RÉSEAUX DE L'AVENIR

L'élaboration d'un réseau de l'avenir constitue une évolution complexe vers les technologies émergentes des systèmes d'information qui habiliteront de plus en plus les gens, les organisations et les processus. On doit toutefois garder à l'esprit que le commandement est et restera une entreprise humaine et que, par conséquent, tout réseau de l'avenir doit d'abord et avant tout faciliter l'exécution des tâches par les humains et permettre de meilleures interactions. L'Armée canadienne s'efforcera sans cesse de devenir de plus en plus réseaucentrique, pour être en mesure d'échanger des informations latéralement et au sein de la chaîne de commandement entre les capteurs, les armes, les véhicules et les nœuds de commandement et de contrôle, afin que la bonne personne puisse avoir accès à la bonne information au bon moment. Mises en place correctement, les opérations réseaucentriques de l'avenir feront appel à un ensemble de soldats et d'éléments d'appui sur le terrain, soutenus par des systèmes de capteurs, d'appui-feu et de commandement et de contrôle interarmées reliés par des systèmes de transmission en phonie et de transmission de données pour améliorer le niveau de connaissance de la situation, la mobilité sur le champ de bataille et l'appui-feu, qui, combinés, empêcheront l'ennemi de comprendre ce qui se passe dans l'espace de combat et mineront sa capacité de réagir.

Le réseau de l'avenir, tout en cherchant à habiliter les commandants, doit rendre possible un cycle de prise de décision plus rapide chez les soldats, inciter à la prise de décisions au niveau approprié le plus bas possible, et permettre aux soldats et aux commandants de reconnaître les occasions et d'en tirer profit dès qu'elles se présentent. Parmi les objectifs importants du réseau de l'avenir, on compte : meilleur rayon d'action, ou accès à un plus grand auditoire; portée améliorée, notamment lors des mouvements; meilleure gestion de l'information, surtout pour l'analyse de la grande quantité de données et d'information recueillies; meilleure collaboration entre tous les utilisateurs. Le succès de l'Armée de terre de demain dans le cadre d'opérations adaptables et dispersées sera fonction de la présence d'un solide réseau de l'avenir.

CENTRE DE GUERRE TERRESTRE DE L'ARMÉE CANADIENNE

Le Centre de guerre terrestre de l'Armée canadienne constitue l'assise intellectuelle de l'Armée de terre en matière de développement des concepts et des capacités plus vastes de demain et des années à venir. Sa mission consiste à fournir des orientations et des spécifications basées sur les concepts et dictées par les capacités, dans la perspective de la conception de la structure de la force; à élaborer le plan de développement et d'expérimentation des concepts de l'Armée de terre; à servir de pivot pour les liens avec les autres centres de guerre, les ministères, les pays partenaires, les organisations extérieures et le milieu universitaire, et à produire des recherches et des publications de haute qualité à l'appui des objectifs de développement des forces de l'Armée canadienne.

CANADIAN ARMY LAND WARFARE CENTRE
CENTRE DE GUERRE TERRESTRE DE L'ARMÉE CANADIENNE

Réseaux de l'avenir : un concept pour l'Armée de terre de demain

CGTAC

Défense nationale National Defence

Canada

RÉSEAUX DE L'AVENIR :
UN CONCEPT POUR L'ARMÉE DE TERRE DE DEMAIN

RÉSEAUX DE L'AVENIR :
UN CONCEPT POUR L'ARMÉE DE TERRE DE DEMAIN

Centre de guerre terrestre de l'Armée canadienne
Kingston (Ontario), 2013

Données au sujet de la publication

1. Réseaux de l'avenir : un concept pour l'Armée de terre de demain

Anglaise
IDDN–NDID B-GL-007-000/JP-005

Française
IDDN–NDID B-GL-007-000/JP-006

Publication – anglaise
Numéro de catalogue du governement du Canada – D2-327/2013E
ISBN– 978-1-100-23023-8

Publication – française
Numéro de catalogue du governement du Canada – D2-327/2013F
ISBN– 978-0-660-21574-7

Version – anglaise en-ligne
Numéro de catalogue du governement du Canada – D2-327/2013E-PDF
ISBN – 978-1-100-23024-5

Version – française en-ligne
Numéro de catalogue du governement du Canada – D2-327/2013F-PDF
ISBN – 978-0-660-21575-4

Conception et design : Bureau d'édition de l'Armée de terre, Kingston (Ontario) APO BEAT

Documents photographiques © Caméra de combat

AVIS

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

NOTICE

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

RÉSEAUX DE L'AVENIR :
UN CONCEPT POUR L'ARMÉE DE TERRE DE DEMAIN

CENTRE DE GUERRE TERRESTRE DE L'ARMÉE CANADIENNE
KINGSTON

TABLE DES MATIÈRES





« Le premier février 2003, une navette spatiale s'est écrasée. Dans les 90 minutes qui ont suivi, il nous a fallu mettre sur pied un environnement pour l'échange d'informations cruciales regroupant 15 organisations avec lesquelles nous n'avions jamais eu de rapport auparavant, même par téléphone. Quel genre de planification peut-on faire lorsqu'on ne connaît même pas les partenaires avec lesquels il faudra collaborer dans tel ou tel genre d'événement? Il faut découvrir la manière de créer dans la foulée des environnements d'échange d'informations fiables, de fusionner ces environnements en cours d'opération et de les dissoudre lorsqu'ils ne sont plus requis. »

– Major-général Dale W. Meyerrose[1]

PARTIE 1 – INTRODUCTION

En raison de son histoire de projets menés en vase clos procurant des capacités en l'absence d'une stratégie de réseau cohérente, l'Armée de terre subit régulièrement la mise en service de capacités réseau souvent incompatibles. C'est ainsi que les quartiers généraux de formation, les unités de manœuvre, les bases et les garnisons ont vécu la mise en service d'outils réseautés acquis en vertu de divers mandats, qui sont globalement incapables d'échanger des informations entre eux et ne permettent pas un échange direct d'informations entre les commandants des niveaux opérationnel et tactique, ni à l'intérieur même de chacun de ces commandements. L'Armée de terre se retrouve donc dans une situation où ses simulateurs ne peuvent échanger facilement des informations avec les systèmes tactiques de commandement du combat, lesquels sont également incapables d'échanger des informations avec les applications bureautiques de base. À ce jour, on pourrait décrire les capacités réseau de l'Armée canadienne comme des enclaves de réseaux ayant une piètre capacité d'échange d'informations et une faible interconnectivité (formats de données incompatibles, latence élevée, petite bande passante et portée limitée) entre ces enclaves. Cela signifie que même si une équipe de combat ou un groupement tactique dispose de ressources réseau suffisantes pour lui permettre d'exécuter ses fonctions principales, l'élément en question est handicapé par une capacité très limitée d'échange d'informations avec toute autre entité que lui-même ou d'accès aux informations stockées ailleurs.

1. Major-général D.W. Mayerrose. Déclaration faite lors de la conférence de planification finale de la Joint Warrior Interoperability Demonstration (JWID) à Chesapeake, Virginia, le 30 mars 2004. Citée dans L. Bubbers, *Transforming Homeland Defence Through Network Centric Operation*, IBM Business Consulting Services, avril 2005.

Les opérations récentes et la recherche actuelle montrent bien qu'une force est beaucoup plus efficace lorsque l'information nécessaire à la prise de décisions est mise à la disposition de la bonne personne au bon moment[2]. En réalité, l'énorme quantité d'informations à la disposition des commandants et la responsabilité connexe dont ces derniers sont investis (parfois une responsabilité personnelle) nourrissent le besoin de pouvoir non seulement gérer ce volume d'informations, mais également de pouvoir trier ces informations du point de vue de la pertinence afin d'obtenir un haut niveau de fiabilité en leur exactitude. En conséquence de la capacité de la technologie actuelle et future de fournir des volumes croissants d'informations, la fourniture de capacités réseautées robustes reliant les commandants, les soldats, les capteurs et les armes est considérée comme une composante centrale du système de combat terrestre de l'avenir (SCTA). L'objectif de relier les décideurs aux sources d'information et aux armes va exiger une approche souple au partage de l'information et une étude détaillée des stress cognitifs associés à la gestion de gros volumes d'informations. Ce qui différencie le réseau de l'avenir (RAv) d'un réseau commercial courant est la nature de l'environnement dans lequel il doit fonctionner et les conséquences potentiellement létales de ses pannes pour les soldats. Le RAv va donc être conçu de manière à faciliter les opérations militaires, à résister aux environnements extrêmes et à s'adapter aux situations évoluant rapidement, en harmonie avec la nature mobile et circonstancielle des opérations de combat.

L'objectif du RAv est d'offrir une capacité réseau imbriquée dans une stratégie exhaustive de C4ISR de l'Armée canadienne (AC)[3], mise en service dans l'Armée canadienne au niveau de la formation et en descendant, pour offrir aux forces déployées des informations pertinentes et efficaces ainsi qu'un soutien à la prise de décisions. Cette capacité vise à habiliter les opérations tactiques terrestres en fournissant une capacité réseau évolutive, durable, pleinement protégée, intégrée et interopérable qui soit adaptable aux besoins de la communauté des opérations terrestres. Le RAv sera un ensemble cohérent d'informations, de matériel (capteurs et plates-formes d'armes réseautés), de logiciels (p. ex. des outils de soutien à la prise de décisions) et de personnes (décideurs, officiers d'état-major et soldats) dont le but est d'offrir une capacité fluide et intégrée.

2. D. Alberts, *Power to the Edge*. www.dodccrp.org/publications/pdf/Alberts_Power.pdf
3. Stratégie de C4ISR AC (DCIT) parue au printemps 2011.

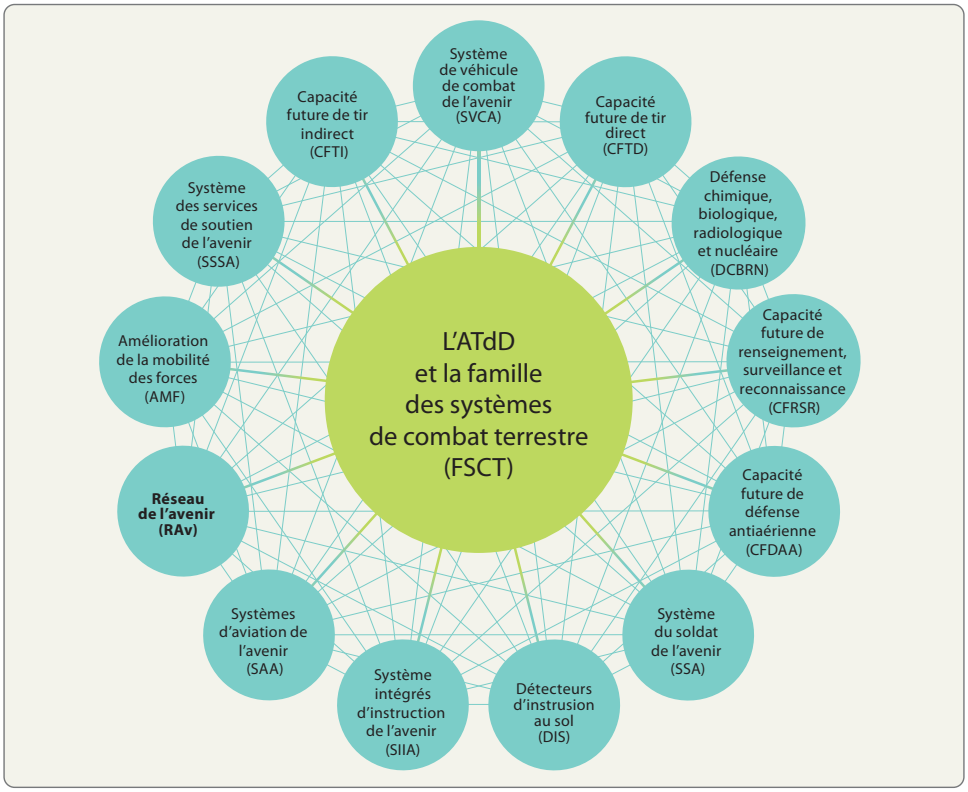

Figure 1 : La famille des systèmes de combat terrestre (FSCT)[4]

Compte tenu de la multitude des besoins des utilisateurs, de la diversité des logiciels d'application, du rythme rapide des changements technologiques et de la nécessité de la souplesse, et face à un adversaire adaptable et dynamique qui évolue dans un environnement opérationnel complexe, aucun système unique ne sera vraisemblablement capable de satisfaire à tous les besoins englobés dans le RAv. Par conséquent, on pense que le RAv sera un système de systèmes (SdS) composé d'un mélange de capacités complémentaires variablement configurées en fonction des divers utilisateurs de l'Armée canadienne. Le présent article ne se propose donc pas de définir le mélange de capacités parfait, car le système sera nécessairement livré graduellement, reposera sur les technologies disponibles au moment de la définition des besoins et évoluera par la suite. Les facteurs à considérer sont trop nombreux pour me permettre d'affirmer catégoriquement que les capacités recommandées

4. La famille des systèmes de combat terrestre (FSCT) a évolué et va continuer de le faire avec le temps.

vont satisfaire tous les intérêts. Par conséquent, cet article recommande les capacités optimales que devrait posséder le système pour satisfaire à la majorité des exigences tout en restant souple et adaptable.

Cet article sur le RAv n'examine pas dans le détail la gestion du cycle de vie, les niveaux de distribution du matériel et les méthodes d'instruction. Ces aspects ne dépendent pas principalement de facteurs opérationnels, mais plutôt des contraintes financières, des pratiques de gestion et des besoins d'apprentissage et, en ce sens, ils méritent un examen particulier dans le cadre d'études subséquentes faites par les directions compétentes.

CONTRAINTES/LIMITES

Le présent article sur le RAv n'examine pas en profondeur l'infrastructure de communications de soutien, ni le système porteur requis pour soutenir les capacités et fonctionnalités souhaitées dudit réseau. Cependant, on peut faire certaines déductions concernant les changements aux caractéristiques pertinentes du système porteur à partir de l'examen des besoins de capacités. En outre, le présent article ne s'intéresse pas à la dimension humaine du réseau, en particulier aux changements possibles qu'il faudrait apporter aux processus de commandement et contrôle pour réaliser le potentiel du RAv dans le contexte des opérations adaptables et dispersées (OAD), sauf si ce n'est que pour signaler qu'il reste encore des aspects mal compris du domaine cognitif qui sont susceptibles de se manifester par suite d'un accroissement presque exponentiel du volume d'informations et des dispositifs réseautés dans l'environnement militaire.

PARTIE 2 – L'ENVIRONNEMENT TECHNOLOGIQUE DE L'AVENIR[5]

L'art de la guerre a toujours été profondément influencé par la science et la technologie[6]. L'amélioration des armes s'est traduite par une augmentation de la précision et de la létalité, ce qui a ensuite changé la façon de combattre par la suite. Les mêmes tendances sont encore présentes aujourd'hui – amélioration de la précision, de la portée, de la puissance des feux et de la létalité, disparités technologiques, commandement et contrôle facilités par les technologies de l'information, et dispersion des troupes. Chacune de ces tendances est sujette à des frictions qui peuvent en ralentir ou en altérer l'évolution. Il est fort probable que le législateur trouvera difficile de suivre le rythme des changements et de l'évolution des sciences et de la technologie. De plus, on s'attend à ce que l'avantage technologique dont profitent les nations développées décroisse rapidement avec le flux des technologies vers les nations sous-développées et les acteurs non étatiques, notamment des adversaires en puissance. Compte tenu de ces réserves, il est assez évident que trois tendances technologiques[7] vont jouir d'une influence considérable sur l'orientation des changements jusqu'en 2020 : les technologies de l'information et des communications (TIC), les biotechnologies et les technologies de l'énergie et de l'environnement.

Informatique. Depuis plusieurs décennies, l'augmentation de la puissance de calcul des ordinateurs a été le moteur de croissance de l'ère de l'information, laquelle croissance a entraîné une démocratisation parallèle de l'accès à l'information et du partage de l'information grâce à l'effondrement des coûts, même lorsque la puissance informatique augmentait dramatiquement. Le résultat de cette croissance remarquablement constante est qu'il est possible aujourd'hui d'acheter un ordinateur personnel d'une puissance équivalente au superordinateur le plus puissant en 1991[8], et ce, pour un dix millième de son prix. La puissance de calcul de ces ordinateurs

5. Partie 2, L'environnement technologique de l'avenir est une adaptation du chapitre 2 de : « Technologies et tendances mondiales en émergence » de *Opérations terrestres en 2021 : un concept en devenir – Études à l'appui du concept d'emploi de la force de l'Armée de terre de demain* (Godfroy et Gisewski).

6. La science est définie comme tout système de connaissances s'intéressant au monde physique et à ses phénomènes, et qui suppose une observation et une expérimentation systématiques non biaisées. Traduction de la définition donnée dans l'Encyclopédia Britannica. Voir www.britannica.com/eb/article-9066286/science.

La technologie est l'application des connaissances scientifiques aux fins pratiques de la vie humaine ou de la modification et de la manipulation de l'environnement humain. La technologie comprend donc des machines et de l'équipement basés sur la connaissance scientifique et, dans le contexte militaire, développés spécifiquement pour le combat. Traduction de la définition donnée par l'Encyclopedia Britannica. Voir www.britannica.com/eb/article-9110174/military-technology.

7. Selon l'Équipe des orientations futures du Conseil national de recherche Canada (CNRC) www.nrc-cnrc.gc.ca/aboutUs/ren/nrc-foresight_f.html.

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

largement disponibles permet de faire des simulations tellement fidèles à la réalité qu'on peut simuler des événements ou des phénomènes qu'on ne pourrait pas même envisager de tenter dans le monde physique réel. Cela signifie aussi que la puissance des superordinateurs peut être mise au service d'outils de simulation intelligents, ce qui permet de répéter les plans avant d'engager des forces. De nouveaux modes de manipulation des données qui encouragent un accès plus efficace aux informations numérisées seront possibles grâce à des interfaces multitouches simultanées, à des dispositifs haptiques[9] et à des contrôleurs à détection de mouvement[10]. Ces dispositifs multitouches ouvrent des possibilités comme les murs et les tables interactifs, lesquels conviennent idéalement aux affichages des systèmes d'information de commandement et de contrôle utilisés dans les quartiers généraux de formation et d'unité. De la même manière, la puissance informatique disponible est utilisée pour résoudre des problèmes de communication de niveau tactique et produire une génération de radios[11] logicielles intelligentes qui permettent la création de réseaux autorégénérants et de réseaux de communication de circonstance sur le champ de bataille. Enfin, les services comme l'informatique en nuage s'accompagnent de la prolifération du stockage sur Internet, de la recherche sur de multiples dispositifs et plates-formes, ce qui offre aux gens une capacité améliorée de s'interconnecter (notamment le réseautage social). Ce que les planificateurs militaires n'ont peut-être pas encore noté est que cette augmentation de la puissance de traitement est maintenant à la disposition des acteurs étatiques et non étatiques, dont certains vont sans aucun doute utiliser cette capacité informatique pour poser des gestes et mener des activités nuisibles aux intérêts du Canada.

Intelligence artificielle. La recherche dans le domaine de l'intelligence artificielle (IA) a connu un renouveau d'intérêt par suite des progrès réalisés dans le domaine des TIC. Avec l'amélioration de leur performance, les systèmes exploitant l'intelligence artificielle pourraient remplacer graduellement ou compléter des fonctions et des procédures exclusivement dévolues à l'être humain, par exemple gérer un réseau d'alimentation[12], guider des missiles ou des satellites, ou assembler d'autres machines[13].

Il va arriver un moment où l'IA militaire va atteindre un seuil de capacité qui menace de franchir des barrières morales, éthiques ou juridiques. Un système

9. Une interface haptique est un dispositif qui permet à l'utilisateur d'interagir avec l'ordinateur grâce à une rétroaction tactile. Voir http://wii.nintendo.com/controller.jsp.

10. Voir http://cs.nyu.edu/~jhan/ftirtouch/.

11. Les radios intelligentes analysent l'environnement radio pour choisir la meilleure bande et le meilleur protocole pour communiquer avec la station ciblée en utilisant la plus basse puissance suffisante.

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

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

autonome capable de prendre des décisions de vie ou de mort dans des environnements chaotiques ou dynamiques n'est pas inconcevable. Compte tenu des récents progrès réalisés dans le domaine de l'IA et de la probabilité que cette forme d'intelligence parvienne à un niveau de développement qui concurrencera les habiletés humaines dans de grands domaines, *il serait avisé pour ceux qui travaillent au développement des capacités de ne pas perdre de vue les ramifications morales, éthiques et juridiques des décisions qu'ils prennent en matière de développement de systèmes exploitant l'IA.*

Robotique. La robotique est sur le point de devenir le prochain grand produit technologique, dépassant peut-être même en cela l'ordinateur[14]. Le département de la Défense américain semble de cet avis; en 2000, le Congrès américain fixait l'objectif qu'un tiers des véhicules militaires terrestres et un tiers des aéronefs d'attaque à long rayon d'action soient robotisés dans une décennie. Un article publié en Australie[15] en 2006 concluait que, au plan stratégique, la robotique avait dépassé le stade de nouvelle menace stratégique pour devenir une menace élargie aux niveaux opérationnels et tactiques. Les robots, notamment les véhicules terrestres sans pilote (VTSP), conviennent bien à l'exécution de tâches répétitives et ennuyeuses. Ils sont sans crainte et infatigables. Ils exécutent des tâches répétitives rapidement et avec précision. Ils peuvent être conçus pour éviter les armes ennemies ou leur résister, et pour exécuter des fonctions militaires particulières. Mais surtout, les robots ont la capacité de réduire les pertes en augmentant l'efficacité au combat des soldats sur le champ de bataille[16]. De plus, lorsque les véhicules robotisés vont entrer en service en 2021, ils pourraient attirer les tirs ou repérer les objectifs, ce qui permettrait aux systèmes de générations antérieures d'engager l'ennemi et de dominer le champ de bataille même s'ils ne possèdent pas nécessairement une puissance de feu ou un blindage supérieurs à ceux de l'ennemi.

S'inspirant du comportement des colonies de fourmis, les chercheurs connaissent du succès dans la création de robots reconfigurables inspirés du milieu biologique et modelés sur le comportement des insectes; ils produisent des robots en essaim[17] dans lesquels il n'y a pas de contrôle centralisé pour diriger l'activité. Au contraire, le comportement collectif et adaptable se manifeste spontanément sans l'aide d'un

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

15. Patrick Chisan Hew, *The Generation of Situational Awareness within Autonomous Systems – Near to Mid Term Study – Issues*, département de la défense de l'Australie, Defence Science and Technology Organization, DSTO-GD-0467, Edinburgh South Australia 5111 Australie, juillet 2006. http://dspace.dsto.defence.gov.au/dspace/handle/1947/4560.

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

17. Robots en essaim : groupe de nombreux petits robots peu dispendieux pouvant agir de façon autonome.

logiciel évolué de prise de décisions. Efficaces et résistants[18] aux pannes mécaniques, ces robots modelés sur les insectes pourraient voler librement autour des bâtiments et entrer par une fenêtre ouverte. Équipés de divers types de capteurs, ils pourraient permettre de mieux surveiller les habitats éloignés ou inhospitaliers.

Se développant à un rythme accéléré, les véhicules aériens sans pilote (UAV) disponibles dans le commerce arrivent sur le marché à une fréquence croissante et sont dotés de caractéristiques de rendement impressionnantes; ils peuvent atteindre 50 % de la vitesse, de la portée et de l'autonomie d'UAV[19] militaires beaucoup plus dispendieux. Grâce à leur moteur électrique silencieux et à leur caméra vidéo intégrée, ces UAV peuvent maintenant être utilisés par les belligérants pour surveiller et détecter des objectifs secrètement.

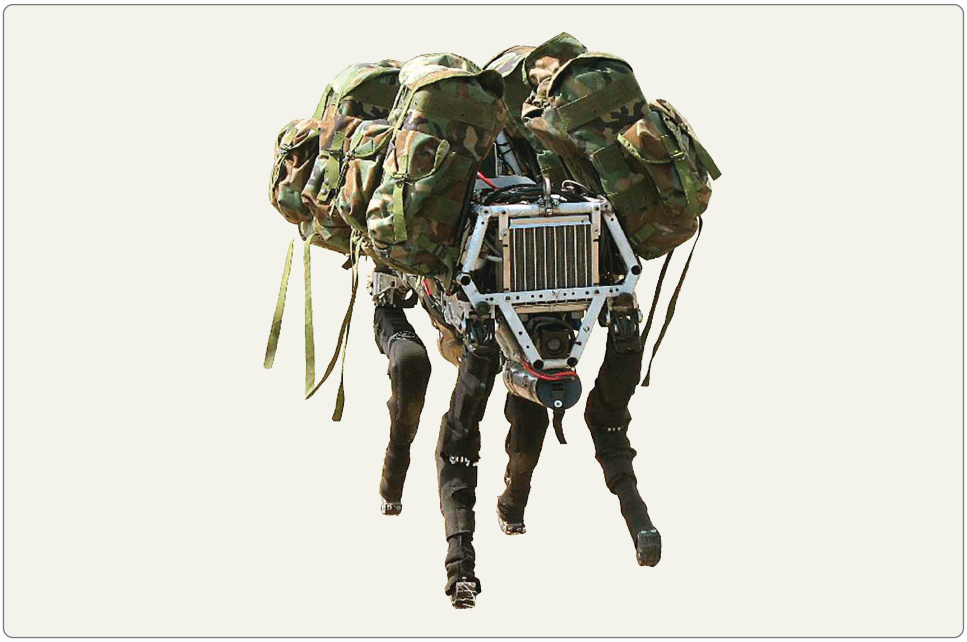

Figure 2 : Robot de bât Big Dog[20]

Réalité virtuelle et modélisation 3D. Un domaine porteur d'effets potentiellement radicaux sur la planification militaire est l'utilisation de la réalité virtuelle (RV) et de la modélisation tridimensionnelle (3D) combinées à une mise à jour en temps presque réel des changements qui surviennent dans l'environnement

18. http://www.sigmascan.org//ViewIssue.aspx?IssueId=302.
19. http://www.rctoys.com/rc-toys-and-parts/DF-TANGORC/INDUSTRIAL.html.
20. http://www.bostondynamics.com/.

réel. Grâce à cette fonctionnalité, les capteurs pourraient ainsi facilement ajouter de nouveaux objets ou de nouvelles caractéristiques au fur et à mesure qu'ils les détectent pour enrichir l'environnement « connu », ce qui aiderait, par exemple, à donner l'alerte en temps presque réel. L'ajout d'interfaces de rétroaction sur la résistance dans l'interaction haptique améliorera encore d'un cran l'expérience en introduisant une façon de réduire la fatigue.

À l'extrémité opposée du même spectre technologique se trouve la « virtualité incarnée » qu'on a décrite comme le processus consistant à extraire l'ordinateur de son boîtier électronique, à le miniaturiser et à l'intégrer dans à peu près n'importe quoi : autos, bâtiments, appareils et corps humains. Le résultat probable de cet environnement informatique omniprésent est la capacité de créer une réalité amplifiée (RA). Les bénéfices de cette avancée technologique pour les établissements d'instruction militaires comportent la possibilité d'offrir une éducation et une instruction d'immersion à n'importe qui, sans égard au moment ou à l'endroit. Déjà, les joueurs qui utilisent la réalité amplifiée transforment le monde réel en zones de combat virtuelles à l'aide de technologies actuelles comme le GPS et le téléphone cellulaire utilisant le Web[21]. Ces quelques exemples révèlent le puissant potentiel d'une force pleinement habilitée par réseau – c.-à-d. une force dotée de services exploitant les communications, l'informatique et la position[22], possiblement tous intégrés dans un seul et unique dispositif portable.

Biotechnologie. Beaucoup des mêmes tendances de croissance sont présentes dans le domaine de la biologie. En effet, les TIC ont révolutionné l'étude de la biologie pour la transformer, essentiellement, en une technologie de l'information sujette à la même croissance exponentielle et au même rendement accélérant.

Malgré une résistance initiale, certains chercheurs anticipent une ère très prochaine où le piratage en biologie deviendra courant, ce qui pourrait amplifier la menace de dangers biologiques. L'arrivée de nouvelles générations d'outils perfectionnés a amené les laboratoires de recherche à se départir de leur vieux matériel à faible prix. Ce matériel peu dispendieux pourrait facilement se retrouver entre les mains d'organisations criminelles ou terroristes et favoriser ainsi une prolifération des menaces biologiques. Si des groupes d'insurgés parviennent à maîtriser le plein potentiel perturbateur de la biologie de synthèse, nos efforts actuels de développement des capacités – qui reposent en grande partie sur les armes à énergie cinétique – pourraient perdre toute leur pertinence.

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

22. Le service de commerce électronique par téléphone mobile (location-based service (LBS)) est un service d'information et de divertissement accessible à l'aide d'un appareil mobile par l'intermédiaire d'un réseau mobile qui exploite la possibilité d'utiliser la position géographique de l'appareil mobile.

La révolution biotechnologique comporte également des conséquences importantes pour la dimension humaine. Par exemple, on fait des progrès vers la compréhension et la manipulation des origines génétiques de la réaction de peur. Bien qu'il ne soit pas déraisonnable de penser que ce genre de manipulation génétique ne puisse pas être effectuée hors laboratoire, les progrès récents laissent présager des capacités ayant des implications offensives et défensives pour l'Armée de terre de demain et l'Armée de terre de l'avenir, et qui soulèvent une myriade de questions. Par exemple, est-ce que l'Armée de terre va exploiter cette capacité pour transformer ses soldats en des guerriers vraiment sans peur face à l'ennemi? Est-ce que ces capacités pourraient finalement atténuer les effets du stress post-traumatique? Si ces questions restent problématiques au plan moral et éthique pour les démocraties occidentales, elles ne le seront pas nécessairement pour les terroristes bien financés ou les réseaux criminels.

Nanotechnologie. La course à la recherche, au développement et à commercialisation de nanomatériaux est mondiale. Les progrès dans le domaine des nanomatériaux promettent de révolutionner de vastes domaines comme les matériaux à haut rendement, les apprêts, la conversion et l'entreposage de l'énergie, les capteurs, l'électronique, l'industrie pharmaceutique et le domaine des diagnostics. La nanotechnologie est encore à l'étape formative, mais se développe rapidement – si rapidement, en fait, que la première interface neurophysique[23] entre un ordinateur et le cerveau humain (probablement au service d'une fonction prosthétique) pourrait faire l'objet d'une démonstration entre 2015 et 2020[24]. Avec l'arrivée de ce genre d'interface, la possibilité pour l'être humain d'interagir directement avec l'ordinateur par la pensée pourrait devenir réalité.

Les implications militaires, économiques et de sécurité de la nanotechnologie sont considérables et ont amené certains organismes fédéraux américains à engager des ressources considérables en recherche et développement (R et D)[25] dans ce domaine[26]. Reconnaissant l'importance et l'impact potentielle des nanotechnologies sur les capacités de l'avenir, l'armée américaine a alloué 50 millions de dollars pour mettre sur pied l'Institute for Soldier Nanotechnologies au Massachusetts Institute of Technology (MIT) à Cambridge, dans le but d'améliorer la protection des soldats, particulièrement en développant de nouveaux uniformes, un meilleur blindage et des capteurs améliorés.

23. Les interfaces neuronales vont assurer un lien direct entre le cerveau ou le système nerveux humain ou animal et un ordinateur ou un réseau informatique.

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

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

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

CHANGEMENT SOCIÉTAL ENGENDRÉ PAR LA TECHNOLOGIE

La technologie est un des principaux moteurs des changements sociétaux. De plus, *le rythme des changements conduit à des perturbations sociétales*, qui sont souvent manifestes dans des lois et des politiques révisées. Des litiges juridiques naissent lorsque des groupes utilisent ou cherchent à utiliser de nouvelles technologies avant que le public en général ou les élus aient eu le temps de considérer les politiques publiques qui devraient les encadrer. Par conséquent, pour éviter l'effet de surprise et l'obligation connexe de poser des jugements irréfléchis qui entraînent souvent des conséquences inattendues, l'étude systématique des enjeux de l'avenir doit devenir partie intégrante des activités de développement des capacités.

Les bases de données à accès libre et les dépôts de connaissances amplifient les risques potentiels évoqués au paragraphe précédent. Par exemple, en vertu des politiques actuelles, les scientifiques et le public en général ont un accès sans restriction aux données génomiques sur les microbes pathogènes. Le débat reste ouvert à savoir si des informations exploitables de cette nature devraient être diffusées pour le bien du public ou si elles devraient être protégées en raison de la menace potentielle qu'elles comportent. Les autorités politiques doivent également envisager la possibilité que les informations de cette nature soient exploitées à des fins destructrices, par exemple pour des actes de bioterrorisme ou pour la guerre. Compte tenu de ces risques, une évaluation continue et minutieuse de la technologie scientifique s'impose du point de vue de ses effets sur la sécurité, la santé et le bien-être nationaux[27]. Les activités de développement des forces doivent tenir compte des changements et des scénarios potentiels qui incluent de telles capacités radicales si nous voulons être prêts à nous défendre à l'avenir et à faire face aux menaces à la sécurité de l'avenir.

Un autre progrès qui va continuer de poser des défis à la société est la facilité avec laquelle les données numériques peuvent être copiées, partagées et manipulées. Malgré les problèmes de manipulation inappropriée des données et de l'information, la collaboration sociale habilitée par réseau demeure une capacité puissante qui va très vraisemblablement continuer de croître en popularité et en importance. L'accès ouvert à l'information, combiné aux logiciels d'exploration de texte, va permettre aux utilisateurs de sonder les liens implicites aux données, ce qui va faciliter leur analyse détaillée. *La libération de l'information va habiliter les individus tout en réduisant le monopole exercé par le gouvernement sur l'information.* Il pourrait même devenir nécessaire pour les organisations de fournir des outils de

27. L'Initiative de recherche et de technologie CBRN dirigée par RDDC est un excellent exemple de l'approche proactive adoptée par le Canada : http://www.crti.drdc-rddc.gc.ca/en/default.asp.

réseautage social à leur personnel. Ces capacités peu dispendieuses, combinées à un réseau mondial de diffusion presque instantanée par Internet, ouvrent toute la porte à la désinformation, à la déception et à la fraude – intentionnelles ou non – et vont accroître la nécessité de faire preuve de diligence raisonnable dans la vérification des sources. Compte tenu du conservatisme institutionnel et du désir d'avoir des politiques sur le contrôle de l'accès et la sécurité de l'information au sein des FC, ce genre d'ouverture et de transparence fera vraisemblablement face à une résistance dans le milieu de la défense.

Si les restrictions en matière de bande passante et de sécurité peuvent être légitimes dans un contexte militaire, elles risquent de devenir de plus en plus intolérables[28] pour ceux et celles qui s'attendent à ce que des outils de collaboration sociale et de communication soient mis à leur disposition. *À l'avenir, toute tentative par une autorité de réprimer les communications entre utilisateurs au sein de ces environnements de collaboration Web 2.0 émergents pourrait ironiquement conduire à une prolifération encore plus grande de l'information dont elle visait initialement à réduire la circulation*[29]**.** On peut donc s'imaginer que les capacités d'opérations civiles facilitées par réseau vont probablement croître en perfectionnement et en puissance pour en arriver à rivaliser avec n'importe quelle capacité mise en œuvre par les grandes armées institutionnelles et bureaucratiques.

Les armées, en tant qu'institutions, sont naturellement conservatrices et évolutionnaires, et leur *culture organisationnelle n'est pas nécessairement bien placée pour accepter le rythme rapide et la nature des changements technologiques*. Il est probable que l'établissement d'une force réseautée optimisée pour les opérations adaptables et dispersées (OAD) va déclencher des changements organisationnels et possiblement entraîner la création de structures plus horizontales et moins hiérarchiques, et plus vraisemblablement la création de forces de circonstance assemblées pour des tâches particulières. Cela étant dit, les possibilités de collaboration créées par les technologies du réseautage social pourraient servir à miner les structures hiérarchiques si familières au sein de l'Armée de terre. L'incertitude associée à de tels changements provoquera vraisemblablement une forte résistance dans certains

28. Récemment, les utilisateurs de Digg.com ont mis en ligne des liens vers un code qui permettait aux concepteurs de logiciels de copier le contenu chiffré de disques HD-DVD. Les créateurs du code en question, Advanced Access Content Systems, ont exigé que les administrateurs de Digg.com suppriment ces liens. Même si les administrateurs du site ont acquiescé à cette demande, les utilisateurs du site se sont rebellés. Le site de Digg a été enseveli sous des milliers de liens menant au code et de protestations au nom de la liberté de parole. Cette rébellion sociale a forcé les administrateurs de Digg à cesser toute tentative d'enlever le code et à plutôt essayer d'élaborer une position légale en vue de l'inévitable poursuite dont ils feront l'objet de la part des créateurs du code en question.

29. Ce phénomène est connu sous le nom de marketing viral, un phénomène qui peut avoir des avantages au plan de la commercialisation, mais des conséquences négatives si on essaie de protéger des informations sensibles. Il y a de plus en plus d'occasions d'explorer les données associées à ces connexions florissantes. Par exemple, les agences de renseignements cherchent à suivre des groupes d'insurgés à l'aide d'outils de cartographie des réseaux sociaux.

secteurs de l'armée. Pareillement, le développement et la mise en service rapide d'un éventail de composantes réseau (évolutives) pourraient produire une force asymétriquement équipée disposant de capacités de réseautage très différentes, ce qui risquerait de faire naître une méfiance entre le soldat et son chef ou de la frustration à l'égard de l'information générée par le réseau et soumise aux fins de décisions. Pour surmonter les problèmes de résistance et de méfiance, il faudra déployer d'importants efforts pour éduquer l'Armée canadienne et faire comprendre à ses membres que la mise en service de capacités réseautées ne va pas supplanter la responsabilité et le contrôle humains.

L'approche actuelle consiste à s'assurer de l'intervention d'une personne dans ce genre de décisions, mais elle ne sera pas nécessairement encore pertinente à l'avenir. Il est possible que certaines situations se présentent dans lesquelles les événements surviennent avec une telle rapidité que les temps de réponse humains habituels soient tout à fait inadéquats. Par exemple, les contre-mesures automatiques des suites d'aides de défense (SAD) doivent se déployer dans un délai calculé en millisecondes, bien avant que l'opérateur humain soit capable de percevoir la menace imminente et d'y réagir.

La communauté de développement des capacités de l'Armée de terre va devoir se tenir au fait de ces enjeux et de leurs incidences sur les ressources humaines. Nos futures recrues, vers l'année 2021, sont actuellement âgées de quatre à huit ans et vont vraisemblablement avoir des attentes très élaborées concernant la collaboration sociale facilitée par réseau. De plus, la capacité d'évoluer dans ce genre d'environnement sera une qualité en forte demande chez les recrues de l'avenir, car le concept d'OAD de l'Armée de terre de demain prévoit un environnement réseauté omniprésent. Cela étant dit, la tâche d'équilibrer les politiques de sécurité face aux exigences des utilisateurs d'avoir accès à la technologie va continuer de représenter tout un défi pour la mise en œuvre des systèmes militaires.

CHANGEMENT DE LA TECHNOLOGIE MILITAIRE

Les changements découlant de la prolifération des capacités de réseautage dans le secteur commercial vont continuer de façonner la société canadienne et l'institution militaire. Les impératifs opérationnels vont évidemment exiger que la bande passante disponible soit en priorité mise à la disposition des forces militaires pour les fins particulières de la mission.

Outre les avantages qu'apportent les progrès du réseautage à la société, il ne faut pas oublier la capacité du réseautage de prolonger la vie de plates-formes et de systèmes d'armes existants en permettant leur utilisation de façons nouvelles et innovatrices – notamment par la dispersion accompagnée d'une meilleure

connaissance de la situation et d'un plus grand potentiel d'engagement en coopération. Les nouveaux systèmes de conduite du tir, capteurs et logiciels peuvent compenser les insuffisances de protection du blindage en offrant une meilleure probabilité de coup au but/destruction du premier coup. De la même manière, les progrès dans la conception et la fabrication des matériaux et dans le domaine des technologies de l'information vont être exploités pour améliorer la protection et la surviabilité. En ce sens, les capacités réseau devraient améliorer la surviabilité en améliorant les couches successives de protection, en passant de la mobilité et de la furtivité à la réduction de la signature et aux SAD de mise hors de combat, aux SAD de destruction, au blindage amélioré et aux systèmes de suppression des éclats.

Les dispositifs de navigation et de brouillage de la navigation[30] sont aujourd'hui des produits commerciaux peu dispendieux que tout le monde peut se procurer, notamment nos adversaires. Même si ces systèmes commerciaux n'ont parfois pas de solides caractéristiques de sécurité, les soldats les achètent à titre privé avant de se déployer dans un théâtre. Lorsqu'on les combine avec les technologies de communication disponibles dans le commerce, ils offrent des capacités de connaissance de la situation comparables à celles des systèmes militaires actuellement déployés. Par exemple, les soldats canadiens ont l'habitude depuis longtemps d'ajouter à leur équipement réglementaire des appareils plus perfectionnés qu'ils achètent personnellement, particulièrement des produits commerciaux exploitant le GPS, ce qui fait qu'au moins une personne par patrouille et souvent tous les membres de la patrouille ont accès à la fonctionnalité GPS. Ce phénomène va probablement se poursuivre, car les innovations commerciales offrent de nouvelles capacités plus rapidement que les programmes d'acquisition militaires ne peuvent le faire.

Ainsi, la compagnie ImageSat International, qui appartient à des intérêts israéliens, offre à sa clientèle d'utiliser son satellite d'imagerie EROS-A et de transférer les données recueillies dans le secret le plus total, et ce, à peu près sans aucune restriction[31]. Ce service revient essentiellement à offrir à des clients privés leur propre satellite de reconnaissance personnel à faible coût. L'industrie des satellites privés est en train de devenir si perfectionnée et omniprésente que beaucoup de forces militaires avancées, notamment les forces militaires américaines, s'en remettent maintenant à elle pour obtenir certains produits d'imagerie et répondre à une bonne partie de leurs besoins de communication.

La confluence de toutes ces tendances influera probablement sur la conduite de la guerre terrestre pour l'amener dans un environnement dominé par des

30. À l'heure actuelle, 28 pays travaillent activement à l'élaboration de systèmes de brouillage. Source : Documents de la conférence de planification Trial Gypsy Hotel.

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

forces beaucoup plus légères, furtives et habilitées par l'information qui exploitent abondamment la robotique. L'utilisation commerciale et militaire accrue de l'espace pourrait entraîner l'émergence d'une vaste gamme de capacités offensives et défensives de contrôle de l'espace. Les outils d'attaque de réseau informatique (CNA), les brouilleurs de GPS et les armes à fréquence radio pourraient être largement utilisés pour attaquer les infrastructures d'information et les forces fortement dépendantes de l'information. Les armes biologiques exclusives et l'émergence des opérations biologiques pourraient également jouer un rôle dominant. Assurément, le défaut d'orienter les activités de développement des capacités à la lumière de ces possibilités constitue un risque important pour l'avenir.

IMPLICATIONS DU FACTEUR HUMAIN

Parallèlement aux changements qui surviennent dans la société, les compétences dont les citoyens ont besoin pour relever les nouveaux défis évoluent également. Les recrues de 2021 vont avoir besoin de compétences de l'ère numérique pour connaître du succès sur le champ de bataille numérique. Le système d'instruction militaire doit évaluer en parallèle pour préparer les soldats en vue de cet environnement. Plus particulièrement, il doit comprendre et accueillir les compétences[32] exigées par les changements technologiques au 21e siècle, notamment :

- ***Littératie visuelle et en information :*** De bonnes compétences de visualisation sont nécessaires pour pouvoir déchiffrer, interpréter, détecter les schémas et communiquer à l'aide d'interfaces graphiques améliorées. La littératie en information comprend la compétence pour trouver l'information efficacement, l'évaluer de façon critique et compétente, et l'utiliser avec précision et créativité.
- ***Littératie culturelle et sensibilité au monde :*** Dans une économie mondiale, en présence d'interactions, de partenariats et de concurrence de tous les coins du monde, il est plus nécessaire que jamais de connaître, comprendre et apprécier les autres cultures, notamment les normes culturelles d'une société technologique. En présence de lacunes sur le plan des connaissances culturelles au sein des FC, le réseau de l'avenir (RAv) pourrait être en mesure de compenser grâce à des capacités comme des bases de connaissances culturelles et la traduction en temps réel.
- ***Adaptabilité/Gestion de la complexité et autonomie* :** L'interconnectivité du monde d'aujourd'hui engendre une complexité sans précédent. Les individus doivent être des apprenants autonomes capables d'analyser

32. Cette liste des compétences du 21e siècle est adaptée de l'étude enGauge 21st Century Skills : http://www.ncrel.org/engauge/skills/skills.htm.

les nouvelles conditions au fur et à mesure qu'elles se présentent, d'identifier les nouvelles compétences qui vont être nécessaires pour faire face à ces nouvelles conditions et de tracer indépendamment un parcours pour s'adapter à ces changements. Ils doivent pouvoir tenir compte des contingences, anticiper le changement et comprendre les interdépendances des systèmes.

- ***Curiosité, créativité et prise de risques :*** Les individus aujourd'hui doivent s'ajuster et s'adapter aux environnements changeants. La curiosité alimente un apprentissage permanent et contribue à la qualité de vie et au capital intellectuel du pays. La prise de risques est tout aussi importante – sans elle, il y aurait peu de grands pas dans les découvertes, les inventions et l'apprentissage. Parmi les soldats, de nouvelles générations d'individus adeptes de technologie vont gravir les échelons de l'Armée de terre; elles vont être à l'aise avec la configuration de dispositifs pour leur usage personnel et vont s'attendre à pouvoir faire la même chose avec les dispositifs SIC2 de l'Armée de terre. Face à une gestion centralisée de l'information, ils vont chercher et réussir à trouver des solutions de rechange – souvent en campagne et en réponse à des besoins de l'utilisateur. Le défi pour l'Armée de terre consistera à comprendre cette créativité et à en tirer profit.
- ***Formation d'équipes et collaboration :*** Le rythme rapide de la société d'aujourd'hui et des réseaux de communication a provoqué, et permis, un déplacement du niveau décisionnel vers le bas, jusqu'aux individus. Parallèlement, la complexité du monde d'aujourd'hui exige un haut degré de spécialisation de la part des décideurs. Cette situation exige la formation d'équipes de spécialistes, dans un domaine de plus en plus virtuel, pour accomplir des tâches complexes de manière efficiente, efficace et opportune. Le courriel, le télécopieur, les messages vocaux, les conférences audio et vidéo, les espaces de clavardage, les documents partagés et l'espace de travail virtuel peuvent offrir des environnements de collaboration plus opportuns et répétitifs.
- ***Responsabilité personnelle et sociale :*** Les technologies émergentes s'accompagnent souvent de dilemmes éthiques et de valeurs. Au gré de l'augmentation de la complexité technique, l'éthique et les valeurs doivent guider l'application de la science et de la technologie aux niveaux personnel, communautaire et gouvernemental. Les individus doivent comprendre cette responsabilité et l'accepter en tant que citoyens informés, à tous les niveaux.

- ***Communications interactives :*** Il est impératif que les individus comprennent comment communiquer au moyen de la technologie. Cela inclut les communications synchrones et asynchrones comme les courriels personnels, les blogues et les interactions wiki, les interactions de groupes dans des environnements virtuels, les espaces de clavardage, les environnements de jeux multiutilisateurs, les vidéoconférences interactives, les interactions téléphone/audio et les interactions par simulations et modèles. Ces interactions exigent une connaissance de l'étiquette parfois particulière à chaque environnement. Les technologies de l'information ajoutent de nouvelles dimensions qui doivent être maîtrisées pour les rendre transparentes (p. ex. l'établissement d'un horaire couvrant plusieurs fuseaux horaires, la diversité culturelle, les problèmes de langue). À défaut, ces technologies pourraient nuire à la communication plutôt que de l'améliorer.
- ***Mise en ordre de priorité, planification et gestion des résultats :*** Les niveaux élevés de complexité exigent une planification et une gestion attentives, ainsi que la capacité d'anticiper les contingences. Cela signifie plus que de simplement se concentrer pour atteindre les objectifs principaux de la mission ou d'exercer un suivi pour détecter les résultats attendus. Cela exige la souplesse et la créativité nécessaires pour anticiper les résultats inattendus également.

Les technologies militaires vont certainement continuer d'être combinées à une amélioration du renseignement, de la vitesse, de la portée, de la furtivité, de la létalité et de l'autonomie dans une course continue pour prendre de vitesse les menaces perçues. En réalité, malgré l'incapacité inhérente de prédire l'avenir, les données sur les tendances sont suffisantes pour prévoir que la technologie (principalement commerciale) va continuer de progresser de manière exponentielle et de converger (sauf si une catastrophe imprévue survient). Cette perspective annonce la possibilité de voir de petits groupes bien financés obtenir un avantage technologique asymétrique dans des domaines bien précis et, ainsi, de menacer la supériorité militaire occidentale actuelle.

Les progrès prévisibles dans les domaines de l'intelligence artificielle, de l'informatique, de la simulation, des communications, des capteurs, de la robotique et de l'énergie portable commencent à peine à influer sur la réflexion entourant le développement des capacités au sein de l'Armée canadienne. Malheureusement, à cause de la lenteur avec laquelle les nouveaux grands systèmes sont livrés, laquelle est amplifiée par un circuit d'acquisition totalement submergé par des équipements et des plates-formes principalement traditionnels, il va être difficile de réagir en temps

opportun aux changements technologiques rapides et continus et encore plus à une possible perturbation de la sécurité (peut-être déjà à l'horizon) engendrée par de nouvelles percées technologiques dans le secteur commercial.

Cette section a présenté un survol bref et nécessairement incomplet des tendances technologiques de l'avenir et illustré les degrés auxquels le changement va conditionner le développement des capacités militaires. La PARTIE 3 du présent article va essayer de résumer les concepts incarnés dans la guerre habilitée par réseau, d'offrir certaines mises en garde concernant l'adoption globale de ces concepts et se conclura par une description de ce qu'est un réseau et des fonctions qu'il remplit. Elle va en outre décrire certains grands types d'échanges d'informations pertinents pour le concept des OAD.

« Enfin, la grande incertitude de toutes les données constitue cette difficulté particulière à la guerre, que l'action s'y poursuit toujours en quelque sorte dans un éclairage crépusculaire qui, comme le brouillard et le clair de lune, donne fréquemment aux choses un aspect étrange et des dimensions exagérées, de sorte que si le talent ne le devine, c'est au hasard seul qu'il faut s'en rapporter pour tout ce qui échappe à la perception dans cette demi-obscurité. »

– Clausewitz[33]

PARTIE 3 – RÉSEAUX ET OPÉRATIONS FACILITÉES PAR RÉSEAUX

La guerre réseaucentrique (GR), les opérations facilitées par réseau (OFR), les capacités facilitées par réseau (CFR), etc., sont des cadres conceptuels élaborés par les États-Unis d'Amérique, le Canada et leurs alliés pour expliquer une approche à la transformation des capacités militaires en changeant la façon de penser des gens, ce qui favorise des processus intelligents pour partager et exploiter l'information et la liaison ou le réseautage des gens, des plates-formes et des capteurs grâce à la technologie. La partie 3 de cet article décrit de façon très simplifiée les principes des OFR, propose certaines occasions et certains risques associés à l'exploitation d'un cadre OFR, et se conclut par une brève discussion sur ce qui constitue un réseau et sur les fonctions générales d'un réseau.

EXPLICATION SIMPLIFIÉE DES OPÉRATIONS FACILITÉES PAR RÉSEAU

Les opérations militaires se caractérisent par leur nature violente, létale, fluide, chaotique et mobile, laquelle est exacerbée par un manque d'informations au sujet de l'espace de combat. C'est ce besoin dominant d'informations qui est resté constant malgré le changement dans la nature de la guerre et qui a inévitablement alimenté la création de réseaux, aussi simples soient-ils, pour accomplir cet échange.

Les êtres humains se sont toujours organisés en réseaux sociaux pour partager l'information entre eux, et ce, dès le moment où ils ont collaboré pour la première fois à l'accomplissement d'une tâche. L'évolution des réseaux humains à partir d'un état circonstanciel et informel, d'abord en réponse au besoin d'échanger des idées, en arrangements pour le commerce et, finalement, en réseaux militaires et

33. Carl Von Clausewitz, *De la guerre*, traduit de l'allemand par le Lieutenant-colonel De Vatry, édition révisée et complétée par Jean-Pierre Baudet, Paris, Éditions Ivrea, 2000.

bureaucratiques officiels, de concert avec l'apparition de l'État-nation, a augmenté l'importance du partage, du stockage et de l'organisation de l'information. En réalité, les demandes faites à l'État pour la défense de ses intérêts nationaux, territoriaux et internationaux ont conduit à l'émergence d'une bureaucratie spécialisée, chargée d'officialiser la pratique systématique des affaires civiles et militaires.

Les réseaux, dans le contexte militaire, ont évolué à partir d'états-majors de campagne constitués temporairement (généralement démantelés ou grandement réduits à la conclusion du conflit) vers une structure d'état-major permanent dont le summum a été celui de l'armée prussienne après la période napoléonienne. La taille grandement accrue des armées de conscrits ou « levées en masse » a entraîné le déploiement d'efforts pour développer et appliquer la gestion scientifique de leurs manœuvres, mouvement, approvisionnement et instruction. À la fin des campagnes napoléoniennes, la plupart des pays européens ont reconnu le besoin de maintenir et de gérer des armées permanentes en temps de paix. C'est ainsi qu'a émergé l'état-major général à titre de manifestation concrète du désir de conserver des réseaux permanents et officiels de personnes, d'informations et de méthodes de transmission. Le fait que la plupart des armées occidentales continuent encore aujourd'hui à avoir besoin d'une structure de commandement et contrôle est la reconnaissance de la nécessité d'un réseau d'information.

Malgré les améliorations substantielles apportées à l'organisation des forces militaires, le contrôle de ces dernières est resté, malgré le passage du temps et jusqu'à très récemment, une activité laborieuse de l'ère industrielle principalement axée sur le processus. Ce qui a changé et ce qui constitue une différence claire par rapport au passé est l'avènement des technologies de l'information et des moyens de communication légers et portables dans l'environnement militaire. Les armées ont mis en service dans l'espace de combat une grande quantité de systèmes d'information, de commandement et de contrôle (SIC2) capables de transmettre, de traiter et de manipuler de vastes quantités de données et de les convertir par l'analyse en informations contextualisées.

La propagation rapide des systèmes d'information portables à tous les niveaux a permis aux commandants et aux états-majors de passer d'un traitement mécanique de l'information (c.-à-d. des calculs arithmétiques simples) à un traitement avancé (c.-à-d. la publication de documents partagés), puis à un traitement automatique (analyse fondée sur des règles) pour arriver à une représentation virtuelle de l'espace de combat. Parallèlement, l'adoption d'une philosophie du commandement de mission au sein de l'Armée canadienne et des armées alliées a renouvelé l'attention portée à l'art de la guerre. Les systèmes de communication de la voix et des données ont bénéficié d'une augmentation de leur portée de transmission et leur capacité

(bande passante). Finalement, l'utilisation accrue des ordinateurs personnels, des jeux vidéo et des téléphones mobiles multifonctionnels a créé une génération de soldats parfaitement à l'aise avec le rythme rapide des changements technologiques. Les commandants, à tous les niveaux, s'attendent à être capables d'exploiter l'information rapidement pour bénéficier d'une meilleure connaissance et compréhension de la situation, et ainsi créer la possibilité de cycles décision-action plus rapides que ceux de l'adversaire. La cohérence de ces attributs a révélé la possibilité de relier ensemble des capteurs, des plates-formes d'armes et les décideurs, rapidement et précisément, sur l'horizon de l'Armée de terre de demain.

Reconnaissant cette application potentielle de la technologie, Cebrowski et Gartska expliquent dans un article fondamental intitulé *Network-Centric Warfare: Its Origin and Future*[34], que l'exploitation de la persistance accrue des liens entre capteurs et plates-formes d'armes va permettre de meilleures communications et un meilleur partage de l'information qui vont se traduire par une souplesse accrue et une meilleure efficacité au combat. Depuis la publication de cet article, la GR a été décrite plus en détail par la Direction des concepts stratégiques (opérations terrestres) (DCSOT) du Canada dans un article intitulé *Towards the Brave New World: Canada's Army in the 21st Century*, et a débouché sur les opérations facilitées par réseau (OFR)[35]. Peu importe le nom qu'on lui donne, la guerre réseaucentrique (GR) s'articule autour des principes suivants :

- Une force bien réseautée favorise un meilleur partage de l'information.
- Le partage de l'information et la collaboration améliorent la qualité de l'information et de la connaissance partagée de la situation.
- La connaissance partagée de la situation habilite la collaboration et l'autosynchronisation[36], et améliore la viabilité et la vitesse du commandement.
- Ces éléments améliorent grandement l'efficacité de la mission[37].

Les avantages clés d'une capacité réseautée, résumés dans la publication interarmées du Royaume-Uni intitulée *Network-Enabled Capability* (JSP 777) sont les suivants :

34. VAdm A.K. Cebrowski et J.H. Garstka, « Network-Centric Warfare: Its Origin and Future. » *Proceedings*, janvier 1998 : p. 139.

35. D'autres termes semblables utilisés par les nations alliées décrivent des concepts semblables ou identiques différenciés jusqu'à un certain point par la technologie, par exemple : Capacité facilitée par réseau (R.-U.), Opérations réseaucentriques (armée américaine), Défense basée sur le réseau (Suède), etc.

36. Alberts et Gartska (1999) : « […] deux entités bien réseautées ou plus, une connaissance partagée de la situation, des règles et une interaction à valeur ajoutée. » Essentiellement, l'autosynchronisation est le fait pour des unités militaires indépendantes d'orchestrer automatiquement leurs actions en fonction de l'intention du commandant plutôt que d'attendre des ordres directs ou des instructions explicites.

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

- **Pleine disponibilité de l'information.** Permet à l'utilisateur de chercher, manipuler et échanger des informations de différentes classifications saisies par toutes les sources internes et externes dans l'espace de combat ou disponibles auprès d'elles.
- **Connaissance partagée de la situation.** Fournit une compréhension et une interprétation partagées de la situation, des intentions des forces amies et des plans d'action possibles par tous les éléments présents dans l'espace de combat.
- **Fonctionnement souple.** Permet aux ressources de se reconfigurer rapidement en fonction des besoins changeants de la mission, ce qui leur permet de travailler ensemble avec un minimum de perturbation et de confusion.
- **Groupes de mission agiles.** Permet la création et la configuration dynamique de groupes de mission qui partagent une même connaissance de la situation et coordonnent et emploient un vaste éventail de systèmes dans le cadre d'une mission particulière. En général, le concept des OAD postule que des groupes spéciaux et adaptables peuvent se constituer en vue d'une mission particulière. Une fois la mission terminée, les membres du groupe retournent à leur organisation d'appartenance. Pour que cette organisation de circonstance performe efficacement, elle doit pouvoir développer et maintenir un haut niveau de connaissance partagée de la situation pour garantir que le groupe a des buts coordonnés et prend des actions synchronisées (effets synchronisés). De plus, si le concept de groupement agile implique l'autonomie (en ce qu'il n'y a pas besoin d'un lien direct avec un commandement central), il est probable qu'une certaine forme de commandement central devra s'exercer, ce qui sous-entend un genre de hiérarchie dans la structure de commandement, en particulier lorsque le groupe réagit à des ordres ou obéit aux règles d'engagement.
- **Effets synchronisés.** Permet au groupe de mission, isolément ou en collaboration avec d'autres groupes de mission, de réaliser des effets écrasants en coordonnant les ressources les mieux adaptées disponibles dans l'espace de combat grâce à une planification et à une exécution distribuées dynamiques.
- **Infrastructure d'information résiliente.** Garantit que les ressources d'information peuvent être gérées et qu'un accès protégé et garanti est offert avec la souplesse nécessaire pour répondre aux besoins de groupes de mission agiles.

➢ **Soutien pleinement réseauté.** Permet l'utilisation immédiate de capacités gouvernementales, industrielles, universitaires et de la fonction publique qui ne se trouvent pas au front pour soutenir les opérations.

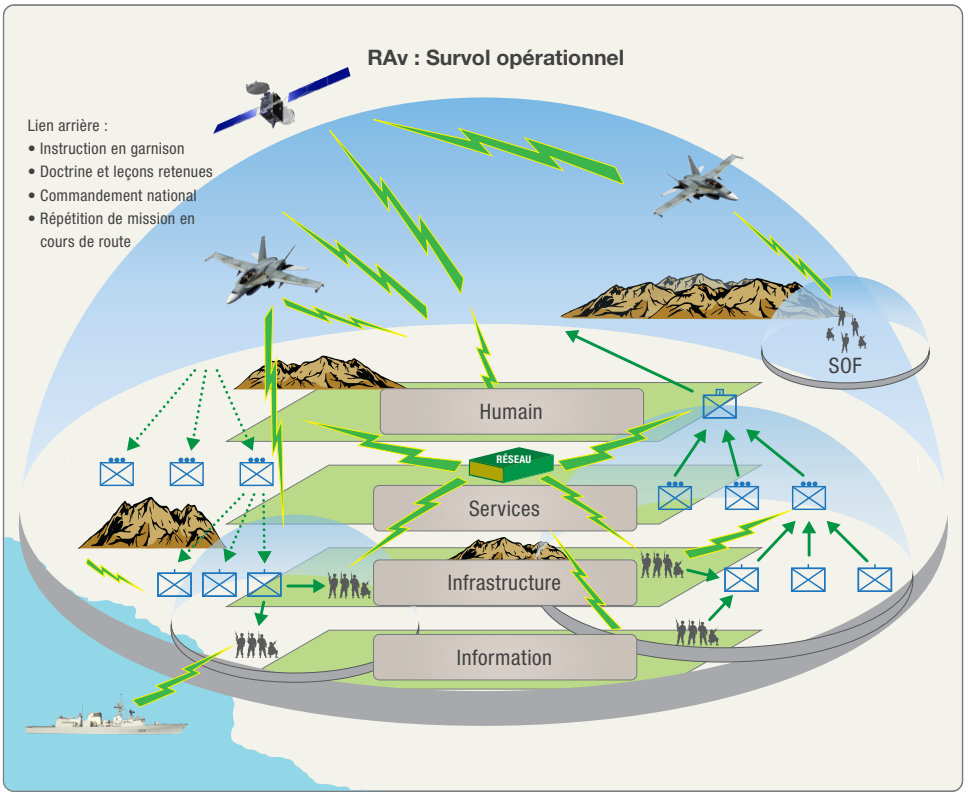

Figure 3 : Survol opérationnel du RAv

Les approches canadiennes aux OFR soulignent que, si le rôle de la technologie dans les OFR est important, la primauté de la doctrine de la guerre de manœuvre avec le commandant humain en son centre ne peut être négligée. Babcock définit les OFR comme suit : « conduite d'opérations militaires caractérisée par une intention commune, une décentralisation des pouvoirs et une information partagée, le tout habilité par une culture, une technologie et des pratiques pertinentes »[38]; pour sa part, l'Armée canadienne (AC) les définit séparément comme suit : « Concept en évolution ayant pour objet d'améliorer la planification et l'exécution des opérations par un partage direct des données, des informations et des technologies des communications

38. S. Babcock, *Canadian Network Enabled Operations Initiatives.*

pour relier des personnes, des processus et des réseaux ad hoc afin de faciliter une interaction efficace et opportune entre les capteurs, les chefs et les effets. »[39] Le RAv, à partir du travail déjà effectué sur les OFR, va exploiter l'information et la technologie pour parvenir à une supériorité sur le plan des décisions plutôt que de se concentrer entièrement sur une solution technologique particulière à appliquer à un problème de commandement et de contrôle[40]. Il doit être absolument clair que si la technologie va jouer un rôle important dans la réalisation d'un réseau de l'avenir, les composantes d'un futur réseau livré à l'Armée canadienne ne peuvent être vues autrement qu'à titre d'éléments habilitants en soutien au commandant humain.

L'Armée canadienne va avoir besoin de chefs qui peuvent s'adapter à des changements rapides et imprévus dans les processus organisationnels, qui sont capables de diriger et de mettre en œuvre des modalités adaptables de commandement et de contrôle, et qui fonctionnent dans une atmosphère qui accepte un niveau de risque plus élevé et l'incertitude. Elle ne peut plus présumer qu'elle va planifier et exécuter des opérations à l'aide d'organisations aux structures homogènes qui lui sont familières. La norme pourrait bien devenir des opérations dans lesquelles des organisations de circonstances se réunissent pour un certain temps en vue d'une opération puis, une fois la tâche terminée, se dissocient pour repasser sous les ordres d'une formation supérieure.

En résumé, les opérations réseaucentriques se caractérisent par un partage de l'information entre de multiples niveaux de commandement et de contrôle établis. Les clés de l'efficacité du RAv seront une adhésion large et complète à la philosophie du commandement de mission, l'abandon du développement de nouvelles plates-formes en isolation, des pratiques et procédures de commandement et contrôle révisées, et une doctrine et instruction mises à niveau qui vont éloigner l'Armée canadienne d'une culture d'» accès sélectif à l'information » pour la rapprocher d'une culture de « mise en commun de l'information »[41]. Cette transformation, combinée à un haut degré de disponibilité de l'information sur le statut et la disposition des forces amies et ennemies, et sur tout autre aspect pertinent de l'environnement opérationnel, sera un multiplicateur de la force pour l'Armée de terre de demain (ATdD).

39. Répertoire de terminologie de l'Armée de terre : définition adoptée pour le commandant de l'Armée canadienne et en vue de l'approbation du Système de doctrine et d'instruction de la Force terrestre (SDIFT), 17 mai 2006.

40. CANADA, *Command Domain Capability Alternative Report 2008*, Chef du développement des Forces (CDF).

41. *Les opérations terrestres 2021 : opérations adaptables et dispersées*, p. 26.

OPPORTUNITÉS ET RISQUES

Sans surprise, lorsqu'on examine le potentiel associé à la mise en œuvre de nouvelles capacités réseautées, il y aura des opportunités à saisir et des risques à éviter. La section qui suit souligne certaines de ces opportunités et met en garde contre certains risques qu'il ne faudrait pas négliger.

Opportunités

- **Cohérence**. Historiquement, les composantes réseau de l'AC ont toujours été conçues, développées, fabriquées et livrées de façon asymétrique avec une piètre coordination entre les bureaux de projet. C'est ainsi que l'Armée de terre prend livraison de capteurs, de plates-formes et d'applications mal intégrées qui exigent un soutien considérable pour parvenir ne serait-ce qu'à un partage minimal de l'information. Il existe donc une belle occasion d'apporter un peu de cohérence au développement des composantes réseau de l'AC, idéalement par la promulgation d'une stratégie de C4ISR[42] exhaustive pour l'Armée canadienne. Cette stratégie décrirait des buts stratégiques, définirait de grands objectifs de capacité à l'aulne desquels les achats d'équipement particuliers pourraient être mesurés et permettrait à l'AC de livrer des capacités progressivement dans le temps.
- **Culture**. Il existe une belle occasion de socialiser l'Armée canadienne et d'influencer sa culture en faveur de l'acceptation des capacités réseautées. L'AC devrait mettre en œuvre un plan délibéré pour mettre en service progressivement certaines composantes d'un futur réseau bien à l'avance de la capacité opérationnelle totale (COT) prévue. Comme il est probable que les composantes du RAv seront développées et livrées progressivement, les chefs de l'Armée de terre doivent s'assurer avec grand soin que la *gestion des attentes* est soigneusement façonnée pour faire comprendre aux chefs que les apports de technologies sont un processus de développement et d'évolution en spirale qui n'entraîne pas la livraison d'un ensemble complet, mais qu'il s'agit plutôt d'un processus géré de mise en œuvre successive de capacités qui va mener à un réseau de l'avenir.
- **Commandement et contrôle**. Une capacité réseautée présente de nouvelles occasions de réviser les processus de commandement et contrôle,

42. Stratégie publiée par la Direction commandement et information (terre) en 2011.

en particulier le processus de planification opérationnelle (PPO). Avec l'augmentation de la quantité et de la qualité des informations et l'adjonction d'outils d'analyse puissants, la valeur associée à l'affectation de ressources d'état-major pour la planification (laquelle consiste essentiellement en une anticipation en l'absence d'informations) pourrait diminuer. À la place, la capacité des commandants et états-majors de réagir rapidement et de s'adapter à une information analysée, avec l'aide de l'intelligence artificielle, pourrait devenir une fonction plus souhaitable en remplacement d'un processus de planification mécaniste. Michael Schrage souligne que : « une autre conséquence perverse de l'argument RAM/réseaucentrique est que l'investissement en souplesse procure un rendement disproportionnellement supérieur à l'investissement dans la planification. Cela signifie que les exercices d'instruction et les expériences devraient logiquement se concentrer moins sur des plans d'attaque exhaustifs et plus sur la capacité de réagir avec souplesse aux événements imprévus et non planifiés. »[43] Il y a également la possibilité d'examiner ce que signifie « contrôle » dans l'expression commandement et contrôle. Le contrôle, en tant qu'élément de C2, pourrait bien ne plus suffire comme terme à utiliser dans l'environnement hautement variable et complexe envisagé dans le concept des OAD. Comme l'a conclu Czarnecki[44] « il est temps d'abandonner ce terme, avec tout ce qu'il sous-entend, du moins dans le contexte des arts militaires. » À la place, si on veut conserver l'abréviation C2, le deuxième C devrait désigner « coordination » ou « collaboration ». Alberts[45] va encore plus loin en affirmant que le langage du commandement et contrôle n'est peut-être pas suffisant pour habiliter *la prise de décisions complexes*. Dans un article récent, il propose que les termes « agilité », « focus » et « convergence » pourraient remplacer l'expression « commandement et contrôle », et par là solliciter de nouvelles approches de réflexion au sujet du C2 en supprimant « l'héritage restrictif des termes utilisés et de leur connotation ». Il est certes souhaitable d'examiner le paradigme de résolution de problèmes de notre processus actuel de C2 pour voir s'il est suffisamment adaptable aux environnements changeant rapidement et si le processus même, dans sa forme actuelle, empêche les commandants

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

44. J. Czarnecki Ph. D., *The Failed Thermostat: The Illusion of Control in an Information Rich Age.*

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

et états-majors d'envisager les complexités d'un problème en tant que système à comprendre, dans un contexte d'intérêts en concurrence.

- **Interopérabilité**. Il existe de belles occasions de réaliser l'interopérabilité, non seulement entre l'Armée canadienne et les FC, mais également entre les réseaux au sein de la coalition. Au gré de la coalescence de la technologie autour des normes commerciales, on peut raisonnablement s'attendre à ce que l'interopérabilité soit plus facile à établir, en particulier dans la sphère des services communs[46]. Néanmoins, l'interopérabilité des données et des méthodes d'échange va continuer d'être problématique, car il reste d'importants ensembles d'équipement et de capteurs militaires qui utilisent des modèles de données propriétaires et des méthodes d'échange incohérentes ou incompatibles[47].
- **Coûts/maintien en puissance**. Il existe des occasions[48] de réduire les coûts globaux de la mise en œuvre du RAv dans les domaines de la gestion de projet, du maintien en puissance et de l'instruction.

Risques

Au moment où l'Armée canadienne s'embarque dans la mise en œuvre des concepts présentés dans *Opérations terrestres 2021*, et en particulier le RAv, il faut reconnaître qu'il y aura des risques inhérents à l'évolution vers une Armée canadienne habilitée par réseau. Dans le contexte du développement et de la mise en œuvre d'une force réseautée, il faut prendre acte de ces risques et ne pas présumer qu'ils vont disparaître d'eux-mêmes par magie.

Le premier risque est celui lié à la prémisse[49]. Les tenants des concepts comme les OFR, la GR, etc. affirment que les forces réseautées seront plus efficaces, jouiront d'une plus grande rapidité de commandement et réaliseront une autosynchronisation. Cette prémisse repose sur la capacité de transmettre et de traiter d'immenses quantités de données et de les transformer en informations utilisables. Cependant, des décisions plus rapides, fondées sur de plus grands volumes d'informations,

46. Par exemple, certains services ont adopté des normes communes, en autres le courriel (SMTP), le clavardage (JFIRE) et les couches de transport (TCP/IP), etc.

47. Par exemple, il existe plusieurs protocoles d'échange distincts qui ne sont pas interopérables entre eux, notamment Tactical Data Links (TADL), ADatP3 et VMF.

48. Par exemple, le projet de RAv omnibus soutenu par Industrie Canada dans le cadre duquel des vendeurs en concurrence sont encouragés, grâce à une compétition et une expérimentation ouvertes, à identifier et mettre en œuvre rapidement des capacités. Les vendeurs gagnants pourraient se faire concurrence et se qualifier pour des tranches de financement conditionnelles à une rétroaction positive des utilisateurs.

49. Certains critiques vont plus loin et suggèrent que la prémisse fondamentale de la théorie de la guerre réseaucentrique de Cebrowski et de Gartska est peut-être incomplète, au mieux, ou entièrement erronée, dans le pire des cas (Giffin/Reid)

ne signifient pas nécessairement de meilleures décisions. Or, comme Van Creveld l'a mentionné dans *Command in War*[50], plus on en sait, moins on est certain de ce qu'on comprend. Comme l'a également signalé Malcolm Gladwell[51], les résultats du plus grand exercice[52] singulier conçu pour vérifier cette prémisse ont révélé que les commandants « se gorgeaient d'informations [...]. Des experts de tous les domaines concevables du gouvernement des É.-U. étaient à leur service […]. Lorsque les tirs commençaient, toute cette information devenait un fardeau ». Il n'est pas non plus certain que l'autosynchronisation est nécessairement considérée par tous les services comme un objectif bien compris et également souhaitable. En particulier, les forces aériennes et maritimes, à cause de leur concentration principalement sur des objectifs stratégiques, pourraient prétendre qu'une méthode décentralisée de prise de décisions articulée autour de l'environnement terrestre et visant à réaliser *l'intention* du commandant est, dans sa forme la plus fondamentale, inadaptée à la majorité de leurs opérations, dans lesquelles l'attribution de ressources rares (avions et navires) exige une méthode de commandement et de contrôle directive plus traditionnelle, de haut en bas. Il serait difficile d'être à l'aise avec une méthode de commandement et contrôle qui, par exemple, conditionnerait la décision de lancer une arme nucléaire à la simple « compréhension » de l'intention du commandant. Des modalités beaucoup plus détaillées et directives seraient probablement avisées en l'occurrence. Les théories des opérations facilitées par réseau ont tendance à négliger les aspects sociaux et culturels (leadership, présence, etc.) du commandement pour se concentrer plutôt sur les promesses de la technologie. Finalement, les partisans de la réseaucentricité aiment à invoquer l'argument de la « sagesse des foules »[53], en affirmant que les foules réseautées sont meilleures pour résoudre les problèmes, favoriser l'innovation, prendre des décisions avisées et même prédire l'avenir que (présumément) les organisations hiérarchiques traditionnelles. Cette sagesse des foules n'est peut-être, au mieux, rien de plus qu'un large échantillonnage d'opinions qui trouve inévitablement consensus dans le plus bas dénominateur commun. Si cette approche est suffisante pour corriger une lacune dans une stratégie de marketing, comme méthode d'organisation de la guerre, elle est tout à fait inacceptable. Les dangers inhérents à la « sagesse des foules » ont été répertoriés et expliqués par Norman Dixon[54] comme suit :

50. M. Van Creveld, *Command in War.*
51. M. Gladwell, *Intuition : comment réfléchir sans y penser?*
52. US Joint Forces Command (JFCOM) Exercise Millennium Challenge 2002.
53. J. Surowiecki, *La sagesse des foules.*
54. N. Dixon, *De l'incompétence militaire : un essai psychologique*, p. 337.

- Une *illusion d'invulnérabilité* partagée par la plupart des membres du groupe.
- *Des tentatives collectives d'ignorer les éléments d'information ou d'en faire abstraction par le raisonnement*, qui sont susceptibles d'amener le groupe à reconsidérer des hypothèses préférées, mais déficientes.
- Une *croyance inconditionnelle dans la moralité inhérente du groupe*, qui permet aux membres de ne pas tenir compte des conséquences éthiques de leurs décisions.
- *Une vision stéréotypée de l'ennemi* le représentant comme trop diabolique pour la négociation ou trop stupide et incapable peut constituer une menace.
- Une *illusion commune d'unanimité* à l'égard d'un point de vue partagé par la majorité, renforcée par la perception fausse que le silence est synonyme de consentement.
- *Des gardiens autodésignés de la conformité* pour protéger le groupe des informations adverses susceptibles de perturber sa complaisance au sujet de l'efficacité et de la moralité de ses décisions. [*traduction*]

Avant d'investir des ressources considérables pour acquérir des dispositifs réseautés encore plus complexes, il vaut la peine de vérifier si les principes de la guerre réseaucentrique résistent ou non à la critique. Giffin et Reid[55] proposent un excellent résumé de cette critique qui mérite d'être répété en détail ici :

- « *Une force dotée d'un bon réseau jouit d'un partage amélioré de l'information.* Ce n'est pas le réseau, ni sa qualité qui déterminent la qualité du partage de l'information. Ce qui compte, c'est la nature de nos processus de réflexion, nos attitudes envers l'information à laquelle nous pouvons théoriquement avoir accès, la situation dans laquelle nous nous trouvons et nos besoins d'informations. Citons ici un exemple contraire : lorsqu'un élément de données particulier répond à nos besoins, l'accès à un téraoctet de données dont nous n'avons pas besoin n'apporte aucune amélioration significative. »
- « *Le partage de l'information et la collaboration améliorent la qualité de l'information et de la connaissance partagée de la situation.* Par « qualité de l'information », ce principe doit vouloir sous-entendre quelque chose comme « information véridique et complète ». Par « qualité de la connaissance partagée de la situation », il doit vouloir sous-entendre quelque chose comme « une compréhension véridique, complète et exacte de la situation partagée par plus d'un observateur ». Si l'inductivisme est

55. R. Giffin, et D. Reid, *A Woven Web of Guesses*, Canto Two, p. 17.

la méthodologie selon laquelle on est supposé parvenir à ces états, ce principe devient intenable, car l'inductivisme n'offre pas un tel moyen. Outre les arguments déjà présentés, il vaut la peine de signaler que les inférences inductives ne sont pas nécessairement des inférences au sens logique; autrement dit, *il est logiquement possible de tirer des conclusions divergentes à partir du même corpus de faits observés*. Donc, il est parfaitement raisonnable pour différents observateurs de tirer des conclusions différentes à partir de l'observation du même corpus de faits et rien dans la logique inductive ne peut empêcher ce résultat ou justifier ce principe. *Il doit revenir à ses tenants de décrire la méthode précise par laquelle la certitude, l'intégralité et la communauté implicites sont obtenues. En attendant, cette affirmation ne peut être acceptée*. Nous affirmons que ce principe est dangereux du point de vue du bon sens. Nous pouvons partager l'information et collaborer tant que nous le voudrons. Nous pouvons arriver à un accord parfaitement harmonieux à tous égards. Mais nous pouvons quand même avoir totalement tort. L'histoire est pleine d'exemples de ce phénomène. Le catalogue des plans militaires ayant échoué est volumineux. Le consensus et la vérité ne sont pas synonymes.

- « *La connaissance partagée de la situation habilite l'autosynchronisation.* La connaissance partagée de la situation n'est ni suffisante ni nécessaire comme condition pour le comportement décrit comme autosynchronisation; deux acteurs ayant une compréhension parfaitement harmonieuse de la situation pourraient théoriquement agir en contradiction l'un avec l'autre par suite, par exemple, d'intérêts et d'intentions personnels divergents. À l'inverse, deux acteurs peuvent être en désaccord total au sujet de la nature de la situation, mais quand même travailler ensemble sans y être forcés par une autorité supérieure, et ce, en raison de leur ouverture d'esprit ou de leur intention commune. *Ce n'est pas l'homogénéité impérieuse, mais la gestion de l'inévitable et probablement bénéfique diversité intrinsèque au champ de bataille qui constitue le défi le plus fondamental et important du commandement.* »
- « *Ces progrès, à leur tour, améliorent grandement l'efficacité de la mission.* Nous sommes tout à fait d'accord avec les tenants de la thèse de la GR selon laquelle les progrès récents dans les domaines des technologies des communications et de l'information ont grandement amélioré et vont continuer d'améliorer les capacités militaires. Nous sommes également

d'accord que ces progrès constituent un argument irréfutable en faveur du changement organisationnel, matériel, doctrinal et comportemental. Mais, pour les raisons évoquées ci-dessus, nous ne pouvons admettre que les trois principes précédents justifient l'affirmation finale. »

Si on ne les examine pas, les lacunes des prémisses de la réseaucentricité risquent de miner la mise en œuvre réussie de la capacité réseau. Des efforts considérables devraient être déployés pour vérifier qui consomme l'information dans le domaine militaire, comment cette information est consommée et à quelles fins, sinon nous risquons d'échafauder un édifice de composantes réseautées très efficaces pour recueillir et diffuser de l'information, mais entièrement inadéquates pour aider les humains à en comprendre le sens.

Instruction. Deux problèmes liés à l'instruction sont appréhendés dans la mise en œuvre des capacités réseautées, en particulier (1) le risque de dégradation des compétences de base du soldat et (2) les demandes cognitives associées à l'adoption d'une nouvelle technologie. La nécessité de donner une formation sur un plus large éventail de nouvelles technologies, combinée aux ressources limitées consacrées à l'instruction individuelle et collective, pourrait nuire à la rétention des compétences de base du soldat. Il y a également le risque que, avec la prolifération des dispositifs réseautés, certaines dépendances se développent de telle manière que, en l'absence du réseau, certaines compétences communes du soldat pourraient disparaître entièrement. Par exemple, avec la mise en service et l'utilisation répandue des technologies du GPS portatif, la capacité des soldats de s'orienter efficacement à l'aide d'une boussole et d'une carte pourrait être menacée. De la même manière, au fur et à mesure que les plates-formes d'armes deviennent semi-autonomes, les compétences comme le ciblage manuel des missions d'artillerie pourraient se dégrader et même disparaître entièrement. Il faudra un effort concerté pour conserver les capacités de base au sein de l'Armée canadienne de manière que, advenant l'indisponibilité du réseau, l'Armée puisse continuer à exécuter les tâches assignées. En outre, avec la prolifération des ordinateurs personnels, des consoles de jeux et de l'accès Internet haute vitesse, et avec l'exposition permanente aux technologies commerciales, les soldats ont des attentes élevées en ce qui concerne la fiabilité et la performance des composantes du RAv. Ils vont s'attendre à une fonctionnalité prête à utiliser, facile d'utilisation et jouissant d'un soutien technique immédiat. Il y aura très peu de tolérance pour les technologies perçues comme laborieuses, redondantes et non intuitives. En réalité, il est probable que toute composante du RAv qui n'offre pas des améliorations claires et immédiates dans l'exécution du travail va être rejetée du revers de la main. Il faudra consacrer beaucoup d'efforts pour s'assurer que les soldats

subissent peu de frustrations[56] et investissent peu d'efforts[57]. L'AC pourrait souhaiter examiner les occasions d'autoapprentissage[58] et de tests bêta[59] comme moyens de réduire les frais d'instruction associés à la mise en service d'un large éventail de composantes du RAv. Avec l'accroissement du volume des données, il faudra investir beaucoup d'efforts pour concevoir des interfaces utilisateur adaptables et simples, et pour tester les composantes du RAv afin de s'assurer que les utilisateurs pourront trouver facilement l'information dont ils ont besoin tout en gardant les pointages de frustration et d'effort à un niveau minimal. Warne et al[60] énumèrent des compétences particulières qui seraient vitales pour le succès des OFR, à savoir :

- Compréhension de ce que les systèmes mis en service peuvent accomplir.
- Liberté de prendre des risques, d'innover et d'apprendre.
- Capacité d'interpréter la situation et de prendre des décisions à partir de données incomplètes.
- Capacité de gérer la surcharge d'informations.
- Capacité d'absorber des quantités substantielles d'informations et de discerner ce qui est le plus important.

Dépendance et contrôle du réseau. Il est possible que les commandants et états-majors en viennent à se fier à la disponibilité générale de capacités réseautées, ce qui aurait pour effet de créer une vulnérabilité importante en cas de perte catastrophique du réseau. À cet égard, l'Armée de terre va devoir identifier un ensemble minimal d'outils réseau, ou un sous-ensemble du réseau « à l'épreuve des pannes »[61], qui doit posséder un haut degré de survivabilité. Un risque connexe déjà largement reconnu au sein des forces militaires occidentales est la crainte que les capacités réseautées permettent ou même encouragent les commandants supérieurs à faire la microgestion des activités de leurs subordonnés. Le réseau « d'information de tous les destinataires » offrant une fenêtre détaillée à chaque niveau comporte la possibilité que les commandants qui n'ont pas suffisamment confiance en leurs subordonnés vont souhaiter avoir la possibilité de voir l'évolution du combat à

56. Pointage de frustration – réalisé lorsque les soldats sont exposés à des produits dont le développement technologique ou la performance sont inégaux.

57. Pointage d'effort – affiché lorsque les produits fonctionnent, mais sont considérés comme difficiles ou lents à utiliser.

58. Les occasions d'autoapprentissage pourraient inclure la création de didacticiels sous forme de jeux, peut-être configurés dans un domaine multiutilisateurs dans lequel plusieurs utilisateurs se familiarisent avec des composantes du système dans un environnement de jeu. Un avantage secondaire serait de créer ou d'encourager la création d'une communauté de testeurs bêta parmi les soldats de l'Armée canadienne.

59. Des versions du logiciel, connues sous le nom de versions bêta, sont communiquées à un groupe limité à l'extérieur de l'équipe de programmation. Le logiciel est ainsi confié à des groupes de personnes pour des tests subséquents visant à s'assurer que le produit est exempt de défaut ou de bogues. (www.wikipedi.org // chercher « bêta test »)

60. DSTO 2004, *The Network Centric Warrior.*

61. Une capacité à l'épreuve des pannes sous-entend un degré élevé de disponibilité, qui peut se traduire par des coûts accrus liés au renforcement et à la protection, à des chemins redondants, etc. Il va falloir examiner attentivement ce qui constitue exactement une composante/capacité à l'épreuve des pannes au sein d'un réseau afin d'en évaluer les coûts et la complexité.

travers la lunette du fantassin, pour ainsi dire. Si l'inclusion d'agents de prédiction intelligents et d'outils connexes dans le RAv pouvait aider à anticiper les futurs plans d'action de la menace, avant et pendant les engagements, ce ne sont pas tous les utilisateurs qui vont être à l'aise avec l'aura de certitude implicite dans le terme « prédiction ». *Une adhésion ferme et sans compromis à la philosophie du commandement de mission* dans la doctrine, l'instruction et la conception du réseau sera nécessaire pour atténuer ce risque.

Forces de la menace. Il a été démontré à maintes reprises que les progrès dans la technologie militaire restent rarement entre les mains de la puissance dominante pour très longtemps. Les forces du marché vont se combiner pour réduire les coûts d'acquisition de capacités réseau par les forces de la menace. La documentation de source ouverte va permettre aux adversaires d'exploiter une bonne part du travail accompli par les efforts de transformation des alliés. En outre, on s'attend à ce que les forces de la menace soient non seulement très adaptables, utilisant les technologies commerciales dans leurs propres réseaux, mais à ce que les types de réseaux sociaux et relationnels qu'ils utilisent fonctionnent probablement en deçà des seuils de détection de beaucoup des capteurs à la disposition de l'AC. Dans les conflits de l'avenir, le recours par l'ennemi à des attaques asymétriques et l'importance de l'interaction humaine et des contacts sociaux, ainsi que de l'improvisation, de l'endurance, de l'engagement et de la confiance pourraient bien rendre non pertinentes les capacités technologiques offertes par le réseau. De plus, beaucoup d'efforts technologiques à l'appui des opérations facilitées par réseau ont été consacrés à des capteurs électro-optiques plus évolués qui, s'ils sont très efficaces pour discerner les plates-formes de la menace en vue d'engagements à l'aide des armes, ne semblent pas être optimisés pour détecter les forces de la menace mêlées à la population civile locale. La dépendance aux capteurs et plates-formes d'armes réseautés pourrait bien exposer l'Armée de terre de demain (ATdD) à des attaques de réseau informatique sophistiquées provenant d'organisations criminelles opportunistes et de tierces parties cherchant à faire des expériences contre notre réseau (pirates, etc.) ou même de sympathisants de l'ennemi ayant accès à la plus récente technologie. Autrement dit, les OFR et la GR pourraient très bien optimiser la capacité de l'Armée canadienne d'opérer contre des entités de même nature ou presque, mais ne seront peut-être pas aussi efficaces contre une menace asymétrique. Les efforts possibles d'atténuation du risque pourraient inclure la création « *d'équipes rouges* » multidisciplinaires permanentes chargées d'inventer des contre-mesures face à une force réseautée et l'inclusion de leur analyse dans les simulations d'exercice[62].

62. *Les opérations terrestres en 2021 : un concept en devenir : études à l'appui*, chap. 7 (Terfry), p. 7-11.

Coûts/viabilité. Un risque potentiel qui devrait faire l'objet d'une attention particulière de la part d'une force aux ressources limitées est celui lié aux coûts et la viabilité du développement, de la fabrication et de l'institutionnalisation d'un réseau de l'avenir. Avec l'évolution de la technologie, il est possible que les coûts globaux augmentent au gré du nombre de plates-formes devenant « sensibles » au réseau. Ce facteur, combiné au besoin que le réseau soit disponible et fiable dans tous les environnements, risque aussi d'exercer une pression considérable sur les coûts de développement des composantes réseautées. L'adoption de normes du commerce, notamment les produits disponibles sur le marché, pourrait réduire les coûts; cependant, la nécessité d'intégrer des politiques de sécurité militaire dans les produits commerciaux va exiger des efforts et des ressources supplémentaires. En présumant que la gestion de l'ensemble du parc va continuer d'exister comme méthode de maintien en puissance, un modèle dans lequel de multiples versions de capacité (VC) exigent un soutien simultané pourrait miner la capacité des FC et de l'AC de maintenir en puissance la capacité réseau dans les établissements d'instruction et dans les opérations de déploiement.

Capacité et rendement de la bande passante d'infrastructure. Lorsque l'AC va adopter une infrastructure de communication en réseau avec capteurs, armes et commandants interconnectés, la demande de quantités de plus en plus grandes d'informations va continuer de progresser, ce qui va exercer une pression sur la capacité du réseau de transmettre, recevoir et stocker toute cette information. La performance d'un réseau est liée au nombre optimal d'utilisateurs et de nœuds, mais il est difficile de préciser exactement ce nombre à l'avance et encore plus difficile d'empêcher ce nombre d'augmenter au-delà de son niveau optimal. Par exemple, le phénomène de la dégradation du réseau est de plus en plus reconnu. Au gré de l'augmentation du nombre de nœuds dans un réseau, il est possible que la dégradation du réseau en raison des retards, de la perte de paquets de données et de la gigue de paquets[63] – ou retard variable des paquets – affecte le rendement du réseau de manières totalement imprévisibles. Ainsi, au gré de l'évolution de la conception du RAv et de ses nœuds constitutifs, il va falloir porter une attention considérable aux caractéristiques comme la redondance, le cheminement intelligent, etc.

Malgré les risques décrits ci-dessus, chacun d'eux peut être atténué en portant une attention particulière à l'identification et à la protection des services réseau

63. M.A. Miller, *Do You Hear What I Hear? – Part II: Defining Key Transmission Impairments*. (http://www.voipplanet.com/backgrounders/article.php/3517541) Dans le protocole Voix par IP (VoIP), le traitement automatique de la voix peut être affecté par des phénomènes comme la gigue de paquets, laquelle se manifeste par une variation dans la vitesse d'arrivée des divers paquets. Comme chaque paquet peut (théoriquement) suivre un chemin unique, il est possible que le retard entre les paquets successifs varie. En d'autres mots, les paquets nos 1 et 2 peuvent arriver à 30 millisecondes d'écart, tandis que les paquets 2 et 3 peuvent arriver à 40 millisecondes d'écart parce que le paquet 3 a suivi un chemin différent des deux premiers. Une gigue de paquets excessive complique le processus de réassemblage des paquets, lequel doit reconstituer le signal vocal au point d'arrivée comme un signal continu d'informations.

essentiels, à l'instruction et à l'expérimentation, ainsi qu'à un engagement en faveur du développement des technologies de soutien connexes.

QU'EST-CE QU'UN RÉSEAU?

Une bonne part de la documentation sur les opérations facilitées par réseau ou la guerre réseaucentrique suppose que le lecteur connaît la terminologie et présume donc que ces expressions sont comprises. Un malentendu sur ce qu'est un réseau a créé une tendance prononcée au sein de l'Armée de terre à immédiatement penser que les réseaux sont simplement affaire de matériel et de communications, et relèvent donc du service des transmissions. Cette tendance a engendré une certaine confusion quant à ce qu'on entend vraiment par réseau, opérations facilitées par réseau, etc. Il est donc justifié à ce stade-ci de proposer une courte et nécessairement imparfaite description de travail de ce que sont un réseau et ses composantes.

À condition de comprendre ce qui constitue un réseau, ses éléments génériques et leurs propriétés, ainsi que les types d'informations à échanger, le processus de développement des capacités pourra passer de la conceptualisation à un niveau de conception plus détaillé et, en fin de compte, à la construction et à la gestion d'un RAv. Dans sa forme la plus simple, un réseau est simplement une entité ou un *nœud*[64] (humain ou non) *relié*[65] en vue d'interagir avec une autre entité ou un autre nœud. Donc, pour qu'on puisse parler d'un réseau, il doit y avoir des entités (ou nœuds), un moyen de communication et une interaction compréhensible ou mesurable. Par exemple, deux êtres humains (entités/nœuds) qui se parlent (moyen de communication : cordes vocales combinées à une interaction mesurable : langue/grammaire) constituent un réseau dans sa forme la plus élémentaire. Pareillement, lorsqu'un aéronef piloté avec ses armes, capteurs et moyens de communication établit la liaison avec une station terrestre et un marqueur d'objectif, on obtient un nœud plus complexe composé, dans cet exemple, de nombreux nœuds interconnectés. Cependant, peu importe leur niveau de complexité, tous ces exemples correspondent à la définition de réseau donnée ci-dessus.

À partir de cette définition, on peut préciser les composantes d'un réseau, les classer et déterminer leurs fonctions et leurs propriétés. Précisons que les

64. « Les nœuds sont les éléments d'un processus qui correspondent à des décideurs, des capteurs, des facteurs d'influence ou des cibles. Par définition, les capteurs reçoivent des phénomènes observables d'autres nœuds et les transmettent aux décideurs. Les décideurs reçoivent des informations des capteurs et prennent des décisions au sujet de la disposition actuelle et future d'autres nœuds. Les facteurs d'influence reçoivent des directives des décideurs et interagissent avec d'autres nœuds pour modifier l'état de ces nœuds. Une cible est un nœud ayant une certaine valeur militaire, mais qui n'est pas un capteur, ni un décideur, ni un facteur d'influence. » (Tiré de J.R. Cares, *An Information Age Combat Model*, p. 6.)

65. Un lien est « un phénomène observable produit par un nœud et détecté par un capteur. Par exemple, les phénomènes détectés par les capteurs et communiqués aux décideurs, ou les décideurs qui donnent des ordres aux nœuds et aux facteurs d'influence, généralement dans le but de détruire d'autres nœuds ou de les rendre inutilisables – constituent des liens ». Paraphrase d'un extrait de J.R. Cares, *An Information Age Combat Model*, p. 7.

composantes et leurs propriétés évoquées dans les sections qui suivent sont de nature conceptuelle[66]. Ces types de réseaux et leurs fonctions existent sans égard à la technologie disponible maintenant et qui le sera à l'avenir, et servent de cadre par rapport auquel toutes les composantes potentielles du RAv pourront être évaluées.

Heureusement, il existe deux excellents documents qui présentent des descriptions détaillées des composantes d'un réseau. Le premier, *An Information Age Combat Model*[67], résume tous les réseaux à quatre nœuds : décideurs, capteurs, facteurs d'influence et cibles, chacun possédant deux propriétés fondamentales, un « côté » (bleu/rouge/ami/ennemi, etc.) et la propriété d'être « contracté » c'est-à-dire que les fonctions de plus d'un nœud peuvent se retrouver dans un plus petit nombre de nœuds. Les abonnés utilisent des liens entre les nœuds pour recevoir et transmettre des informations et des données, dont le type et la complexité dépendent de la nature du réseau et des besoins d'autres participants du réseau. À souligner que ce modèle, en désignant le destinataire d'informations comme un type de nœud « cible », permet à un cadre de modeler les effets du réseau (en particulier les activités d'influence) sur les nœuds amis, neutres **et** adversaires. Le modèle de Cares possède des avantages, principalement celui de sa capacité de représentation mathématique des réseaux. Cependant, sa représentation des types de nœuds est peut-être trop simplifiée aux fins de la présente étude.

Le deuxième document intéressant, *Netforce Principles*[68], propose six types de nœuds caractérisés par les *actions* qu'ils exécutent (collecteurs, fournisseurs d'informations, décideurs, exécutants, communicateurs et éléments de soutien) combinés à une ou plusieurs *propriétés* (identité, statut, capacité, structure, contrôle, sécurité, intégration et interaction) pour créer un ensemble complexe de capacités réseau. Avec l'une ou l'autre définition, il est possible de définir et de comprendre ce qu'est un réseau. Cependant, Keus offre plus de précisions et s'appuie sur des concepts opérationnels, c'est pourquoi la présente étude va adopter la terminologie de Netforce. Par conséquent, la section qui suit s'inspire fortement du modèle de Keus.

Nœuds et types de nœuds. Un *nœud* est une entité qui exécute une ou plusieurs actions et peut interagir avec d'autres nœuds. Un type de nœud est une caractérisation d'un nœud selon son action principale. Dans les réseaux militaires, les composantes doivent pouvoir (1) collecter, traiter et interpréter les données et l'information (jusqu'à maintenant, l'interprétation relève en grande partie de l'être

66. Contrairement aux définitions très précises que l'on retrouve par exemple dans le modèle de réseautage informatique Interconnexion de systèmes ouverts (OSI).

67. J.R. Cares, *An Information Age Combat Model*.

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

humain), (2) fournir des informations de qualité aux décideurs, (3) habiliter les décideurs à coopérer et à créer des mesures et (4) fournir la capacité d'exécuter les mesures en question. Par exemple, en se fondant sur le modèle de Keus, on pourrait classer l'être humain comme un nœud, tandis que le commandant, en raison de ses actions, est un « type de nœud », notamment le décideur. En outre, le type de nœud que constitue le commandant humain peut également posséder certaines propriétés, notamment l'identité (Smith), le statut (formé/actif/opérationnel, etc.), une structure (commandant de compagnie), etc. En réalité, le modèle fonctionnel proposé par Keus s'applique à n'importe quel type de réseau, qu'il se compose entièrement d'êtres humains, de machines ou d'une combinaison des deux.

- Les nœuds collecteurs rassemblent des données et des informations passivement, activement ou par une combinaison de ces deux modes. Un nœud de collecte pourrait être un capteur (radar, MET, etc.) ou un agent de collecte de données, p. ex. un programme d'exploitation des données. Les comportements de ces nœuds peuvent être définis et contrôlés.
- Les nœuds fournisseurs d'informations traitent, interprètent, corrèlent, fusionnent et fournissent l'information dans le format voulu au demandeur. Ces nœuds remplissent les fonctions de traitement, fusion, interprétation et administration des données de connaissance de la situation. « Dans une architecture optimale (RAv), le nœud fournisseur d'informations devrait idéalement être réparti de manière à combler les besoins d'informations (vitesse, latence, précision, niveau de détail, format, etc.) des décideurs »[69].
- Les décideurs traitent l'information afin de choisir les plans d'action possibles. La responsabilité et l'imputabilité résident dans ces nœuds.
- Les nœuds exécutants sont les entités qui changent l'état des cibles (par exemple, un changement de comportement ou un changement d'état physique). Ainsi, un exécutant pourrait être létal (un obus d'artillerie) ou non létal (un produit d'OPSPSY).
- Les nœuds communicateurs transportent les données d'un endroit à l'autre. Dans leur forme la plus simple, les nœuds de communication reçoivent et transmettent les données, sans interagir avec elles. Les nœuds communicateurs comportent des mécanismes de sécurité.
- Les nœuds de soutien remplissent les fonctions de gestion de nœuds, de gestion des données et de gestion de la sécurité.

69. *Ibid.*, p. 13.

Divers types de nœuds peuvent ensuite être combinés pour remplir des fonctions multiples et, ainsi groupés, peuvent être constitués en sous-réseaux ou en réseaux enclavés, optimisés pour remplir des tâches particulières par exemple le contrôle du réseau. Une fédération de sous-réseaux ou d'enclaves peut également permettre la création d'équipes virtuelles, peut-être enfermées dans des espaces de travail régis par des conditions multiples, ou habiliter l'optimisation de secteurs du réseau pour fonctionner à l'aide de suites de communication à petite bande passante dans le cas des utilisateurs débarqués ou pour d'autres fonctions. Cette combinaison de nœuds et de leurs fonctions favorise des fonctions spécialisées du réseau comme le monitorage et l'administration du système à distance, et aide à renforcer le réseau contre les intrusions et les menaces.

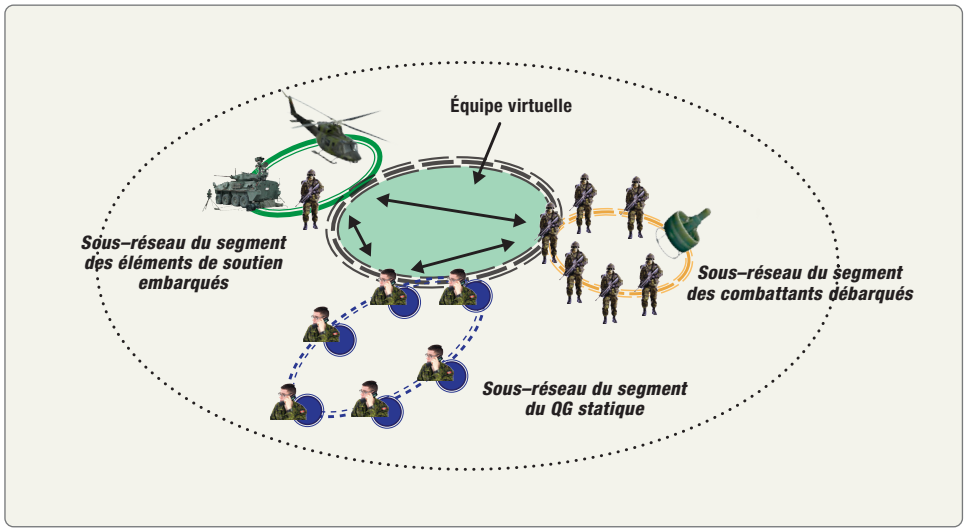

Figure 4 : Fédération conceptuelle de réseaux

Chaque réseau est ensuite connecté à d'autres réseaux par des liaisons, communément définies comme des chemins de communication. Ces chemins sont caractérisés par des attributs qualitatifs et par des mesures de rendement quantitatives. Les caractéristiques qualitatives incluent la complexité, la qualité du service, la variabilité et la topologie, tandis que les mesures de rendement incluent la latence, l'efficience, la tolérance aux erreurs, etc.

Les nœuds existent rarement dans les seules formes pures décrites ci-dessus; ils sont plutôt conçus comme des entités composites pour améliorer leur efficacité (p. ex. une munition à guidage optique peut remplir en même temps les fonctions réseau de collecteur et d'exécutant). Parallèlement, les nœuds doivent pouvoir interagir

entre eux et, en conséquence, ils combinent une ou plusieurs des caractéristiques d'interface suivantes :

- Enregistrement et découverte. Les nœuds peuvent se joindre au réseau (prêt-à-tourner) et être reconnus par les autres nœuds du réseau. Pour la découverte, les nœuds possèdent des propriétés comme *identité, intégration* et *interaction* – c'est-à-dire qu'ils se connaissent, ils ont un moyen d'interagir et partagent un certain niveau d'intégration pour « connaître » ou découvrir les autres nœuds du réseau. Lorsque les nœuds subissent des changements dans leurs capacités, ils doivent aussi avoir le moyen de faire connaître ces changements grâce à une fonction de *compte rendu d'état*.
- Les abonnés et les nœuds ont besoin de divers degrés *d'accès* à un ou à tous les nœuds du RAv. Une autre catégorie de base d'interaction dans le réseau est le besoin *d'actualité* de l'information. Encore une fois, les abonnés ont besoin que l'information soit échangée entre les nœuds à divers degrés de latence. Pour certains abonnés, l'actualité n'est pas un facteur important, mais pour d'autres, elle est cruciale. Enfin, il y a également un besoin *d'assurance de l'information*.

TAXONOMIE DES FONCTIONS RÉSEAUX

Pour que le réseau soit utile aux utilisateurs ciblés, il doit offrir des fonctions distinctes, opérationnelles et à valeur ajoutée, ou accomplir les activités et tâches que nous voulons qu'il accomplisse. En se référant à nouveau au modèle de Keus, on peut définir les *fonctions réseau* et, si on les rassemble, présenter une taxonomie utile énonçant leur valeur opérationnelle, à l'aide de laquelle chaque composante d'un RAv peut être mesurée[70]. Plus d'une seule fonction réseau peut être combinée au sein d'une seule composante, tandis que d'autres composantes, pour des questions de coût, d'efficacité opérationnelle ou de capacité spécialisée, peuvent être optimisées pour remplir une seule et unique fonction. Néanmoins, chaque composante dont l'inclusion dans le RAv est envisagée devrait être évaluée du point de vue de la mesure dans laquelle elle remplit les fonctions suivantes :

- **Collecte**. La fonction de collecte permet de fournir des données riches aux fins d'analyse et d'inclusion dans l'image partagée. Elle inclut l'affectation, la gestion et le contrôle des capteurs et de leurs caractéristiques configurables. Les activités de soutien à la collecte

70. À signaler également que les fonctions réseau s'insèrent très harmonieusement dans la hiérarchie cognitive et révèlent les points de la chaîne données-décision où les machines sont optimisées du point de vue du rendement.

incluent l'orientation, l'exploitation et l'affectation, lesquelles sont améliorées par des sous-fonctions comme l'assignation, l'évaluation de la menace, l'identification et la mise en ordre de priorité pour l'engagement. Dans un environnement de COIN, il sera important d'avoir des mécanismes pour permettre la collecte d'informations[71] par des êtres humains.

- Orientation : Inclut notamment la validation des DI, la CCIRM, la gestion de pistes et l'aide à la compilation de l'ICSO.
- Exploitation : Inclut notamment le suivi, la découverte et la fusion.
- Affectation, ou *désignation*, est la fonction d'analyse de l'ensemble des nœuds exécutants (unités, capteurs et armes), l'harmonisation (ou élimination des conflits) et l'inscription des tâches à l'horaire, puis l'affectation d'un nœud pour engager l'objectif.

- **Dissémination**. La communication d'informations entre nœuds nécessite l'existence d'un moyen physique de transmission ou d'un système porteur. Ce système inclut le matériel, le câblage et les protocoles de transmission, qui peuvent se présenter sous plusieurs formes, par exemple la radio (UHF, VHF, WiMax, cellulaire, etc.) ou un réseau filaire. La méthode de dissémination peut inclure la voix, les échanges de données structurés et non structurés, la vidéo plein écran, etc.
- **Analyse**. Le traitement des données pour produire des informations qui se prêtent au jugement.
  - **Planification et coordination**. Cette fonction est le processus d'examen des informations disponibles pour se préparer en vue des opérations. Les logiciels de soutien comme les outils intelligents de soutien aux décisions, les jeux de guerre et les outils de simulation sont la clé de l'exécution efficace de cette fonction.
  - **Évaluation de la situation**. Cette fonction est le processus d'évaluation ou d'analyse d'un objet ou d'une entité particulier pour évaluer son potentiel de causer des dommages; elle inclurait également une évaluation après engagement, le cas échéant.

71. La collecte d'informations par des humains est caractérisée par son caractère aléatoire et des rencontres inopinées, en particulier dans l'environnement de COIN.

➢ **Compilation.** C'est la fonction d'assemblage des informations pertinentes obtenues des collecteurs participant en vue de leur présentation aux utilisateurs (c.-à-d. *la création d'une image commune ou partagée)*. L'efficacité de la compilation d'une image dépend, en partie, de la facilité d'accès à l'information, des applications disponibles pour représenter cette information et de la manière dont cette information est ensuite utilisée dans les cycles de décision et de planification[72]. Parce qu'elle soutient le processus de planification et parce que les divers utilisateurs vont probablement avoir une vue différente de l'opération, la compilation efficace d'une image commune ou partagée va nécessairement devenir l'objet d'un processus géré.

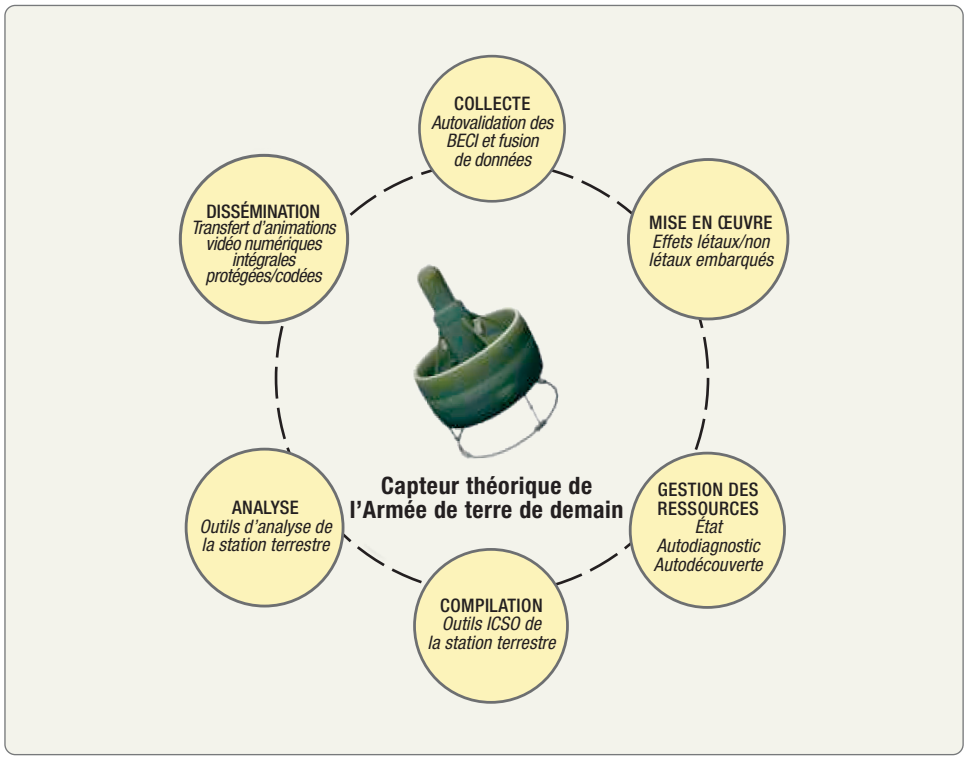

Figure 5 : Fonctions réseau représentées dans un nœud de capteurs réseau théorique

➢ **Mise en œuvre**. Cette fonction d'exécution ou d'action d'un ou plusieurs nœuds (unités/armes/capteurs) vise à réaliser l'effet souhaité. La mise

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

en œuvre comprend toutes les fonctions nécessaires pour commander les nœuds en vue d'engager un objectif. Elle soutient la fonction de synchronisation des effets, notamment ceux des capteurs et de l'appui-feu.

- **Gestion des ressources**. C'est la fonction de logistique et de maintenance des diverses composantes du réseau. Elle ne se limite pas simplement à la gestion du système, mais inclut l'analyse nécessaire pour soutenir les unités en combat rapproché.

Le problème pour les développeurs de capacité est qu'ils ne peuvent tout simplement pas aller dans les magasins et s'acheter « un réseau », du moins pas un réseau qui sera utile à l'Armée canadienne en déploiement. Il faut étudier attentivement les besoins des utilisateurs pour définir la nature, le nombre et les caractéristiques de chaque nœud et des liens qui les unissent.

QUEL GENRE D'INFORMATION?

Le but de l'échange d'informations entre utilisateurs est de définir l'environnement. Après avoir défini ce qui constitue un réseau et les fonctions qu'il remplit, nous pouvons maintenant aborder la question du genre d'informations que le RAv va devoir échanger. La prémisse des OAD accepte le fait qu'une force habilitée par réseau va devoir exploiter sa supériorité en matière d'information pour prendre l'avantage sur ses adversaires, mais peu d'efforts ont été consacrés à la description de la nature de ces informations elles-mêmes. Selon Keus : « Pour chaque environnement multinœuds, dans lequel les nœuds travaillent ensemble pour accomplir des buts communs, il y a quatre catégories générales de *types d'informations* : (1) conscience de soi, (2) connaissance de la situation, (3) intention et (4) opérations en cours. » En outre, nous pouvons proposer une catégorie d'informations au sujet de l'organisation elle-même, à savoir (5) les services communs.

La ***conscience de soi*** est la catégorie d'informations au sujet des ressources disponibles, en particulier au sujet des nœuds et de leurs capacités. Cette catégorie d'informations s'intéresse à définir les caractéristiques (paramètres de rendement) du nœud lui-même, ainsi que les changements dans ces caractéristiques (diagnostic). Elle pourrait inclure des informations au sujet de la hiérarchie organisationnelle du nœud, de l'état du commandement et contrôle, etc.

Connaissance de la situation ou informations au sujet de la situation opérationnelle (le monde réel) à tous les niveaux hiérarchiques. Cette catégorie représente les informations compilées à partir de nombreuses sources, notamment les données brutes, fusionnées ou analysées, et repose sur les fonctions réseau de collecte, d'évaluation et de gestion. La présentation de ces informations doit

être configurable selon les besoins du commandant. Cette catégorie comprend l'information sur l'environnement en fonction duquel les opérations sont planifiées et dans lequel elles seront exécutées.

L'intention, ou *les informations au sujet de l'intention et des plans du commandant*. Cette catégorie d'informations s'intéresse principalement aux opérations à venir ou à l'exécution projetée de l'opération en cours. Elle s'intéresse aux buts de l'organisation. Cette catégorie est nécessaire pour suivre les actions directes des diverses composantes réseautées afin de déterminer le succès ou le potentiel de succès de l'intention énoncée du commandant. Lorsque les informations de cette catégorie sont fusionnées et analysées à l'aide des informations sur les opérations en cours, elles contribuent à la réalisation de la connaissance de la situation et au développement des plans subséquents.

Les opérations en cours, où l'information au sujet de l'exécution d'une opération. L'information contenue dans la catégorie des opérations en cours se compose en grande partie *d'informations périssables de pertinence immédiate* pour ceux qui exécutent le combat actuel ou rapproché. Cette catégorie se compose nécessairement d'abord d'actions et d'événements, amis et hostiles (ou au sujet d'autres hostilités), ou d'informations au sujet des actions et événements en cours qui ont été mis en œuvre pour réaliser l'intention énoncée et qui sont utilisées pour tenir compte des actions imminentes et déterminer les actions successives aux fins d'harmonisation (élimination des conflits) et de synchronisation. Les informations de cette catégorie sont étroitement combinées aux informations contenues dans les catégories intention et connaissance de la situation et, après analyse et jugement, constituent un apport important à la catégorie connaissance de la situation.

Services communs, ou informations au sujet des principes d'organisation de l'institution elle-même. Cette catégorie d'informations soutient les processus d'entreprise globaux dans toutes les organisations géographiquement dispersées. Ainsi, cette catégorie pourrait inclure l*a doctrine, les politiques, la gestion de l'information, la gestion du personnel et l'instruction*. L'ajout de la catégorie des services communs permet aux composantes du RAv de s'étendre aux activités d'instruction et de garnison, et de rendre le matériel d'instruction disponible dans l'environnement opérationnel, au besoin.

PRÉSENTATION DE L'INFORMATION

Le fait de décrire clairement les types d'informations à échanger permet non seulement de comprendre la nature et l'étendue des échanges d'informations, mais également d'éclairer la discussion sur la manière dont ces informations sont mises à la disposition des utilisateurs. Il y a en réalité un lien direct entre la fonction

réseau « *compilation* » et le format sous lequel l'information est présentée. Le dictionnaire Petit Robert définit « forme » comme suit : « manière dont quelque chose, quelqu'un se manifeste à la vue, au toucher ». À partir de cette définition, on comprend facilement que l'information est habituellement perçue par les utilisateurs d'abord par la vue et l'ouïe (avec le soutien du toucher, de l'odorat et du goût). Donc, les utilisateurs, par exemple les soldats débarqués, peuvent raisonnablement s'attendre à continuer à se fier abondamment à la perception auditive et visuelle comme principal moyen de consommation de l'information. La dissémination des informations par les soldats débarqués pourrait continuer de reposer en grande partie sur les communications vocales, peut-être avec l'aide d'informations graphiques et textuelles simplifiées, tandis que d'autres destinataires pourront utiliser des outils optimisés de présentation textuelle de grand volume comme les applications de feuille de calcul, de courriel, etc. Bien entendu, même si l'information est d'abord perçue dans sa forme brute, elle est consommée ou traitée à l'aide d'un ensemble de filtres, qu'ils soient culturels, psychologiques ou autres. Cette adaptation de l'information survient, peu importe le moyen de dissémination, et les utilisateurs vont continuer d'exiger que la technologie leur permette de filtrer l'information ou d'en adapter la présentation.

CONCLUSION

En conclusion, les réseaux existent pour *partager* et *exploiter* l'information. Chaque composante doit remplir une ou plusieurs des fonctions réseau pour offrir une certaine valeur opérationnelle. Même si la définition de ce qu'est un réseau, de ses divers types et de ses fonctions est un bon point de départ pour décrire les composantes génériques d'un réseau, elle ne nous en dit pas beaucoup sur ce qui constitue un réseau utile ou, plus particulièrement, sur la manière dont un réseau habilite le concept des OAD. Dans la PARTIE 4 de la présente étude, nous décrivons le rapport entre le réseau et l'être humain qui commande et, en général, comment le réseau pourrait fonctionner dans le cadre des opérations terrestres en 2021.

« Il n'y a rien de commun au sujet de l'image de la situation opérationnelle. Nous créons notre propre perception de la situation et nous interprétons les faits à notre propre manière. Nous avons tous notre image personnelle et particulière de la situation opérationnelle. Le commandant n'a pas à éliminer ces diverses images individuelles, mais doit plutôt identifier et gérer toutes contradictions entre elles. Dans la mesure où nous utilisons une base de données homogène, notre décision d'accepter l'image commune est délibérée et cette image a pour but non pas de créer une compréhension commune, mais plutôt de fournir une base acceptée pour l'échange et la comparaison de nos conjectures et des résultats de nos tests. »

– Lcol Ralph E. Giffin[73]

PARTIE 4 – LE COMMANDEMENT ET LE RÉSEAU DANS LES OAD

Alors que l'AC entreprend un programme visant à réaliser une force habilitée par réseau, il ne faut pas oublier que, nonobstant les tendances technologiques, les armées vont continuer de confier le commandement et d'accorder leur confiance à des êtres humains, et que cette situation ne risque pas de changer. La partie 4 commence par une courte introduction aux principes du commandement, se poursuit avec une courte discussion du réseau dans les OAD et se conclut par une description des informations générales dont a besoin une force habilitée pour les OAD.

PRINCIPES IMMUABLES DU COMMANDEMENT

Peut-être que la principale raison pour laquelle le commandement demeure une fonction humaine est que, malgré les progrès rapides de la logique machine et de l'intelligence artificielle, seuls les êtres humains possèdent la capacité réelle de réagir à des menaces imprévues et de reconnaître les occasions qui se présentent. Par conséquent, le commandement est un art qui fusionne personnalité, compétences, connaissances et créativité. L'AC reconnaît[74] que le commandement est « l'activité la plus importante en temps de guerre, en garnison et dans l'ensemble du spectre des opérations ». La doctrine actuelle[75] place l'exercice du commandement dans le domaine humain en signalant que « le combat terrestre est avant tout une

73. Lieutenant-colonel Ralph E. Giffin, *A Woven Web of Guesses*, Canto deux.

74. B-GL-300-003/FP-002, *Le commandement dans les opérations terrestres*, 27 juillet 2007, p. 1-3.

75. *Ibid.*, p. 1-5.

interaction humaine » et que cela ne devrait pas changer sur l'horizon de l'ATdD. Le commandement humain des forces militaires repose fortement sur les qualités de [*leadership*, *compétence*, *responsabilité* et *confiance*, etc.] des personnes qui participent au processus de décision et sur la dynamique interpersonnelle entre les commandants et leurs subordonnés[76]. Par conséquent, il est important de comprendre que la conception et l'exploitation du RAv ne doivent pas nuire à l'exercice du commandement humain, mais plutôt lui servir de complément.

C'est cette capacité de profiter des aspects intangibles de la nature humaine qui renforce le rôle fondamentalement humain du commandement et qui a été reconnu par plusieurs auteurs, notamment le Col Forgues dans son article intitulé *Le commandement et la guerre réseaucentrique* :

> *Les éléments fondamentaux du commandement, tels qu'ils sont définis dans la PFC 300-1, sont l'unité d'effort, la décentralisation, la confiance et la compréhension mutuelle, ainsi que la prise de décisions opportune et efficace. Le commandement favorise la cohésion de la force dans le but de réaliser l'unité d'effort. Dans la mesure du possible, le commandement doit être décentralisé et compter sur la capacité des sous-unités de fonctionner indépendamment tout en maintenant l'unité d'effort. Cette situation favorable est le fruit de la confiance et de la compréhension mutuelles. Dans un tel milieu, les commandants peuvent prendre des décisions opportunes et efficaces. [...] Il est bien sûr beaucoup plus difficile d'unifier l'effort quand le commandement est décentralisé. Dans la PFC 300-1, on peut lire que la manière de résoudre le conflit entre l'unité d'effort et la décentralisation est de s'assurer que les intentions du commandant sont communiquées et comprises, que l'effort principal est clairement défini, qu'un climat de commandement approprié règne et que les forces opèrent selon une doctrine commune. Ce document insiste sur le rôle du chef, qui est d'établir un objectif, de fournir une direction et de favoriser la cohésion et la motivation*[77].

Deux thèmes ressortent : premièrement, la question de la *confiance*, et deuxièmement, l'impératif de communiquer, en termes non ambigus, l'*intention* du commandant. La confiance a toujours été un facteur important dans le succès des opérations militaires, mais elle risque de devenir encore plus cruciale au moment où

76. Direction de la doctrine de l'Armée de terre, Dossier de développement des capacités de commandement, septembre 2006.

77. Colonel P. Forgues, « *Le commandement et la guerre réseaucentrique* », Revue militaire canadienne, (été 2001), p. 23-30.

nous élargissons le cercle des décideurs à des personnes (et peut-être même des entités non humaines) et des organisations à l'extérieur de la chaîne de commandement immédiate. Parce que la confiance et la compréhension de l'intention du commandant sont fondamentales au succès d'une opération, tout réseau de l'avenir incapable de fournir une assurance de l'information sans compromis risque de miner la confiance des utilisateurs envers lui. La communication claire et la compréhension de l'intention du commandant sont tellement fondamentales au commandement de mission que le défi pour ceux qui vont mettre en œuvre le RAv sera de trouver des moyens de communiquer cette intention, en particulier à des entités non humaines, autres que les méthodes traditionnelles de communications vocales et écrites.

Il est à noter que seuls les êtres humains sont actuellement capables d'*appliquer le jugement* à la connaissance. Ce facteur est important parce que, même si les données, l'information et, dans une certaine mesure, les connaissances peuvent être maîtrisées par les machines, la compréhension découlant de l'expérience, de l'intuition et de l'instruction ne risque pas d'être maîtrisée par l'intelligence machine dans un avenir rapproché.

L'ÊTRE HUMAIN AUX COMMANDES

Le commandement est une fonction essentiellement humaine qui repose sur les facteurs intangibles de la nature humaine, notamment, par exemple, un code moral et éthique, le jugement, les relations interpersonnelles et les liens de confiance. Cependant, la nature complexe de la guerre exige que des mécanismes pour réduire le risque d'incertitude et accélérer la vitesse de prise de décisions soient mis à la disposition du commandant. C'est dans ce rôle à l'appui de *contrôle* que la technologie, et en particulier une capacité réseau, excelle. Lorsque l'armée entreprend un cycle de planification, de préparation, d'exécution et d'évaluation, le commandant « doit s'appuyer sur un système de contrôle qui l'aide à relever le défi du temps et de l'incertitude par la gestion et la production d'informations et de connaissances opportunes, pertinentes et précises à partir desquelles il pourra comprendre la situation et visualiser ce qu'il doit faire ensuite »[78]. La clé de la visualisation du champ de bataille par le commandant réside dans un processus de transformation de données brutes en compréhension[79] – un processus illustré par

78. B-GL-300-003/FP-002, *Le commandement dans les opérations terrestres*, p. 1-11.

79. La transformation de données en connaissances pour arriver en fin de compte à la décision comporte une chaîne de dépendances cognitives dans laquelle les machines et l'être humain sont optimisés différemment pour accomplir des tâches particulières. Les machines sont beaucoup plus en mesure de collecter de gros volumes de données, de les rassembler en informations et d'en faire une analyse brute pour transformer cette information en connaissances, lesquelles contribuent ensuite à la connaissance de la situation. Les humains contribuent aussi à l'analyse de l'information, mais sont beaucoup mieux adaptés à la tâche consistant à appliquer le jugement aux connaissances pour établir une compréhension et parvenir à des décisions.

la hiérarchie de l'information illustrée ci-dessous. Comme nous le verrons plus tard, la technologie peut aider à la vitesse et à la précision de ce processus, et ainsi compléter l'activité humaine.

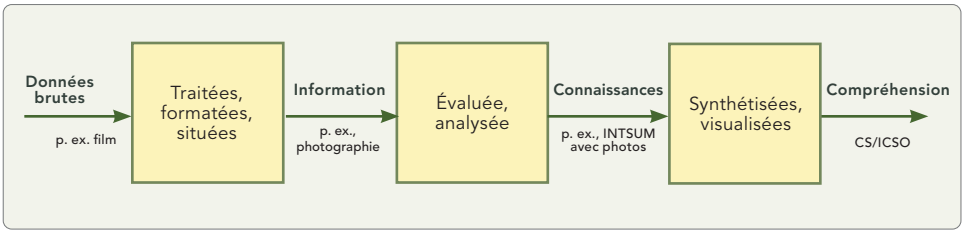

Figure 6 : Hiérarchie de l'information

Les besoins du réseau de l'Armée canadienne sont différents de ceux des autres services – par exemple, l'exercice très personnel du commandement va conditionner les besoins du réseau de l'AC et différencier la solution réseau de l'AC de celles des FC ou de l'Armée de l'air et de la marine. Le commandement de soldats dépend beaucoup des liens de confiance, de la motivation, du leadership et de l'esprit d'équipe – c'estàdire qu'un commandant de l'Armée de terre doit démontrer courage, force morale et présence personnelle, et utiliser son influence au bon endroit et au bon moment sur le champ de bataille. Mais parce que le commandant ne peut pas être partout en tout temps et en raison de la vaste quantité d'informations à sa disposition, de laquelle il doit extraire des données pertinentes, il faut un réseau d'information complexe, mais intuitif. Ce réseau doit d'abord être absolument capable de permettre au commandant de communiquer son intention et son but d'une manière concise et claire jusqu'au niveau du soldat pour ainsi fournir aux subordonnés suffisamment d'informations pour leur permettre de prendre les décisions décentralisées nécessaires à l'exécution du plan. Cette capacité de prise de décisions décentralisée est en soi presque unique parmi les trois armées et un concept commun de réseau des FC ne sera pas suffisant.

De plus, le réseau de l'AC doit répondre aux besoins d'un large éventail d'utilisateurs allant des combattants débarqués qui transportent sur eux presque tout ce dont ils ont besoin, aux éléments de combat et de soutien embarqués où les composantes réseau physiques doivent coexister avec les systèmes d'arme du véhicule ou de la plate-forme, jusqu'aux quartiers généraux statiques et établissements d'instruction en garnison ou, grâce aux ressources et à la bande passante plus grandes, il n'est pas nécessaire que l'empreinte des composantes soit optimisée en vue du déploiement. Cette diversité des éléments utilisateurs signifie que le RAv se composera vraisemblablement d'une fédération de sous-réseaux spécialisés, chacun

optimisé pour des éléments utilisateurs et des environnements particuliers, mais également capables de partager l'information entre eux.

Par ailleurs, la transmission de l'information au sein de l'AC est en mutation vers des systèmes plus numérisés, ce qui laisse entrevoir que les humains ne seront plus les seuls consommateurs de l'information et que celle-ci sera également consommée par des capteurs et des plates-formes d'armes automatisés. Cependant, l'information la plus cruciale, l'*intention du commandant*, ne circule pas à l'heure actuelle en tant que données, ce qui limite notre capacité de fournir des instructions aux entités non humaines dans l'espace de combat.

À l'heure actuelle, les capacités réseau de l'Armée canadienne peuvent être caractérisées comme des enclaves réseau bien alimentées, reliées par une infrastructure d'échange d'informations mal alimentée (haute latence, petite bande passante et portée limitée) entre les enclaves. Il est également important de noter que les capacités réseau adoptées par l'AC sont en grande partie des processus analogues préexistants qui ont été convertis au numérique, ce qui a permis aux FC et à l'AC de devenir assez compétentes dans le stockage ou « entreposage » d'informations. Malheureusement, en raison d'un manque d'outils intelligents de partage de l'information, l'AC est pratiquement incapable de fournir efficacement des informations pertinentes aux commandants. De plus, il y a peu ou pas d'intégration des réseaux qui existent en garnison (logiciels de base), dans les établissements d'instruction (outils de simulation) ou dans les déploiements au niveau tactique. Ainsi, même si on peut affirmer qu'il existe bel et bien un réseau, cette existence est piètrement réalisée. L'incapacité de partager facilement le contenu des dépôts d'informations engendre la frustration de savoir que l'information existe quelque part dans des dépôts d'informations déconnectés, mais sans savoir où la trouver. Les outils de gestion de l'information basés sur le wiki et récemment développés dans le théâtre sont porteurs de promesses d'affranchissement de ce paradigme.

Finalement, l'exécution d'opérations dans l'ensemble du spectre dans un contexte d'OAD va exiger un ensemble de systèmes réseautés de la famille des systèmes de combat terrestre (FSCT) pour soutenir les principes fondamentaux[80] des opérations dispersées développés à partir des principes de la manœuvre : trouver, fixer et frapper. Par conséquent, le RAv va exiger, au minimum, des caractéristiques et des fonctionnalités qui lui permettent de fonctionner dans l'ATdD en vertu du concept des OAD[81].

---

80. (1) Développer la situation avant le contact, (2) Permettre à la manœuvre de profiter de positions avantageuses, (3) Influer sur l'adversaire au-delà de la portée de ses armes grâce à des capacités létales et non létales, (4) Permettre la destruction de l'ennemi, au besoin, grâce à des effets de précision et de zone, (5) Permettre l'exécution d'engagements rapprochés, au besoin, au moment et à l'endroit de notre choix, et (6) faire la transition d'une opération à l'autre sans perdre l'objectif de vue ni l'élan.

81. B-GL-310-001/AG-002, *Opérations terrestres 2021 : le concept d'emploi de la force de l'Armée de terre canadienne de demain*, p. 20-21.

Une autre façon d'exprimer cette réalité est que, nonobstant les progrès dans les domaines des sciences et de la technologie décrits à la section précédente, dans l'avenir prévisible, les humains vont rester les maîtres de l'*art* de la guerre, tandis que les machines pourraient en venir à dominer la *science* de la guerre.

LE RÉSEAU DANS LES OAD

L'Armée de terre de demain (ATdD) sera une force moyenne, hautement technologique, optimisée pour les opérations dans l'ensemble du continuum au sein des États défaillants ou en déroute, évoluant dans un environnement IIMP et capable d'opérer dans l'ensemble du spectre des conflits. *Opérations terrestres en 2021* reconnaît que la clé du succès de cette armée dans « l'intégration de systèmes d'information, d'armes et d'autres plates-formes productrices d'effets », postulant une force qui va opérer dans des environnements complexes et des zones d'opérations (ZO) non contiguës; former des organisations de circonstances; se disperser et se rassembler n'importe où sur le champ de bataille; et ne va pas toujours se fier à sa masse pour produire les effets souhaités. « En reliant dans l'espace de bataille les éléments qui détiennent les connaissances, les forces seront plus aptes à obtenir la supériorité en matière d'information, et la mission en sera d'autant plus efficace. » Bien que le concept admette le besoin d'un réseau, *Opérations terrestres 2021* « ne fournit pas de détails sur la doctrine du déploiement des formations et unités de l'Armée canadienne »[82] et laisse sans réponse des questions comme celle sur la manière dont une force habilitée pour les OAD pourrait exploiter un réseau de l'avenir.

À noter qu'*Opérations terrestres 2021* affirme implicitement que la notion selon laquelle les sous-unités et pelotons ne se contenteront plus d'exécuter ce qu'on appelle des « opérations militaires classiques » – on s'attendra à ce qu'ils exécutent des opérations dans l'ensemble du spectre des opérations, à l'aide d'éléments habilitants IIMP (possiblement déployés au niveau tactique), et à ce qu'ils soient dispersés physiquement et probablement hors de portée de l'appui-feu direct et indirect intégrale. Cela signifie que les composantes physiques du RAv vont devoir être légères, capables de fonctionner à faible puissance pendant des périodes prolongées et capables d'offrir toute une gamme de services à l'utilisateur.

Limites du concept d'emploi de la force. La force habilitée pour les OAD peut s'attendre à opérer dans l'une des quatre zones d'opérations (ZO) de base tout en conservant la capacité de faire une transition rapide et d'opérer dans les autres types de ZO[83]. Chapman (2008) propose une liste de facteurs qui vont « limiter la capacité de l'unité de se disperser », notamment des facteurs comme l'appui-feu direct et

82. Major B. Chapman, *Bounding the Force Employment Concept*, p. 4.

83. *Ibid,.,*

indirect, l'évacuation des blessés, le réapprovisionnement (maintien en puissance), le C2 et les communications, les renforts, la surveillance et le regroupement des forces dans des délais prescrits. À partir de ces facteurs de Chapman, on peut formuler des hypothèses générales au sujet de la nature du RAv dans les OAD :

- Les ressources d'appui-feu indirect vont demeurer en forte demande, rares et généralement centralisées dans leur attribution, en particulier les ressources d'appui-feu interarmées. En outre, l'appui-feu indirect va continuer d'être caractérisé par un haut degré de contrôle centralisé, une planification préalable (RE et critères de choix des objectifs) et des procédures de demande spéciales. Sur l'horizon 2021, on peut s'attendre à ce que les systèmes d'arme de tir direct et indirect possèdent des protocoles d'autodécouverte, ce qui leur permettra d'enregistrer leur disponibilité, d'échanger des informations au sujet des objectifs qu'ils sont en mesure d'engager, de créer automatiquement une liste d'objectifs en ordre de priorité d'engagement (et de transfert ou de défection), et à ce qu'ils intègrent des outils d'analyse de bord qui peuvent aider au choix automatique des types de munitions appropriés. Pour soutenir les demandes de tir indirect, le RAv va devoir offrir un haut degré de disponibilité et, fort probablement, un chemin réservé à l'échange des ordres de tir.
- Les armes d'appui-feu direct vont continuer d'être employées dans des positions en appui réciproque, ce qui limitera la zone qu'il est possible de dominer par le tir. L'accroissement de la portée et de la létalité, et l'acquisition intelligente d'objectifs devraient permettre une augmentation de la couverture de zone. Les systèmes de tir direct vont devoir posséder beaucoup des mêmes capacités que celles énoncées ci-dessus à l'égard des systèmes de tir indirect, mais pourraient en plus posséder des capacités comme des suites d'aides de défense (SAD) intégrées, des capacités d'engagement coopératif (CEC), etc.
- Évacuation des pertes. Des SSS de haute qualité vont continuer d'être exigés et cette attente va imposer des limites à la dispersion spatiale des forces. Pour atténuer ces limites, il pourrait être souhaitable d'équiper les combattants débarqués et embarqués de moniteurs biométriques susceptibles, en cas de CASEVAC d'urgence, de mettre à la disposition des spécialistes des SSS et des secouristes de combat des informations sur l'état du patient, ce qui permettra de fournir de meilleurs soins sur place ou de faire des préparatifs adaptés dans les installations spécialisées de SSS.

- Maintien en puissance. On s'attend à ce que les sous-unités consomment des munitions, de la nourriture et de l'eau à un rythme dépassant les chiffres de planification standard[84]. Par conséquent, le RAv va devoir fournir un réseau de SLC permettant la logistique et le ravitaillement adaptés, offrant des outils d'analyse et une vision SLC de l'espace de combat adaptée. Les composantes réseau optimisées pour le déploiement dans le contexte des OAD vont devoir être configurées en fonction *d'une empreinte logistique réduite* (par exemple, une demande réduite pour des sources d'alimentation électrique jetables ou la fourniture de sources d'alimentation régénérantes). Les outils d'analyse et les agents intelligents offerts à la communauté du SLC font devoir être en mesure de fournir une analyse rapide des options de SLC, combinée à un suivi en temps réel des ressources et des marchandises pour permettre une configuration rapide des chargements de ravitaillement. Le réseau pourrait apporter des avantages importants dans le domaine du maintien en puissance grâce à la prestation de services localisés, particulièrement une activation par proximité (p. ex. une alarme de bas niveau de carburant ou de munitions pourrait déclencher des tâches de ravitaillement) et un avis de proximité.
- Commandement et contrôle. Une capacité réseau de base comme les communications en phonie protégées partout sur le champ de bataille, complétée par une connaissance de la position fiable, est nécessairement au cœur d'un réseau tactique – un réseau disponible, viable et facile à utiliser. Il faudra examiner attentivement la présentation de l'information sur les dispositifs mobiles et portables. Par exemple, les composantes fournies aux éléments de combat débarqués vont devoir présenter des informations simplifiées tout en permettant une plus grande fidélité au besoin. En outre, les besoins d'informations vont être diversifiés, changer rapidement et être suffisamment larges dans leur nature qu'il est concevable que les soldats vont vouloir accéder à un large éventail d'informations presque n'importe quand.
- Communications. On présume que les communications par satellite ne seront pas disponibles sur tous les réseaux et que les capacités radio actuelles et en évolution vont être exploitées. Les sous-unités

84. Par exemple, la veste tactique réglementaire peut accueillir quatre chargeurs de munitions, ce qui correspond au chiffre de planification d'une journée d'approvisionnements de cinq chargeurs (un dans le fusil). Cependant, il n'était pas rare durant l'Op *Archer* que les soldats transportent entre 12 et 15 chargeurs durant leurs patrouilles quotidiennes, ce qui dépasse grandement les barèmes de consommation.

embarquées doivent maintenir leur connectivité avec le quartier général supérieur à l'aide de radios tactiques d'une portée d'au moins *40 km*.

- Les demandes en concurrence vont nécessairement amener des compromis dans la conception qui vont continuer d'exister sur l'horizon de l'ATdD. Par exemple, l'efficacité en taille, poids et puissance suggère que le soldat devrait peut-être accepter des compromis sur la bande passante et ainsi une réduction de sa capacité d'accès à l'information. À l'inverse, les utilisateurs dans les QG statiques et en garnison pourraient souhaiter une augmentation importante de la bande passante et être disposés à des compromis sur la taille, le poids et la puissance.
- Les communications en phonie vont continuer d'être une norme nécessaire et doivent particulièrement être disponibles en tant que capacités « à l'épreuve des pannes » lorsque les autres moyens de communication sont hors d'état.
- Les communications en phonie vont être en forte demande de la part des éléments de la force qui ne disposent pas actuellement de suites de communication (par exemple les véhicules B de SLC). Donc, beaucoup plus de plates-formes seront équipées de suites de communication en phonie que ce n'est le cas actuellement, ce qui va augmenter dramatiquement le nombre de nœuds de réseau distincts qui vont relever de la planification des transmissions et vont exiger gestion et maintenance du réseau.
- La bande passante va demeurer une ressource cruciale et continuera d'être particulièrement limitée sous le niveau de la sous-unité. On peut en outre présumer que, dans cet environnement de bande passante limitée, les communications en phonie vont demeurer une méthode de communication de haute priorité.
- Avec la prolifération des bases de données (dans les QG statiques et sur les plates-formes mobiles), l'information va persister dans l'ensemble de l'espace de combat, ce qui va nécessiter des politiques de gestion agile du réseau et un modèle amélioré de sécurité de l'information.

SOMMAIRE

C'est l'être humain qui commande; il dirige par sa présence et sa volonté, et doit évaluer la situation, concevoir de nouvelles solutions et prendre des décisions. C'est l'être humain qui reste responsable des résultats de ses actions, notamment celles des entités non humaines. Au gré de la conception des composantes du RAv, il faudra faire un effort particulier pour s'assurer que, dans l'ensemble du système, un mécanisme d'imputabilité des êtres humains pour leurs décisions est mis en œuvre. Par conséquent, tous les systèmes du RAv, à partir des capteurs et des armes jusqu'aux structures organisationnelles et aux changements de commandement, doivent exister pour appuyer le potentiel humain d'accomplir la mission[85].

En acceptant le fait que le commandant reste l'élément le plus important et l'instrument à travers lequel la force utilise l'information, on peut entrevoir la manière dont le réseau offrira des fonctionnalités particulières au commandant. Ensemble, les fonctions réseau et les échanges d'informations doivent appuyer le besoin supérieur du commandant de préciser les détails de la mission à ses principaux subordonnés. Cette information est généralement formulée dans un énoncé de mission dans lequel des éléments comme *qui* [ressources] va accomplir *quoi* [action/tâche] *contre qui* avec *quelles* [ressources], *où* [lieu], *quand* [date/heure], *pourquoi* [but/intention] et *comment*[86]. Incidemment, et de façon importante pour les applications potentielles au sein du RAv, les formulations comme celle évoquée ci-dessus se prêtent facilement à la création d'instructions lisibles par machine et donc adaptées à des acteurs non humains autonomes.

Dans la partie 4, nous avons fait une brève description des rapports entre le réseau et l'être humain aux commandes, et avons expliqué comment le réseau pourrait fonctionner dans les *Opérations terrestres 2021*. Dans la partie 5, nous poursuivons avec la description des buts généraux et des objectifs particuliers du réseau, et avec une étude des éléments qui vont l'utiliser.

85. English et coll., *Beware of putting the cart before the horse*…. p. 13.

86. STANAG 2287 Verbes à utiliser pour la planification de tâches et de missions et la diffusion des ordres.

Comme l'Armée canadienne sera extrêmement dépendante du réseau, il faudra aussi veiller particulièrement à ce que ce dernier soit fiable, à l'abri des attaques physiques et cybernétiques, et doté de redondances pour le cas où des éléments du système tomberaient en panne. L'Armée canadienne préconisera une approche globale en matière de réseautage — en insistant particulièrement sur les dimensions technologique et humaine du réseau. Pour ce faire, elle devra choisir les bonnes technologies au bon moment, afin de complémenter la dimension humaine, toujours cruciale, d'une Armée canadienne réseaucentrique.

– Opérations terrestres 2021

PARTIE 5 – OBJECTIFS GÉNÉRAUX DE LA CAPACITÉ RÉSEAU

BUTS GÉNÉRAUX

Le RAv, caractérisé par son *accent sur l'humain, sa fédération modulaire et intégrée de sous-réseaux/d'enclaves*, soutenu par une *architecture intégrée*, va offrir une capacité réseau terrestre à l'ATdD qui va permettre aux commandants, soldats, capteurs et armes d'accéder à l'information au-delà des limites tactiques, du théâtre, interservices et IIMP afin de partager des informations exploitables, le tout à l'appui de la manœuvre. Les buts généraux clés de cette capacité sont les suivants :

- ***Un réseau central***. Le RAv va devoir posséder une série de capacités « à l'épreuve des pannes » ou réversibles qui le rendent hautement disponible, résistant et autorégénérant[87], sûr et fiable. Une capacité de communications en phonie protégée à tous les destinataires est considérée comme la capacité fondamentale du réseau qui doit être mise à la disposition de tous les segments d'utilisateurs.
- ***Utilisateurs débarqués***. Les utilisateurs débarqués vont avoir besoin d'appareils configurables à faible puissance et d'applications ou services à petite empreinte. Les composantes réseau débarquées vont devoir s'intégrer en continu avec les dispositifs de bord du véhicule. Les dispositifs conçus pour être utilisés en périphérie tactique vont

87. Des radios logicielles sont en voie d'être réalisées à l'heure actuelle avec la mise en œuvre de la Soldier Radio Waveform dans le cadre du projet US Army Battle Command on the Move (Commandement mobile au combat de l'Armée américaine). L'autorégénération permet aux composantes de communication d'un réseau de « trouver » un chemin optionnel jusqu'au destinataire souhaité au cas où un chemin de communication réservé serait perturbé.La technologie requise pour habiliter l'autorégénération amène également la capacité de constituer des réseaux de circonstance lorsque les nœuds de communication se découvrent l'un l'autre. La création et l'utilisation de réseaux de circonstance vont probablement être un atout crucial pour le succès des opérations en milieu urbain et en terrain complexe dans le cadre desquelles de petites équipes de soldats se constituent rapidement en équipes temporaires.

devoir posséder un éventail de services d'information automatiques et sur demande, configurés selon l'identité/les accréditations/le rôle de l'utilisateur. Ainsi, les services comme l'alarme de proximité, les alertes et avertissements de position, des services de traduction en temps quasi réel, des lexiques culturels, des documents de doctrine, un service de messagerie en texte simple, etc. pourront être offerts au besoin, soit par radio (semblablement à l'informatique en nuage), soit configurés et préchargés dans les appareils, sur la base du profil de l'utilisateur.

- ***Présentation de l'information***. Les composantes du RAv doivent offrir une interface homme-machine (IHM) simplifiée et configurable, peut-être habilitée par des technologies de réalité amplifiée (RA). Elles doivent posséder des interfaces qui reproduisent facilement le processus décisionnel de l'utilisateur, encouragent une interaction en confiance[88] et habilitent l'utilisateur à mieux accomplir ses tâches.
- ***Système de systèmes modulaire***. Compte tenu de la technologie et du rythme de son institutionnalisation au sein de l'AC, ainsi que de la nécessité de soutenir les systèmes existants, il est souhaitable d'adopter une approche modulaire à la conception et à la livraison des composantes du RAv. Une telle approche va permettre de concevoir et de fabriquer lesdites composantes de façon à ce qu'elles soient interopérables en leur intégrant un protocole d'échange d'informations et un même modèle de données.
- ***Environnement de partage de l'information en collaboration***. Beaucoup d'efforts devraient être investis pour fournir des outils de collaboration distribuée[89] afin de permettre à certains utilisateurs ou à tous les utilisateurs d'être à la fois éloignés physiquement du QG central tout en favorisant la cohésion de l'équipe. En fait, la capacité d'établir la collaboration entre n'importe quels groupes d'utilisateurs (y compris les capteurs ou les systèmes autonomes), en particulier la création d'un groupe d'utilisateurs de circonstance, est un facteur habilitant hautement souhaitable pour les opérations IIMP et les opérations nationales.

88. La règle des trois clics est une règle non officielle de conception de sites Web touchant la navigation. Elle suppose que l'utilisateur d'un site Web devrait pouvoir trouver toute l'information qu'il cherche sans avoir à cliquer plus de trois fois. Cette règle repose sur la conviction que les utilisateurs d'un site vont éprouver de la frustration et quitter le site s'ils ne peuvent trouver l'information qu'ils cherchent en moins de trois clics. Les critiques de cette règle prétendent que le nombre de clics n'est pas aussi important que l'efficacité de chaque clic. Peu importe, ce qui est clair, est que l'information est livrée jusqu'à la périphérie du réseau, jusqu'aux utilisateurs tactiques, et que les dispositifs doivent permettre de présenter l'information rapidement.

89. Ce genre de capacités habilite le remue-méninges d'équipe, l'assemblage de documents et la manipulation de l'information.

La capacité d'établir des connexions de circonstance entre des personnes ou entre des espaces d'informations partagées, offerte par des structures de réseautage social comme Facebook et Twitter, pourrait offrir des solutions de collaboration à court terme[90].

- ***Intégrité assurée de l'information***. Une capacité d'assurance de l'information centrée sur la qualité et la fiabilité garanties de l'information va être une caractéristique nécessaire du réseau. La qualité de l'information va être grandement améliorée par des investissements dans la définition claire de ce que sont les données (ontologies, terminologie, etc.) de façon que leur représentation soit cohérente d'une application à l'autre. Comme ce ne sont pas tous les individus d'un segment d'utilisateurs qui vont avoir besoin du même degré d'accès au réseau, des protocoles d'accès fondés sur le rôle et les accréditations vont permettre de garantir la sécurité de l'information. Grâce à des méthodes de codage communes, à des gardiens fiables et rapides, et à de filtres, le RAv pourra fonctionner dans des environnements de sécurité multiniveaux.
- ***Imputabilité***. Des mécanismes d'imputabilité dans l'ensemble du réseau, notamment à partir des nœuds situés à la périphérie, vont aider à cultiver la confiance envers la qualité et l'exactitude de l'information. La conception des composantes du RAv doit faire en sorte que lorsque ce sera pratique de le faire, les abonnés sont accrédités et leurs décisions sont suivies et conservées.

Outre les objectifs de capacité généraux décrits ci-dessus, le RAv sera en outre caractérisé par une philosophie qui promeut :

- ***La gestion du système.*** À son stade fini, le RAv va comporter une augmentation substantielle du nombre de nœuds réseautés, ce qui va nécessairement impliquer un plan exhaustif de gestion du système. Cependant, il pourrait être avisé d'adopter une philosophie qui reconnaît la tendance de l'AC à centraliser le contrôle des systèmes de SI, et tente de la compenser à la lumière du désir des divers utilisateurs de faire des expériences (apporter des améliorations) avec les outils mis à leur disposition. Ainsi, on pourrait adopter une philosophie de gestion du système qui admet qu'il y aura un certain nombre de services « à l'épreuve des pannes » qui doivent rester sous gestion centrale, tandis que

90. Un espace de partage dans un environnement wiki a été développé pour l'Op *Archer* Roto 3-07 et a prouvé l'utilité opérationnelle des outils de partage de l'information en collaboration au sein de la FO.

d'autres pourront être dévolus à la gestion des formations et unités. Une telle philosophie, en offrant certaines responsabilités de développement et de gestion de certains services aux utilisateurs en périphérie, pourrait favoriser un climat d'expérimentation et d'amélioration et, en fin de compte, l'acceptation par l'utilisateur.

- ***Gestion de l'information***. La quantité d'informations échangées entre les composantes du réseau, combinée aux besoins particuliers et variables des utilisateurs, signifie que le RAv va devoir adopter une stratégie exhaustive de gestion de l'information. Une telle stratégie serait habilitée par une ontologie commune et officielle du domaine militaire, ce qui permettrait la représentation uniforme de l'information dans l'ensemble des composantes du RAv.
- ***Gestion de la connaissance***. Le RAv va devoir offrir une solide capacité de gestion de la connaissance (GC) pour permettre aux utilisateurs de distiller l'information provenant d'un large éventail de sources, notamment des humains, des capteurs et des armes. Cette GC devrait comprendre des agents intelligents pour permettre la diffusion d'avis automatiques, le suivi intelligent, l'assemblage dynamique de l'information, le parsage en langue naturelle[91] et les recherches sémantiques[92]. Des caractéristiques comme les agents intelligents[93], l'historique intelligent des données, les applets Web et les avatars[94], etc., qui permettent tous à l'abonné d'assembler des informations pertinentes et configurables, sont importantes pour habiliter une force réseautée. Une capacité automatisée de GC permettant l'analyse humaine devrait être soutenue par des moteurs d'analyse exhaustifs qui peuvent parser les données

91. Un système de parsage en langage naturel convertit des échantillons de langue humaine en représentations plus structurées qui sont plus faciles à manipuler pour les logiciels. Les applications intelligentes intégrant le traitement du langage naturel pourraient offrir une capacité qui aide à discerner l'intention véritable et la signification d'un terme ou d'un acronyme pour lequel il existe plusieurs définitions. Grâce au parsage du champ de texte non structuré d'un courriel, d'un clavardage ou d'un autre support, les agents de parsage en langage naturel (PLN) pourraient chercher des termes et acronymes connus, puis proposer à l'auteur des significations possibles pour le terme utilisé. Parallèlement, le PLN pourrait aider le destinataire à parser toute la phrase dans laquelle le terme ou l'acronyme apparaît pour en déduire le contexte et proposer un petit nombre de résultats de recherche/fiches de données probables pour le terme en question.

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

93. L'intégration d'agents intelligents semblables à la fonction de recommandation d'achat d'Amazon (les cinq derniers officiers d'état-major qui ont planifié une campagne d'opérations d'information ont utilisé ce plan comme point de départ), ou une fonction de recommandation fondée sur les commentaires d'un groupe comme dans TripAdvisor (quatre des cinq abonnés mentionnés ci-dessus considèrent cette source de renseignements comme utile) ou les applets composites Web basés sur Google Maps qui présentent à l'utilisateur des informations définies au sujet d'un point ou d'une zone particuliers vont permettre aux abonnés de rapidement trouver et assembler plus d'informations immédiatement pertinentes pour leurs opérations.

94. Un avatar est la représentation informatique d'un utilisateur, que ce soit une représentation tridimensionnelle servant aux jeux informatiques ou une image bidimensionnelle utilisée dans les forums Internet et dans d'autres communautés, ou encore une description en texte comme on en trouvait dans les premiers systèmes, par exemple les dimensions multiutilisateurs (MUD). Il s'agit d'un objet qui représente l'incarnation de l'utilisateur. (www.wikipedia.org // chercher « avatar »)

produites par les capteurs, les registres de clavardage, les courriels et les comptes rendus, et ce, à la lumière des BECI, DI, plans et appréciations permanents pour y déceler l'information utilisable. À ce sujet, la GC automatisée ne doit pas nécessairement être déployée dans le théâtre; elle pourrait plutôt être faite depuis des endroits éloignés. Une telle capacité permettrait la transformation des informations non structurées en informations structurées adaptées aux demandes de données, ce qui étendrait la collaboration aux composantes non humaines du RAv. De plus, les données fournies par les partenaires IIMP[95] vont devoir être intégrées dans un objectif de capacité de GC. Nonobstant l'assistance technologique, les analystes humains vont devoir continuer à remplir un rôle nécessaire de GC.

- ***Dissémination de l'information.*** Lorsque des éléments de l'Armée canadienne vont exécuter des opérations dispersées, l'information nécessaire va devoir être disséminée à divers segments d'utilisateurs largement dispersés. Pour que cela soit possible, une *infrastructure de communications* à grand bande passante, capable de transmettre voix et données, sera une caractéristique nécessaire du RAv. Des radios à grande bande passante configurées pour être installées à bord des véhicules ou dans un harnais tactique personnel et des postes de retransmission automatique (PRA) (intégrés à des UAS aéroportés ou de petits aérostats attachés au sol) disponibles au moins jusqu'au niveau du peloton pourraient être considérées comme des composantes possibles du RAv.

OBJECTIFS PARTICULIERS DU RÉSEAU

Certains objectifs[96] pourraient recevoir une plus haute priorité en fonction du besoin à la lumière du risque associé à l'adoption de la technologie. De la même manière, la décision de réaliser les objectifs de capacité devrait éviter si possible la tendance à fournir des solutions « uniques » adaptées aux besoins perçus d'une branche ou d'une fonction en particulier. En tout temps, il faut se rappeler que les capacités, au moment de les définir, devraient favoriser la capacité des commandants et subordonnés de communiquer et de partager l'information. Les objectifs suivants sont considérés comme prioritaires :

95. *Les opérations terrestres en 2021 : Un concept en devenir – Études à l'appui du concept d'emploi de la force de l'Armée de terre de demain*, chapitre 7.

96. Cette section ne cherche pas à préciser les outils ou la technologie, même si elle va parfois citer certains exemples pour décrire les caractéristiques possibles d'un outil susceptible d'atteindre un objectif de capacité particulier.

Améliorer la présentation de l'information. Dans le cours de leurs fonctions, les soldats seront soumis à des périodes prolongées de stress et de fatigue qui, combinées aux actions imprévisibles de la menace, peuvent entraîner des erreurs de perception, de compréhension et de décision. En réponse à ce risque, il faudra consacrer des efforts considérables à comprendre la dimension humaine[97] des flux d'informations multifacettes et du partage de l'information pour parvenir ultimement à une interface utilisateur fonctionnelle et améliorée. Les outils de visualisation du champ de bataille à haute fidélité, intégrant idéalement des fonctions de réalité amplifiée (RA)[98] ou de réalité virtuelle (RV) dans le but d'améliorer l'affichage de l'information, la performance, la viabilité du système et l'intégration de la conception, sont des domaines idéaux dans lesquels investir :

- Parmi les capacités fonctionnelles qui contribuent à l'amélioration de la présentation de l'information, mentionnons, notamment :
  - La *Connaissance de sa propre position* pour fournir des informations à ce sujet en utilisant les dispositifs de géorepérage disponibles est désignée comme une capacité « à l'épreuve des pannes ».
  - Soutien à la navigation pour améliorer la connaissance de sa propre position, facilité par des fonctions de planification limitées, axé sur le soutien en cours de route avec navigation pas-à-pas.
  - *Connaissance de sa propre position* améliorée par l'ajout de la position et des activités des forces amies, neutres et hostiles, d'alarmes de proximité, etc.
  - Soutien à la CS partagée de décideurs dispersés grâce à des outils de planification en collaboration et de représentation de l'information.
- Outils habilitants :
  - Affichage tactique intégré, habilité par la réalité amplifiée (RA)[99]/la réalité virtuelle (RV) pour offrir une fonction d'affichage configurable par l'utilisateur des informations disponibles auprès de multiples sources de données. Aux plus bas niveaux, le degré de configuration par l'utilisateur

97. La dimension humaine comprendra la compréhension de la structure sociale et organisationnelle, ainsi que la structure des tâches et des compétences des groupes d'utilisateurs.

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

99. Les dispositifs du RAv, en particulier les viseurs de capteurs, pourraient être améliorés à l'aide d'informations supplémentaires superposées aux données du capteur pour fournir des détails plus fins au sujet de la zone d'objectif. Par exemple, un viseur habilité par RA exploitant des services géoréférencés qui sait où se trouvent l'opérateur et la cible, pourrait fournir à l'utilisateur des informations contextuelles supplémentaires et configurables comme le profil de l'objectif (lorsque c'est une personne), les capacités de l'objectif, etc.

pourrait bien être limité par la bande passante et les impératifs de la sécurité; cependant, pour d'autres segments d'utilisateurs, la demande pourrait être plus forte pour une image de la situation opérationnelle définie par l'utilisateur (ISODU) ou définie par l'individu[100] :

- Se concentrer sur n'importe quelle zone d'intérêt dans le monde et obtenir des données à son sujet à partir des ressources régionales et nationales pertinentes.
- Créer des images de la situation opérationnelle pertinentes à de multiples niveaux d'abstraction, à partir de la perspective de C2 du théâtre destinée à l'équipe de prise de décisions au niveau stratégique, jusqu'à des vues détaillées et axées sur le niveau tactique qui sont adaptées aux besoins des soldats ou des sections pour la prise de décisions.
- Transformer de grandes quantités de données brutes en scénarios significatifs, compréhensibles à première vue et animés vers le passé et vers l'avenir.

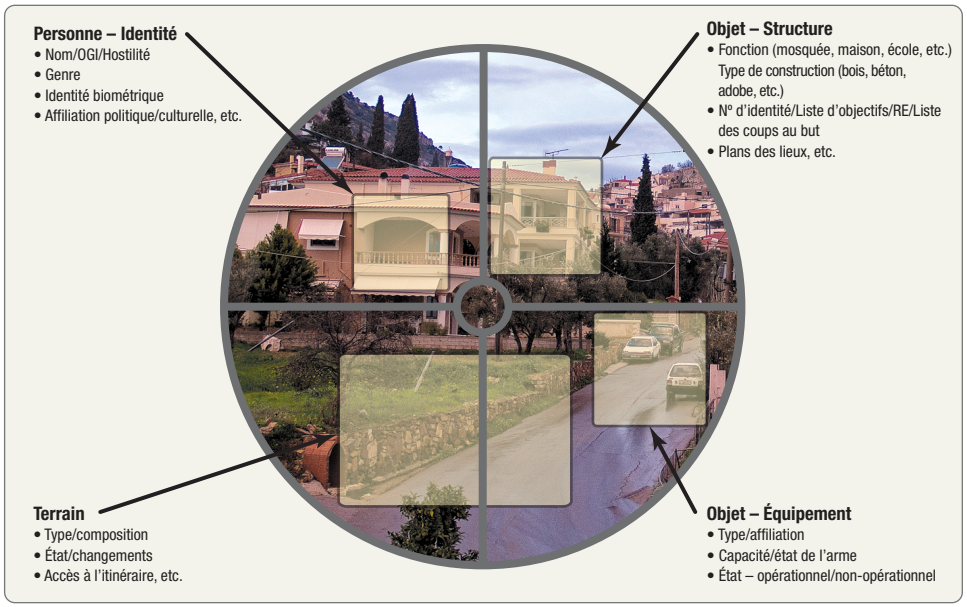

Figure 7 : Exemple de viseur de capteur à réalité amplifiée

100. Une ISODU offre une vue personnalisée et adaptable des informations pertinentes pour l'opération à divers abonnés en fonction de leurs besoins.

- Répétitions en trois dimensions – Une fonction hautement souhaitable serait la visualisation de l'espace de combat en trois dimensions – reliant l'imagerie numérique, des données de relief numériques (DTED) et des mises à jour en temps réel des changements de l'environnement physique – ce qui permettrait aux commandants et états-majors de tenir des jeux de guerre/des répétitions plus réalistes.
- Des concepts comme une *table des opérations numérique* légère, multitouches/multiutilisateurs (MTMU)[101], compacte et horizontale, autour de laquelle les commandants et leurs subordonnés pourraient se rassembler pour faire la planification et qui intègre des couches d'informations en temps quasi réel et réel pour compléter les données provenant des capteurs procureraient un outil idéal.

Améliorer la portée. Le but de l'expansion de la portée est d'augmenter l'auditoire ou les destinataires de l'information offerte sur le réseau. La capacité « à l'épreuve des pannes » la plus importante pour augmenter la portée sera un réseau en phonie protégé à tous les destinataires. Ce réseau va devoir offrir une grande disponibilité, être redondant, offrir des transmissions multiprotocoles et permettre aux utilisateurs de communiquer par la voix, par texte ou au moyen de graphiques :

- **Service de réseau en phonie protégé à tous les destinataires**.
  - Un service de transmission en phonie protégée à tous les destinataires, partout, en tout temps, avec une capacité de transmission en phonie qui ressemble à celle du poste radio tactique. Il s'agit d'une capacité « à l'épreuve des pannes ».
  - La communication en phonie privée partout, en tout temps, offre une fonction semblable à celle du téléphone, c'estàdire que la communication privée en phonie entre deux personnes peut être établie entre les nœuds équipés du matériel voulu**.**
- **Nœuds de sécurité multiconditions-multiniveaux**. Dans les OAD, les soldats canadiens peuvent s'attendre à devoir échanger des informations dans un environnement IIMP. Ces accords d'échange d'informations vont probablement être temporaires, évoluer rapidement et se dérouler dans un environnement où les réseaux de la coalition ne

101. Un MTMU est un écran tactile élevé verticalement ou horizontalement au-dessus du niveau du sol. Le mode standard d'utilisation est celui où l'utilisateur se tient à côté pour utiliser l'écran. Le contrôle de l'écran se fait au moyen de gestes accompagnés de touches simultanées sur l'écran. Les gestes habituels sont les gestes simples d'utilisation d'une souris (pointer, traîner, etc.) et des gestes plus complexes comme par exemple de tracer des cercles. Le dispositif peut reconnaître un nombre arbitraire de points ou de gestes. N'importe quel support graphique peut être affiché sur l'écran. Un exemple concret de MTMU est l'écran multitouches du Centre de contrôle des élections de la chaîne CNN.

seront pas nécessairement certifiés et accrédités (fiabilité) au même niveau d'interconnectivité que le nôtre. Donc, les dispositifs/nœuds mis à la disposition de la plupart des segments d'utilisateurs vont devoir être en mesure d'échanger des informations dans des contextes de sécurité multiconditions, multiniveaux. Les dispositifs du RAv vont avoir besoin d'une solution *de sécurité interdomaines* qui étend la portée de l'information au-delà des domaines de sécurité – à cet égard, un modèle qui élargit les types actuels de classification de l'information de Très secret (RENS stratégique, etc.) en passant par Secret (RENS tactique, planification à long terme, etc.) jusqu'aux informations sans classification. Une classification proposée connue sous le nom de *Sensible, mais non classifiée* (SNC) associée à des conditions de sensibilité pourrait permettre l'inclusion ou l'exclusion des partenaires IIMP, selon qu'ils sont fiables ou non, dans l'échange d'informations (en grande partie périssables).

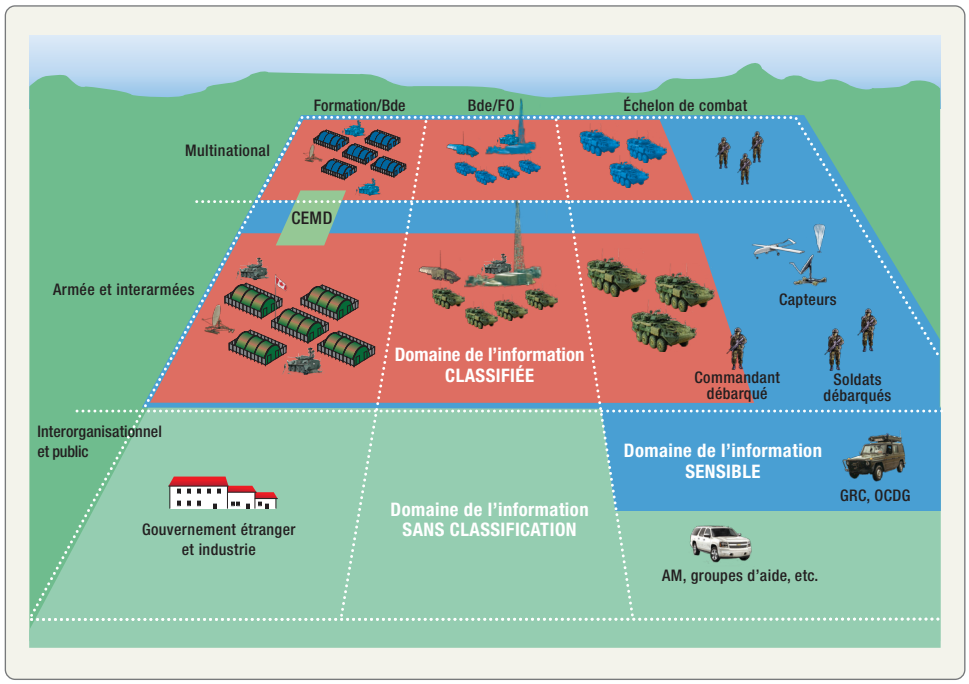

Figure 8 : Niveaux de sécurité indépendants multiples – Étendus à l'environnement IIMP

- **Intégration et interopérabilité**. Un des objectifs du RAv devrait être l'interopérabilité avec les réseaux interarmées et de la coalition, initialement en périphérie du domaine réseau de l'AC, entre l'AC et les partenaires de la coalition.
    - L'intégration du plus grand nombre possible de composantes du RAv est un objectif de capacité souhaitable si ce n'est que pour réduire ou éliminer les intergiciels (comme points de défaillance) qui sont actuellement nécessaires pour permettre à des systèmes disparates de communiquer les uns avec les autres.
    - Les composantes réseautées vont devoir être interopérables avec le système porteur du réseau (connectivité physique avec les diverses composantes), au niveau des données (modèle de données commun), au niveau des applications et services, et au niveau des politiques de sécurité.
    - Compte tenu de la nécessité d'opérer dans un environnement IIMP[102], le RAv doit être interopérable au niveau opérationnel avec les réseaux de nos alliés, en particulier les armées ABCA, les FC (interarmées et services) et d'autres ministères (AM).
- **Amélioration de la production**. Le réseau de l'ATdD devrait être amélioré par l'ajout d'une bande passante à grande capacité dans l'ensemble de la ZO.
- **Communications interactives en temps réel (CITR)**. Des capacités[103] de ce genre pourraient permettre aux soldats de clavarder rapidement – un à un, un avec plusieurs, point à point, messages de texte non structuré – sans devoir utiliser des systèmes de communication en phonie. Les CITR pourraient être améliorées au moyen d'une recherche parsable, de carnets d'adresses intégrés, de médias intégrés, de réglage de priorité des messages et de signatures numériques.

---

102. Dans un environnement où on s'attend à ce que l'information soit partagée entre les partenaires IIMP, le projet de commandement et contrôle intégré des FC a identifié « trois types d'informations qui pourraient être partagées dans le cadre d'une collaboration interministérielle de mission » :
    - Liste (base de données) de problèmes/questions qui n'ont pas encore trouvé de solution/réponse.
    - Liste (base de données) de ressources qui pourraient être disponibles en cas de crise dans l'ensemble des autres ministères/agences pertinents.
    - Une « Image de la situation opérationnelle connue » pour chaque mission en cours, produite par le ministère responsable pour confirmer les actions prises collectivement et le degré de succès obtenu.

103. N'importe quel service de clavardage par exemple.

Capteurs réseautés. La liaison de divers capteurs les uns avec les autres va non seulement permettre de partager les produits de ces capteurs, mais également l'attribution intelligente des ressources des capteurs, la collaboration machine-machine, etc. :

- **Produit de capteur partagé**. Le produit du capteur en format multimédia devrait être partageable, à de nombreux niveaux des segments d'utilisateurs.
- **Attribution des capteurs**. Tous les capteurs devraient non seulement être visibles à l'autorité d'affectation, mais également les uns pour les autres (découverte).
- **Collaboration machine-machine**. La mise en file d'attente (défection) des capteurs et armes est une capacité particulièrement utile qui permet l'identification, l'acquisition et l'engagement d'objectifs à distance de sécurité.
- **Discrimination active et passive de la menace**. Il s'agit d'une capacité qui, conjointement avec l'utilisateur humain, permet l'identification des menaces dans un environnement à forte densité.

Portée améliorée

- Étendre la portée des suites de communication en offrant des capacités d'expansion comme les postes de retransmission automatique placés à bord d'aérostats.
- Mobilité, particulièrement par l'optimisation des communications et à l'aide de composantes réseau petites, légères et à faible puissance.
- Services géoréférencés. Compte tenu de la dispersion physique prévue de la force habilitée pour les OAD, les composantes du RAv vont devoir non seulement être conscientes de leur propre position, mais également être capables de « découvrir » d'autres dispositifs (des capteurs, par exemple) et être en mesure d'accéder à des services sur demande qui sont configurés pour l'utilisateur et la position. Les services géoréférencés peuvent inclure des services comme l'état de la circulation, la navigation pas-à-pas jusqu'à des adresses particulières, le suivi des ressources, les avis ou alertes de proximité, etc.

Améliorer la distribution des produits du renseignement. Le réseau devrait fournir des renseignements exploitables dans divers formats multimédias à un large éventail d'utilisateurs. La force habilitée pour les OAD va devoir être mieux en mesure que maintenant de partager les données brutes entre soldats, entre le soldat et le commandant, débarqués ou embarqués, et entre le soldat et les éléments à l'appui. Par exemple, la fourniture de lunettes de fusil à technologie numérique pour

améliorer la capacité du soldat de servir de premier capteur devrait permettre, par exemple, le partage en temps presque réel d'images numériques entre soldats tout en alimentant simultanément les outils d'analyse du renseignement.

Améliorer la létalité

- Les éléments de la force habilitée pour les OAD vont avoir besoin d'un accès réseauté aux ressources d'appui-feu interarmées. Comme l'appui-feu indirect d'une force se caractérise généralement par un haut degré de contrôle centralisé, une forte demande, une planification longtemps à l'avance (RE et critères de sélection des objectifs), ainsi que par des procédures de demande spéciales, le RAv va devoir permettre aux observateurs de recueillir et de disséminer des informations sur l'objectif aux éléments d'appui-feu interarmées.
- Deuxièmement, beaucoup de segments d'utilisateurs vont avoir besoin de la capacité de mieux contrôler l'engagement des objectifs par les ressources d'appui-feu indirect que ce n'est le cas actuellement. Ce besoin pourra être satisfait par une combinaison de capteurs intégraux et d'observateurs formés et autorisés présents à des niveaux beaucoup plus bas que ce n'est le cas actuellement. De toute façon, il va continuer d'y avoir une forte demande pour l'appui-feu, combinée à des priorités en concurrence pour l'utilisation de ressources limitées, et c'est pourquoi le RAv va devoir fournir l'accès à des mécanismes d'attribution de l'appui-feu tout en encourageant une allocation agile des ressources en question.
- Plates-formes d'armes comme nœuds du RAv. Le réseau va devoir habiliter l'échange de données de surveillance et d'acquisition d'objectifs entre les plates-formes d'armes, autonomes et avec servants, en les traitant comme des nœuds du réseau.
    - Mettre en œuvre une capacité d'engagement coopérative[104] dans un éventail de systèmes d'armes et de capteurs, notamment les systèmes embarqués et débarqués d'appui-feu direct et indirect. La CEC permet au soldat ou au système d'armes hors de contact avec la menace d'engager un objectif qu'un soldat ou capteur en contact avec cette

104. Capacité d'engagement coopérative (CEC). La CEC permet à un capteur d'arme source de communiquer des données sur l'objectif au capteur d'arme destinataire et aux décideurs. Le décideur accepte ou rejette l'invitation à engager et, tant qu'il ne l'a pas acceptée, il conserve le plein contrôle du système d'arme. Si le décideur accepte l'invitation à engager l'objectif, le système d'arme se déplace automatiquement vers l'azimut de l'objectif. Le décideur reprend ensuite le contrôle du système d'arme et termine le processus d'engagement.

dernière a désigné. Aussi bien le capteur/marqueur que le tireur peuvent voir la cible par l'entremise du capteur.

- ✦ Collaboration entre armes/plates-formes intelligentes. Les logiciels de ciblage vont devoir être intelligents et encourager la collaboration entre les plates-formes de capteurs et d'armes. Une capacité qui permet le parsage automatique des demandes de tir en fonction de la disponibilité d'une plate-forme pour attaquer l'objectif, choisir les munitions et mettre en file d'attente les missions de tir et la défection[105], devrait être l'objectif de capacité de base au sein de la capacité d'appui réseautée.
- ✦ Permettre au soldat de servir de marqueur d'objectif et de partager cette information avec un large éventail de nœuds du RAv (nœuds de commandement, autres soldats, capteurs et plates-formes d'armes, etc.).
- ✦ Permettre au décideur de modifier l'effet des munitions après le tir ou le lancement.

Protection du réseau

- ➢ **Sécurité de l'information**. Le RAv va devoir offrir des plates-formes informatiques protégées. Parmi les solutions possibles, mentionnons l'architecture de la plate-forme à un niveau d'assurance élevé parrainée par la NSA, qui soutient de multiples domaines de sécurité sur une même plate-forme informatique et des machines virtuelles exploitées sur une plate-forme informatique fiable.
- ➢ **Autoprotection**. Compte tenu de la prolifération prévue des capteurs autonomes, des nœuds réseautés éloignés, des chemins de dissémination et du stockage des données, le RAv va avoir besoin d'un niveau élevé de protection contre les attaques de réseau informatique (CNA), le brouillage et le sabotage.

Abaisser le coût d'utilisation

- ➢ **Instruction simplifiée**. La mise en service d'un réseau ne peut réussir sans un plan exhaustif de mise en service et de formation. Reconnaissant cette exigence, l'Armée de terre va devoir s'assurer que la livraison des composantes du RAv est coordonnée avec le chemin menant au

105. Pour en apprendre davantage sur la modélisation de la mise en file d'attente et de la défection, en particulier sur l'efficacité des systèmes pour répondre aux demandes de tir en tenant compte du délai d'intervention, de la distance entre les systèmes de tir et les objectifs, et du nombre d'objectifs à attaquer, voir S. Wheeler, *An Application of Queues to Offensive Support Indirect Fire Weapon Systems*.

niveau de préparation élevé, comprend des outils d'autoapprentissage, encourage la rétroaction des utilisateurs sur la convivialité des systèmes et la facilité d'utilisation, et s'engage en faveur d'une mise en service évolutive de la technologie. Autrement dit, éviter le piège décrit comme suit : « essayer de voir comment utiliser correctement une nouvelle technologie en plein milieu d'un échange de feu est la clé de l'échec »[106].

- **Soutien du système**. Le RAv va avoir besoin d'un degré élevé de fiabilité, de disponibilité, de soutenabilité et de durabilité (FDSD) et ne devra pas imposer un fardeau de maintenance à chaque soldat.
    - Fiabilité. Les composantes du RAv doivent pouvoir s'autorégénérer dynamiquement et reformer le réseau lorsqu'un ou plusieurs chemins de communication entre ses nœuds sont perturbés.
    - Disponibilité. Il y a nécessité opérationnelle que le RAv puisse fonctionner 24/7 dans tous les climats et dans toutes les conditions météo et de terrain.
    - Soutenabilité. Grâce à la technologie des matériaux légers, les composantes du RAv vont être optimisées pour réduire leur taille, leur poids et leur puissance.
    - Durabilité.
- **Gestion du système**. Les capacités de gestion du système devraient viser à réduire le fardeau de gestion des dispositifs du RAv pour les gestionnaires de systèmes, les opérateurs, les techniciens et les utilisateurs.
    - Intégration des dispositifs grâce à l'autodétection qui permet aux dispositifs réseautés de se découvrir l'un l'autre et de s'enregistrer l'un auprès de l'autre.
    - Service de planification des transmissions. Une capacité semi-automatique de planification des transmissions pour aider à l'élaboration du plan des transmissions.
    - Tableau de contrôle de la plate-forme. Suivi et contrôle des dispositifs et services intégrés aux plates-formes à partir d'un point d'entrée unique.
    - Lancement automatique des actions du système fondé sur l'état du dispositif ou du service (par exemple, à la détection

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

d'un bas niveau de carburant, un véhicule réseauté pourrait déclencher automatiquement une demande de PP).

- ✦ Transfert accru de données à tous les segments d'utilisateurs.

Maintien en puissance. Compte tenu de la dispersion des nœuds dans l'espace, le réseau va devoir être conçu pour permettre des fonctions de SLC intelligentes tout en réduisant le besoin de soutien spécialisé du système :

- ➢ **Fonctions de SLC**. La force habilitée pour les OAD va avoir besoin d'une empreinte logistique réduite (par exemple, une demande réduite de sources d'alimentation jetables ou la fourniture de sources d'alimentation régénérantes) et la capacité de configurer intelligemment les chargements de ravitaillement. Donc, un des objectifs de capacité du RAv devrait être de fournir des rapports automatiques sur les fournitures consomptibles, peut-être à l'aide de technologies semblables à celle des dispositifs à identification par radiofréquence (IRF) – fixés sur des palettes de munitions, des contenants d'eau et de nourriture, etc.).
- ➢ **Fonctions de SSS**. Les systèmes de monitoring psychologique peuvent améliorer la survie des soldats en fournissant des informations de triage en cours de route aux éléments de soutien médical et en assurant une intervention médicale opportune. Donc, un objectif de capacité SSS pour le RAv pourrait être la fourniture de dispositifs individuels de monitoring biométrique pour appuyer le diagnostic des blessés.

SEGMENTS D'UTILISATEURS

Après avoir décrit les buts généraux et certains objectifs de capacité particuliers du RAv, nous pouvons maintenant nous intéresser à la question de savoir quels segments génériques d'utilisateurs[107] existent et quels genres d'informations ils vont consommer. La présente étude évite délibérément d'identifier les besoins très particuliers des branches et des métiers spécialisés puisque les structures de l'AC vont probablement évoluer dans le temps et que les capacités vont se déplacer d'une branche à une autre. Il faut donc une structure utile composée de classes très larges, laquelle existe déjà heureusement sous la forme des catégories d'utilisateurs identifiées dans le cadre du projet de prolongation de la durée de vie du système d'aide au commandement terrestre (SACT). La présente section évite à dessein

107. Différents utilisateurs sollicitent le réseau de différentes façons et vont souvent utiliser la même information dans différents contextes et il va donc falloir que le réseau offre une gamme d'applications et de capacités adaptées à la manipulation de ces informations.

toute discussion ciblée sur les groupes d'utilisateurs à l'extérieur du RAv; ces groupes pourraient par exemple inclure les réseaux ministériels au sein du MDN, ou encore des segments d'utilisateurs avec lesquels nous pourrions souhaiter échanger des informations, mais en fonction desquels le RAv n'est pas conçu. Finalement, il est important de noter que ces grandes classes d'utilisateurs peuvent comprendre des entités humaines et non humaines. En étendant la classe des utilisateurs aux acteurs non humains, on peut intégrer les systèmes autonomes dans la discussion sur le RAv.

Les segments d'utilisateurs sont les suivants :

- ***Segment débarqué – Combattants.*** Ce segment regroupe habituellement les soldats des armes de combat; ce soldat est le module de base de la section ou du détachement et constitue un niveau d'entrée humain commun et important de l'information dans le RAv. Les soldats livrent des combats rapprochés et peuvent être dispersés physiquement dans l'accomplissement de leurs tâches, lesquelles incluent, notamment, le combat rapproché à découvert et en terrain complexe, et les opérations aéromobiles. Les engagements sont habituellement de courte durée et exigeants physiquement, et font appel à des ressources cognitives substantielles pour l'accomplissement de tâches clairement définies. Les soldats débarqués sont hautement mobiles et doivent être entièrement autonomes pour survivre jusqu'à 72 heures de contacts très intenses. Les capacités prioritaires que le soldat va demander du RAv seront une capacité de communication protégée partout et des outils de visualisation du champ de bataille qui offrent une présentation simplifiée de l'image tactique locale. Le soldat a donc besoin que les composantes du RAv puissent répondre à ses besoins dans des situations évoluant rapidement où le temps manque pour une planification délibérée, ou pour la production et l'évaluation de plans d'action (PA) détaillés[108]. En combat rapproché, le soldat va avoir besoin de mécanismes faciles à utiliser pour chercher et transmettre des informations, notamment dans le but de modifier les plans et de se resynchroniser avec les forces amies sur les flancs. Les composantes offertes à ce segment vont avoir besoin d'une interface à « sélection par coups d'œil rapides » comportant peu d'options d'entrée initiale, conformément à un principe de conception supérieur offrant des composantes qui (1) sont *simples à utiliser*, (2) sont légères et *portables*, (3) ne nuisent pas aux mouvements individuels et (4) ne

108. A. Tate, J. Levine, P. Jarvis et J. Dalton, *Using AI Planning Technology for Small Unit Operations*. Voir http://www.aiai.ed.ac.uk/~oplan.

distraient pas l'attention de la vision localisée de l'espace de combat. « L'information[109] qui devait être acheminée en vitesse aux membres du peloton devrait se limiter uniquement à l'information cruciale qui a une incidence sur leurs décisions et leurs actions. On réduirait ainsi la densité des affichages pour en faciliter la lecture et la compréhension. Les soldats devraient pouvoir « demander » des informations qui sont moins cruciales et dont ils n'ont besoin qu'occasionnellement. Le caractère crucial de la connaissance des positions des forces ennemies au-delà de la portée des armes légères depuis la zone de l'objectif augmente en parallèle avec le niveau de leadership. »

- ***Segment embarqué – Combattants.*** Ce segment se compose des soldats qui font normalement partie des armes de combat. Dans ce rôle, ils livrent combat à partir de plates-formes mobiles en engageant des objectifs à l'aide d'armes à tir direct depuis des distances souvent plus grandes que lorsqu'ils sont employés comme combattants dans le segment débarqué. Ils peuvent s'attendre à exécuter des mouvements dans l'espace de combat sur de longues distances, à faire des appréciations de combat avec des outils simplifiés et à donner et recevoir des ordres, ainsi que d'autres instructions en mouvement. Outre les capacités prévues pour le segment débarqué – combattants, les nœuds du RAv installés à bord des plates-formes du segment embarqué vont devoir (1) être simples à utiliser, (2) capables d'assurer les communications en phonie, en texte et par graphiques et (3) offrir une vue organique et inorganique des données transmises par les capteurs, le tout optimisé en fonction d'un environnement où la bande passante est limitée.
- ***Segment PC tactique/QG.*** Dans le segment PC tactique/QG, le RAv est optimisé pour appuyer un commandant d'unité ou de sous-unité tout en fournissant simultanément un certain soutien à son état-major de combat. Les commandants à tous les niveaux ont besoin d'une très bonne connaissance et compréhension de la situation. Le commandant utilise les composantes du RAv pour recevoir et diffuser une image commune de la situation opérationnelle, pour communiquer avec les subordonnés, pour planifier et contrôler les opérations, et pour collaborer avec d'autres utilisateurs. On peut résumer les besoins d'informations des commandants à un intérêt pour l'état de l'opération en cours, les PA disponibles pour les opérations à venir et des informations au sujet

109. E. Redden, *Virtual Environment Study of Mission-based Critical Information Requirements*, ARL-TR-26-36, mars 2002, p. 2.

de l'intention du commandant supérieur. Les besoins d'informations du commandant se caractérisent par un équilibre entre opportunité, qualité et pertinence – autrement dit, il peut avoir grand besoin d'un éventail d'informations dans des circonstances évoluant rapidement.

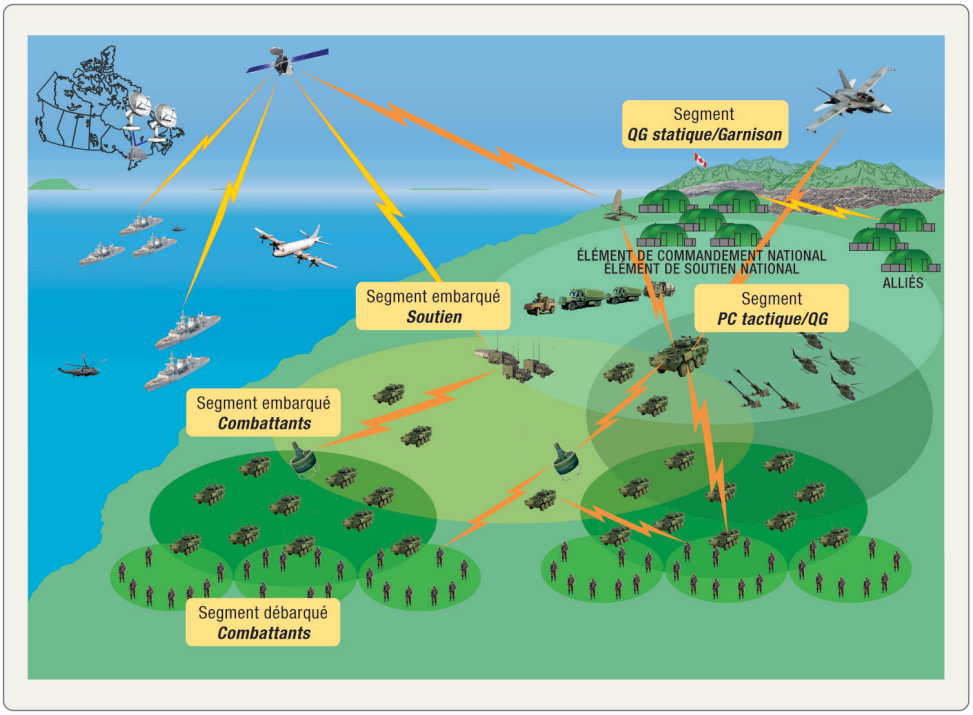

Figure 9 : Segments d'utilisateurs

- ***Segment embarqué – Soutien***. Les éléments de soutien sont informellement groupés selon que leur tâche première est d'aider le commandant grâce à un appui au combat spécialisé (appui-feu, génie de combat, etc.) ou d'assurer le maintien en puissance (SLC, SSS, etc.) de la force. Ce segment peut se subdiviser en ceux qui ont pour fonction principale de soutenir la disponibilité du réseau et de l'infrastructure de communications. En tant qu'éléments de soutien, leurs besoins d'informations sont complexes; ils consomment un grand volume d'informations et doivent avoir accès à des outils d'analyse spécialisés. Leurs besoins réseau sont passablement différents de ceux des combattants en ce que leur rôle premier est un rôle de gestion des ressources; ils ont moins besoin de composantes légères et portables,

mais plus besoin de composantes qui peuvent fournir une analyse plus poussée, adaptée à la spécialité du soutien (par exemple, les éléments de soutien SLC ont besoin d'un meilleur accès à l'information et d'informations plus complexes au sujet de l'état des ressources).

- ***Soutien au QG statique/à la garnison***. Dans ce segment, les composantes du RAv sont optimisées aux fins du commandant et de son état-major dans un environnement statique. Le segment de soutien au QG statique/en garnison appuie le commandant grâce à l'analyse et à des conseils. L'état-major doit avoir accès à des outils de planification collaborative et d'analyse, aux services communs et à des documents de doctrine et d'opération, et, évidemment, à la connaissance de la situation. Les commandants et états-majors à tous les niveaux ont besoin d'une très bonne connaissance et compréhension de la situation. Le commandant utilise les composantes du RAv pour recevoir et disséminer l'image commune de la situation opérationnelle, pour communiquer avec les subordonnés, pour planifier et contrôler les opérations, et pour collaborer avec d'autres utilisateurs. Les besoins en information du commandant peuvent se résumer en un intérêt pour l'état de l'opération en cours, les PA disponibles pour les opérations à venir et des informations au sujet de l'intention du commandant supérieur.
- ***Acteurs non humains***. Avec la prolifération des capteurs, des plates-formes d'armes et des acteurs non humains sur le champ de bataille, les commandants vont avoir besoin d'un moyen de diffuser des instructions claires et de communiquer leur intention[110] à des machines ou à des acteurs non humains dans le RAv. En fait, il va falloir consacrer beaucoup d'efforts pour développer et livrer une solution technique[111] capable d'exécuter le C2 entre humains et acteurs non humains. En outre, les acteurs non humains vont devoir être équipés de protocoles de validation pour déterminer la pertinence des critères de décision comme les règles d'engagement, les permissions ou interdictions de tirer, la sélection des tâches, la survivabilité, etc.

Il reste encore beaucoup à expliquer au sujet de la manière dont une force habilitée pour les OAD pourrait être organisée, équipée et entraînée pour combattre et,

110. Les travaux exécutés jusqu'à maintenant au sein de la Simulation Interoperability Standards Organization (SISO) visant à créer un langage de gestion du combat (LGC) adapté à la transmission d'informations de C2 à des nœuds non humains pourraient bien nous guider dans la réalisation de cet objectif.

111. Bien qu'il soit possible dès maintenant de communiquer des instructions simples (où, qui, quand, comment, etc.) entre nœuds humains et non humains, il faudrait investir des efforts considérables pour réaliser un moyen de communiquer l'intention du commandant (pourquoi) combiné à l'impératif moral entre les nœuds humains et non humains.

en l'absence de ce modèle d'emploi, il va être difficile de décrire pleinement les capacités réseau requises. Finalement, il est important de se rappeler que le réseau sera conçu pour le combattant, peut-être un officier supérieur commandant une formation ou un sous-officier commandant de section et que, dans cette optique, la technologie à mettre en œuvre doit améliorer la prise de décisions plutôt que d'ensevelir le décideur sous un grand volume d'informations. La clé pour atteindre ce but réside dans une instruction réaliste de niveau avancé sur l'utilisation des nouvelles technologies, combinée à l'habilitation des soldats comme juges et décideurs.

AUTRES OBJECTIFS

Les objectifs énumérés ci-dessous ne s'insèrent pas facilement dans la structure des segments d'utilisateurs ci-dessus, mais ils sont importants pour la réalisation d'un RAv :

- **Instruction**
  - Autoformation. Les composantes du RAv devraient être conçues pour encourager leur utilisation, l'expérimentation et l'autoformation par modules dans le cadre de logiciels d'instruction intégrés. Des concepts comme les dimensions multiutilisateurs intégrées (MUD) pourraient être envisagés.
  - Facteurs humains
    (a) Les composantes sont centrées sur l'utilisateur et ne créent pas de fardeau supplémentaire ou n'empêchent pas autrement l'utilisateur de remplir ses tâches habituelles.
    (b) Les composantes sont intuitives et faciles à utiliser, grâce à une interface homme-machine intuitive, à des procédures d'utilisation simples et à une grande simplicité.
    (c) Les composantes ont aussi peu de parties que possible. Les composantes du RAv ne doivent pas nuire aux mouvements, embarqués et débarqués, et doivent être légères (idéalement 4,5 kg ou moins, avec batteries et câbles).
  - Éducation et instruction intensives. Inévitablement le RAv, en tant que système de systèmes, aura certaines composantes qui comprendront des systèmes de communication et de logiciels d'application complexes. Il est donc fort probable

que certaines de ces composantes, en particulier celles dédiées à l'administration du système, vont continuer d'exiger beaucoup d'instruction et d'éducation, même si le but reste de réduire ce besoin le plus possible.

- **Souplesse :** Le RAv doit être souple dans ses configurations physiques et logiques. Les configurations souples vont permettre au RAv de s'adapter aux utilisations d'une vaste gamme d'organisations et d'environnements, ainsi qu'à une variété de circonstances opérationnelles. Il faut reconnaître que ce ne sont pas toutes les composantes du RAv qui exigent le même degré de souplesse; par exemple, certaines suites de communications peuvent avoir certaines propriétés physiques ou logiques (taille, sécurité, etc.) qui, en réalité, restreignent cette souplesse. L'idéal est de parvenir à une souplesse universelle, tout en admettant que cet objectif n'est pas nécessairement réalisable aujourd'hui compte tenu des contraintes actuelles en matière de technologie et des exigences d'emploi particulières :
  - Les composantes du RAv devraient pouvoir s'adapter rapidement et automatiquement à la configuration du segment d'utilisateurs et au type d'opération. Par exemple, le RAv sera capable de configurer automatiquement les services en fonction du profil de l'utilisateur, des exigences particulières de la mission et du type d'opération. En fin de compte, les composantes du RAv devraient être conçues pour s'adapter à toute structure ou circonstance opérationnelle.
  - Certaines composantes du RAv, en raison de leur complexité ou par suite des exigences de sécurité, pourront encore nécessiter l'intervention d'un spécialiste sur place pour les configurer aux fins de l'utilisateur.

Outre ces exigences de capacité générales, les composantes du RAv devraient être hautement adaptables et évolutives pour satisfaire les besoins de l'Armée de terre après 2021.

Chaque composante possible du RAv devra également être soigneusement étudiée pour comprendre toutes les implications de l'analyse PRICIE[112] et pour s'assurer qu'elle est viable en vertu de l'enveloppe budgétaire globale de l'ATdD.

112. La mnémonique PRICIE fournit un cadre d'analyse normalisé pour évaluer et construire de nouvelles capacités. Les lettres de l'acronyme représentent les éléments suivants : Personnel, instruction et leadership; Recherche, développement et recherche opérationnelle (plus l'expérimentation); Infrastructure, environnement et organisation; Concepts, doctrine et instruction collective; gestion et technologie de l'Information; Équipement et soutien.

ÉTAT FINAL

Le réseau de l'avenir va relier commandants, soldats, capteurs et armes dans un réseau d'échange d'informations continu qui va permettre à l'Armée de terre de dominer l'espace de combat. Le RAv va offrir un réseau protégé et robuste qui fournit la connectivité nécessaire à tous les nœuds opérationnels de l'Armée canadienne – y compris la liaison arrière avec les réseaux nationaux/interarmées – et qui peut être étendu à l'environnement IIMP.

PARTIE 6 – RECOMMANDATIONS ET CONCLUSIONS

Recommandations

- Élaborer une stratégie de C4ISR de l'Armée canadienne pour identifier les capacités requises et gérer leur mise en œuvre en tenant compte des limites de ressources, du besoin d'accommoder les plans de prolongation de la durée de vie des systèmes existants et du besoin de mettre en œuvre une capacité réseau de manière évolutive.
- Élaborer une stratégie exhaustive de gestion de l'information de l'Armée de terre incluant l'environnement IIMP.
- Élaborer une architecture générale de réseau de la FT pour régir la mise en œuvre du RAv jusqu'en 2028. Cette architecture devrait être conforme à l'architecture C4ISR des FC (CAMDN).
- Élaborer un modèle d'emploi de la force pour les OAD, ainsi que des modèles détaillés d'utilisation des composantes du RAv dans diverses opérations.
- Élaborer une ontologie exhaustive du domaine militaire. Coordonner les chevauchements de zones d'intérêt entre l'ontologie militaire et l'environnement IIMP.

Domaine de recherche pour optimiser le RAv

- Élaborer une ontologie détaillée du commandement et contrôle.
- Élaborer un modèle de découverte/enregistrement automatique des plates-formes de tir direct et indirect, la mise en file d'attente et la défection, ainsi que les méthodes de commandement et contrôle dans un environnement semi-automatisé.
- Quelle sera la nature des échanges d'informations avec les partenaires IIMP au sein du QG de l'ATdD?
- Étudier les représentations pictographiques simplifiées[113] des objets[114] du champ de bataille.

113. Voir l'iPhone Apple.

114. Le développement d'icônes graphiques pour l'utilisation militaire découle du besoin de représenter les objets militaires au moyen de formes simples et analogues sur les quelques militaires. Au cours des récentes années, peu de travaux ont été faits en vue de simplifier la représentation de ces symboles militaires dans le domaine numérique, en particulier dans le but de numériser une image sur un petit écran d'affichage. Pour communiquer des informations complètes sur des dispositifs manuellement sans encombrer l'affichage, il est probable que les composantes du RAv vont avoir besoin de présentation graphique encore plus simplifiée pour représenter les objets du champ de bataille que ce qu'offre actuellement le lexique des symboles militaires de la doctrine actuelle.

APPENDICE 1 – REVUE DES DOCUMENTS SUR LES OPÉRATIONS FACILITÉES PAR RÉSEAU

Généralités. Les ouvrages sur les opérations facilitées par réseau se sont grandement multipliés au cours des cinq dernières années. En commençant par Cebrowski et Gartska, on voit que le développement des concepts est généralement resté dans le domaine du développement des capacités aux États-Unis d'Amérique. Récemment, les rédacteurs de la doctrine canadienne et alliée, et les responsables du développement des capacités ont produit un plus vaste corpus de réflexion dans le but d'examiner et d'expliquer en détail les exigences à remplir pour réaliser des OFR. Vous trouverez ci-dessous une courte liste, nécessairement incomplète, des lectures recommandées sur le sujet; cependant, il est fortement recommandé à ceux qui sont chargés de la définition des besoins de consulter la bibliographie en fin d'ouvrage. Les documents énumérés ci-après ne suivent aucun ordre particulier :

- **Beware of Putting the Cart Before the Horse: Network Enabled Operations as a Canadian Approach to Transformation**. Rapport préparé par Allan English, Ph. D., Richard Gimblett, Ph. D. et Howard Coombs pour Recherche et développement pour la défense Canada (RDDC) qui conclut que « le Canada et les FC devraient faire preuve de prudence dans l'utilisation de la guerre réseaucentrique (GR) comme base pour les OFR, car le contexte et les besoins associés à la GR ne sont peut-être pas conformes aux besoins du Canada ». Les auteurs poursuivent en affirmant de façon explicite que les théories de la GR et des OFR ne sont peut-être pas suffisamment élaborées pour répondre aux besoins particuliers du Canada et de sa culture militaire. Ils suggèrent que le réseau humain et non pas le réseau technique « devrait servir de base pour les approches de l'avenir à la transformation des FC » et que, en conséquence, la conception des réseaux de l'avenir, et en particulier le RAv, va exiger « que les architectes du réseau non seulement envisagent la technologie de l'information comme un élément habilitant, mais qu'ils se penchent sur la question beaucoup plus complexe de la création de réseaux sociaux efficaces ».
- **A Woven Web of Guesses**. Présentation du Lieutenant-colonel Ralph Giffin (CA) et de Darryn J. Reid (AUS) au 8th International Command and Control Research and Technology Symposium (ICCRTS) tenu à Washington (D.C.) en juin 2003, à l'occasion duquel les prémisses sous-jacentes de Cebrowski et Gartska présentées dans *Network-Centric*

Warfare: Its Origins and Future sont attaquées; en particulier, ils prédisaient que « le réseau militaire sera construit principalement pour satisfaire les besoins du contrôle centralisé et non ceux des opérateurs ». C'est une présentation stimulante qui va sonner l'alarme chez les concepteurs des réseaux militaires de l'avenir.

- **LandWarNet 2015**. Produit par le U.S. Army Training and Doctrine Command (TRADOC), ce document présente un concept d'opérations (CONOPS), notamment une petite vignette, et répertorie les capacités prévues dans les concepts déjà approuvés, en plus de décrire un réseau de référence unique pour toutes les fonctions opérationnelles.
- **Operational Requirements Document for the Future Combat Systems**. Produit par le Unit of Action Maneuver [sic] Battle Lab en janvier 2005, ce document énonce explicitement les paramètres de rendement clés de chaque élément du système de systèmes de combat de l'avenir de l'Armée américaine, à partir des véhicules avec et sans pilote, des réseaux de l'avenir et des suites de capteurs, en précisant les paramètres seuils et les paramètres visés pour chaque système. Il s'agit d'une ressource exhaustive pour l'élaboration des besoins de l'ensemble de la famille des systèmes de combat terrestre (FSCT).
- **NATO Network Enabled Capability Feasibility Study, Volume 1**. Document produit par l'Agence de consultation, de commandement et de contrôle de l'OTAN (NC3A) qui s'intéresse à la transformation au sein de l'OTAN et veut renforcer la capacité de l'Organisation de mieux s'acquitter de l'ensemble de ses missions et de répondre collectivement aux nouveaux défis en matière de sécurité.

APPENDICE 2 – ABRÉVIATIONS

AAP	Publication administrative interalliée (AAP)
ABCA	Programme de normalisation des armées américaine, britannique, canadienne et australienne (ABCA)
OAD	Opérations adaptables et dispersées (ADO)
ATdD	Armée de terre de demain (AoT)
EDC	Évaluation des dommages de combat (BDA)
BLOS	Au-delà de la portée optique (BLOS)
C2	Commandement et contrôle (C2)
FC	Forces canadiennes (CF)
IDCbt	Identification au combat (CID)
CNA	Attaque de réseau informatique (CNA)
ICSO	Image commune de la situation opérationnelle (COP)
SLC	Soutien logistique du combat (CSS)
DCSFT	Directeur – Concepts et schémas de la Force terrestre (DLCD)
GE	Guerre électronique (EW)
CEF	Concept d'emploi de la force (FEC)
MEF	Modèle d'emploi de la force (FEM)
SCA	Système de combat de l'avenir (Armée américaine) (FCS)
FSCT	Famille de systèmes de combat terrestre (FLCS)
RAv	Réseau de l'avenir (FNC)
ESA	Environnement de sécurité de l'avenir (FSE)
SSF	Système de suivi des forces (FTS)
PEIS	Projet d'équipement intégré du soldat (ISSP)
ISTAR	Renseignement, surveillance, acquisition d'objectifs et reconnaissance (ISTAR)
IIMP	Interarmées, interorganisationnel, multinational et public (JIMP)
AC	Armée canadienne (CA)

LOS	Observation directe (LOS)
NLOS	Observation indirecte (NLOS)
OR	Opérations réseaucentriques (É.-U.) (NCO)
OFR	Opérations facilitées par réseau (NEOps)
GTO	Groupement tactique optimisé (OBG)
PRICIE	Personnel, Recherche et développement, Infrastructure, Concepts et doctrine, technologie de l'Information et Équipement (PRICIE)
RE	Règles d'engagement (ROE)
CITR	Communications interactives en temps réel (RTOC)
CompS	Compréhension de la situation (SU)
VoIP	Voix sur IP (VOIP)

APPENDICE 3 – GLOSSAIRE

Acteur

Un acteur est une unité de responsabilité indépendante de la mise en œuvre qui exécute une action pour produire un effet qui contribue à un état final souhaité. Chaque acteur peut remplir ou plusieurs rôles. Un acteur peut être un consommateur de services. C'est généralement le rôle du commandant. Un acteur peut également être producteur de services. C'est généralement le rôle de ceux qui reçoivent du commandant l'ordre d'exécuter une tâche. Un acteur peut remplir plusieurs rôles, p. ex. un commandant peut demander un service à un subordonné, mais il fournit aussi un résultat à son commandant. Des équivalents communs sont (1) acteur d'affaire, (2) exécutant, (3) nœud logique. ***(Actor)***

Architecture

Structure fondamentale d'un système incarnée dans ses composantes, leurs rapports réciproques et à leur environnement, ainsi que les principes guidant sa conception et son évolution.

Un cadre architectural[115] est simplement une méthode de classification et d'organisation des informations et processus complexes. Il s'agit fondamentalement d'une structure dans laquelle peuvent être situés les concepts de système, une série de composantes génériques qui peuvent (ou doivent) être utilisées dans les systèmes, un ensemble de rapports (interfaces) génériques qui peuvent (ou doivent) être utilisés entre ces composantes et certaines règles au sujet de tous ceux qui guident et limitent leur utilisation, et au sujet de l'ajout de nouvelles parties ou de nouvelles composantes au cadre en question. À noter qu'en utilisant des rapports et des composantes génériques, il est possible d'étudier les capacités et caractéristiques souhaitées au sein du RAv sans être limité par les contraintes des technologies particulières. ***(Architecture)***

Architecture client-serveur

Une architecture client-serveur sépare le nœud qui héberge le logiciel utilisateur du serveur où résident les données que le logiciel utilisateur manipule. Un bon exemple d'architecture client-serveur est un moteur de recherche sur le Web. ***(Client–Server Architecture)***

115. Pour de plus amples informations sur les cadres architecturaux, veuillez consulter les Cadres d'architecture du ministère de la Défense nationale et des Forces canadiennes (CAMDN/FC) ou le Cadre d'architecture de l'OTAN (NAV v3).

Identification au combat (IDCdt) (Publication interarmées 1-02)

L'identification au combat est le processus qui permet de caractériser les objets détectés dans l'environnement opérationnel avec un niveau de précision suffisant pour permettre la décision d'engagement. ***(Combat Identification (CID))***

Image commune de la situation opérationnelle (Banque de terminologie de l'Armée de terre, approuvé le 2 octobre 2002)

Représentation des opérations, modifiable au gré des utilisateurs, fondée sur des données et des informations partagées par plus d'un commandement. ***(Common Operating Picture)***

Système de suivi de la force (Chairman Joint Chiefs of Staff Instruction (CJCSI) 8910.01A).

Utilisation de techniques pour identifier et suivre activement ou passivement les forces américaines, alliées ou de la coalition dans le but de donner au commandant des forces de combat une meilleure connaissance de la situation dans l'espace de combat et de réduire les tirs fratricides. ***(Force Tracking System)***

Élément d'information

Un élément d'information est une représentation, indépendante de la mise en œuvre, des faits qu'il faut connaître au sujet des objets et de leur cohérence pour transformer l'ensemble ou la représentation en information. Le but de la saisie des éléments d'information est d'identifier et de décrire clairement tous les éléments d'information et leurs propriétés qui sont pertinents pour l'exécution des tâches dans l'espace de la mission. ***(Information Object)***

Intégration

Intégrer : compléter (chose incomplète) par ajout de parties; combiner (des parties) en un tout. *Pour le RAv :* 1. État de combinaison ou processus de combinaison pour rendre complet et harmonieux. 2. En informatique, permettre aux données d'un dispositif ou d'un logiciel d'être lues ou manipulées par un autre. ***(Integration)***

Interopérabilité (Répertoire de terminologie de l'Armée de terre, approuvé le 15 septembre 2005)

L'aptitude des forces militaires à s'entraîner, à s'exercer et à opérer efficacement ensemble en vue d'exécuter les missions et les tâches qui leur sont confiées. OTAN : (1) La capacité des systèmes, des unités ou des forces d'assurer des services à d'autres systèmes, unités ou forces ou d'en recevoir, et d'utiliser les services ainsi échangés pour opérer efficacement ensemble.

Interopérabilité physique – Connexion de l'infrastructure des systèmes de communication et d'information d'un utilisateur avec celle d'un autre.

Interopérabilité syntaxique – Les utilisateurs parlent la même langue, par exemple oralement ou en langage machine.

Interopérabilité sémantique – Les utilisateurs ont la même compréhension des concepts linguistiques. Par exemple, les utilisateurs ont une interprétation commune de l'information échangée.

Interopérabilité pragmatique – Le destinataire est capable d'anticiper comment agir. Le destinataire réalise l'intention de la communication transmise par l'expéditeur. Cette capacité d'agir de concert est considérée comme une condition préalable pour parvenir à l'autosynchronisation. ***(Interoperability)***

Gestion de la connaissance (Répertoire de terminologie de l'Armée de terre, recommandé en 2003)

Stratégie exhaustive qui permet la collecte, le partage, l'utilisation et la conservation efficaces des connaissances cruciales que possèdent les membres du personnel de l'Armée de terre. ***(Knowledge Management)***

Latence (Banque de terminologie de la Défense, approuvé le 3 mai 2005)

Intervalle entre l'instant où une unité de commande déclenche un appel de données et celui du début du transfert effectif de ces données. ***(Latency)***

Lieu

Un lieu est un endroit géographique, p. ex. une position représentée par des coordonnées spatiales. Le but de la saisie des lieux est de comprendre où sont exécutées les activités des acteurs. Le même acteur peut exécuter les mêmes activités à différents endroits. ***(Location)***

Commandement de mission (Répertoire de terminologie de l'Armée de terre, approuvé le 10 octobre 2002)

Philosophie de commandement qui encourage l'unité d'effort,le devoir et l'autorité d'agir, et donne l'initiative aux commandants subordonnés. ***(Mission Command)***

Temps quasi réel (Banque de terminologie de la Défense, approuvé le 11 novembre 1991)

Qualificatif appliqué à l'acheminement des données et des informations qui s'effectue sans retard si ce n'est celui du traitement automatique et de la transmission électronique. Cela implique que les délais sont presque négligeables. La distinction entre temps quasi réel et temps réel est un peu nébuleuse et doit être définie dans le contexte à l'étude. ***(Near Real Time)***

Ontologie (http://en.wikipedia.org/wiki/Ontologie_ (informatique**)**

(1) Branche de la philosophie qui s'intéresse à l'étude de l'être.

(2) En informatique et en science de l'information, l'ontologie est l'ensemble structuré des termes et concepts représentant le sens d'un champ d'informations, que ce soit par les métadonnées d'un espace de noms, ou les éléments d'un domaine de connaissances. L'ontologie constitue en soi un modèle de données représentatif d'un ensemble de concepts dans un domaine, ainsi que des relations entre ces concepts. Elle est employée pour raisonner à propos des objets du domaine concerné. ***(Ontology)***

Processus

Ensemble d'activités déclenchées par un événement qui transforme un intrant particulier en un extrant significatif. ***(Process)***

Communications interactives en temps réel (CITR)

Les communications interactives en temps réel sont un ensemble de normes et de protocoles de communication numérique en phonie et en texte pour le clavardage, les messages instantanés, etc. ***(Real Time Online Communications)***

Architecture orientée services

Une architecture orientée services (SOA) est une structure de système distribué dans lequel les applications sont décomposées en services distincts mis à la disposition des consommateurs. Ainsi, une SOA se compose de producteurs d'informations (nœuds de capteurs, soldats et commandants) et de consommateurs d'informations (commandants, planificateurs, systèmes d'armes, etc.). La relation producteur/consommateur est à la base du terme SOA. La prémisse principale d'une SOA est que les services

ne doivent pas se limiter forcément à un système; ils sont plutôt associés de façon informelle au système et fonctionnent indépendamment d'une plate-forme ou d'un système d'exploitation en particulier. Cela permet au consommateur de « découvrir » et de consommer un service sans que le client ait besoin de savoir l'origine du service. Cette caractéristique permet à la SOA de servir de multiples utilisateurs en même temps. Pour exploiter la puissance de la SOA et assurer l'interopérabilité, les nombreux services doivent être mis en œuvre suivant une norme et un protocole. Pour que le consommateur puisse déterminer quels services conviennent le mieux à ses besoins (par exemple les données provenant d'un capteur éloigné), le service doit être annoncé (ou publié) à l'utilisateur. Les politiques de sécurité des réseaux restreignent l'accès aux services et à l'information, et offrent des quantités diverses de capacités à différents utilisateurs selon leur accréditation. ***(Service-Oriented Architecture)***

Compréhension de la situation (Répertoire de terminologie de l'Armée de terre, approuvé le 10 octobre 2002)

Connaissance de la situation conditionnée par le jugement humain.

Endsley propose trois niveaux de connaissance de la situation, le niveau 1 Perception (des données), le niveau 2 Compréhension (la fusion de données fragmentaires en information) et le niveau 3 Projection (transformation de l'information en compréhension). ***(Situational Understanding)***

Système de systèmes

Grande collection complexe et durable de systèmes interdépendants en développement dans le temps par de multiples autorités indépendantes dans le but de fournir des capacités multiples et interdépendantes pour soutenir de multiples missions. ***(System of Systems)***

Durée de vie

La durée de vie est une limite de temps ou du nombre de répétitions ou de transmissions dans le contexte de la technologie *informatique* et des réseaux informatiques d'une unité de données (p. ex. un *paquet*) avant d'être éliminées. ***(Time to Live)***

SOURCES PRINCIPALES

Australie. ADDP-D.3.1. *Enabling Future Warfighting: Network Centric Warfare*, février 2004.

Australie. Defence Science and Technology Organization. *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*. DSTO-CR-0373, juillet 2004.

Australie. Defence Science and Technology Organization. *An Application of Queues to Offensive Support Indirect Fire Weapons Systems*. DSTO-TR-1662, janvier 2005.

Australie. Defence Science and Technology Organization. *Network-Centric Warfare Prioritisation and Integration*. ACPL-Report 20-2005-J53v1.0, publié le 24 avril 2006.

Canada. Ministère de la Défense nationale. *Beware of Putting the Cart Before the Horse: Network Enabled Operations as a Canadian Approach to Transformation*. Allan English Ph. D., Richard Gimblett Ph. D. et Howard Coombs. Recherche et développement pour la défense Canada, CR 2005-212, 19 juillet 2005.

Canada. Ministère de la Défense nationale. *Human Factors Implications and Issues in Network Enabled Operations*. Allan English Ph. D., Richard Gimblett Ph. D. et Howard Coombs. Recherche et développement pour la défense Canada, CR 2006-217, 26 août 2006.

Canada. Ministère de la Défense nationale. *Capability Development Record – Command: Enabling Command for the Contemporary Operational Environment*. Majors Darryl Gutscher et Robert Hart, directeurs de projet. Kingston, Direction de la doctrine de l'Armée de terre, septembre 2006.

Canada. Ministère de la Défense nationale. *Cadre d'architecture du ministère de la Défense nationale et des Forces canadiennes (CAMDN)*, Sous-ministre adjoint (SMA) Gestion de l'information (GI), Ottawa, mars 2007.

Canada. Ministère de la Défense nationale. *Les opérations terrestres 2021 : opérations adaptables et dispersées : le concept d'emploi de la force de l'Armée de terre canadienne de demain*. Major Andrew B. Godefroy, réd., Direction – Concepts et schémas de la Force terrestre, 2007.

Canada. Ministère de la Défense nationale. B-GL-323-004/FP-004, *Opérations de contre-insurrection* (Nov. 2007 ébauche).

Canada. Ministère de la Défense nationale. B-GL-351-001/FP-002, *Les transmissions au cours des opérations terrestres*, 1er mai 2008.

Canada. Ministère de la Défense nationale. *Les opérations terrestres en 2021 : un concept en devenir – Études à l'appui du concept d'emploi de la force de l'Armée de terre de demain*. Major Andrew B. Godefroy, réd., Kingston, Direction – Concepts et schémas de la Force terrestre, 2009.

OTAN. *NATO Network Enabled Capability Feasibility Study, Volume 1: NATO Network-Centric Needs and Implications for the Development of Net-Centric Solutions*, octobre 2005.

OTAN. *NATO Network Enabled Capability Feasibility Study, Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing and NNEC Networking and Information Infrastructure (NII)*, octobre 2005.

OTAN. *NATO Architectural Framework (NAF) Version 3*, 2007.

OTAN. Publication administrative interalliée (AAP) 6, Glossaire OTAN de termes et définitions.

NCOIC. Network-Centric Operations Industry Consortium. *Interoperability Framework, Communications*, février 2006.

Nouvelle-Zélande. New Zealand Defence Force. *Future Land Operating Concept: Precision Manoeuvre 2020*, janvier 2007.

Royaume-Uni. Ministry of Defence. *Network Enabled Capability, JSP 777, Edition 1*, Londres, 2005.

États-Unis d'Amérique. Department of Defence. Office of Force Transformation. *The Implementation of Network-Centric Warfare*, 5 janvier 2005.

États-Unis d'Amérique. Congressional Research Service RL32411. *Network Centric Operations: Background and Oversight Issues for Congress,* 15 mars 2007.

États-Unis d'Amérique. Department of the Army. « The United States Army Functional Concept for Battle Command 2015–2024 », TRADOC *Pamphlet 525-3-3*, Leavenworth, avril 2007.

États-Unis d'Amérique. Department of the Army. « The United States Army Functional Concept for Strike 2015–2024 », TRADOC *Pamphlet 525-3-4*, Leavenworth, 30 avril 2007.

États-Unis d'Amérique. Department of the Army. « The United States Army's Concept of Operations: LandWarNet 2015 », TRADOC *Pamphlet 525-5-600*, Leavenworth, février 2008.

États-Unis d'Amérique. Department of the Army. « The United States Army Commander's Appreciation and Campaign Design », Version 1.0, TRADOC *Pamphlet 525-5-500*, Leavenworth, janvier 2008.

États-Unis d'Amérique. Department of the Army. *Air Assault Expeditionary Force (AAEF) Spiral D Experiment Final Report*. US Army Test and Evaluation Command, Alexandria Virginie, mars 2008.

SOURCES SECONDAIRES

Alberts, David S. et Gartska, John J. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised). Washington, D.C. Department of Defence (DoD) Command and Control Research Program (CCRP), 1999.

Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military* (revised). Washington DC: Department of Defence (DoD) Command and Control Research Program (CCRP), juin 2002.

Alberts, David S. et Hayes, Richard E. *Power to the Edge: Command and Control in the Information Age*. Washington D.C. Department of Defence (DoD) Command and Control Research Program (CCRP), juin 2003.

Alston, Anthony et Dodd, Lorraine. *C2 and Agility: Complex Adaptive and Inquiring Systems Theory for Contemporary Military Operations – A Multiperspective Approach*. Présentation donnée à l'occasion du 14e International Command and Control Research and Technology Symposium, 2009.

Barnes Ph. D., D. *A Vision of the Infantry Soldier in 2020*, RUSI Defence Systems, printemps 2005.

Barnett, Thomas P.M. *The Seven Deadly Sins of Network-centric Warfare*. Proceedings, janvier 1999.

Bain, Matthew D. *Supporting a Marine Corps Distributed Operations Platoon: A Quantitative Analysis*. Naval Post Graduate School, Thèse, septembre 2005.

Callahan, LCol W.E. *The Effects of Network Centric Enabled Distributed Operations Forces on the Principles of War*, Strategy Research Project, U.S. Army War College, mars 2008.

Cebrowski, VAdm A.K. et Garstka, J.H. *Network-Centric Warfare – Its Origins and Future*, Proceedings, janvier 1998, p. 139.

Craig, Clayton A. et Tsirlis, Christopher S., *Command and Control for Distributed Operations: An Analysis of Possible Technologies, Structure and Employment*. Naval Post Graduate School, Thèse, juin 2007.

Czarnecki Ph. D., Jonathan E. *The Failed Thermostat: The Illusion of Control in an Information-Rich Age*. Présentation au 13e International Command and Control Research and Technology Symposium, 2008.

Deakin, Colonel S. *Managing FIST (Future Integrated Soldier Technology)*, RUSI Defence Systems, printemps 2005.

Foltz, Kevin et Chandersekaran, Coimbatore. *Sharing Resources Through Dynamic Communities*, Institute for Defence Analyses, Présentation à l'occasion du 10e International Command and Control Research and Technology Symposium, 2005.

Forgues, Colonel P. « Le commandement et la guerre réseaucentrique », *Revue militaire canadienne*, p. 23-30, été 2001.

Garth, Dennis J. *Network Centric Warfare and Its Impact on Operational Functions*. Naval War College, 3 février 2003.

Giffin, Lieutenant-Colonel Ralph E. et Reid, Darryn J. *A Woven Web of Guesses, Canto One: Network Centric Warfare and the Myth of the New Economy*. Présentation à l'occasion du 8e International Command and Control Research and Technology Symposium, 2003.

Giffin, Lieutenant-Colonel Ralph E. et Reid Darryn J. *A Woven Web of Guesses, Canto Two: Network Centric Warfare and the Myth of Intuitivism*. Présentation à l'occasion du 8e International Command and Control Research and Technology Symposium, 2003.

Giffin, Lieutenant-Colonel Ralph E. et Reid, Darryn J. *A Woven Web of Guesses, Canto Three: Network Centric Warfare and the Virtuous Revolution*. Présentation à l'occasion du 8e International Command and Control Research and Technology Symposium, 2003.

Gizewski, P. *The Future Security Environment 2021 – Implications for Canadian Armies*. Recherche et développement pour la défense Canada, RDDC CORA TM 2007-61, septembre 2007.

Gladwell, M. *Intuition : Comment réfléchir sans y penser*, Montréal, éditions Transcontinentales, 2005.

Gompert, David C., Lachow, I. et Perkings J. *Battle-wise: Seeking Time-Information Superiority in Networked Warfare*. NDU Press 2006.

Gonzales, D., Johnson M., McEver J., et coll. *Network-Centric Operations Case Study: The Stryker Brigade Combat Team*. RAND Corporation 2005.

Gonzales, D., Hollywood, J., Sollinger, J.M. et coll. *Networked Forces in Stability Operations 101st Airborne Division, 3/2 and 1/25 Stryker Brigades in Northern Iraq*. RAND Corporation, 2007.

Grau, Lester M. « Urban Combat: Confronting the Spectre. » *Military Review*, juillet-août 1999.

Johnson, Chris. « Net-centric Fogs Accountability ». *US Naval Institute Proceedings*, Vol. 129, N° 5, mai 2003.

Kaplan, Robert D. « The Coming Normalcy? » *Atlantic Monthly*, avril 2006.

Keus, H.E. *Netforce Principles: An Elementary Foundation of NEC and NCO.* Présentation à l'occasion du 10e International Command and Control Research and Technology Symposium, juin 2005.

Libicki, Martin C., Gompert, D., Frelinger, D.R., et coll. *Byting Back: Regaining Information Superiority against 21st Century Insurgents*. RAND Corporation 2007.

Luddy, John. *The Challenge and Promise of Network-Centric Warfare*. The Lexington Institute, février 2005.

McCaskill, Lawrence P. *Beyond PowerPoint Deep: A Concept of Operations for Implementing Net-Centric Warfare*. Présentation à l'occasion du 12e International Command and Control Research and Technology Symposium, septembre 2007.

McKenna, T., Moon, T., et coll. « Science & Technology for Australian Network-Centric Warfare: Function, Form and Fit », *Australian Defence Force Journal*, N° 170, 2006.

Murphy, Colonel (retraité) D., et Groh Ph. D., J.L. *Landpower and Network-Centric Operations: How Information in Today's Battlespace can be Exploited*. U.S. Army War College, Centre for Strategic Leadership, 2006.

Nwana, H.S. « Software Agents: An Overview. » *Knowledge Engineering Review*, Vol. 11, N° 3, p. 1-40, sept 1996. © Cambridge University Press, 1996.

Polydys, M.L. « Interoperability in DOD Acquisition Programs through Enterprise Architecting », *Acquisition Review Quarterly*, été 2002.

Shade, U. et Hieb, M.R. *Development of Formal Grammars to Support Coalition Command and Control: A Battle Management Language for Orders, Requests and Reports*. Présentation à l'occasion du 11e International Command and Control Research and Technology Symposium, septembre 2006.

Schade, U. et Hieb, Michael R. « Improving and Replanning: Using a Formal Grammar to Automate the Processing of Command and Control Information for Decision Support. » *The International C2 Journal*, Vol. 1, N° 2, 2007.

Schrage, Michael. *Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*. Massachusetts Institute of Technology, Security Studies Program White Paper, mai 2003.

Schmidtchen, Lieutenant-Colonel D. *Network-Centric Warfare: The Problem of Social Order*. Land Warfare Studies Centre, Working Paper 125, juin 2005.

Smith, Edward Allen. *Complexity, Networking, and Effects-based Approaches to Operations*. Department of Defence, Command and Control Research Program, 2006.

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

Unewisse, M., Wilson S., Perry, A., et Boyd, C. *An Australian Approach to Assessing Force-Level Network-Centric Warfare (NCW) Readiness*. Présentation à l'occasion du 11e International Command and Control Research and Technology Symposium, septembre 2006.

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