'information. L'IPB pour des opérations d'information offensives utilise un processus de chevauchement et d'actions simultanées produisant des mises à jour de situation, de cette façon fournissant aux CFO et à leurs commandants subalternes des options d'opérations d'information offensives flexibles. L'IPB en soutien des opérations d'information offensives. L'IPB en soutien des opérations d'information offensives bâtit le combat traditionnel mais aussi a besoin de ce qui suit:

(1) Connaissance des besoins techniques d'un vaste ensemble de systèmes d'information.

(2) Connaissance des influences politiques, sociales et culturelles.

(3) La capacité de conduire un processus hautement technique pour produire un plan d'action des gabarits d'opérations d'information offensives (COA).

(4) Une compréhension de l'adversaire ou du processus de prise de décision d'un adversaire potentiel.

(5) Une compréhension en profondeur de l'arrière-plan biographique des leaders adversaires clés, des décideurs, des communicateurs et leurs conseillers pour inclure des facteurs de motivation et de style de leadership.

d. Voir aussi l'IPB au chapitre 5 Planification des opérations d'information.

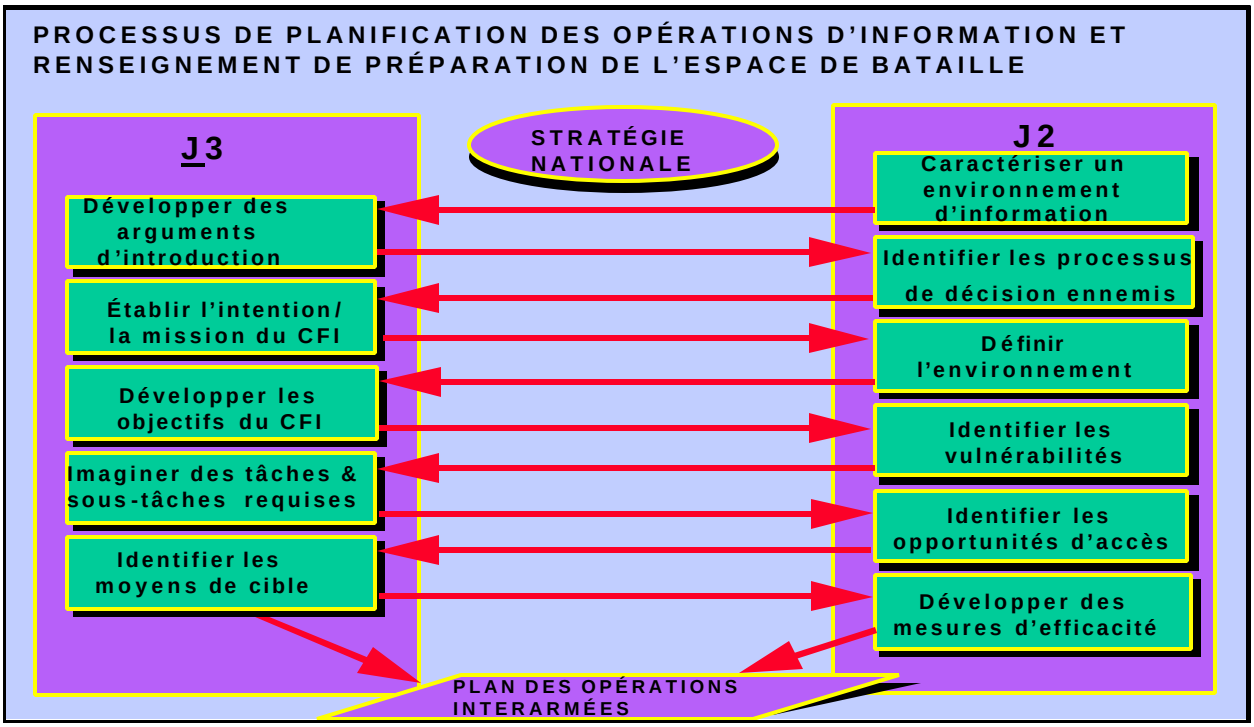


Tableau 2-3. Processus de planification des opérations d'information et de renseignement de préparation de l'espace de bataille

2. Soutien de systèmes d'information aux opérations d'information offensives

a. Les systèmes d'information rassemblent, transportent, traitent, diffusent et exposent l'information utilisée pour soutenir les opérations d'information offensives. Ces systèmes permettent aux CFO et à leurs subalternes d'utiliser de l'information efficacement pour maintenir une vision précise de l'espace de bataille et de planifier et d'exécuter les opérations d'information.

b. Les systèmes d'information fournissent aussi aux CFO et à leurs subordonnés des moyens de connecter avec l'infrastructure d'information globale (GII) de façon à maximiser la portée et axer sur l'efficacité des opérations d'information offensives.

c. Enfin, les systèmes d'information soutiennent les opérations d'information offensives en fournissant la capacité de portée globale permettant aux décideurs amis et commandants la synchronisation, la coordination et la normalisation du conflit des opérations d'information à tous les niveaux de la guerre dans toute la portée des opérations militaires.

205. CIBLAGE DES OPÉRATIONS D'INFORMATION OFFENSIVES

1. Généralités

a. Le ciblage des opérations d'information offensives doit maintenir son attention sur l'influence des décideurs et peut être efficace contre tous les éléments de pouvoir national. Le ciblage des opérations d'information offensives devrait considérer tous ces éléments pour déterminer la façon de mieux atteindre les objectifs désirés.

b. Les opérations d'information offensives peuvent agir sur les processus de décision humains (facteurs humains), l'information et les systèmes d'information utilisés pour soutenir la prise de décision (liens), l'information et les systèmes d'information utilisés pour mettre en oeuvre les décisions (hiérarchie). Les

efforts des opérations d'information devraient examiner toutes les trois zones cibles pour maximiser l'opportunité pour le succès. La sélection des cibles des opérations d'information doit être logique avec les objectifs canadiens et les conventions internationales applicables et les règles d'engagement. Voir Tableau 2-4.

c. La sélection cible des opérations d'information sera menée par le module de coordination des opérations d'information selon l'orientation du commandant en utilisant toute l'information disponible et le renseignement. L'IOCC accordera une priorité aux cibles proposées et recommandées au commandant ou le module de coordination du choix des objectifs (TCC) avec une stratégie d'engagement recommandée.

d. Le module de coordination des opérations d'information sera une source importante d'information pour le CFO durant le processus de ciblage culminant avec l'intrant au TCC. La représentation de l'IOCC au TCC devrait fournir un moyen efficace d'assurer la coordination de l'information des opérations d'information et cibler les besoins avec les cibleurs.

e. Les considérations de gain/perte produites par l'état-major du renseignement devraient être incluses dans le processus de ciblage des opérations d'information.

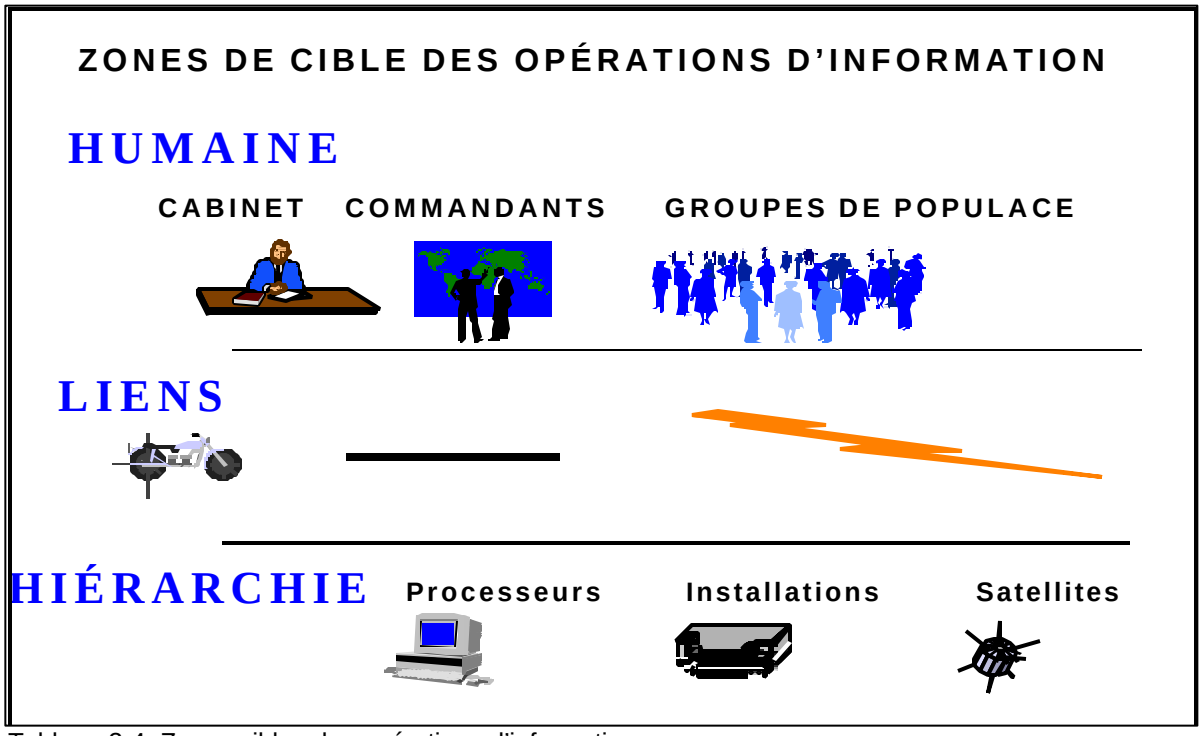


Tableau 2-4. Zones cibles des opérations d'information

2. Ciblage stratégique

a. L'attention initiale de ciblage des opérations d'information offensives au niveau stratégique est d'agir sur un centre de gravité de l'adversaire à l'intérieur des éléments de pouvoir national. Le ciblage des opérations d'information offensives stratégiques peut impliquer des attaques directes, indirectes et de soutien. Le but de ce ciblage est d'empêcher un adversaire ou un adversaire potentiel à partir des actions menant le déclenchement des hostilités ou d'autres activités militaires ou non militaires non dans les meilleurs intérêts du Canada.

b. Une attaque directe est menée sur un ensemble cible de "centre de gravité" d'un adversaire. Une attaque indirecte est menée pour affecter le "centre de gravité" de l'adversaire mais est dirigée contre un

ensemble cible associé. Une attaque de soutien est menée contre des ensembles cibles n'influençant pas le "centre de gravité" de l'adversaire, mais fournit de la pression compatible avec l'effort principal et en soutien de l'atteinte de l'objectif.

c. Le ciblage des opérations d'information offensives les plus stratégiques est l'extension logique de la planification des opérations d'information en temps de paix menées sur une base courante contre des adversaires connus et des adversaires potentiels.

3. Réponse au ciblage

a. Le ciblage de réponse implique l'exécution ponctuelle de ciblage des opérations d'information offensives pour les objectifs des opérations d'information initiaux et les attaques de premier renfort des cibles d'opérations d'information basées sur l'estimation des dégâts de combat (BDA) ou de soutenir le processus de réponse dans le système des opérations d'information défensives décrit au chapitre 3, "Opérations d'information défensives."

b. La surprise et la sécurité sont importantes au ciblage des opérations d'information offensives depuis que la préscience ou le compromis de la source peut nier l'effort de ciblage des opérations d'information offensives initiales. Les capacités des opérations d'information offensives doivent être préparées pour coordonner, synchroniser et exécuter le ciblage des opérations d'information offensives initiales de façon hautement réceptive.

c. Les opérations à tempo élevé peuvent exiger une réponse rapide aux demandes d'attaques de premier renfort des cibles d'opérations d'information offensives basées sur des estimations des dégâts de combat (BDA) menées par les atouts de la force interarmées nationaux, dans le théâtre ou subordonnés. Les capacités des opérations d'information offensives doivent être préparées pour répondre rapidement aux demandes de telles attaques de premier renfort.

d. Des capacités des opérations d'information offensives peuvent aussi être nécessitées pour répondre rapidement aux demandes d'attaques des opérations d'information contre les capacités adversaires ciblant l'information amie et les systèmes d'information, de ce fait faisant le lien vital entre les opérations d'information offensives et défensives.

"L'Iraq avait perdu la guerre avant qu'elle ne commence. C'était une guerre basée sur le renseignement, la GE, le commandement et le contrôle et la contre-ingérence. Les troupes irakiennes étaient aveuglées et sourdes... La guerre moderne peut être gagnée par l'informatique. C'est maintenant vital pour les États-Unis et l'U.R.S.S."

Lieutenant-général S. Bogdanov, chef du General Staff Center for Operational and Strategic Studies, octobre 1991

CHAPITRE 3

OPÉRATIONS DES INFORMATIONS DÉFENSIVE

> ***"Nous avons la preuve qu'un grand nombre de pays autour du monde développent la doctrine, les stratégies et les outils pour conduire les attaques d'information sur les ordinateurs reliés aux militaires."***
>
> **John M. Deutch, Directeur, CIA**
> ***Washington Post*, 26 juin 1996**

301. GÉNÉRALITÉS

1. Les militaires canadiens dépendent de l'informationpour planifier les opérations, déployer des forces et exécuter les missions. Les progrès dans les technologies de l'informationont amélioré de façon importante l'efficacité potentielle et le volume de circulation de l'information. Des systèmes d'information complexes soutiennent des infrastructures puissantes améliorant dramatiquement les capacités militaires; toutefois une dépendance accrue sur ces technologies évoluant rapidement rend les forces interarmées plus vulnérables. Les opérations d'information défensives assurent une protection nécessaire et de la défense d'information et des systèmes d'information à l'intérieur des forces interarmées sur lesquelles les décideurs dépendent pour atteindre leurs objectifs. Une fois combinées avec les opérations d'information défensives, le résultat net sera une opportunité améliorée pour utiliser les opérations d'information pour exploiter avec succès toute la gamme de conflit.

a. Des opérations d'information défensives intègrent et coordonnent la protection et la défense de l'information, les processus et les systèmes d'information fondés sur l'informationimportants pour l'atteinte des objectifs. Le processus d'opérations d'information défensives est une partie inhérente de la protection de la force.

b. Des opérations d'information défensives consistent en trois éléments:

   (1) Opérations d'information - Protection: du contrôle de l'accès de l'adversaire à ces éléments amis de l'environnement de l'informationimportants pour l'accomplissement des objectifs amis,

   (2) Contre-opérations de l'informationdéfensives: la réaction des attaques des opérations de l'informationadversaires et la restauration de la performance et la fonctionnalité des éléments amis importants, et

   (3) Contre-opérations de l'informationoffensives: empêcher la neutralisation de la capacité des opérations de l'informationadversaires.

c. La protection de l'informationest une combinaison des deux premiers éléments. Le dernier élément est nécessaire pour empêcher l'intention de l'adversaire d'employer les opérations d'information et d'exploiter et/ou de neutraliser la capacité et l'opportunité des opérations de l'informationadversaires soit de façon préventive ou en guise de réponse.

d. Le processus des opérations d'information défensives intègrent et coordonne les politiques et procédures, les opérations, le personnel et la technologie de la protection de l'informationpour protéger l'informationet les processus fondés sur l'informationet défendre les systèmes d'information.

e. Les opérations d'information défensives assurent un accès à l'informationactuelle, précise et pertinente en niant aux adversaires l'opportunité d'exploiter de l'informationamie et les systèmes pour leurs propres fins. Les opérations de l'informationdéfensives incluent les capacités techniques de la protection de

l'informationainsi que les capacités de protection universelle telles que l'éducation et l'instruction, la sécurité des opérations et la contre-ingérence.

f. La protection de l'informationprotège et défend l'informationet les systèmes d'information en assurant leur disponibilité, l'intégrité et la confidentialité. Ceci inclut la fourniture de la restauration des systèmes d'information en incorporant les capacités de protection, de détection et de réaction. La protection de l'informationest axée sur les capacités techniques et les processus comme la sécurité multiniveau, les logiciels de filtrage, préserver les serveurs de réseau et la détection effraction de logiciel ainsi que les mesures de sécurité de matériel, de personnel et des mesures de sécurité procédurales (p. ex. les mesures prises pour sauvegarder l'équipement cryptographique et du matériel contre l'accès non autorisé.) Voir Tableau 3-1.

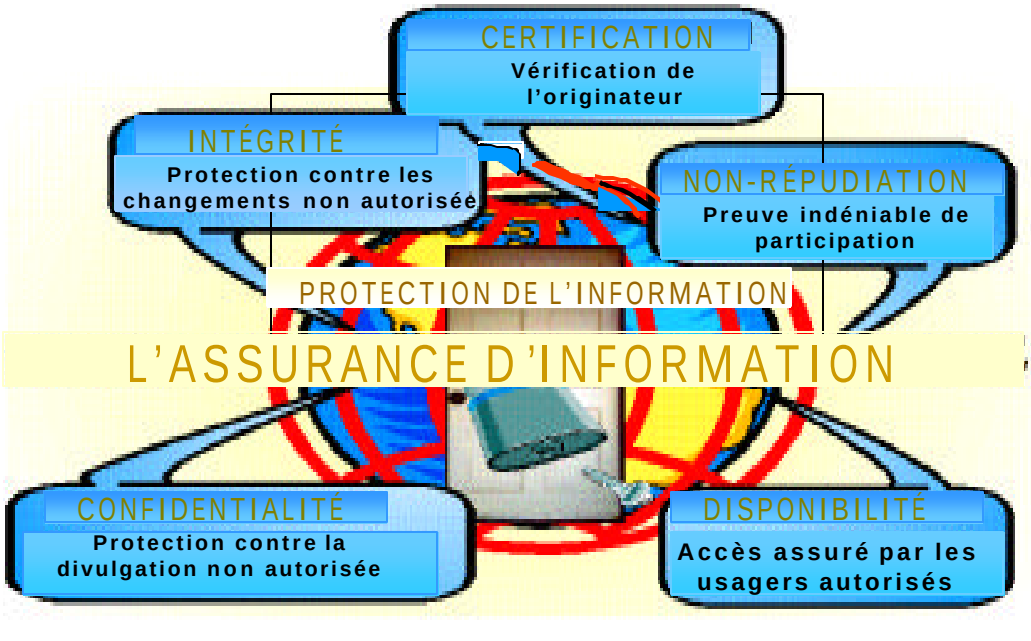


Tableau 3-1 Protection de l'information

g. L'intégration des opérations d'information défensives. Les efforts des opérations d'information défensives devraient être intégrés dans toutes les opérations militaires pour inclure les activités par d'autres organismes gouvernementaux et non gouvernementaux ou organisations oeuvrant dans la zone d'opérations (AO) du CFO.

(1) L'intégration des opérations d'information défensives avec les opérations d'information offensives. Les opérations d'information défensives doivent être intégrées avec les opérations d'information offensives pour fournir une réponse opportune contre des menaces identifiées et potentielles aux informations amies et systèmes d'information. L'IOCC intègre les opérations d'information défensives et les opérations d'information offensives pour les CFO. Les commandants subordonnés devraient assurer que les plans d'opération de soutien (OPLAN) et les ordres d'opération (OPORD) fassent des provisions en vue de cette intégration.

(2) L'intégration des opérations d'information défensives à l'intérieur d'une force interarmées. L'intégration des opérations d'information défensives à l'intérieur d'une force interarmées est nécessaire pour assurer que les trois processus interreliés (protection, détection et réaction (ou réponse) sont compris uniformément et mis en pratique. En outre, l'intégration des opérations d'information défensives assure l'emploi des capacités les plus appropriées de la réponse des

opérations d'information de la force interarmées. Le module de coordination des opérations d'information du CFO est responsable de l'intégration des opérations d'information défensives.

(3) L'intégration des opérations d'information défensives à l'intérieur d'une force multinationale. La technologie fondée sur l'information, les systèmes d'armes, le renseignement et les autres capacités sont souvent partagées, intégrées et synchronisées dans des opérations multinationales pour améliorer les opérations. En fournissant des avantages aux opérations multinationales, l'intégration de l'information canadienne, alliée ou de coalition, les processus fondés sur l'information et les systèmes d'information créent des vulnérabilités qu'un adversaire peut exploiter en utilisant les opérations d'information.

(a) Le module de coordination des opérations de l'information du commandant de la force combinée est la référence pour l'intégration des opérations d'information dans les opérations multinationales.

(b) À l'intérieur du contexte des lignes directrices communicables promulguées et tel que conseillé par le J3 et le J2, le module de coordination des opérations d'information peut se voir délégué la responsabilité de partager l'information essentielle aux opérations d'information avec les forces multinationales. Malgré cela, dans tous les cas les opérations nationales canadiennes et les autorités du renseignement (p. ex. QGDN J3 et J2) devront demeurer le pouvoir final de décision pour l'autorisation des opérations et l'information des renseignements secrets pouvant étaler les opérations canadiennes, les sources du renseignement ou les méthodes ou risquer l'information ou les systèmes d'information important à la sécurité nationale.

(c) Sujet aux conditions ci-dessus, le module de coordination des opérations d'information peut considérer le partage des données de menace, les vulnérabilités, le ciblage et l'estimation des dégâts de combat et les capacités des opérations d'information pouvant aider à réduire les vulnérabilités. Voir *Doctrine interarmées des Forces canadiennes interarmées et des opérations combinées*, B-GG-005-004/AG-000 pour une orientation supplémentaire.

(4) Niveaux de guerre. Les opérations d'information demandent une étroite collaboration entre les organisations internes et externes militaires et non militaires au CFO soutenu à tous les niveaux.

(a) Les efforts des opérations d'information défensives en temps de paix à tous les niveaux de la guerre devraient être synchronisés pour soutenir toutes les phases d'une opération militaire.

(b) Pour avoir une unité d'efforts, les opérations d'information défensives à tous les niveaux de la guerre devraient être synchronisées avec les opérations d'information planifiées ou offensives continues.

> ***"****Dans la guerre, la défense existe principalement pour que l'offensive puisse agir plus librement.****"***
>
> *Contre-amiral* **Alfred Thayer Mahan,** *Stratégie navale*, **1911**

g. Le processus des opérations d'information défensives. Trois processus interreliés comprennent des opérations d'information défensives: opérations d'information-protection, contre-opérations d'information défensives et contre-opérations d'information offensives. Le Tableau 3-3 fournit un aperçu du processus de mise en oeuvre des opérations d'information défensives et est un modèle à l'échelle de tous les niveaux de la guerre. Le processus de mise en oeuvre des opérations d'information défensives intègre toutes les capacités défensives disponibles pour assurer une défense en profondeur. Les CFO et leurs commandants subalternes en sous-ordre devraient planifier, exercer et employer les capacités défensives disponibles pour appuyer les trois processus des opérations d'information défensives. Les

capacités des opérations défensives contribuant à une défense en profondeur s'échelonnent du sens de l'instruction de base aux solutions de la protection de l'information technique telles que les équipements d'INFOSEC et de logiciel de détection de l'intrusion automatisée.

302. PROCESSUS (OPÉRATIONS D'INFORMATION-PROTECTION) DE PROTECTION DES OPÉRATIONS D'INFORMATION

1. Définir les besoins d'information de force interarmées et les dépendances est le point central du processus des opérations d'information-protection. L'environnement d'information de la force interarmées est lié par ce qui importe aux opérations de la force interarmées.

a. L'environnement de l'information est une combinaison des systèmes physiques et installations ainsi que des processus abstraits comme le renseignement et la prise de décision.

b. La protection de l'environnement d'information prendra racine dans une approche solide dans la gestion du risque. Les processus de gestion du risque incluent la considération des besoins d'information, la valeur ou la sensibilité de l'information pouvant être compromise ou perdue si l'environnement de l'information protégée est percé (perte de contrôle d'accès), vulnérabilités de système, menaces posées par des adversaires potentiels et phénomènes naturels, ressources disponible pour la protection et la défense et le risque résiduel (R_r) à l'environnement de l'information une fois que les mesures de protection ont été mises en place. En outre, la valeur ou la sensibilité de l'information peut changer d'une phase d'une opération militaire à l'autre et cela doit être considéré dans le processus de gestion du risque.

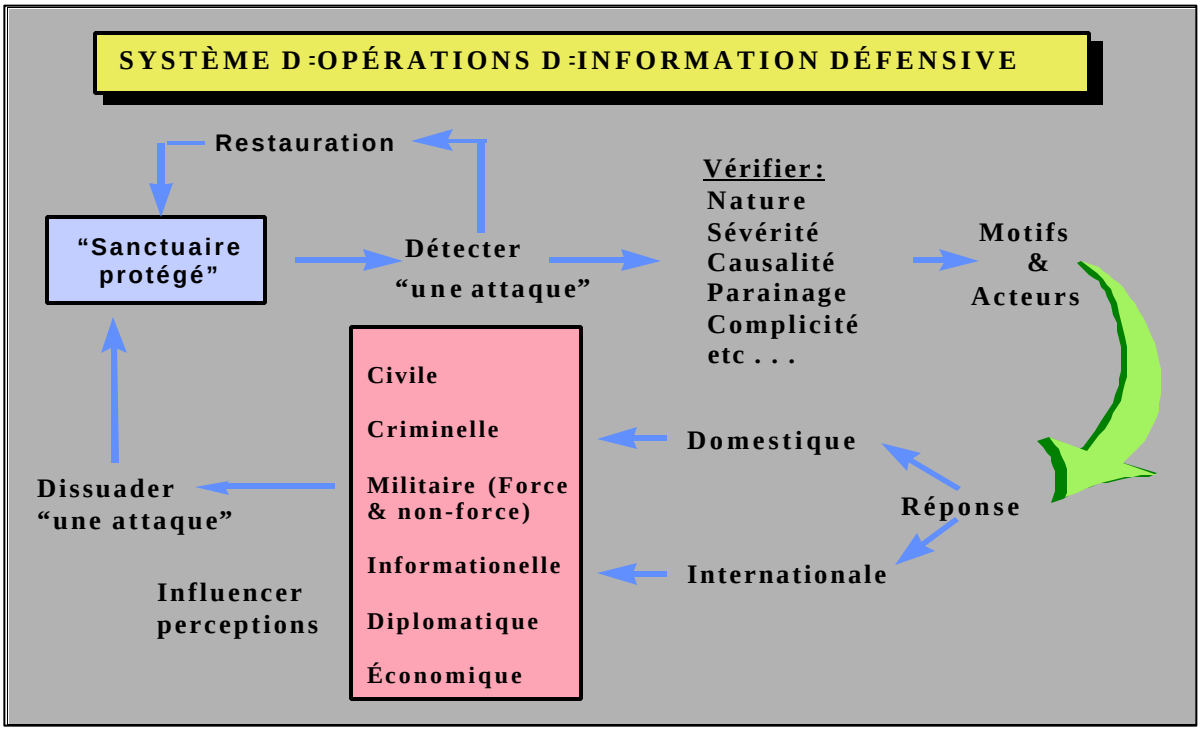


Tableau 3-2. Système d'information défensive

c. L'environnement de l'information protégé ne fournit pas seulement le degré de protection proportionné à la valeur ou la sensibilité ou de son contenu mais assure aussi que les capacités soient en place pour répondre à une vaste gamme d'attaques.

d. La protection de l'information s'applique à tout médium d'information ou formule incluant une copie papier (message, lettre, télécopieur), électronique, magnétique, vidéo, imagerie, voix, télégraphe,

ordinateur et humain). Le processus de protection de l'information implique la détermination de la portée (ce qui doit être protégé basé sur la valeur ou la sensibilité de l'information) et les normes de protection (à quelle étendue au moyen des opérations et de l'application des mesures de protection et des technologies). Voir Tableau 3-3. Le processus de protection devrait refléter la valeur en mutation ou la sensibilité de l'information durant chaque phase opérationnelle.

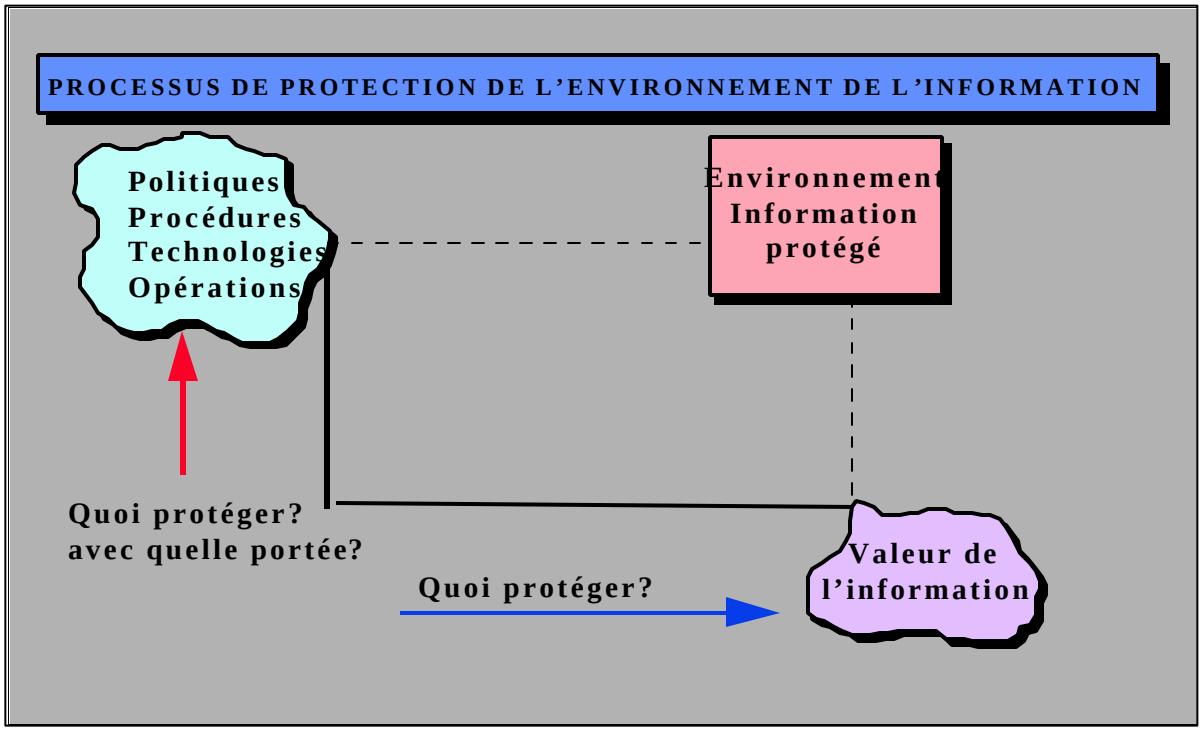


Tableau 3-3. Processus de protection des opérations d'information

e. Les CFO devraient mettre en oeuvre le processus de protection des opérations d'information au moyen de l'adoption des politiques communes et des procédures, l'emploi de capacités technologiques et des opérations de planification incluant les objectifs des opérations d'information défensives.

(1) Politiques. Les CFO ont besoin d'augmenter les politiques des opérations d'information défensives permanentes avec les politiques spécifiques de la force interarmées pour fournir une protection de l'environnement de l'information centrée taillée en fonction de leurs zones d'opérations spécifiques. Ces politiques devraient traiter des vulnérabilités et des menaces, des capacités de force amies, des dépendances d'infrastructure commerciales et des vulnérabilités ayant un impact sur les diverses phases d'une opération.

(2) Procédures d'opérations d'information défensives. Les procédures de force interarmées pour mettre en oeuvre des politiques de protection des opérations d'information devraient employer l'identité à la plus grande portée possible. L'utilisation de procédures communes aidera à atteindre l'interopérabilité sûre entre les composantes de la force interarmées. Ces procédures incluent jusques y compris ce qui suit:

(a) Éducation, instruction et sensibilité. Un élément clé de la protection de l'environnement de l'information est l'éducation et l'instruction des utilisateurs de système, administrateurs, gérants, ingénieurs, concepteurs et développeurs. Le sens rehausse l'appréciation de menace et l'importance d'adhérer à des mesures de protection. L'éducation fournit les concepts et la connaissance pour développer des technologies appropriées, des politiques, des procédures et des opérations pour protéger les systèmes. L'instruction développe les compétences et les capacités requises pour travailler en réduisant les vulnérabilités.

(b) Gestion du risque. Les décisions de gestion du risque déterminent les limites d'application des contre-mesures. Le processus de gestion du risque inclut la considération des besoins d'information, la valeur ou la sensibilité de l'information à risque, les vulnérabilités du système, les menaces posées par des adversaires potentiels et les phénomènes naturels, les ressources disponibles pour la protection et la défense et le risque résiduel (R_r) à l'environnement de l'information une fois les mesures de protection mises en place. Les CFO devraient aussi établir un programme d'évaluation du risque périodique.

(c) Soutien du renseignement. Un élément important du processus de renseignement est l'identification de la menace. L'information sur la menace est un intrant primaire au processus de gestion du risque et contribue directement à la protection de l'environnement de l'information.

1. Menace. Le renseignement fournit une compréhension de la menace à l'information et des systèmes d'information par l'identification des adversaires d'information potentiels, leur intention et leurs capacités connues et évaluées. L'information sur la menace est une considération clé dans le processus de gestion du risque.

2. Les menaces des opérations d'information devraient être définies en termes d'intention adversaire spécifique, de capacité et d'opportunité pour influencer ces éléments de l'environnement d'information ami important pour l'atteinte des objectifs de force amies. Voir Tableau 3-4.

3. Le renseignement peut fournir aux CFO l'information nécessaire pour conduire des évaluations de risque et développer des options de gestion du risque pour limiter leurs vulnérabilités.

4. L'évaluation de la menace est un processus continu reflétant les changements dans l'élément en opération, la technologie et les menaces.

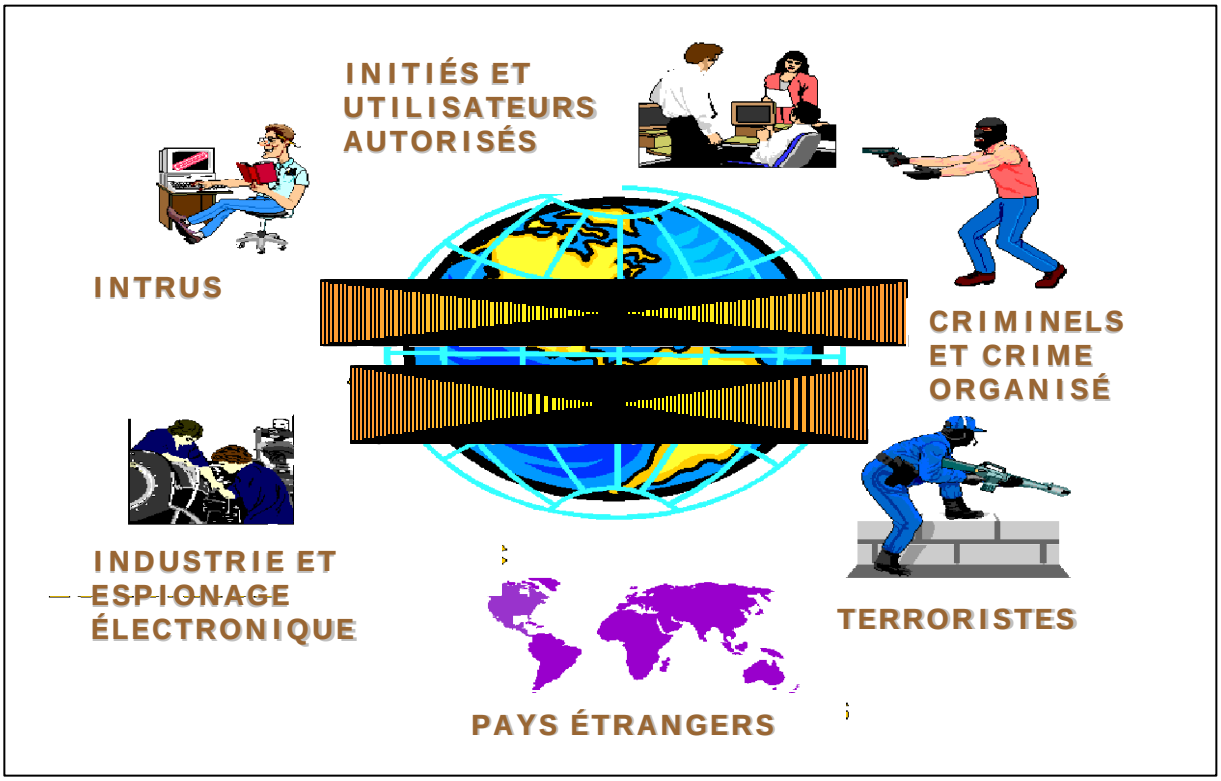


Tableau 3-4. Menace croissante

(d) Contre-déception. Les activités du renseignement contribuant à la sensibilité de la position de l'adversaire et de l'intention servent aussi à identifier les tentatives de l'adversaire à tromper les forces amies.

(e) Contre-psychologie. Les activités du renseignement identifiant les opérations de guerre psychologiques adversaires contribuent à la sensibilité situationnelle et servent à dénoncer les tentatives adversaires pour influencer les populations amies et les forces militaires.

(f) Affaires publiques (PA). Les programmes des PA contribuent à la protection de l'information en diffusant de l'information factuelle. La diffusion de l'information factuelle contre la déception de l'adversaire et les OPSPSY. Les programmes d'information de commandement servent le même but comme les PA concernant les opérations d'information défensives. Les programmes d'information du commandement normalement sont trouvés à l'intérieur des composantes de la force interarmées et des unités de niveau inférieur où il n'y a pas de programme de PA élaboré.

(g) Sécurité. La CI, la sécurité du personnel, la mesure de sécurité administrative sont des exemples de mesures contribuant indirectement à la protection de l'information. Une application coordonnée de toutes ces activités fournit l'organisation d'une évaluation de vulnérabilité plus complète et assiste dans la gestion du risque.

(h) Analyse de la vulnérabilité et évaluations. Les forces interarmées devraient conduire des analyses de vulnérabilité et des évaluations pour identifier des vulnérabilités potentielles dans les systèmes d'information et fournir une évaluation globale de la position du système de sécurité. Basé sur une évaluation du risque posé au système d'information (SI) de telles vulnérabilités devraient-elles être éliminées. L'intégration des capacités d'analyse de

vulnérabilité en formation interarmées et d'exercices aide à identifier et limiter les vulnérabilités et contribue directement à la protection de l'information.

1. Les menaces étrangères ne sont qu'une partie de toute la menace aux systèmes d'information. Les menaces internes provenant de sources malicieuses (travailleurs mécontents) et accidentelles (émanations magnétiques ou impulsions électriques) sont des menaces importantes. Les phénomènes naturels tels que les taches solaires, les ouragans, les tornades, tremblements de terre et les inondations posent aussi des menaces aux systèmes. L'analyse de vulnérabilité des systèmes doit inclure la considération de ces facteurs.

2. Les efforts de vulnérabilité et d'évaluation axent sur les types spécifiques de systèmes d'information. Un Programme d'analyse de vulnérabilité de réseau a été établi avec le MDN axant spécifiquement sur les vulnérabilités du SI.

(3) Capacités de protection de l'information (IP). Les CFO devraient assurer que les capacités des IP protégeant l'information et défendant les systèmes d'information sont intégrés dans leurs systèmes C4 et testés de manière approfondie par des exercices réalistes et des événements d'instruction. Les capacités incluent les mesures de sécurité comme les instruments d'INFOSEC.

(a) NFOSEC. L'INFOSEC, est le système de protection d'information contre l'accès non autorisé ou la corruption de l'information. L'INFOSEC inclut ces mesures nécessaires à détecter, documenter et contrer de telles menaces.

(b) La sécurité informatique (COMPUSEC). La sécurité informatique est la protection résultant de toutes les mesures conçues pour prévenir la communication, l'acquisition, la manipulation, la modification ou la perte d'information contenues dans un système informatique ainsi que des mesures conçues pour empêcher la négation de l'utilisation autorisée du système.

(c) SECOM. La SECOM inclut les mesures prises pour empêcher le compromis de l'information emmagasinée, transmise ou traitée dans un système d'information. La SECOM assure aussi l'authenticité des télécommunications. La SECOM inclut la sécurité cryptographique, la sécurité de transmission, la sécurité d'émission, la sécurité d'émission et la sécurité matérielle des matériaux de la SECOM et de l'information.

(d) GE. Les procédures de GE défensives (connues comme les MPE (mesures de protection électronique)), incluant les procédures de SECOM et les indicatifs d'appel ou mots et fréquences en mutation. Les autres incluent les procédures de COMPUSEC, la SECOP et les contrôles d'accès à l'information personnelle.

(4) Opérations. Les CFO ont besoin de considérer et d'inclure les objectifs des opérations d'information défensives quend la planification et l'exécution d'opérations. Les opérations menées dans les buts autres que les vulnérabilités des opérations d'information limitées puissent avoir des effets collatéraux soutenant les objectifs des opérations d'information défensives.

303. PROCESSUS DES CONTRE-OPÉRATIONS D'INFORMATION DÉFENSIVES

1. Étant données la vulnérabilité des SI et l'importance croissante de l'information sur ces SI, il y a un besoin de détection, poursuite, analyse et capacité de réponse en guise de défense contre l'intrusion, la dégradation et la perte au moyen des opérations d'information externes et internes. La vitesse avec laquelle les incidents du système d'information (délibérés ou accidentels) se produisent dépassent la capacité de détection manuelle et de réponse. Cela entraîne un besoin de capacités de détection automatisée et de réponse. Ces capacités devraient détecter des intrusions de système ou des aberrations et générer des alertes sur-le-champ.

En outre, l'atténuation de la menace automatique limitant l'étendue de dommage ou d'étendue des incidents devrait être à déclenchement automatique.

a. Des incidents hostiles peuvent être dirigés contre les différents plans de SI et varieront facilement avec ce qu'ils peuvent détecter. Les réponses doivent être taillées en fonction de la nature et de l'étendue de l'incident.

(1) Des attaques contre la couche physique d'un SI sont les plus faciles à identifier et contre lesquelles se défendre. Elles impliquent l'approche traditionnelle d'utilisation d'armes conventionnelles pour détruire physiquement une composante ou des composantes d'un SI. La destruction de composantes critiques identifiées au moyen de liens et d'analyse hiérarchiques à un point clé dans une opération peut paralyser la capacité d'un adversaire de fonctionner.

(2) Les attaques contre une couche logique (ou syntaxique) d'un SI, qui consistent généralement du logiciel et des systèmes d'opération d'un SI ainsi que les modes de fonctionnement sont plus difficiles à détecter comme elles se manifestent typiquement comme des erreurs de systèmes (p. ex., lente exécution des procédures, orientation défectueuse de renseignement). La capacité de distinguer entre les erreurs de système accidentelles et délibérées est la clé pour répondre à cette forme d'attaque.

(3) Les attaques contre la couche sémantique du SI ne sont plus dirigées sur les composantes ou les systèmes d'opération mais cherchent à affecter et exploiter la confiance que les utilisateurs de confiance ont dans l'intégrité et la validité de l'information dans le SI (p. ex., La gestion de perception). Tout le personnel impliqué dans les opérations d'information (dans tout le spectre de conflit) auront accès à de l'information émanant d'une source non secrète, de médias et peut-être de désinformation. Ce sont les plus difficiles à détecter et le CFO a besoin d'être conseillé par des organismes appropriés quand cela se produit et préparé à réagir selon le cas. Des programmes de contre-déception efficaces et de contre-OPSPSY sont importants.

b. Une détection d'incident ponctuelle et le rapport sont les clés de l'initiation du processus des contre-opérations d'information défensives. Le processus de contre-opérations d'information défensives inclut les éléments suivants

(1) Renseignement. Le renseignement contribue aux contre-opérations défensives en fournissant les avertissements d'activité adversaire potentielle et l'appel de la désignation approximative des objectifs à des indicateurs d'activité spécifiques. Une étroite collaboration est requise entre le renseignement, l'application de la loi, les concepteurs de système, les fournisseurs, les administrateurs et les utilisateurs pour assurer un partage opportun d'information pertinente. Le renseignement et les processus du C3 forment la fondation d'indications et avertissements (I&W). Voir Tableau 3-5.

(a) I&W. Les I&W pour les opérations d'information défensives tirent leur inspiration des rapports de renseignement actuels, des atouts de la force interarmées, du soutien I&W de commandement de la composante et la corrélation des mouvements de la force dans la zone d'opérations. En outre, les atouts de renseignement de niveau national fournissent des I&W d'une activité adversaire imminente.

(b) Une défense contre une attaque, une base de données de renseignement du CFO ou une composante du réseau électrique prédit la façon dont comment bien la menace du renseignement et les processus d'I&W fonctionnent et sur la capacité de fournisseurs de systèmes, les utilisateurs et les administrateurs pour mettre en oeuvre des contre-mesures préventives.

(c) Dans les opérations d'information défensives, les I&W fusionnent la connaissance des capacités des opérations d'information adversaires avec le renseignement pour évaluer la

probabilité des actions des opérations d'information adversaires et fournit un avertissement suffisant pour devancer, contrer ou autrement modérer leur effet.

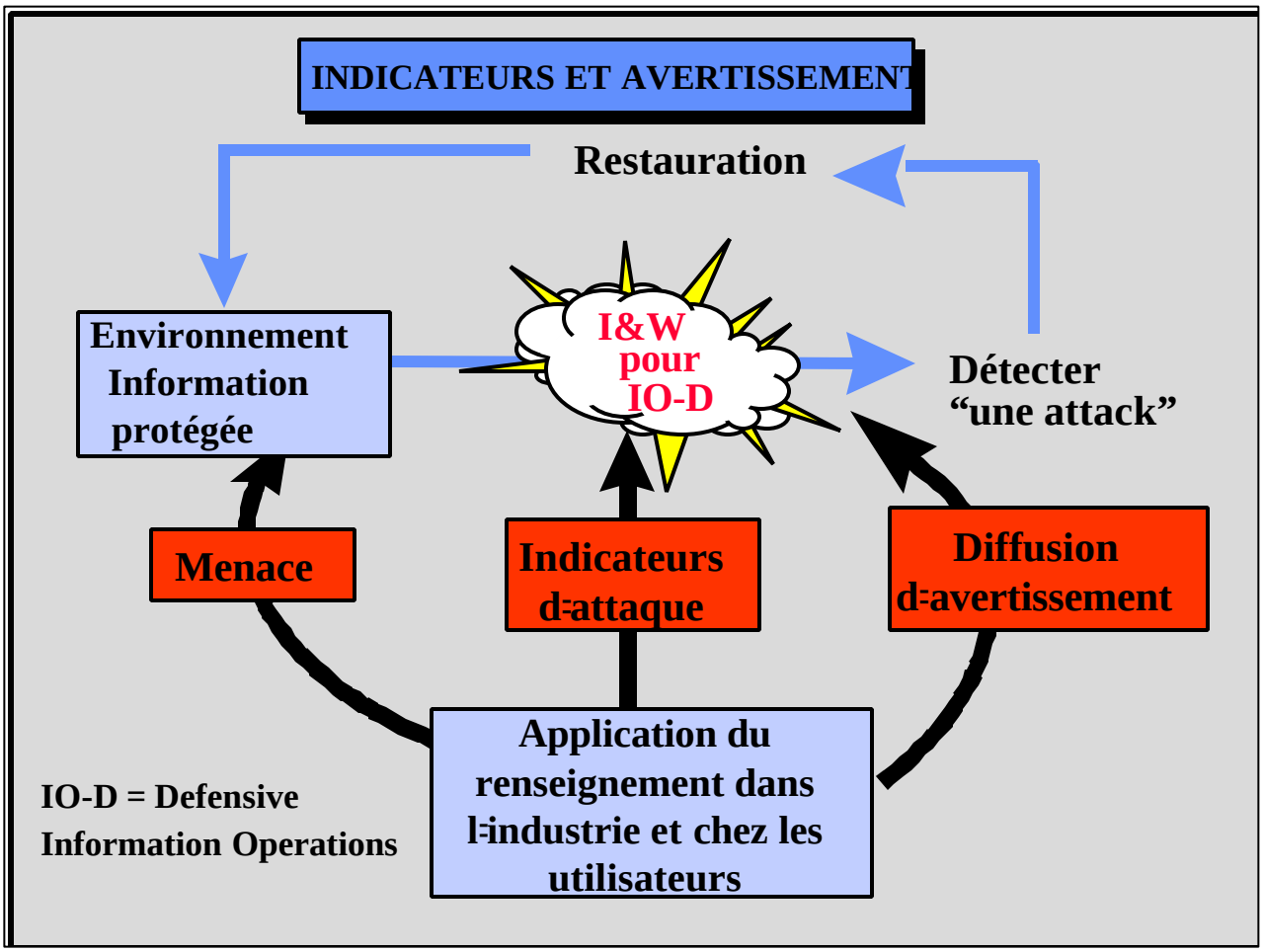


Tableau 3-5. Indications and warning

(d) Le soutien en I et W de la force interarmées aux opérations d'information défensives repose sur les indicateurs de sources internes et externes du MDN. Les forces interarmées devraient continuer à analyser les indicateurs d'attaque traditionnelle jusqu'à ce qu'un processus I et W national global soit établi reflétant les caractéristiques uniques des opérations d'information. Pour de plus amples renseignements concernant le processus I et W national, référer au MC 166, MIP 260 et les CONOPS - Soutien du renseignement aux forces déployées.

(2) Détection d'incident. Les systèmes conçus pour détecter les incidents et alerter les gérants et les administrateurs à tous les niveaux aux anormalités aident à contribuer aux processus de contre-opérations d'information défensives. La détection de l'incident peut être menée sur une base de temps réel ou autonome, centralisée ou décentralisée. Les techniques de détection traditionnelle comme l'examen de la liste de contrôle peuvent être complétées avec des outils automatiques et avec des programmes de contre-déception efficaces et contre OPSPSY. Une disposition devrait être prise pour des mises à jour de systèmes de détection ou de réduction des impacts. La technique de détection utilisée dépendra de la menace opérationnelle, la pertinence du système protégé, la sensibilité de l'information sur ce système et des conséquences de tout délai de réponse à un incident.

(3) Rapport d'incident. Quand un accident se produit, il est essentiel que des détails spécifiques de l'incident soient rapportés dans des buts d'analyse. Le module de coordination d'opérations

d'information du CFO établira des procédures de rapport normalisé. Le rapport consistera en un rapport initial immédiat pour engager le processus d'I et W, avec un rapport de suivi au besoin. La nature et la portée de l'incident précisera la portée du rapport. Une collecte opportune, la corrélation, l'analyse d'information et la diffusion d'avertissement demande une structure de fonctionnement continue. Une structure de rapport liée au renseignement, à l'application de la loi, aux technocrates et la communauté de systèmes d'information, gouvernementales et commerciales est essentielle aux opérations d'information défensives.

(4) Repérage d'un incident. Les intrusions peuvent se produire sur une grande période de temps ou une série de sessions d'utilisateur ou peuvent être initiées par de multiples intrus travaillant de concert. Selon la sophistication de l'intrus, une intention hostile peut seulement être déterminée quand la séquence d'une attaque est assemblée, comme chaque action individuelle peut avoir une apparence de légitimité. Il est donc essentiel qu'une fois un incident détecté, les activités de l'intrus soient repérées de façon à rassembler de la preuve pour une poursuite possible, et dans le but d'I et W. La consignation automatisée aidera à cet égard. Le module de coordination des opérations d'information du CFO sera responsable de la coordination de repérage d'incident dans les composantes de la force.

(5) Analyse d'incident. La nature et la portée de l'incident seront déterminés soit par l'utilisation d'outils automatisés ou des techniques plus traditionnelles. Une distinction doit être faite entre les attaques délibérées et les anormalités accidentelles de façon à employer les contre-mesures pour limiter les effets de l'incident. En plus de mettre en place des courants de signature intrusives, l'identification des faiblesses dans les mécanismes de sécurité et aidant au développement des contre-mesures, l'analyse d'incident permettra la conduite d'information sur l'évaluation du dommage causé par la bataille (I-BDA).

(6) Une fois les actions de restauration complétées, il y aura un besoin de mener de l'information défensive sur l'évaluation du dommage causé par la bataille. Cela impliquera l'identification du dommage causé par l'attaque, toutes les conséquences résultant d'actions de restauration elles-mêmes (p. ex., la dégradation temporaire de service en attendant la restauration provenant de sources fonctionnelles) ainsi qu'une évaluation de l'impact potentiel sur les opérations.

b. Réponse d'incident. Les mécanismes de détection d'incident servent à déclencher le processus de réponse. L'identification opportune des acteurs et de leurs motifs établissant la cause, la complicité et la capacité de restauration sont les pierres angulaires d'une réponse efficace et adéquatement axée. L'efficacité du processus de réponse dépend de l'intégration efficace de la détection de l'intrusion et les capacités d'analyse ainsi qu'ayant établi et testé les procédures de réponse. Le processus contribue aux opérations d'information défensives en contrant les menaces et améliorant la dissuasion.

(1) La réponse d'incident pourrait impliquer une certaine forme d'action contre les agresseurs. La portée des actions possibles en réponse aux actions adversaires sera gênée par les règles d'engagement établies par le gouvernement et le CEMD et par le droit national et international en vigueur. Les réponses peuvent s'échelonner de la terminaison de la relation avec l'activité illégale incluant jusques y compris la force militaire. Les RDE devraient définir clairement ce que constitue la légitime défense et toutes les réponses devraient être basées sur le principe de proportionnalité.

(2) La terminaison immédiate de l'accès du système adversaire de protection contre des actions supplémentaires et de l'exploitation du renseignement est une réponse possible. La terminaison devrait être appréciée en regard des besoins des communautés légales et du renseignement de collecte auprès de l'adversaire et de son exploitation. Le propriétaire de système, l'autorité d'approbation désignée ou une autorité supérieure décide de permettre à un intrus de maintenir l'accès de façon à rassembler l'information au processus de réponse. La décision repose sur l'évaluation du risque d'accès continu, la considération d'opérations présentes et futures et l'impact du renseignement.

(3) La restauration de capacité repose sur les mécanismes préétablis et éprouvés pour la restauration en priorité des capacités essentielles minimum. Le commandant établira les priorités de restauration selon une directive en provenance d'une autorité supérieure

(a) La restauration de capacité peut reposer sur le double, les liens superflus ou les composantes de systèmes, les bases de données en double ou même des moyens auxiliaires de transfert d'information. La conception de système d'information et la modification devraient tenir compte de l'incorporation des capacités de restauration automatisées et autres options superflues.

(b) Dans certains cas, les capacités techniques requises sont au delà des capacités des sites touchés. Les capacités d'aide à la restauration en ligne ou déployables peuvent fournir une expertise additionnelle requise pour restaurer les services. Ces capacités peuvent prendre la forme d'un service d'assistance d'une équipe de réponse d'incident de système d'information (ISIRT).

(c) Les ISIRT peuvent être formées d'une réponse rapide aux forces déployées et par certains commandants de composante pour une réponse semblable à des forces subordonnées à l'intérieur de la zone d'opérations.

(d) Une étape clé dans le processus de restauration de la capacité est de faire l'inventaire des ressources du système pour identifier les implants adversaires subreptices.

(3) Les incidents de sécurité de système d'information impliquent fréquemment une infraction aux lois nationales ou internationales. Dans de tels cas, les organismes d'application des lois militaires et civils devraient être contactés pour fournir une aide experte.

(a) Une aide d'application de la loi peut s'échelonner de l'avis sur la façon de préserver de la preuve à la fourniture de compétences de spécialistes d'enquête. La capacité d'enquête sur un incident dans des buts de vengeance peut dissuader d'autres adversaires. Les incidents du système d'information ou d'intrusions détectés et rapportés aux agents d'application de la loi militaires et civils pendant que les enquêtes criminelles aident les administrateurs de systèmes de soutien, la communauté du renseignement, les concepteurs de système et si nécessaire, les producteurs et les utilisateurs de l'information touchée. Les procédures d'enquête devraient protéger la capacité d'application de la loi pour continuer leur opération tout en protégeant les droits à la vie privée.

(b) Une analyse après l'attaque fournit de l'information au sujet de la vulnérabilité exploitée et mène à des améliorations de la sécurité. Des vérifications rétrospectives comme l'enregistrement automatisé de techniques d'événements d'attaque spécifiques et d'attaque durant un incident peuvent fournir l'information requise pour l'analyse. Ces mêmes capacités peuvent aussi fournir la preuve nécessaire pour exercer des options légales.

(4) La force militaire est une option réponse éliminant directement la menace ou interrompt les moyens ou les systèmes qu'un adversaire utilise pour mener une attaque d'information. La force militaire pourrait être appliquée de façon préventive (contre-opérations d'information offensives) ou de façon réactive (contre-opérations défensives) et peut inclure des attaques conventionnelles ou d'opérations d'information. Aux niveaux stratégiques de théâtre ou tactique, des options de réponse possibles seront définies en termes de règles d'engagement fournies au commandant.

304. CONTRE-OPÉRATIONS D'INFORMATION OFFENSIVES

1. Il pourrait y avoir des occasions où il est nécessaire de dissuader un adversaire de mener des opérations amies contre des forces amies ou de neutraliser les capacités des opérations d'information adversaires de façon à défendre les systèmes d'information amis. Une stratégie proactive et agressive pour nier

une information adversaire, la capacité électronique, le commandement et le contrôle peut être très efficace. Une application judicieuse des activités des opérations d'information avant les hostilités peut amener l'ennemi vers une non-exécution du conflit avant le commencement de ce conflit.

a. Une analyse de contre-opérations d'information offensives identifie les systèmes d'intérêt des opérations d'information adversaires et détermine les hiérarchies importantes, les liens et les processus dans ces systèmes. Un renseignement stratégique et tactique joue un rôle important en fournissant de l'information sur les capacités des opérations d'information adversaires. L'analyse des contre-opérations offensives a comme objectif l'augmentation du facteur décisif en identifiant les vulnérabilités de cible clés. Le module de coordination coordonnera l'analyse des contre-opérations d'information offensives au nom du CFO.

b. L'analyse tiendra compte des moyens de destruction physique, de GE, de déception et d'OPSPSY disponibles au CFO et la façon dont ils pourraient être appliqués à des systèmes d'opérations d'information adversaires. Le produit sera une liste de priorités des hiérarchies importantes, des liens et des processus devant être attaqués de façon à paralyser le système adversaire ainsi que les recommandations comme la meilleure méthode d'attaque et un concept pour la conduite des contre-opérations d'information.

   (1) Les plans de contre-opérations d'information offensives devraient être fondés sur la mission du CFO, l'intention du commandant et le concept de l'opération.

   (2) Les contre-opérations offensives seront synchronisées et soutiendront le plan du commandant.

   (3) Les contre-opérations offensives devraient viser à prendre et conserver l'initiative par la dégradation des capacités des contre-opérations d'information de l'adversaire.

   (4) Les cibles des opérations d'information au niveau opérationnel doivent être évaluées soigneusement. Les cibles des opérations d'information des opérations d'information seulement au niveau tactique sans surveillance interarmées risquent de perdre des voies utiles menant à des cibles opérationnelles valables.

c. Une fois les contre-opérations d'information offensives menées, il devrait y avoir certains moyens de voir si une attaque a réussi. Cela sera semblable à l'évaluation de dommage de la bataille conventionnelle mais à moins d'une attaque de nature physique, il sera plus difficile de déterminer l'effet de l'attaque sur le système adversaire. Le renseignement de toute source importera à cette analyse. Le module de coordination des opérations d'information coordonnera l'évaluation du dommage des opérations d'information.

"Les petits esprits essaient de tout défendre à la fois, mais les gens de bon conseil regardent le point principal seulement; ils parent les pires coups et supportent une petite blessure si de ce fait ils en évitent une plus grande. Qui trop embrasse, mal étreint."

Frederick the Great
cité dans Foertsch, *L'art de la guerre moderne*, 26 juin 1996

CHAPITRE 4

ORGANISATION DES OPÉRATIONS D'INFORMATION

> ***"L'organisation est le véhicule de la force. Celle-ci est de nature triple; elle est mentale , morale et physique."***
>
> **Major-général J.F.C. Fuller,**
> ***La fondation de la science de la guerre,* 1926**

401. GÉNÉRALITÉ

1. Un module de coordination des opérations d'information (IOCC) pleinement fonctionnel équivaut à des opérations d'information réussies au niveau national et opérationnel. L'IOCC intègre une vaste gamme d'actions des opérations d'information potentielles contribuant aux résultats attendus du commandant dans une zone d'opérations.

a. La structure organisationnelle de planification et de coordination des opérations d'information devrait être suffisamment flexible pour accommoder une variété de circonstances de planification et opérationnelles. Ce chapitre est axé sur la façon d'organiser la planification et l'application des opérations d'information.

b. Les opérations d'information devraient être une partie intégrale de toutes les opérations militaires. Cela requiert une planification globale et une coordination parmi plusieurs éléments des quartiers généraux interarmées, les états-majors des composantes, les autres ministères et les organismes pour assurer que les opérations d'information sont pleinement intégrées avec d'autres portions des plans de mission et d'opération.

c. C'est la responsabilité du commandant de créer un module de coordination des opérations d'information à l'intérieur du théâtre soutenu par le module de coordination des opérations d'information national. Depuis que les états-majors avec une structure diverse, la portée des responsabilités et l'infrastructure de soutien appuient les FO, les commandants devraient adapter leurs organisations selon les besoins uniquement de la mission.

d. Les états-majors principaux pouvant être impliqués dans la planification des opérations d'information sont l'état-major interarmées, le CFO et les états-majors des composantes subordonnées. Les circonstances dans lesquelles ces états-majors conduisent des opérations d'information peuvent affecter l'organisation optimale pour accomplir leurs responsabilités.

(1) L'état-major du CFO peut demander l'expertise de personnel assigné à leurs commandants subordonnés et à l'état-major des opérations d'information national pour aider au processus de planification tel que spécifié par le processus de planification des opérations. Durant la crise ou d'autres opérations à court préavis, le CFO peut demander l'expertise et le soutien technique de l'état-major des opérations d'information national.

(2) Un état-major de force interarmées (normalement un CFO) peut être désigné pour planifier et/ou exécuter des opérations d'information avec un court préavis. Un état-major du CFO peut être requis pour planifier et/ou exécuter des opérations d'information immédiatement à l'arrivée dans la zone opérationnelle, pendant la conduite d'opérations de présence militaire avancée ou après un déploiement avec un court préavis pendant que l'infrastructure pour soutenir l'état-major est développée.

e. Le module de coordination des opérations d'information est formé des représentants de chaque élément d'état-major, de composante et d'organismes de soutien responsables de l'intégration des capacités et des disciplines des opérations d'information dans un plan synergique. Le module coordonne les éléments d'état-major et/ou les composantes représentées dans le module de coordination des opérations d'information pour faciliter le soutien détaillé nécessaire à la planification et l'exécution des opérations d'information. Le tableau 4-1 fournit un aperçu général d'un module d'opérations d'information typique. La composition actuelle ou les membres et leur statut --résident ou non-résident--du module de coordination des opérations d'information peut varier basée sur toute la mission de la force interarmées, le rôle des opérations d'information dans l'accomplissement des objectifs du commandant et la capacité de l'adversaire ou d'un adversaire potentiel de conduire des opérations d'information. Les positions sont décrites comme résidentes ou non résidentes. La notion de résident implique que l'individu accomplissant la fonction devrait être de préférence situé au même endroit ou à proximité d'autres membres du module de coordination des opérations d'information. La notion de non- résident implique un idividu accomplissant la fonction ne nécessitant pas un contact fréquent avec d'autres membres de l'IOCC mais joue encore un rôle important dans la planification et la coordination des opérations d'information.

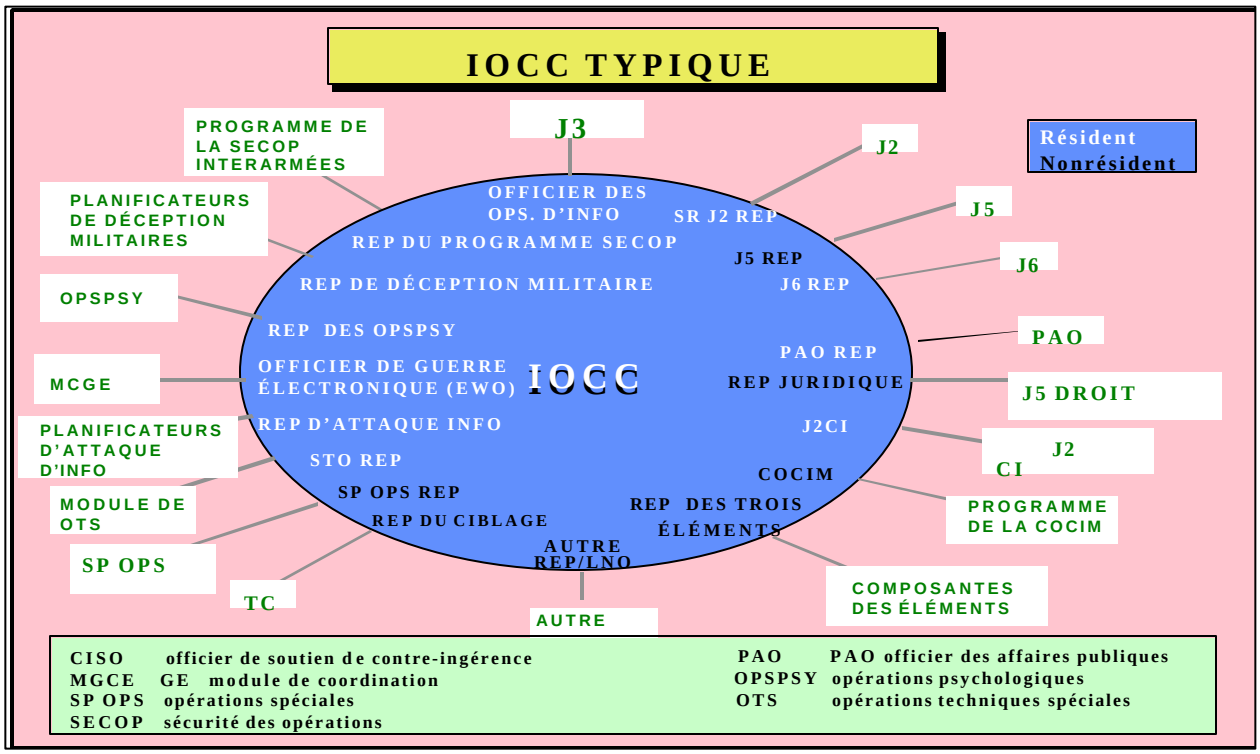


Tableau 4-1 IOCC typique

f. L'IOCC et la relation du MCGE. Le MCGE coordonnera de près les activités de GE avec l'IOCC pour assurer les effets synergiques de leurs activités respectives. *Le Manuel des opérations des Forces canadiennes, B-GG-005-004/AF000*, chapitre 33, "Guerre électronique", fournit des renseignements supplémentaires pour le développement et l'utilisation de la GE et du MCGE. Cela fournit au CFO la capacité d'intégration, de coordination et de résolution de conflit du spectre entier de la zone d'opérations.

402. ORGANISATION DES OPÉRATIONS D'INFORMATION

1. Le commandant devrait fournir l'orientation de la planification et de la conduite des opérations d'information et assigner la responsabilité à l'emploi des ressources des opérations d'information dans les opérations interarmées. Dans les opérations multinationales, le CFO est responsable de la coordination de

l'intégration des opérations d'information interarmées avec les atouts des opérations d'information multinationales, la stratégie et la planification. Le CFO peut déléguer la responsabilité des opérations d'information à un membre de l'état-major interarmées, normalement le J-3. Si autorisé, le J-3 aura la responsabilité d'état-major principale de planification, coordination et d'intégration des opérations d'information de la force interarmées.

2. Organisation des opérations d'information. Pour assister le J-3 dans l'exercice des responsabilités des opérations d'information un officier des opérations d'information sera désigné. La fonction importante d'un officier des opérations d'information devrait être la coordination de la stratégie des opérations d'information et les capacités de soutien et les disciplines entre les divers CFO, un plus haut échelon, une plus haute composante et les états-majors multinationaux. L'officier des opérations d'information assurera que les opérations d'information soient mises en oeuvre par l'orientation du commandant. Cela peut impliquer la coordination entre les organisations d'état-major ou les composantes responsables de chaque élément des opérations d'information.

a. J-3 Opérations/Plans: **Résident.** L'officier d'état-major principal des opérations d'information, le JTCB (ou l'équivalent fonctionnel) représentant et coordonnateur de toutes les zones fonctionnelles des opérations d'information. Le J-3 Opérations/Plans ou le représentant désigné aura accès aux travaux et aura aussi la connaissance du Comité de coordination d'information du CFO (ICC) (ou son équivalent fonctionnel) pour assurer la résolution de conflit et l'unité d'effort pour les activités d'information à l'intérieur d'une zone d'opérations. L'officier des OPSPSY du CFO participe comme membre du module de coordination des opérations d'information. Comme Chef de l'IOCC, le J3 Ops/Plans ou son sous-chef désigné assure normalement que les fonctions décrites au Tableau 4-2 sont accomplies.

FONCTIONS DE L'OFFICIER DES OPÉATIONS D'INFORMATION

- **Coordination et direction de l'effort des opérations d'information global pour le CFO**
- **Coordination des questions à l'intérieur de l'état-major interarmées et des planificateurs des opérations d'information de la contrepartie sur les états-majors subalternes**
- **Coordination des concepts défensif et offensif des opérations d'information en soutien au concept des opérations du CFO**
- **Établissement de priorités des opérations d'information pour accomplir des objectifs planifiés**
- **Détermination de la disponibilité des responsabilités des opérations d'information pour mettre les plans à exécution.**
- **Recommandation de la tâche au J-3 pour les organisations interarmées, état-major et éléments (p. ex., MCGE, planificateurs de déception militaires, etc.) ce plan et superviser les différentes capacités à utiliser. La tâche du J-3 consolidée assure l'efficacité d'effort dans la planification et l'exécution d'opérations d'information intégrées.**
- **Servant d'"avocat" principal des cibles des opérations d'information proposées en vue de l'attaque au moyen de la nomination cible et du processus de révision établi par le CFO**
- **Coordination de la planification et de l'exécution des opérations d'information entre les organisations interarmées responsables de chaque élément des opérations d'information.**
- **Coordination du soutien du renseignement aux opérations d'information.**
- **Coordination des intrants provenant des autres ministères et des organismes en dehors du MDN**

Tableau 4-2. Fonctions d'officier des opérations d'information

(1) Méthodes du module de coordination des opérations d'information. Le J-3 ou l'officier des opérations d'information devrait déterminer les méthodes utilisées par le module de coordination des opérations d'information pour s'acquitter des responsabilités assignées. Durant les phases de planification d'une opération, les planificateurs des opérations d'information devraient faciliter les efforts de planification entre les états-majors différents, les organisations et les parties d'état-major du CFO responsables de la planification des éléments des opérations d'information. Durant la phase d'exécution d'une opération, les planificateurs des opérations d'information devraient être disponibles au centre des opérations interarmées (JOC) ou son équivalent pour aider à la résolution de conflit, soutien ou d'ajustement des efforts des opérations d'information si nécessaire. Si l'administration des opérations d'information le permet et le J-3 ou l'officier des opérations d'information le crée, le personnel des opérations d'information peut être une partie du centre de l'équipe de surveillance de l'opération interarmées ou déployer une surveillance séparée durant la phase d'exécution d'une opération. Le personnel des opérations d'information devrait avoir une connectivité des communications soit à travers le JOC ou séparément pour coordonner efficacement le changement des besoins des opérations d'information durant la phase d'exécution. Tous les membres du module de coordination des opérations d'information devraient avoir l'habilitation de sécurité et l'accès nécessaire pour s'acquitter de leurs responsabilités dû à la nature délicate de certains aspects des opérations d'information comme la déception militaire.

b. DG RENS: Rep J2 princ: **Résident**. Planifie tout le soutien du renseignement requis pour appuyer les opérations d'information parcellisées et non parcellisées. Quand un module de coordination des opérations d'information est mis sur pied dans une localité autre que le QGDN, il sert de liaison de théâtre pour le DG Rens (pour toutes les matières reliées aux opérations d'information traitant du soutien aux analyses finies) et toutes autres entités du renseignement.

c. Planificateur J-5: **Non-résident**. Intègre les Affaires civiles dans le processus de planification des opérations de planification.

d. J-6 Planificateur: **Résident**: Facilite la coordination des opérations d'information défensives entre les planificateurs de système d'information et les gérants et les membres du module de coordination des opérations d'information. Coordonne avec le J3 pour minimiser l'impact des opérations d'information offensives sur la propre force du C2. Liaison principale avec le centre de contrôle des communications interarmées (JCCC). Coordonne le soutien de système d'information au module de coordination des opérations d'information. Sert de point d'entrée à l'activité de surveillance de la SECOM interarmées dans l'état-major. Les capacités de l'activité de surveillance de la SECOM interarmées offrent le potentiel d'une évaluation d'une évaluation de temps quasi réel de la posture de sécurité des communications des efforts de planification et des opérations continues.

e. Planificateur des OPSPSY: **Résident**. Information internationale/planificateur des OPSPSY. Intégration, coordination, résolution de conflit et synchronisation des plans des OPSPSY avec les efforts d'information gouvernementale canadiens. Sert de point d'entrée de liaison avec les modules des OPSPSY multinationales, selon le cas.

f. Planificateur de GE: **Résident**. Sert de leader du MCGE et d'officier de liaison des Services en électronique, communications et spectre de la Défense (DECSS). Coordonne de près avec le planificateur J6 la résolution de conflit des opérations d'information sur le spectre des communications amies.

g. Planificateur de la SECOP: **Résident**. Coordonne les activités du CFO ou le commandement subalterne de la SECOP. Travaille en étroite collaboration avec le planificateur J6 de la liaison des activités de surveillance de la SECOM interarmées.

h. Planificateur de la déception: **Résident**. Coordonne les intrants des opérations d'information à la planification de déception militaire.

i. Opérations techniques spéciales (STO): **Résident**. Le planificateur des STO devrait être pleinement intégré au module de coordination des opérations d'information pous assurer que la planification et les capacités des STO soient pleinement intégrées et coordonnées.

j. Contre-ingérence du J2: **Résident**. Coordonne les intrants des opérations d'information aux opérations de CI ayant des rôles importants dans la protection de l'attaque et de l'information. Fonctionne sous la surveillance globale et la direction du représentant J2 principal.

k. Planificateur d'attaque d'information: **Résident**. Sert de liaison principale avec le CST (centre de la sécurité des télécommunications), les activités des opérations d'information des trois armées, les modules de coordination des opérations d'information et des composantes de soutien direct de cryptologie des trois armées pour toutes les questions cryptologiques reliées aux opérations d'information incluant les zones des opérations d'information reliées à un ordinateur. Soutient la résolution de conflit pour les évaluations de gain ou de perte de renseignement et des opérations d'information.

l. Officier des affaires publiques: **Résident**. Interface des médias. Coordonne l'interface des médias.

m. Avocat militaire: **Non résident**. Assure que toutes les opérations d'information sont conformes au droit national et international.

n. Officier des Affaires civiles (CA): **Non résident**. Assure l'uniformité du message des OPSPSY à l'audience-cible dans les situations où les activités des CA ou les unités de la COCIM sont employées.

o. Planificateur des opérations spéciales (selon le besoin): **Non résident**. Coordonne l'utilisation des forces des opérations spéciales à l'intérieur d'une zone des opérations du CFO en soutien des opérations d'information.

p. Représentant du choix des objectifs et des moyens de traitement: **Non résident**. Représente le (s) module(s) de choix des objectifs et coordonne le choix des objectifs des opérations d'information avec le(s) module(s) du choix des objectifs.

q. Autres représentants et officiers de liaison: le Tableau 4-1 devient un guide déterminant les membres d'un état-major interarmées devant coordonner les planificateurs des opérations d'information. Le commandant devrait adapter la composition du module nécessaire pour accomplir la mission.

3. Rôle des représentants fonctionnels et des éléments dans la zone d'opérations. Les commandants d'élément devraient organiser leurs états-majors pour planifier et conduire les opérations d'information. Un point de contact des opérations d'information ou un officier des opérations d'information devrait être désigné. Cet officier ou un assistant fera la jonction avec le module de coordination des opérations d'information de la force interarmées pour fournir une expertise d'élément et agir comme liaison dans les questions des opérations d'information entre la force interarmées et la composante. Ces représentants peuvent aussi servir de membres d'une organisation de soutien ou plus des opérations d'information (p. ex., le MCGE). En outre, les composantes fonctionnelles demandant le soutien des opérations d'information spécifiques provenant des sources internes et externes normalement devraient demander un tel soutien au moyen du module de coordination des opérations d'information.

4. Le rôle des autres ministères et les organismes/représentants des forces multinationales et de leurs gouvernements. Les autres ministères et les organismes peuvent avoir un rôle d'organismes dans l'accomplissement des opérations d'information. Les CFO et leurs officiers des opérations d'information devraient assurer que les autres ministères et les organismes ayant des programmes continus et des intérêts dans la zone d'opérations sont consultés dans le développement des plans des opérations d'information. Les autres

ministères de soutien et les organismes devraient être considérés comme partie du plan des opérations d'information selon le cas. Également, les contributions potentielles et les préoccupations des forces multinationales et de leurs gouvernements devraient être considérées selon le cas.

> ***"En temps de guerre il n'est pas toujours possible de voir ses désirs accomplis. En travaillant avec les alliés il arrive quelquefois qu'ils suivent leur idée."***
>
> **Sir Winston Churchill, *The Hinge of Fate, 1950***

403. RELATIONS AVEC LES AUTRES ORGANISATIONS

1. Généralités. Tel que discuté ci-dessus, les planificateurs des opérations d'information utilisent les autres organisations pour planifier et exécuter les opérations d'information. Le soutien provenant de ces organisations inclut jusques y compris actuellement l'augmentation du personnel à partir du Centre de guerre électronique des Forces canadiennes (CFEWC), des Services en électronique, communications et spectre de la Défense (DECSS) et de l'activité de surveillance de la SECOM interarmées. En outre, au moyen des organisations de planification variées planifiant et administrant les capacités et les éléments des opérations d'information, les planificateurs des opérations d'information ont accès à l'expertise de la composante de l'élément ou fonctionnelle nécessaire à la planification de l'emploi ou de la protection des systèmes de la composante de l'élément ou des unités.

2. Centre de guerre électronique des Forces canadiennes (CFEWC). Le CFEWC peut fournir un soutien direct au commandant avec le commandant du module de coordination des opérations d'information.

3. Les Services en électronique, communications et spectre de la Défense (DECSS). Le DECSS peut fournir le soutien direct suivant au commandant par le biais du commandant du module de coordination des opérations d'information:

a. Les caractéristiques de localité et techniques sur les systèmes du C2 de la force amie.

b. L'aide au développement de la liste de fréquence restreinte interarmées (JRFL) dans un but de la résolution de conflit. Le DECSS peut déployer une augmentation de l'équipe pour préparer la JRFL ou fournir de l'instruction et de l'aide sur la façon de préparer une JRFL.

c. L'aide à la résolution de l'interférence opérationnelle et des incidents de brouillage. Le DECSS peut déployer du personnel pour assister à localiser rapidement et identifier les sources d'interférence et recommander des modifications techniques et opérationnelles pour résoudre les sources d'interférence identifiées.

d. Les caractéristiques locationnelles et techniques sur les systèmes du C2 de la force adversaire.

e. Les études de zone du C3 & I non classifiées sur l'infrastructure du C3 régionale incluant les caractéristiques physiques et culturelles, l'aperçu des systèmes de télécommunications et les fréquences électromagnétiques enregistrés pour l'usage à l'intérieur des frontières géographiques de chaque pays dans la région.

5. Le Groupe des opérations d'information des FC (CFIOG) conjointement avec le Centre de la sécurité des télécommunications (CST).

a. Fournit à la SECOM le soutien à la surveillance et de l'analyse.
b. Fournit un rapport opportun, adapté aux commandants de l'unité. Quand ce rapport est de nature de renseignement il devra être sous la direction globale et la coordination du représentant du J2.

6. J6 Ops. Les commandants normalement reçoivent le soutien des communications tactique, incluant l'augmentation d'une vaste gamme d'équipement de communications tactiques et commerciales provenant du J6 Ops. Le personnel du J6 Ops fournit une expertise de planification des opérations d'information et de résolution du conflit au module de coordination des opérations d'information et assure une protection appropriée pour des services de télécommunications fournis du J6 Ops et des systèmes d'information.

7. Le centre de contrôle des communications interarmées (JCCC). Les commandants établissent normalement un JCCC pour soutenir le contrôle et la gestion du réseau de haut rang à l'intérieur de la zone d'opérations. Les JCCC jouent un rôle vital dans les opérations d'information, en particulier dans le processus des opérations d'information défensives où ils fournissent la connectivité du J-6 à travers la chaîne de commandement

404. RELATIONS DU MODULE DE COORDINATION DES OPÉRATIONS D'INFORMATION DU CFO AVEC LES ORGANISATIONS DU MDN DE SOUTIEN

1. CST. Si un représentant du CST lui est assigné, le module de coordination des opérations d'information devra recevoir le soutien direct pour ce qui suit:

a. conseil, orientation et services au MDN sur la planification, l'acquisition, l'installation et les procédures à l'usage des systèmes de communications sécuritaires;

b. fournir du matériel clé cryptographique, de l'équipement et de la documentation;

c. mener des recherches, l'élaboration et l'évaluation des aspects de sécurité de l'information automatisée et des systèmes de communication avec la vue de conseiller le CFIOG sur la sécurité de ces systèmes et de leur application

d. conseiller et orienter le groupe des opérations d'information des FC (CFIOG) en développant des communications sûres et des systèmes d'information pour les besoins du gouvernement; et

e. fournir des conseils, de l'orientation et des services pour la protection de la sécurité et les intérêts privés des Canadiens.

2. Le DG Rens/J2. Un représentant DG Rens/J2 au module de coordination planifiera et coordonnera tous les besoins en renseignement des opérations d'information. Cela inclura jusques y compris ce qui suit:

a. Des renseignements précis et opportuns pour le choix des objectifs des opérations d'information et l'analyse postnucléaire.

b. Coordonner les besoins des opérations d'information et l'interface avec les activités I&W du J2 incluant une capacité d'analyse et de diffusion des avertissements d'attaque des opérations d'information.

c. Coordonner la disposition d'aide en renseignement dans la planification et l'exécution des activités des opérations d'information défensives.

d. Aide en identifiant les vulnérabilités amies et les objectifs amis les plus vraissemblables à l'intérieur des capacités de l'adversaire ou du potentiel de l'adversaire et du concept de l'opération.

3. CFIOG. Une fois assigné un représentant du CFIOG, le soutien suivant sera fourni au module de coordination des opérations d'information:

a. Coordination avec le DG Rens/J2, le Centre de la sécurité des télécommunications (CST) et les éléments pour assurer un soutien de base de données suffisant pour la planification, l'analyse et l'exécution des opérations d'information.

b. Assistance dans les avertissements de diffusion des attaques des opérations d'information.

c. Assistance dans l'établissement de l'architecture de sécurité et des normes de protection et de défense de l'élément d'information intégré (IIE) à l'intérieur de la zone d'opérations.

d. Développement d'un programme d'incident de système d'information et une capacité de réponse d'incident de sécurité pour la protection et la défense de l'élément d'information intégré (IIE) dans la zone d'opérations.

e. Évaluation des vulnérabilités de l'information et des systèmes d'information et de développement à l'intérieur des capacités de procédures pour atténuer les vulnérabilités évaluées et les effets de menace.

f. Développement des lignes directrices du programme d'éducation INFOSEC, d'instruction et des lignes directrices du programme de sensibilisation incluant des normes d'instruction minimum pour usage par les quartiers généraux du CFO, les composantes et les commandements subordonnés.

"L'objet premier de l'organisation est de protéger les personnes contre leurs pouvoirs d'adaptabilité, de jugement et de décisions."

General Sir Ian Hamilton,
***Soul and Body of an Army,* 1921**

CHAPITRE 5

PLANIFICATION DES OPÉRATIONS D'INFORMATION

> ***"Les plans de guerre couvrent chaque aspect de la guerre et les incorporent dans une simple opération devant avoir un objectif simple, ultime dans lequel tous les buts particuliers sont réconciliés."***
> **Major Général Carl von Clausewitz**
> ***"On War,"* viii, 1832, tr. Howard and Paret**

501. MÉTHODOLOGIE DE LA PLANIFICATION DES OPÉRATIONS D'INFORMATION

1. Généralités

   a. La planification des opérations d'information est une partie intégrale du processus de planification des opérations.

   b. La planification des opérations d'information doit être généralisée et comprendre l'emploi de toutes les ressources d'opérations d'information disponibles - MDN, autres ministères et multinationales.

   c. La planification des opérations d'information spécifique à une mission doit commencer à l'étape la plus opportune. Idéalement, la planification des opérations d'information en temps de paix sera continue en tout temps, et comme telle, servira de base aux opérations d'information subséquentes dans une opération hors guerre et/ou de conflit dans cette zone d'opération.

   d. La planification des opérations d'information doit analyser le risque de compromis, de représailles, de l'escalade des hostilités et de la réaction non coordonnée ou par inadvertance des activités par les divers fournisseurs de capacité interarmées, des éléments et/ou interinstitutions autorisées par le commandant de la force opérationnelle (CFO) pour l'emploi.

2. Fondements de la planification des opérations d'information. La planification de l'emploi des opérations d'information commence avec la compréhension et l'articulation de l'objectif, du but des opérations et de l'intention du commandant. Une campagne interarmées est la synchronisation de la Marine, de l'Armée et de l'Aviation et des opérations spéciales (ainsi que l'interinstitution) en harmonie avec la diplomatie, l'économique et les opérations d'information pour atteindre les objectifs nationaux et multinationaux. Les mêmes bases de la planification des opérations énumérées au chapitre 1/Sect 1/Art 102/para 2 du *Manuel des opérations des FC*, B-GG-005-004/AF 000 s'appliquent à la partie des opérations d'information d'un plan. Certains de ces principes sont particulièrement importants dans la planification et l'exécution des opérations d'information.

   a. La synchronisation et l'intégration des opérations d'information nécessitent une orientation stratégique nationale claire. Cette stratégie, formée et orientée selon les politiques de sécurité nationale doit fournir l'orientation globale au CEMD. Cette orientation est requise pour assurer que la planification et l'exécution des opérations d'information soutiennent les objectifs nationaux. Le CEMD à son tour fournit l'orientation et la direction pour l'emploi des Forces canadiennes dans des opérations militaires interarmées ou combinées et comme soutien aux autres ministères nationaux et alliés. Ces stratégies devraient soutenir les objectifs énoncés du CEMD dans toute la gamme des opérations militaires. Le CEMD et le CFO doivent considérer l'environnement stratégique durant le processus de budget et de planification de façon à déterminer les contraintes potentielles. Ces contraintes limiteront la liberté d'action du CFO et influenceront le moment et la forme de l'opération. Le CFO doit fournir une orientation de planification importante aux composantes et aux forces interarmées subordonnées incluant les cibles/buts principaux et ces zones/actions à éviter. Cette orientation établira les "limites" pour la planification des opérations d'information, identifiera les limites cibles basées sur la politique et serviront à réduire l'incertitude associée avec la planification des opérations d'information.

b. La planification des opérations d'information nécessite un horaire de décisions ordonné. Généralement, les opérations d'information nécessiteront un développement à long terme du renseignement et de la préparation de l'espace de bataille pour une utilisation optimale des capacités. L'utilisation des opérations d'information en temps de paix comme moyen principal d'atteindre les objectifs nationaux et de prévenir un autre conflit demande une capacité d'intégration des capacités des opérations d'information dans une stratégie cohérente.

c. Le niveau stratégique des planificateurs des opérations d'information doit aussi considérer l'intégration et le soutien aux modules de coordination des opérations d'information opérationnelles et tactiques dans le développement du plan des Opérations d'information pour soutenir les objectifs du commandant. La direction et les intrants nécessaires pour ces modules de coordination des opérations d'information de fonctionner efficacement doivent être fournis clairement d'une manière opportune. Les plans et activités des opérations d'information doivent aussi être intégrés et coordonnés avec les actions d'autres ministères et autres organismes impliqués.

d. L'établissement de l'organisation des forces opérationnelles et des relations de commandement désigné est aussi très important dans le développement et l'exécution des opérations d'information. L'établissement de ces relations est la base d'atteinte de l'unité de commandement et d'effort dans la Marine, l'Armée et l'Aviation et les forces d'opérations spéciales. Cela établit aussi l'entente interinstitutions sur le processus de synchronisation, la coordination et la résolution du conflit pour la planification et l'exécution des opérations d'information.

e. Dans la planification des opérations d'information, les planificateurs identifieront les vulnérabilités d'un adversaire, concevront les tâches nécessaires et les sous-tâches et identifieront les méthodologies pour exploiter ces vulnérabilités de façon à atteindre les objectifs désirés. Les moyens ou les capacités employés peuvent inclure les capacités non organiques/internationales. Cela nécessite des planificateurs/IOCC pour identifier toutes les ressources disponibles des opérations d'information pour l'opération de façon à fournir au CFO un ?coffre à outils? à utiliser dans le développement du plan des opérations d'information et faciliter une capacité efficace à l'adaptation de la cible. Comme partie du processus de planification, la désignation du pouvoir d'autorisation et d'exécution pour les opérations d'information spéciales est nécessaire. Le pouvoir d'autorisation accorde l'approbation d'emploi des opérations d'information et spécifie normalement l'allocation d'opérations d'information offensives spécifiques et des capacités disponibles au CFO et/ou ses subalternes. Le pouvoir exécutif est le pouvoir de mener des opérations d'information spécifiques à un moment et/ou place désigné. Le pouvoir exécutif sera normalement dévolu au CFO.

f. L'identification des centres de gravité stratégique et opérationnel de l'adversaire et le développement d'une méthodologie pour les vaincre est un principe de la planification des opérations d'information. La préparation du renseignement d'un espace de bataille (IPB) pour les opérations d'information diffère des besoins traditionnels et nécessitera normalement un plus grand délai et des besoins de collecte augmentés. La communauté du renseignement doit avoir accès aux systèmes; fournir la connaissance des schémas des installations et de la connectivité physique et virtuelle et développer les outils dynamiques pour exploiter cette information et l'autre information spécialisée comme les profils psychologiques et les modèles d'infrastructure. Le tableau 5-1 montre un moyen de planification et d'évaluation des opérations d'information de gabarit contre un adversaire. La planification des opérations d'information défensives a des besoins de renseignement spécifiques de déterminer les capacités et les intentions des opérations d'information adversaires et de développer un processus d'indications et d'avertissement des opérations d'information.

g. L'identification et l'offre d'orientation sur la protection de centres de gravité d'information amie importants au niveau opérationnel du CFO et ceux au niveau stratégique d'environnement de l'information intégré sont importants. L'identification de priorités d'informations amies exige une collaboration étroite et une coopération entre le MDN, les autres ministères et l'industrie. La protection de l'environnement d'information intégré demande des efforts coopératifs pour mettre en oeuvre des mesures protectrices proportionnées à la valeur de l'information ou des systèmes d'information protégés.

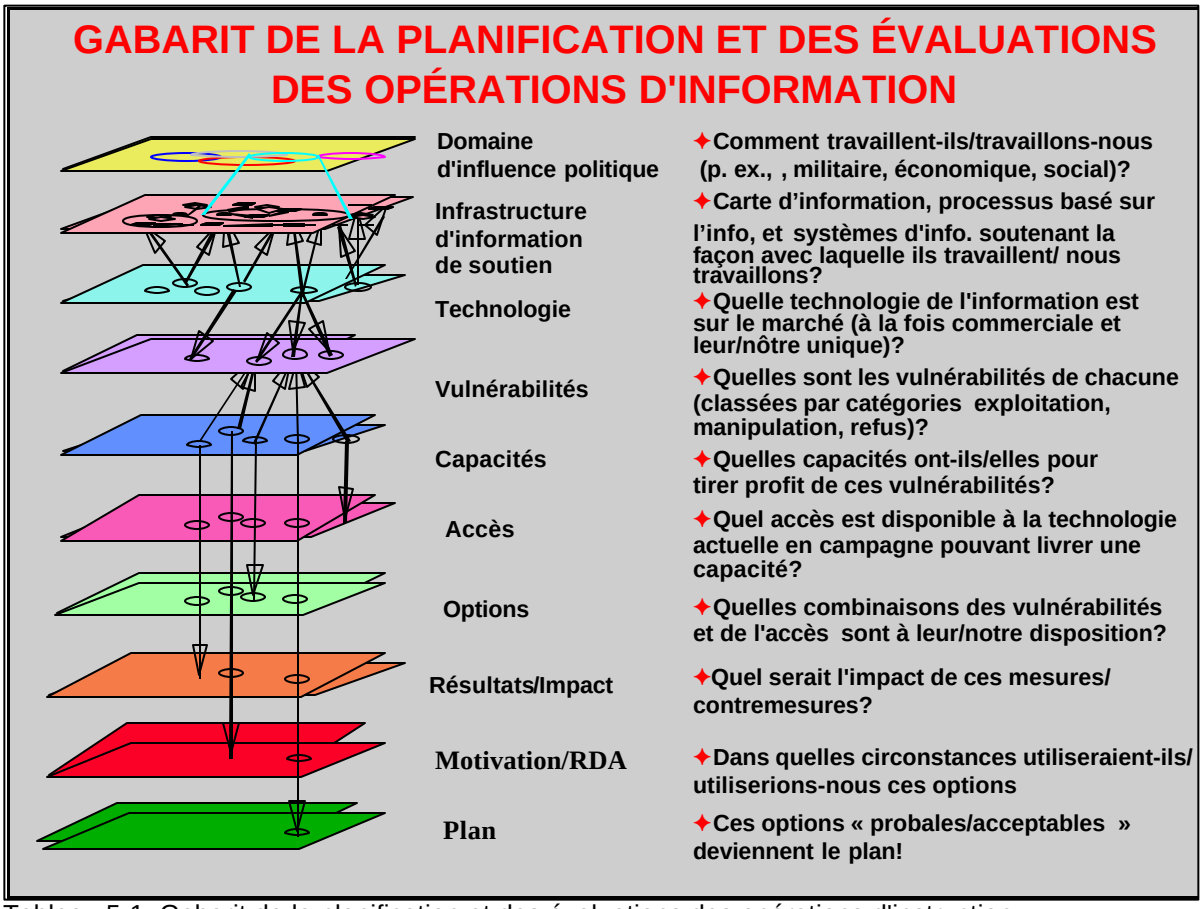


Tableau 5-1. Gabarit de la planification et des évaluations des opérations d'instruction

L'adhésion à un niveau commun de protection demande la détermination de la portée de ce qui a besoin d'être protégé et les normes de protection nécessaires.

3. Module de coordination des opérations d'information (IOCC)

a. Aux niveaux stratégique et opérationnel, le IOCC est le point central de la planification des opérations d'information devant inclure la synchronisation, la coordination et la résolution de conflit de toutes les ressources et les efforts des opérations d'information disponibles. La fonction première de cette coordination est l'intégration et la résolution de conflit des capacités des opérations d'information pour accomplir les objectifs de la mission.

b. Le IOCC devrait être représenté dans toutes les activités de planification. La relation avec le IOCC à d'autres actitivités de planification est présentée au paragraphe 503 ci-dessous.

502. PRINCIPES DES PLANS D'OPÉRATION

1. Il y a plusieurs principes importants devant être inclus dans les Plans d'opérations.

a. Fournir des concepts de l'opération stratégiques généraux et le soutien pour atteindre les objectifs multinationaux, nationaux et stratégiques de la zone d'opérations.

b. Fournir un horaire ordonné des décisions.

c. Atteindre une unité d'efforts avec les forces des opérations de la Marine, de l'Armée et de l'Aviation conjointement avec les organisations des interinstitutions, non gouvernementales ou privées bénévoles ou des Nations Unies ou d'autres forces multinationales, selon le cas.

d. Incorporer l'intention stratégique du CFO et le centre opérationnel

e. Identifier toutes les forces spéciales ou capacités pouvant être présentes dans la zone d'opérations.

f. Identifier les centres de gravité stratégique et opérationnel de l'adversaire et fournir l'orientation aux subordonnés pour la conduite des opérations contre les centres de gravité identifiés.

g. Identifier les centres de gravité stratégiques amis et opérationnels et fournir l'orientation à des subalternes pour les protéger.

h. Ordonner une série d'opérations interarmées principales importantes menées simultanément en profondeur.

i. Établir l'organisation des forces subordonnées et désigner les relations de commandement.

j. Servir de base à la planification subordonnée et définit clairement ce que constitue le succès incluant les objectifs de terminaison de conflit et les activités de l'après-guerre.

k. Fournir une direction stratégique; le centre opérationnel et les tâches importantes, objectifs et concepts aux subalternes.

2. Voir le Manuel sur l'emploi de la force des FC, au chapitre 4, pour de plus amples renseignements sur les principes des plans d'opérations.

503. COORDINATION DE LA PLANIFICATION DES OPÉRATIONS D'INFORMATION

1. Généralités. La coordination des opérations d'information est continue, à partir de l'indication la plus opportune de nécessité d'action militaire, durant toutes les étapes de planification, la génération de la force, l'emploi de la force et finalement les actions après les conflits ou les activités à l'intérieur de la zone d'opérations. Ces actions/activités après les conflits incluent la transition de l'opération aux organismes militaires et non militaires et organisations.

2. Équipe de gestion de l'état-major interarmées (ÉGÉAI). L'ÉGÉAI doit avoir une représentation à partir du IOCC pour assurer que les aspects des opérations d'information d’une ou de toutes les opérations sont considérées aux stades initiaux des délibérations concernant les actions militaires possibles.

3. Équipe de planification interarmées (JPT). L'équipe de planification du CFO doit aussi avoir une représentation du IOCC. Un échange d'information initial et continu entre l’équipe de planification interarmées et le IOCC est essentiel à l'intégration réussie de la planification des opérations d'information dans le Processus d'emploi de la force global.

4. Module de coordination cible (TCC). Comme avec l’équipe de planification interarmées (JPT), la représentation dans le module de coordination cible (TCC) (si établie) est essentielle si une coordination des opérations d'information efficace doit être fournie aux cibleurs. Cette représentation fournira aussi un moyen de coordonner les capacités de la FO avec l'application aux opérations d'information et d'autres opérations conventionnelles.

504. INTÉGRATION DES OPÉRATIONS D'INFORMATION ET RÉSOLUTION DE CONFLIT

1. Intégration des opérations d'information. De façon à assurer des opérations d'information efficaces, leur planification doit être intégrée avec d'autres aspects de l'opération au stade le plus rapproché possible. Cette planification doit franchir toutes les frontières entre les éléments, les groupes, les organisations et/ou les organismes pouvant être impliqués dans l'exécution de l'opération.

a. Les opérations d'information de par leur nature sont souvent décentralisées. En conséquence, il est impérieux que les niveaux de commandement praticables les moins élevés prennent connaissance du plan et participent à son développement selon le cas.

b. Le IOCC devrait fournir la stratégie d'intégration globale pour les opérations d'information et assurer son intégration.

(1) Le IOCC devrait avoir normalement le personnel assigné, les liens de communication et la connectivité avec le J-6 et les fournisseurs des opérations d'information défensives pour intégrer efficacement la planification des opérations d'information défensives.

(2) Strictement à l'intérieur du contexte des opérations d'information, l'IOCC maintient aussi la connectivité avec les autres ministères comme le Centre de la sécurité des télécommunications (CST), le SCRS et la GRC qui ont un rôle dans les opérations d'information.

c. Capacités des opérations d'information compartimentées. Les membres du IOCC possédant la bonne habilitation de sécurité et l'accès intégreront les capacités des opérations d'information dans des plans. Normalement, le module est l'entité appropriée pour mener cette intégration. En outre, le IOCC a la connectivité avec une autorité supérieure pour l'approbation du plan normalement associée avec les opérations compartimentées. Une coordination étroite entre l'IOCC et le module des opérations techniques spéciales de la force interarmées est essentielle à cet effort d'intégration. Des considérations additionnelles sont traitées à l'Annexe A.

2. La résolution de conflit des opérations d'information. La résolution des opérations d'information sera normalement nécessaire à plusieurs niveaux de planification, p. ex., à l'intérieur, ci-dessus et ci-dessous la force interarmées et à plusieurs niveaux de guerre. En traitant de la résolution de conflit il sera nécessaire de traiter des aspects inter-niveau et intra-niveau. Comme avec l'intégration, la déstabilisation des opérations de conflit devrait commencer au stade le plus rapproché de la planification des opérations d'information.

a. La résolution de conflit des opérations d'information doit être un processus continu permettant la mise en phase d'options d'emploi des opérations d'information. La probabilité des opérations d'information simultanées à tous les niveaux de guerre et de commandement est assez élevée. En outre, le grand nombre relatif de capacité des opérations d'information potentielle dans la même zone d'opérations , particulièrement quand les opérations d'information sont un élément de premier ordre d'une opération du CFO, rend essentielle l'identification opportune rapprochée essentielle des questions de déstabilisation des opérations d'information.

b. Le IOCC est la meilleure entité de coordination et de surveillance de déstabilisation de conflit d'opérations d'information comme il a une connectivité avec tous les fournisseurs d'opérations d'information à l'intérieur de la Force interarmées. En outre, le IOCC a une connectivité avec les IOCC ci-dessus et ci-dessous dans la chaîne de commandement. Enfin, le IOCC travaille de concert et sert d'intrant aux opérations d'information défensives à l'intérieur de la Force interarmées, de ce fait fournissant au IOCC le meilleur aperçu global d'assurer la résolution de conflit des opérations d'information.

505. ORIENTATION POUR LA PLANIFICATION DES OPÉRATIONS D'INFORMATION

1. Généralités. Les plans des opérations d'information devraient être développés comme soutien au plan opérationnel global. *Le Manuel du processus d'emploi de la force des FC B-GG-005-004/AF-004* est le guide du planificateur opérationnel aux OPLAN développés au moyen du processus de planification.

a. Opérations d'information au niveau stratégique. Le Tableau 5-2 fournit un guide général à la planification des opérations d'information comme une partie intégréedu processus de planification de niveau stratégique tel que montré dans le *Manuel du processus d'emploi de la force des FC*, B-GG-004-005/AF-004, Annexe A, chapitre 4. Le Tableau peut être adapté à une orientation de planification des opérations d'information semblable aux niveaux de FO subordonnés et de composante selon le

cas. Quand une planification des opérations d'information est menée au dessous du niveau stratégique, les IOCC subordonnées devraient conserver l'IOCC au prochain niveau le plus élevé pleinement informé de toutes les activités de planification des opérations d'information pouvant exiger la synchronisation, la coordination ou la résolution de conflit.

Étape du processus stratégique	**Action de planification du IOCC**	**Résultat de planification des opérations d'information**
Analyse de mission	Identifier les besoins d'information nécessaires à la planification de la mission.	Attribution des tâches pour rassembler/obtenir l'information nécessaire.
	Aider la planification des opérations d'information au développement de l'orientation de du CEMD pour soutenir l'orientation de planification opérationnelle globale.	Orientation de planification du CEMD pour les opérations d'information.
Développer des plans d'action initiaux	Soutenir l'élaboration du budget d'état-major du renseignement, des opérations et des communications .	Portion d'opérations dinformation du budget d'état-major .
Déterminer le plan d'action préféré	Assister dans la conversation du budget de l'état-major en budget du commandant dans l'aspect des opérations d'information du concept opérationel selon le cas.	Portion des opérations d'information du plan global approuvé.
Préparer l'ordre d'avertissement	Liaison initiale avec des unités et des organismes pouvant participer ou appuyer des opérations IO .	
Conduire une planification des opérations détaillée	Développer le plan des opérations d'information complet et les plans de chacun des éléments des opérations.	Appendices approuvés offensifs et défensifs avec des onglets d'élément, des plans de soutien complets et l'inclusion de besoin des opérations d'information dans le TMTFQ
	Unités subordonnées et organismes de soutien préparent leurs propres plans d'opérations d'information. Coordonnent/assistent les plans d'opérations d'information subordonnés et de soutien organismes si nécessaire. Assurent que le TMTFO soutient le plan des opérations d'information.	Complètent les plans d'organismes de soutien. Plan des opérations d'information soutenues par le TMTFO

Tableau 5-2. Planification des opérations d'information au niveau stratégique

b. Opérations d'information au niveau stratégique. Le tableau 5-3 fournit une orientation générale à la planification des opérations d'information au niveau opérationnel de concert avec l'Annexe A au chapitre 3 du *Manuel du processus d'emploi de la force des FC*, B-GG-004-005/AF-004. Comme au

Tableau 5-2, le Tableau 5-3 peut être adapté tel qu'exigé pour l'orientation de planification des opérations d'information similaires aux niveaux de la FO subordonnée et de la composante.

2. Orientation des opérations d'information offensives. Le produit de planification des opérations d'information offensives finales aux niveaux de planification stratégique et opérationnelle. Ce plan contient le concept global des opérations d'information offensives et défensives concernant le plan ou l'OPORD dans lequel il apparaît. Cela devrait inclure le moment, les contraintes et les buts de chaque effort d'action/de force.

3. Orientation des opérations d'information défensives. Le produit de planification des opérations d'information défensives finales aux niveaux de planification stratégique et opérationnel est un OPLAN approuvé. Ce OPLAN sera inclus comme une Annexe séparée dans l'ordre d'opération global. Une orientation spécifique sur la préparation de cet appendice est inclus comme Annexe B.

"Stimulation du génie décidant de l'issue d'une bataille? Je n'y crois pas. Une bataille est une opération compliquée que vous préparez laborieusement. Si l'ennemi fait cela, il faut se dire Je vais faire cela. Si ceci et cela se produit, voici les étapes à suivre pour l'accomplir. Vous pensez à chaque développement possible et décidez de la façon de transiger avec la situation créée. Un de ces développements se produit; vous mettez votre plan en oeuvre et tout le monde dit "Quel génie..." alors que tout le crédit va à la préparation."

Ferdinand Foch, entrevue, avril 1919

ÉTAPES	ÉLÉMENTS CLÉS	TÂCHES DU IOCC	PRODUCTION
INITIATION	Recevoir la tâche de planification	Notifier les membres du IOCC du besoin de planification. Identifier les besoins d'information nécessaires à la planification de la mission.	Attribution des tâches pour rassembler/obtenir l'information nécessaire.
ORIENTATION	Conduire une analyse de mission Assister à un briefing sur l'analyse de mission Planification du commandant Orientation émise	Assister au développement de l'orientation de planification des opérations d'information du CFO en soutien à l'orientation de planification opérationnelle .	Planification de l'orientation pour les opérations d'information
DÉVELOPPEMENT DU PLAN D'ACTION	Analyse des facteurs Développer un plan d'action Note d'information	Soutien du développement, du budget d'état-major du renseignement, des opérations et des communications.	Portion des opérations d'information du budget d'état-major.

ÉTAPES	ÉLÉMENTS CLÉS	TÂCHES DU IOCC	PRODUCTION
DÉCISION	Décision du commandant	Assister à la transformation du budget d'état-major dans le budget du CFO. Assister dans l'aspect des opérations d'information du concept du CFO selon le besoin.	Portion des opérations d'information du plan global approuvé selon le besoin.
DÉVELOPPEMENT DE PLAN	Développer, Coordonner Demander l'autorisation. Émettre un plan.	Développer le plan des opérations d'information et les plans de chacun des éléments des opérations d'information en coordination avec les sections d'état-major appropriées, les unités opérationnelles et les organismes de soutien.	Appendices offensifs et défensifs approuvés avec des tabs d'élément, des plans de soutien complétés et l'inclusion de besoins des opérations d'information dans le TMTFO.
RÉVISION DE PLAN	Examen de plan Évaluation de plan Briefing de décision révisée (selon le besoin)	Modifier/raffiner le plan si nécessaire.	Appendices des opérations d'information offensives et défensives approuvées.

Tableau 5-3. Planification des opérations d'information au niveau opérationnel

CHAPITRE 6

OPÉRATIONS D'INFORMATION DURANT L'INSTRUCTION ET LES EXERCICES

601. ÉLÉMENTS ESSENTIELS EN INSTRUCTION DES OPÉRATIONS D'INFORMATION

1. Généralités

   a. Un emploi efficace des opérations d'information dans les opérations interarmées dépend de la capacité d'organisation et d'instruction de façon à ce que le Canada vise à employer la force militaire. La tâche fondamentale est d'instruire le personnel et les organisations responsables de la planification et de la conduite des opérations d'information relativement aux concepts et à la doctrine trouvés dans cette publication. Il y a des opportunités pour l'instruction des opérations d'information dans l'industrie durant les exercices alliés et à des cours d'instruction alliés; l'instruction des opérations d'information est introduite à tous les niveaux d'instruction d'état-major. L'état-major politique devrait assurer que les opérations d'information demeurent une partie importante de l'instruction formelle.

   b. Les commandants à tous les niveaux devraient assurer que le personnel clé responsable de la planification et de la conduite des opérations d'information participe pleinement à toutes les opportunités d'instruction des opérations d'information disponibles et recevoir l'instruction d'opérations d'information appropriées. Cette instruction devrait être axée sur la zone d'opérations où les opérations d'information sont normalement menées. Cette instruction devrait être dirigée vers les activités d'opérations d'information en temps de paix de routine dans chaque zone d'opérations du commandant ainsi que la transition à la résolution de crise et de conflit.

   c. Le système d'éducation militaire des Forces canadiennes devrait assurer que les officiers comprennent l'importance des opérations d'information comme stratégie globale aux niveaux stratégique, opérationnel et tactique à travers le continuum de conflit.

2. Instruction des opérations d'information offensives

   a. L'instruction des opérations d'information offensives devrait inclure l'intégration de toutes les capacités des opérations d'information offensives disponibles incluant les capacités des opérations d'information multinationales et autres MDN et en dehors du MDN.

   b. L'instruction des opérations d'information offensives devrait être composée de l'instruction individuelle et organisationnelle et devrait souligner la planification d'attaque des opérations d'information.

   c. L'instruction des opérations d'information offensives devrait inclure la planification et l'utilisation de toutes les capacités des opérations d'information potentiellement disponibles offensives.

3. Instruction des opérations d'information défensives. L'instruction des opérations d'information défensives devrait:

   a. inclure l'intégration de toutes les capacités des opérations d'information défensives disponibles incluant le MDN, un autre ministère et les capacités des opérations d'information commerciales et défensives;

   b. inclure l'instruction des individus et des organisations, soulignant la protection des systèmes d'information et de défense d'information; et

   c. bâtir sur les procédures de l'information en temps de paix de routine et de protection de systèmes d'information utilisés à l'intérieur du MDN, des autres ministères et du secteur commercial.

602. OPÉRATIONS D'INFORMATION DANS LES EXERCICES

1. Généralités

a. Les opérations d'information devraient être incorporées dans tous les exercices, interarmées et combinés, à un niveau approprié à la portée et la durée de l'exercice. La mise en oeuvre des opérations d'information durant les exercices illustre les questions complexes soulevées par la stratégie aux planificateurs d'exercices; le besoin de coordination à l'intérieur des ministères du MDN avec les autres ministères et le secteur commercial sont aussi soulignés.

b. Les exercices peuvent incorporer l'instruction des opérations d'information de deux façons: autonome et de soutien.

(1) Autonome:les opérations d'information sont la seule stratégie utilisée pour faire tort à l'adversaire.

(2) Soutien: les opérations d'information sont utilisées comme un multiplicateur de force à l'intérieur d'une campagne conventionnelle.

c. Le Tableau 6-1 contient des considérations de planification d'exercice des opérations d'information principales.

CONSIDÉRATIONS DE PLANIFICATION D'EXERCICE DES OPÉRATIONS D'INFORMATION PRINCIPALES

- **Développer des objectifs d'opérations d'information concrets, réalisables**
- **Fournir des actions d'opérations d'information suffisantes pour soutenir les objectifs de l'exercice**
- **Créer un environnement d'exercice d'opérations des informations aussi réaliste que possible**
- **Estimer et évaluer l'emploi des opérations d'information**
- **Exercer les opérations d'information offensives et défensives utilisant toutes les capacités des opérations d'information disponibles et compatibles avec le scénario d'exercice**
- **Exercice du soutien du renseignement aux opérations d'information**
- **Utiliser les mesures de sécurité appropriées pour protéger les tactiques, les techniques et les procédures des opérations d'information**
- **Évaluer l'utilisation des produits de soutien d'ordinateur pour planifier et évaluer les opérations**
- **Évaluer l'utilisation des simulations pour réaliser certains objectifs d'instruction des opérations d'instruction**

IO - Opérations d'information

Tableau 6-1. Considérations de planification d'exercice des opérations d'information importantes

2. Opérations d'information offensives

a. La planification et l'exécution des opérations d'information offensives dans les exercices interarmées devraient souligner les capacités d'attaque et d'utilisation des opérations d'information normalement disponibles à la force interarmées menant l'exercice.

b. Les capacités des opérations d'information offensives dans les exercices interarmées devraient avoir le soutien du renseignement entier, en particulier le renseignement concernant la Force d'opposition. En outre, la Force d'opposition devrait avoir une voie libre réaliste pour fournir un défi approprié aux développements du renseignement ami et des efforts de ciblage des opérations d'information.

3. Opérations d'information défensives

a. La planification et l'exécution des opérations d'information défensives dans les exercices interarmées devraient souligner la protection de l'information, vulnérable à l'attaque au moyen d'opérations contrepsychologiques, la contre déception et la propagande d'un adversaire et les systèmes de défense d'information. Les capacités des opérations d'information défensives normalement disponibles à la force interarmées devraient être exercées.

b. La planification des opérations d'information défensives dans les exercices devrait aussi inclure les considérations de protection et de défense pour le MDN, les autres ministères et l'infrastructure des communications commerciales de soutien.

c. Comme dans les jeux des opérations d'information offensives dans les exercices, la Force d'opposition devrait avoir la voie libre pour que les capacités des opérations d'information défensives soient soulignées ou exercées au niveau approprié. Des participants d'exercice principaux devraient permettre le commandement et contrôle et d'autre chaos de dépossession d'information survenant quand des mesures d'opérations d'information défensives inefficaces sont planifiées et mises en oeuvre. Cela encouragera les participants à l'exercice à travailler à l'aide de problèmes d'opérations d'information défensives causés par des opérations d'information adversaires efficaces.

603. OPÉRATIONS D'INFORMATION DANS LA PLANIFICATION ET LE MODÈLE ET LA SIMULATION D'EXERCICE

1. Généralités. Les opérations d'information devraient être incorporées dans toute la planification et l'exercice de modèle et simulation à l'étape praticable du développement du modèle. Seulement de cette façon le modèle et simulation peuvent être intégrés approximativement avec celle des autres zones de guerre.

2. Opérations d'information dans les modèles de planification

a. Opérations d'information offensives. Les modèles de planification devraient incorporer des capacités d'opérations d'information offensives et des principes incluant des capacités d'opérations d'information offensives normalement organiques au MDN et aux autres ministères. Les capacités des opérations d'information offensives multinationales devraient être inclues comme elles deviennent connues et disponibles dans des buts de planification.

b. Opérations d'information défensives. Les modèles de planification devraient inclure les capacités des opérations d'information défensives à partir des FC, les autres sources du MDN et autres ministères en dehors du MDN et de telles capacités des opérations d'information défensives commerciales raisonnablement attendues dans des buts de planification. Les capacités des opérations d'information défensives multinationales potentielles devraient être cataloguées et incluses dans les modèles de planification.

3. Opérations d'information dans le modèle et simulation d'exercice (M&S)

a. Opérations d'information offensives. Les capacités des opérations d'information offensives devraient être incorporées dans l'exercice du modèle et simulation pour avoir la voie libre entre les forces interarmées amies et la Force d'opposition. Si possible et pratique, les capacités devraient être taillées en conformité avec les capacités des opérations d'information offensives des forces amies participantes et de la Force d'opposition normale pour l'exercice de la zone d'opérations. En outre, les capacités d'opérations d'information offensives multinationales normalement disponibles pour la planification et les opérations dans la région devraient être ajoutées au(x) modèle(s) si possible.

b. Opérations d'information défensives. Les capacités d'opérations d'information défensives organiques à la force d'exercice, le MDN, les autres ministères et le secteur commercial normalement disponible dans la zone d'opérations devraient être ajoutées au(x) modèle(s) d'exercice. Les capacités d'opérations d'information défensives commerciales et les ressources des opérations d'information défensives multinationales connues pour être disponibles dans la région d'exercice touchée devraient être ajoutées si possible; cela permettra des jeux d'opérations d'information de modèle et simulation (M&S) réalistes entre la force interarmées et ses partenaires multinationaux et la Force d'opposition.

c. Estimation et évaluation. Le modèle utilisé dans le modèle et situation (M&S) devrait fournir un moyen d'estimer et d'évaluer l'emploi des opérations d'information dans les opérations d'information offensives et défensives et permettre une rétroaction claire aux participants à l'exercice, à la fois des forces amies et de la Force d'opposition. L'estimation et l'évaluation aussi devraient fournir un moyen de contrôle de jeu des opérations d'information et faire des ajustements si les opérations d'information nuisent les autres objectifs d'instruction de l'exercice ou les nient.

ANNEXE A

ORIENTATION DES OPÉRATIONS D'INFORMATION

L'orientation dans cette annexe est liée au développement des parties d'un ou de tous les plans développés des opérations d'information à l'usage des FC.

1. Situation

a. Ennemi

(1) Quelle est la situation de l'ennemi, la disposition de la force, les capacités d'information et les plans d'action possibles?

(2) Y a-t-il de l'information spécifique portant directement sur les opérations d'information planifiées?

b. Ami

(1) Quelle est la situation des forces amies pouvant affecter directement l'atteinte des objectifs des opérations d'information?

(2) Y a-t-il des limites importantes et d'autres opérations d'information planifiées?

c Hypothèses

(1) Quelles sont les hypothèses concernant les capacités amies, ennemies ou d'une tierce partie, les limites ou les plans d'action?

(2) Quelles conditions prévaudront d'après le commandant quand le plan deviendra un ordre?

2. Mission. Quelle est la mission des opérations d'information (qui, quoi, quand, où et pourquoi)?

3. Exécution.

a. Concept de l'opération

(1) Comment le commandant voit-t-il l'exécution des opérations d'information du début à la fin?

(2) Comment les opérations d'information soutiendront-elles la mission du commandant?

(3) Quels sont les concepts de supervision et de finition des opérations d'information?

b. Tâches des opérations d'information

(1) Quelles sont les tâches importantes de déception militaire? Voir Appendice A, "Orientation (déception militaire) des opérations d'information" pour plus d'orientation.

(2) Quelles sont les tâches principales de la GE? Voir Appendice B, "Orientation (guerre électronique) des opérations d'information," pour plus d'orientation.

(3) Quelles sont les tâches principales de la SECOP? Voir Appendice C, "Orientation (sécurité des opérations) des opérations d'information," pour plus d'orientation.

(4) Quelles sont les tâches importantes des OPSPSY? Voir Appendice D, "Orientation (opérations psychologiques) des opérations d'information," pour plus d'orientation.

(5) Quelles sont les tâches importantes de destruction physique reliées aux opérations d'information? Voir Appendice E, "Orientation (destruction matérielle) des opérations d'information," pour plus d'orientation.

(6) Quelles sont les tâches principales des affaires publiques (Voir Appendice F, "Orientation (affaires publiques) des opérations d'information," pour plus d'orientation.

(7) Quelles sont les tâches principales des CA? Voir Appendice G, "Orientation (affaires civiles) des opérations d'information," pour plus d'orientation.

c. Coordination des instructions. Lesquelles, s'il y a lieu, sont les questions de soutien mutuel concernant les éléments des opérations d'information?

4. Administration et logistique

a. Quels sont les besoins administratifs liés aux opérations d'information?

b. Quels sont les besoins logistiques liés aux opérations d'information?

5. Commandement et contrôle

a. Quelles sont les instructions de commandement et contrôle reliées aux opérations d'information?

b. Quelle est la structure de commandement des opérations d'information?

c. Y a-t-il des communications spéciales et des besoins de rapport pour les opérations d'information? Si oui, quels sont-ils?

ORIENTATION (DÉCEPTION MILITAIRE) DES OPÉRATIONS D'INFORMATION

L'orientation dans cet appendice est reliée au développement de la portion de déception militaire d'un ou tous les plans développés à l'usage des FC.

1. Situation

a. Généralités. Quelle est la situation globale générale concernant la déception militaire?

b. Ennemi

(1) Capacités générales. Quelles sont les capacités militaires ennemies reliées directement à la déception planifiée?

(2) Cibles de déception. Quelles sont les cibles de déception?

(3) Les tendances cibles et les prédispositions. Quelles sont les tendances cibles et les prédispositions?

(4) Plan d'action de l'ennemi vraisemblable. Quel est le plan d'action de l'ennemi vraisemblable? (Référer à la portion du renseignement du plan de base.)

c. Ami

(1) Quelle est la situation des forces amies?

(2) Quelles sont les limites importantes?

(3) Quel est le concept des opérations amies?

d. Hypothèses.

(1) Quelles sont les hypothèses concernant les capacités amies, ennemies ou de tierce partie, les limites ou les plans d'action?

(2) Quelles conditions prévalent selon le commandant au moment où le plan devient un ordre?

2. Mission

a. Mission opérationnelle. Voir le plan de base ou l'ordre.

b. Mission de déception.

(1) But de déception. Quel est l'effet désiré ou les résultats attendus du commandant que celui-ci veut atteindre?

(2) Objectif(s) de déception. Quelle est l'action désirée ou l'inaction par l'adversaire en temps et lieu critiques?

(3) Perceptions de l'ennemi désirées. Quelles est la cible de déception à viser pour atteindre l'objectif de déception?

(4) Histoire de déception. Quel scénario amènerait la cible de déception à adopter la perception désirée? Considérer un des plans d'action abandonnés durant la préparation du plan.

3. Exécution

a. Concept de l'opération

(1) Généralités. Quel est le cadre de l'opération? Inclure une brève description des phases de l'opération de déception.

(2) Autres éléments des opérations d'information.

(a) Quels autres éléments des opérations d'information seront utilisés pour soutenir l'opération de déception?

(b) Quels sont les autres plans et opérations d'élément des opérations d'information pertinents à la déception?

(c) Quelle coordination et résolution de conflit sont nécessaire?

(3) Rétroaction et surveillance

(a) Quel type de rétroaction est attendu, s'il y a lieu, et comment sera-t-il obtenu?

(b) Quel impact aura l'absence de rétroaction sur le plan?

(4) Moyens. Par quels moyens la déception sera-t-elle mise en oeuvre?

(5) Tâches. Quelles seront les tâches d'exécution et de rétroaction aux organisations participantes dans l'exécution et la surveillance de la déception?

(6) Risques

(a) La déception est réussie. Quelle est la réponse normale de l'adversaire? Quel sera l'impact sur les forces amies à partir du partage du renseignement de l'adversaire?

(b) La déception échoue. Quel est l'impact si la cible de déception ignore la déception ou échoue d'une certaine façon à prendre les actions visées?

(c) La déception aboutit aux partenaires multinationaux ou adversaires. Quel est l'impact d'un tel compromis sur les forces amies et l'atteinte d'objectifs amis?

b. Coordination des instructions

(1) Quelles sont les tâches ou instructions énumérées dans les paragraphes précédents appartenant à deux ou plusieurs unités?

(2) Quel sont le jour J et l'heure H, selon le cas, et toute autre information nécessaire assurant une action coordonnée entre deux éléments ou plus de commandement?

4. Administration et logistique

a. Administration

(1) Généralités. Quelles sont les procédures générales à utiliser pendant la planification, la coordination et la mise en oeuvre des activités de déception?

(2) Spécificités. Quelles sont, s'il y a lieu les mesures administratives spéciales nécessaires à l'exécution de l'opération de déception?

b. Logistique. Quels sont les besoins de logistique pour l'exécution de l'opération de déception (transport de matériel spécial, fourniture d'équipement d'impression et de matériels, etc.)?

c. Coûts. Quels sont les coûts applicables associés à l'opération de déception?

NOTE: Ne pas inclure ces actions administratives, de logistique et les actions médicales ou stratagèmes faisant réellement partie de l?opération de déception.

5. Commandement, contrôle et communications

a. Liens de commandement

(1) Approbation. Quel est le pouvoir d'approbation pour l'exécution et la terminaison?

(2) Pouvoir. Qui sont les commandants appuyés désignés et de soutien et quels sont les organismes de soutien?

(3) Méprise. Quelles sont les responsabilités de méprise, particulièrement pour les exécutions par les unités non organiques ou les organisations en dehors de la chaîne de commandement?

(4) Coordination

(a) Quelles sont les responsabilités de coordination dans la zone d'opérations et les besoins reliés aux exécutions de déception et de la rétroaction d'exécution?

(b) Quelles sont les responsabilités de coordination en dehors de la zone et des besoins reliés aux exécutions de déception et de la rétroaction de l'exécution?

b. Communications

(1) Quels sont les moyens de communication et les procédures à utiliser par du personnel de contrôle et des participants dans l'opération de déception?

(2) Quels sont les besoins de rapport de communications à utiliser par le personnel et les participants dans l'opération de déception?

6. Sécurité

a. Généralités. Quelles sont les procédures de sécurité générale à utiliser durant la planification, la coordination et la mise en oeuvre des activités de déception?

b. Détails

(1) Quelles sont les restrictions d'accès et les instructions d'assistance à l'appendice de la déception ou du plan?

(2) Qui a le pouvoir de permettre l'accès à l'appendice de la déception ou du plan?

(3) De quelle façon les légendes, les mots codés et les mots conventionnels seront-ils utilisés?

NOTE:Des pièces additionnelles à la partie du plan de déception militaire peuvent être demandées comme sous-mentionné:

Pièces:

1-- Organisation des tâches

2-- Renseignement

3-- Opérations

4-- Administration et logistique

5-- Relations de commandement

6-- Calendrier d?exécution

7-- Distribution

ORIENTATION (GUERRE ÉLECTRONIQUE) DES OPÉRATIONS D'INFORMATION

L'orientation dans cet appendice est liée au développement de la partie de la guerre électronique d'un ou des plans réalisés à l'usage des FC.

1. Situation

a. Forces ennemies

(1) Quelles sont les capacités, les limites et les vulnérabilités des systèmes de communications ennemies, non émettrices et de GE?

(2) Quelle est la capacité de l'ennemi d'interférer avec l'accomplissement de la mission de la GE?

b. Forces amies

(1) Quelles sont les installations de GE amies, les ressources et les commandants subordonnés?

(2) Quelles sont les forces étrangères amies avec lesquelles les commandants subordonnés peuvent fonctionner?

c. Hypothèses. Quelles sont les hypothèses concernant les capacités amies ou ennemies et les plans d'action influençant d'une façon significative la planification des opérations de GE?

2. Mission

a. Concept de l?opération

(1) Quel est le rôle de la GE dans la stratégie des opérations d'information du commandant?

(2) Quelle est la portée des opérations de la GE?

(3) Quelles méthodes et ressources seront employées? Inclure les capacités organiques et non organiques.

(4) Comment la GE appuiera-t-elle les autres éléments des opérations d'information?

b. Tâches. Quelles sont les tâches et les responsabilités de la GE individuelles pour chaque composante ou subdivision de la force? Inclure toutes les instructions uniques à cette composante ou subdivision?

c. Coordination de l'instruction

(1) Quelles instructions, s'il y a lieu, s'appliquent à deux composantes ou subdivisions ou plus?

(2) Quels sont les besoins, s'il y a lieu, de coordination des actions de GE entre les éléments subordonnés?

(3) Quelle est l'orientation de l'emploi de chaque activité, des mesures spéciales ou de la procédure à utiliser mais non couverte nulle part dans ce tab?

(4) Quelle est l'orientation du contrôle des émissions? Placer une orientation détaillée ou longue dans une pièce de ce tab.

(5) Quelle coordination avec le J6 est requise pour dresser la liste de fréquence secrète interarmées (JRFL)?

4. Administration et logistique

a. Administration

(1) Quelle orientation administrative, le cas échéant, est nécessaire?

(2) Quels sont les rapports, le cas échéant, nécessaires? Inclure un (des) exemple(s).

b. Logistique. Quelles sont, s'il y a lieu, les instructions spéciales concernant le soutien logistique des opérations de GE?

5. Commandement et contrôle

a. Rétroaction

(1) Quel est le concept de surveillance de l'efficacité des opérations de GE

(2) Quels sont les besoins de renseignement détaillés en rétroaction?

b. Comptes rendus. Quels sont les besoins en compte rendu?

c. Signaux. Quels sont les besoins spéciaux ou exceptionnels en communications reliés à la GE?

Appendice C à
l'annexe A

ORIENTATION (OPÉRATIONS DE SÉCURITÉ) DES OPÉRATIONS D'INFORMATION

L'orientation dans cet appendice est liée au développement de la partie de la sécurité des opérations d'un ou de tous les plans développés à utiliser par les FC.

1. Situation

a. Forces ennemies

(1) Évaluation du renseignement de l'ennemi actuel

(a) Quelle est l'évaluation de l'ennemi estimée des opérations amies, des capacités et des intentions?

(b) Quelle est la connaissance de l'ennemi connue de l'opération amie abordée dans le plan de base?

(2) Capacités du renseignement de l'ennemi

(a) Quelle sont les capacités de collecte du renseignement de l'ennemi selon les grandes catégories (renseignement sur les transmissions, HUMINT, renseignements obtenus par des techniques de représentation, etc.)?

(b) Quelles sources de potentiel (incluant les autres nations) fournissent du soutien à l'ennemi?

(c) De quelle façon le système du renseignement de l'ennemi fonctionne-t-il? Inclure le temps nécessaire au renseignement pour atteindre les décideurs clés.

(d) Quelles sont les organisations analytiques importantes et les

(e) Quelles organisations du renseignement non officielles, s'il y a lieu, appuient le commandement national?

(f) Quelles sont les forces et les faiblesses des capacités du renseignement ennemi?

b. Forces amies

(1) Opérations amies. Quelles sont les actions importantes à mener par les forces amies dans l'exécution du plan de base?

(2) Information importante. Quelle est l'information importante identifiée? Inclure l'information importante de quartiers généraux supérieurs. Pour les opérations par étapes, identifier l'information importante par phase.

c. Hypothèses. Quelles sont les hypothèses sur lesquelles ce plan de SECOP est fondé?

2. Mission. Quelle est la mission de la SECOP (qui, quoi, quand, où, pourquoi)?

3. Exécution

a. Concept de l'opération

(1) Quel est le rôle de la SECOP dans la stratégie des opérations ?

(2) Quel est le concept général de la mise en oeuvre des mesures planifiées (manoeuvre, logistique, communications, etc.), selon le cas.?

(3) Quel sera le soutien de la SECOP à d?autres éléments des opérations d'information?

b. Tâches. Quelles sont les mesures spécifiques de la SECOP à prendre? Énumérer celles-ci par phases et inclure des responsabilités spécifiques pour les éléments subordonnés.

c. Coordination des instructions

(1) Quels sont les besoins de coordination des mesures de la SECOP entre les éléments subordonnés?

(2) Quelle est la coordination requise avec les affaires publiques?

(3) Quelle est l'orientation sur la terminaison des activités reliées à la SECOP?

(4) Quelle est l'orientation sur la déclassification et la diffusion publique d'information reliée à la SECOP?

4. Administration et logistique

a. Quels sont, s'il y a lieu, les besoins de soutien administratif reliés à la SECOP ou à la logistique?

b. Quelles sont, s'il y a lieu, les mesures administratives ou de logistique reliées à la sécurité des opérations?

5. Commandement et contrôle

a. Rétroaction

(1) Quel est le concept de surveillance de l?efficacité des mesures de la SECOP pendant l'exécution?

(2) Quels sont les besoins du renseignement spécifiques concernant la rétroaction?

b. Enquête de la SECOP. Quels sont les plans de conduite d'enquêtes de la SECOP de soutien à l'opération?

c. Comptes rendus. Quels sont les besoins en compte rendu?

d. Transmissions. Quels sont les besoins, s'il y a lieu, spéciaux ou exceptionnels de communications reliés à la SECOP?

Appendice D à
l'annexe A

ORIENTATION (OPÉRATIONS PSYCHOLOGIQUES) DES OPÉRATIONS D'INFORMATION

L'orientation dans cet appendice est reliée au développement de la partie des opérations psychologiques d'un ou de chacun des plans développés à l'usage des FC.

1. Situation

a. Aperçu

(1) Quelle est la situation psychologique générale dans la zone d'opérations?

(2) Quels sont, s'il y a lieu, les programmes continus des OPSPSY?

(3) Quels sont les facteurs importants influençant les activités des OPSPSY?

(4) Quels sont les buts des OPSPSY de compétition dans la zone d'opérations?

(5) Quelle est la tâche des OPSPSY à accomplir?

b. Perspective canadienne (ou canadienne et alliée/de coalition)

(1) De quelle façon la tâche des OPSPSY assignée sera-t-elle accomplie?

(2) Quelles ressources seront utilisées?

(3) Quelles seront les étapes générales des actions actuelles avec les actions futures?

c. Perspective neutre (selon le cas)

(1) Quelles sont les intentions neutres estimées dans des circonstances variées?

(2) Quelles activités et ressources sont consacrées à ces intentions neutres?

(3) Quelles actions neutres et quel comportement favoriseraient l'accomplissement de la mission?

(4) Quels plans d'action actuels apparents pourraient avoir une incidence sur l'accomplissement de la mission?

(5) Quelles ressources sont disponibles pour appliquer des plans d'action de rechange?

(6) Quels facteurs objectifs et subjectifs pourraient influer sur l'efficacité des décisions et des ressources?

(7) Quelles sont les actions de l'état-major et qui sont les individus ayant particulièrement une influence?

(8) Quelles sont les caractéristiques des décideurs et des conseillers clés, des planificateurs d'état-major importants, des factions d'état-major (incluant des individus ayant particulièrement une influence), et des analystes de système du renseignement?

(9) Quels sont les groupes d?éléments essentiels d?information amie (EEFI) de planificateurs reliés et de décideurs?

(10) Quelle est la connaissance de l'arrière-plan estimée et les appréciations souhaitées et nuisibles pour chaque groupe?

d. Perspectives ennemies

(1) Décideur et état-major

(a) Qui sont les décideurs pouvant diriger le développement ou l'allocation de ressources du plan d'action pertinent à la tâche assignée?

(b) Quelles actions de rechange faisables favoriseraient ou nuiraient à l'efficacité opérationnelle amie?

(c) Quels plans d'action pourraient affecter l'accomplissement de la tâche amie?

(d) Quelles ressources sont disponibles pour exécuter chaque plan d'action?

(e) Quelles sont les caractéristiques des décideurs ennemis, leurs conseillers clés et leur état-major (particulièrement les analystes du renseignement)?

(2) Systèmes du renseignement

(a) Quels systèmes du renseignement soutiennent les décideurs et leur état-major?

(b) Quelles sont les capacités des systèmes du renseignement pertinentes à la situation?

(c) Quels sont les facteurs objectifs et subjectifs et les caractéristiques des planificateurs de collecte et des décideurs affectant leur développement et la sélection pour l'utilisation des ressources de rassemblement d'information?

(d) Quels sont les groupes de planification d'éléments essentiels d'information amie (EEFI) de planificateurs reliés et de décideurs?

(e) Quelle est la connaissance de l'arrière-plan estimée et souhaitée et les appréciations nuisibles pour chaque groupe?

(3) Audiences-cibles

(a) Quels groupes peuvent influencer les plans, les décisions et l'efficacité opérationnelle dans l'accomplissement de la tâche?

(b) Quelle est la susceptibilité de ces groupes aux OPSPSY?

(c) Quel comportement de groupe est propice ou nuisible à l'accomplissement de la tâche?

(d) Quels sont les buts apparents, les motivations et les caractéristiques de chaque groupe?

(e) Qui sont les leaders pouvant amener ces groupes à se conduire de diverses façons?

(f) Quels sont les groupes d'audience-cible reliés aux éléments essentiels d'information amie?

(g) Quelles sont la compétence d'arrière-plan évaluée et désirée et les appréciations nuisibles pour chaque groupe?

(4) Systèmes de commandement

(a) Quels systèmes de communications et centres de commandement seront utilisés pour planifier les plans d'action et de contrôle, coordonner et superviser l'exécution du plan d'action planifié?

(b) Quel est le but et quelles sont les caractéristiques de chaque réseau de communications de commandement et de contrôle?

(c) Quelles sont les cibles des OPSPSY de brouillage ou d'attaque?

(d) Quand les OPSPSY devraient-elles être exécutées pour démoraliser et désorganiser le commandement d'opposition?

(e) Quand les OPSPSY devraient-elles être exécutées pour diminuer l'efficacité opérationnelle des forces d'opposition ?

(f) Quand les opérations des OPSPSY devraient-elles être exécutées en vue d'améliorer l'efficacité des déceptions planifiées et des OPSPSY?

(g) Quand les OPSPSY devraient-elles être exécutées pour appuyer la sécurité des opérations à leur avantage maximum?

2. **Mission.** Comment la mission des OPSPSY appuiera-t-elle le commandant de manoeuvres?

3. **Exécution**

a. Concept de l'opération

(1) Aperçu

(a) Quelle est l'intention du commandant?

(b) Quel est le concept global de l'utilisation des OPSPSY appuyant l'accomplissement de la tâche?

(c) Qui planifiera et conduira les OPSPSY en temps de paix et en appui à des options de dissuasion avant le conflit? Qui sont les commandants de soutien?

(d) Qui planifiera et conduira les OPSPSY stratégiques et opérationnelles en appui d'hostilités soutenues? Qui sont les commandants

(e) soutien des plans d'action opérationnels? Qui sont les commandants de soutien?

(2) Orientation générale donnée aux Unités et Forces

(a) Quels sont les thèmes des OPSPSY valides à encourager pour

(b) Quels sont les thèmes des OPSPSY valables ou non à désapprouver? Inclure les indications des sensibilités et de dommage à une audience-cible spécifique pouvant survenir une fois les thèmes acceptés par des audiences-cibles.

(c) Actions appropriées des OPSPSY à utiliser

1. Quelle est l'orientation pour la conduite des opérations militaires, des actions et du comportement du personnel pour promouvoir les thèmes des OPSPSY valables?

2. Quelle est l'orientation pour éviter des opérations militaires et des actions et du commandement du personnel pouvant résulter dans des attitudes et un comportement de l'audience-cible nuisible?

3. Quelles sont les caractéristiques culturelles et psychologiques des audiences-cibles aidant les planificateurs opérationnels et le personnel en choisissant les plans d'action et interagissant avec les membres de l'audience-cible?

(d) OPSPSY adversaires

1. Quelles OPSPSY adversaires seront dirigées vers le personnel canadien et les groupes étrangers dans la zone d'opérations.

2. Quelle est l'orientation pour contrer les opérations adversaires?

(3) Aperçu de chaque opération des OPSPSY planifiée

(a) Quelle est l'audience-cible et l'ensemble des objectifs des OPSPSY, des thèmes globaux, des sous-groupes à cibler (incluant leurs caractéristiques) et des thèmes spécifiques à promouvoir pour chaque sous-groupe?

(b) Quelles sont les dispositions pour l'épreuve, la production, le stockage et la diffusion de matériels des OPSPSY et pour mesurer l'efficacité des OPSPSY?

(c) Quels sont les arrangements de commandement et d'état-major? Qui sont les commandants de soutien?

(d) Quelles ressources sont requises pour planifier et mener des actions des OPSPSY? Inclure les capacités civiles; avoirs des habitants; exploitation des prisonniers de guerre ennemis (EPW), internés et détenus des OPSPSY et des ressources des OPSPSY militaires.

(e) Quels sont les besoins en logistique? Inclure la préparation, la distribution et le stockage des matériels des OPSPSY; le transport du matériel et du personnel des OPSPSY aux zones opérationnelles et leur base et soutien pendant la conduite des OPSPSY; les provisions pour la fourniture et la maintenance du matériel des OPSPSY canadien et des habitants et les questions de fiscalité et de personnel.

(f) Quels sont les besoins de mise en oeuvre des horaires et des feuilles de contrôle de l'opération des OPSPSY?

(g) Quel est le mot chiffré des OPSPSY concernant la sensibilité de la SECOP?

(4) Quelle est l'orientation de la planification de la SECOP? Inclure la planification, la préparation et la conduite des OPSPSY et des actions des OPSPSY pour garder le secret essentiel à l'intention du commandant, gagner et garder le secret essentiel des plans d?action des OPSPSY concernant la sensibilité de la SECOP.

b. Surveillance de la situation

(1) Comment le renseignement, la CI multidiscipline, la surveillance de la sécurité et la rétroaction opérationnelle seront-ils fournis?

(2) Quel est le besoin d'effectuer des prévisions de situation; des prévisions périodiques des appréciations des objectifs répondant aux actions des EEFI, des actions, des attitudes et de comportement; et du rapport actuel du renseignement et des informations de CI multidisciplinaire, les résultats de surveillance de sécurité et de mise en oeuvre des actions.

(3) Quelles sont les ressources nécessaires? Quelle est leur disponibilité?

c. Contrôle

(1) Comment le contrôle sera-t-il touché et la mise en oeuvre coordonnée centralement?

(2) Quelles sont les instructions de coordination?

(3) Comment la planification de mise en oeuvre et la supervision de l'action planifiée sera-t-elle accomplie?

(4) Quel est le besoin en OPSPSY spécifiques?

(5) Quelle coordination est nécessaire avec des commandements adjacents et des organismes civils incluant les missions diplomatiques canadiennes?

(6) Quelle coordination est requise avec la déception militaire et les planificateurs de la SECOP, les planificateurs de la GE et les planificateurs dans les domaines de l'action civique, l'aide humanitaire, les affaires civiles, les prisonniers de guerre ennemis, la CI, les détenus, le C3, le droit, le personnel canadien ou allié capturé et les opérations?

d. Tâches

(1) Quelles responsabilités doivent être assignées pour mettre le concept en oeuvre?

(2) ce que la désignation d'un agent exécutif pour coordonner la mise en oeuvre parmi de multiples organisations est requise?

(3) Comment la rétroaction pour assurer l'efficacité des tâches est-elle produite?

4. Administration et logistique

a. Logistique

(1) Quelle est l'orientation sur le stockage du matériel de propagande et d'information et les dispositions des organisations de diffusion?

(2) Quelles sont les dispositions pour la fourniture et la maintenance des approvisionnements et de l'équipement uniques des OPSPSY?

(3) Quelles sont les dispositions de contrôle et de maintenance d'équipement et de matériels des habitants?

(4) Quelles sont les questions fiscales concernant les fonds spéciaux?

(5) Quelles sont les questions en personnel concernant le personnel venant des habitants?

b. Administration

(1) Quels sont les besoins en rapports spéciaux?

(2) Quels sont les besoins en planification et opérations en soutien des programmes d'éducation concernant les prisonniers de guerre ennemis et les détenus civils?

(3) Quelle sera la participation à l'interrogatoire des prisonniers de guerre ennemis et des détenus pour obtenir de l'information importante ou particulière aux OPSPSY?

5. **Commandement et contrôle.** Référer à des sections appropriées le plan de base et fournir des extraits d'information inclus dans le plan de base pour inclure ce qui suit:

a. Quelles sont les instructions de reconnaissance et d'identification?

b. Quelle est la politique électronique?

c. Quels sont les localités des quartiers généraux et les mouvements?

d. Quels sont les mots chiffrés?

e. Quelle est l'attribution de fréquence?

ORIENTATION (DESTRUCTION PHYSIQUE) DES OPÉRATIONS D?INFORMATION

L'orientation dans cet appendice est liée au développement de la destruction matérielle partie d'un ou de tous les plans à l'usage des FC.

1. Situation

a. Situation de l'ennemi. Quelle est la situation générale dans le pays cible?

b. Situation amie

(1) Quelle est la situation de ces forces amies (plus élevées, adjacentes, de soutien de l'infrastructure clé?

(2) Quelles sont, le cas échéant, les limites importantes et toute autre opération d'information planifiée?

c. Hypothèses. Quelles sont, le cas échéant, les hypothèses sur lesquelles ce plan est basé?

2. Mission. Quelle est la mission de destruction matérielle du C2 et de l'infrastructure?

3. Exécution

a. Aperçu

(1) Comment le commandant voit-il l?exécution de ce plan de soutien au plan des opérations d'information du début à la fin?

(2) Quelles sont les phases de l'opération?

(3) Quelle est l'intention du CFO et quels sont les résultats attendus du commandant?

b. Tâches des commandements subordonnés. Quelles sont les tâches principales de chaque commandement subordonnés?

c. Coordination des instructions. Quelles sont les règles d'engagement touchant le C2 et quel est le plan de destruction de l'infrastructure?

4. Administration et logistique

a. Quels sont les arrangements administratifs applicables, le cas échéant, non couverts dans le plan de base?

b. Quels sont les arrangements logistiques applicables, le cas échéant, non couverts dans le plan de base?

5. Commandement et contrôle. Quel est le commandement et quels sont les arrangements de contrôle applicables, selon le cas, non couverts dans le plan de base?

Appendice F à
l'annexe A

ORIENTATION (AFFAIRES PUBLIQUES) AUX OPÉRATIONS D'INFORMATION

L'orientation dans cet appendice est reliée au développement de la partie des affaires publiques d'un ou des plans développés à l'usage des FC.

1. Situation

a. Généralités. Quelles sont les responsabilités générales et l'orientation pour des actions des AP militaires (information publique, commandement et information interne et service des relations avec le public)?

b. Ennemi. Quelles sont les actions attendues des forces ennemies et des forces hostiles aux intérêts canadiens?

c. Ami. Quels sont les organismes amis n'étant pas sous le contrôle du CFO qui contribueront à l'effort des AP? Inclure le directeur général des affaires publiques, les ambassadeurs canadiens et les programmes des AP alliés/de coalition.

d. Politique. Quelle est la politique applicable appartenant à ce plan?

e. Hypothèses

(1) Quelles sont les préférences du pays hôte à considérer dans les programmes de développement et d'exécution des AP?

(2) Le CFO devrait-il être préparé pour animer le groupement des médias nationaux du MDN (National Media Pool) durant les stages initiaux des opérations?

2. Mission. Quels sont la tâche et le but des AP dans l'opération?

3. Exécution

a. Concept de l'opération

(1) Quel soutien des AP sera nécessaire dans les cinq phases suivantes:

(a) Avertissement

(b) Préparation

(c) Déploiement

(d) Emploi

(e) Redéploiement

b. Tâches

(1) Quelles sont les tâches des AP à compléter durant les phases énumérées ci-dessus?

(2) Quelles sont, selon le cas, les instructions délivrées d'informations additionnelles au CFO et des autres commandements de soutien incluant le pouvoir de libération et l'orientation concernant les

pertes et la mortalité, des affaires de la poste et les prisonniers de guerre ou de disparus au combat et des questions de prisonniers de guerre ennemis?

(3) Quels sont les besoins d'information visuelle des AP et de caméra de combat (combat camera)?

(4) Quels sont les besoins de soutien de personnel détaillés et d'équipement aux commandements de la composante? Inclure l'accès pour sécuriser la voie téléphonique reliant le Bureau d'information interarmées (JIB) et le commandant sur le terrain, le commandant opérationnel appuyé et le ministère des Affaires étrangères et du Commerce international, l'accès à des installations de message de copie papier entre les mêmes points; et le transport entre théâtre et intra-théâtre pour des médias escortés.

(5) Quel est le CFO et les autres besoins de soutien de commandements d'appuis?

c. Coordination des instructions

(1) Relations de commandement. Quelles sont les relations de commandement des AP?

(2) Coordination de la communication d'information. Quelles sont les procédures détaillées pour tous les commandements de soutien pour la manutention ou le suivi des enquêtes de commandement d'appui, de réponses et de communiqués de presse proposés pour les formalités?

(3) Autres coordinations des instructions

(a) Quelle est l'orientation concernant les entrevues et les conférences de presse avec le personnel canadien retourné et les prisonniers de guerre ennemis ou le personnel détenu?

(b) Quelle est la coordination requise avec les autres éléments d'état-major impliqués dans la communication d'information hors du commandement?

(c) Quelles sont les procédures pour garder des dossiers historiques des AP?

4. **Enregistrement.** Quelle est l'orientation du soutien militaire aux médias?

5. **Examen de sécurité.** Quelles sont, le cas échéant, les procédures d'examen de sécurité?

6. **Arrangements pour les médias.** Quels sont les détails concernant le soutien des médias planifiés? Inclure les détails concernant les repas, le cantonnement, le traitement médical d'urgence, l'accès au transport et les installations de communications aux frais du gouvernement, l'accès à des renseignements opérationnels à diffusion libre et autre soutien.

a. Installations. Quelles installations de soutien seront fournies aux membres du groupement des médias du MDN et des autres médias?

b. Inoculations. Quelles inoculations seront données aux correspondants accompagnant les troupes en campagne ou embarquées sur les navires des forces opérationnelles?

c. Dépenses

(1) Quels services seront fournis aux médias sur une base remboursable?

(2) Quels sont les besoins de remboursement?

d. Rang simulé. Quel sera le rang simulé des représentants des médias d'information pour les repas, le cantonnement et le transport?

e. Communications. Quelles seront les procédures pour se charger du trafic des médias

f. Transport. Quelles sont les procédures pour le transport du personnel des médias dans la zone d'opérations, hors de celle-ci ou à l'intérieur de celle-ci?

g. Ordres de mission. Quelles sont les procédures d'autorisation et d'émission des ordres de mission pour les correspondants.

h. Groupements. Quelles sont les procédures détaillées pour la participation des médias aux groupements des médias?

7. Sécurité des opérations et du personnel

a. Opérations. Quelles sont les lignes directrices à suivre quand les correspondants sont présents dans les zones d'opérations? Inclure un équilibre entre la sécurité et la fourniture d'information au public. Des considérations diplomatiques et politiques de toutes les déclarations et tous les communiqués de presse aux représentants des médias devraient être évalués soigneusement à tous les échelons du commandement.

b. Personnel

(1) Sécurité du personnel. Quelles mesures de sécurité du personnel s'appliquent aux correspondants dans les zones d'opérations?

(2) Sécurité matérielle. Quelles mesures de sécurité matérielle s'appliquent aux correspondants dans les zones d'opération?

8. Sécurité des opérations. Quelles procédures de sécurité détaillées, le cas échéant, doivent être suivies par le personnel des AP?

9. Information audiovisuelle et visuelle. Quelles sont les lignes directrices s'appliquant à fournir aux AP la couverture d'informations audiovisuelle et visuelle de l'opération.

10. Information interne. Quels sont les besoins d'information interne pour les commandements subordonnés?

11. Service des relations. Quelle est, s'il y a lieu, la coordination requise avec le DGAP ou le représentant désigné?

Appendice G à
l'annexe A

**ORIENTATION (COOPÉRATION CIVILO-MILITAIRE/AFFAIRES CIVILES)
DES OPÉRATIONS D'INFORMATION**

L'orientation dans cette annexe est liée au développement des affaires civiles ou de la portion de la COCIM d'un ou de chaque plan développé à l'usage des FC.

1. Situation

a. Généralités

(1) Quelle est la base légale des activités de la COCIM/des CA dans cette opération?

(2) Quelle est la portée normale des activités de la COCIM/des CA dans cette opération? Inclure l'identification des ententes internationales et civilo-militaires correspondantes.

(3) Quel est le but de cet appendice? Normalement, le but est de fournir des instructions pour orienter toutes les relations entre la force militaire, les autorités civiles et les habitants de la zone d'opérations.

b. Ennemi

(1) Quel est l'impact des capacités de l'ennemi et des plans d'action probables sur la situation de la COCIM/des CA? Mettre un accent particulier sur l'identification des besoins des fonctions et activités de la COCIM/des CA.

(2) Quelle est la situation attendue de la COCIM/des CA? Inclure les institutions gouvernementales, les coutumes et les attitudes de la population et la disponibilité des ressources des habitants.

c. Ami

(1) Quelles sont les fonctions de la COCIM/des CA à accomplir par les autorités civiles du Canada et les gouvernements amis dans la zone opérationnelle?

(2) Quels avoirs des habitants sont disponibles pour soutenir et assister dans les activités de la COCIM/des CA?

d. Hypothèses. Quelles sont les hypothèses de base sur lesquelles la planification de la COCIM/des CA est basée? Inclure l'attention aux plans d'action ennemis, la disponibilité des ressources des habitants, la conclusion des ententes nécessaires avec les gouvernements étrangers sur les forces.

2. Mission. Quelle est la mission à accomplir par les activités de COCIM/CA en appui aux opérations envisagées dans le plan de base?

3. Exécution

a. Concept de l'opération

(1) Les opérations n'impliquant pas l'établissement d'un gouvernement militaire

(a) Quelles sont les variations opérationnelles dues à des plans d'action en alternance dans le plan de base?

(b) Quel sera le soutien de COCIM/CA aux efforts diplomatiques, économiques ou autres en route?

(c) Quelles activités de COCIM/CA soutiennent le découpage du temps de l'opération?

(d) Quel sera le déploiement et l'emploi de forces pour soutenir les opérations de COCIM/CA?

(e) Quelle sera la portée et la durée des opérations de COCIM/CA? Inclure les opérations après les conflits.

(f) Quels sont les résultats attendus du commandant dans les activités de COCIM/CA? Celles-ci devraient être claires, concises et subdivisées si nécessaire pour décrire la réussite de l'achèvement de chaque phase et plan d'action.

(g) Quelle est l'allocation planifiée et l'utilisation d'unités militaires et des

(h) Quelles sont les principales fonctions de COCIM/CA à accomplir à l'intérieur de la zone de commandement? Inclure toutes les variations importantes par pays, État ou région.

(i) Quelle sera la fonction et l'opération des centres d'opérations civilo-militaires une fois mis en place?

(2) Opérations impliquant l'établissement d'un gouvernement militaire

(a) Quelle est l'orientation constructive ou restrictive de chaque zone fonctionnelle de COCIM/CA?

(b) Quelles autorités de COCIM/CA sont nécessaires?

(c) Quelle coordination de COCIM/CA additionnelle est nécessaire?

b. Tâches. Quelles sont les tâches spécifiques assignées à chaque élément du CFO et des commandements de soutien? Chaque tâche devrait être un énoncé concis d'une mission à accomplir soit dans la planification future de l'opération ou sur l'exécution de l'OPORD et doit inclure tous les éléments clés requis pour des fonctions de COCIM/CA.

c. Coordination des instructions

(1) Quelles sont les instructions applicables à tout le commandement; deux éléments ou plus du commandement et le commandement ou ses éléments et organismes externes au commandement?

(2) Quelles sont, le cas échéant, les limites de COCIM/CA déterminées?

(3) Quels sont, le cas échéant, les arrangements de liaison avec des forces alliées/de coalition et entre des commandements subordonnés?

(4) Quelles sont les politiques de revendication? Voir aussi l'annexe juridique.

(5) Quelle est l'application ou la négociation des conventions sur le statut des forces? Voir aussi l'annexe juridique.

(6) Quelle est la liaison nécessaire et la coordination avec le gouvernement canadien et les organismes non gouvernementaux? Voir aussi l'annexe juridique.

(7) Quelles proclamations doivent être émises à la populace civile en coordination avec l'annexe juridique?

(8) Quelle est la liaison nécessaire et la coordination avec le pays hôte ou d'autres pays amis et des organismes gouvernementaux et non gouvernementaux?

(9) Quelles sont les mesures d'urgence, le cas échéant, pour la défense des populations civiles?

(10) Quel sera l'appui des OPSPSY à des opérations de COCIM/CA?

4. Administration et logistique

a. Besoins en ressources militaires. Quels sont, le cas échéant, les besoins applicables au maintien de l'équipement militaire et des fournitures pour le soutien de la fonction de COCIM/CA?

b. Personnel civil. Quelle est la main-d'oeuvre civile locale estimée nécessaire et disponible pour soutenir l'opération?

c. Installations civiles et fournitures. Quelles sont les installations civiles locales estimées et les fournitures requises et disponibles pour soutenir l'opération?

d. Rapports. Quels sont, le cas échéant, les besoins de rapport administratifs?

5. Commandement et contrôle

a. Quelles sont, le cas échéant, les différences entre les canaux de commandement pour la conduite des activités de COCIM/CA et les relations de commandement établies.

b. Qui a la responsabilité de commandement pour le contrôle opérationnel, le contrôle administratif et la logistique des forces de COCIM/CA et des activités? Soulignez la différence entre les activités et les forces et inclure tout changement ou transition entre les organisations du C2 et le temps du virage attendu.

c. Quels sont les ententes d'arrangement de commandement et les protocoles d'entente utilisés. Lesquels de ceux-ci exigent une élaboration?

ANNEXE B

ORIENTATION DES OPÉRATIONS D'INFORMATION DÉFENSIVES

L'orientation dans cette annexe est reliée au développement des portions des Opérations d'information défensives d'un ou de tous les plans développés à utiliser par les FC.

1. Situation

a. Généralités

(1) Quels sont les objectifs des opérations d'information défensives?

(2) Comment ces objectifs sont-ils liés à la réussite de la mission?

b. Ennemi. Quelles sont les capacités de l'ennemi affectant l'information amie et les systèmes d'information et les opérations d'information non encore discutées?

c. Ami. Quelles sont les organisations non subordonnées à ce commandement et les tâches spécifiques assignées à chaque objectif des opérations d'information défensives de soutien?

2. Mission Comment les opérations d'information défensives soutiennent-elles la réussite de la mission assignée dans le plan de base?

3. Exécution

a. Concept de l'opération

(1) Généralités. Quel est le concept global pour assurer l'accès à l'information amie et la disponibilité malgré l'utilisation des opérations d'information ennemies? Faites attention tout particulièrement à la sécurité matérielle et la surviabilité des capacités du système d'information amie et des installations.

(2) Incorporation progressive

1 Quelles sont les activités des opérations d'information défensives survenant dans chaque phase opérationnelle? Décrire les suites dans chaque phase harmonisée à l'initiation de la phase et des événements opérationnels de soutien.

2 Quelle est l'orientation échelonnée pour accomplir les actions mettant en oeuvre le plan des opérations d'information défensives?

b. Tâches

(1) Quel élément de commandement est responsable de la coordination des actions des opérations d'information défensives?

(2) Quelles sont les tâches assignées et les responsabilités de chaque commandement subordonné pour mettre en oeuvre et exécuter les actions des opérations d'information défensives, incluant l'identification des vulnérabilités?

c. Instructions de coordination

(1) Intégration

(a) Quelles sont les instructions détaillées pour réaliser l'intégration de la sécurité matérielle et des mesures de surviabilité, des mesures de protection électronique, de l'INFOSEC, de la contre-ingérence (CI), des affaires publiques, des contre-opérations psychologiques, de la contre-déception et des moyens de performance des opérations d'information défensives de la SECOP?

(b) Quelle est l'orientation des capacités d'atténuation et/ou de négation des opérations d'information adversaires?

(2) Coordination. Quels sont les besoins détaillés de coordination parmi les éléments impliqués dans les opérations d'information défensives? Soulignez la coordination étroite avec les opérations d'information, la guerre de commandement et contrôle, la déception, la SECOP, la GE, les OPSPSY, le renseignement et les autres planificateurs clés reposant sur les ressources d'information amies.

(3) Sécurité. Quels sont, s'il y a lieu, les besoins de sécurité spéciale ou des actions de planification et d'actions des opérations d'information défensives envisagées par cette Annexe?

(4) Rapports. Quels sont les besoins de rapport opérationnels nécessaires à la surveillance efficace des activités des opérations d'information défensives?

4. Administration et logistique

a. Personnel. Quels sont les besoins , s'il y a lieu, de qualifications de personnel spécialisé et/ou de qualification?

b. Fourniture. Quels sont, s'il y a lieu, les besoins d'approvisionnement de fournitures spécialisés?

c. Rapports. Quels sont, s'il y a lieu, les rapports administratifs requis?

5. Commandement et contrôle. Quels systèmes spéciaux ou procédures, s'il y a lieu, sont requis pour le commandement et contrôle des actions des opérations d'information défensives?

LISTE DES ABRÉVIATIONS

AO	zone d'opérations
BDA	estimation des dégâts de combat
C2	commandement et contrôle
GCC	guerre de commandement et de contrôle GCC
C3	commandement, contrôle et communications
C4	commandement, contrôle, communications et ordinateurs
C4I	commandement, contrôle, communications, ordinateurs et information
CA	affaires civiles
CERT	équipe d'intervention en cas d'urgence concernant les ordinateurs
CFEWC	Centre de guerre électronique des Forces canadiennes
CFIOG	Groupe des opérations du renseignement des Forces canadiennes
CI	contre-ingérence
COCIM	coopération civilo-militaire
CISO	officier de soutien à la contre-ingérence
COA	plan d'action
COMPUSEC	sécurité informatique
SECOM	sécurité des communications
CONPLAN	plan d'opération de format conceptuel
CST	Centre de la sécurité des télécommunications
DII	Infrastructure d'information de la Défense
DECSS	Services en électronique, communications et spectre de la Défense
EEFI	éléments essentiels d'information amie
CME	contre-mesures électroniques
MSGE	mesures de soutien de guerre électronique
MPE	mesures de protection électronique
PG	prisonnier de guerre
GE	guerre électronique
MCGE	module de coordination de guerre électronique
GII	infrastructure d'information globale
HUMINT	renseignement humain
I & W	indications et avertissement
IADS	système de défense aérien intégré
I-BDA	évaluation des dommages du combat-information
IIE	environnement d'information intégré
INFOSEC	sécurité de l'information
IO	opérations d'information
IOCC	module de coordination des opérations d'information
IP	protection de l'information
IPB	préparation du renseignement de l'espace de bataille
IS	système d'information
ISIRT	équipe d'intervention en cas d'incident de système d'information
JCCC	centre de contrôle des communications interarmées
JCMA	activité de surveillance de la SECOM interarmées
JIB	Bureau d'information interarmées
JOC	centre des opérations interarmées
JPT	équipe de planification interarmées
JRFL	liste de fréquence restreinte interarmées

JSAT	Équipe de gestion de l'état-major interarmées
M&S	modélisation et simulation
NBC	nucléaire, biologique et chimique
SCICC	système national d'information de commandement et de contrôle
NII	Infrastructure d'information nationale
OGD	autres ministères
OOTW	opérations hors guerre
OPFOR	force d'opposition
OPLAN	plan des opérations
O op	ordre d'opération
SECOP	sécurité des opérations
PA	affaires publiques
OPSPSY	opérations psychologiques
SATCOM	communications par satellite
SIO	opérations d'information spéciales
STO	opérations techniques spéciales
TCC	module de coordination du choix des objectifs et des moyens de traitement
TFC	commandant de la force opérationnelle