

Applications militaires des technologies de l'information

PAR PAUL W. PHISTER JR, PE, PH.D.
ET IGOR G. PLONISCH*

Résumé de l'éditeur : L'âge de l'information a augmenté la quantité de données à la disposition de tous les commandants. C'est la raison pour laquelle l'Air Force Research Laboratory's Information Directorate – AFRL/IF (Direction de l'informatique du Laboratoire de recherches de l'Armée de l'Air) cherche à transformer les opérations militaires en développant des systèmes orientés vers la satisfaction des besoins propres à la Force aérienne. Les efforts se concentrent principalement sur la connaissance planétaire, la planification et l'exécution dynamiques et l'entreprise d'information planétaire. Ces développements s'appuient sur des technologies ciblées, allant de l'exploitation de l'information à la connectivité aérienne et spatiale et au commandement/contrôle.

ENTRE AUTRES RAISONS, la guerre change constamment parce que les progrès de la technologie conduisent à des progrès dans l'« art de la guerre ». L'âge de l'information qui prévaut aujourd'hui a donné naissance à une explosion dans la quantité d'informations qui est (ou sera) à la

*Nous souhaitons remercier l'ensemble du personnel affecté à la Direction de l'informatique du Laboratoire de recherches de la Force aérienne (AFRL/IF). Nous n'aurions pas pu écrire cet article sans son dévouement et son sens du devoir. Nos remerciements s'adressent spécialement au docteur Northrup Fowler III (Directeur scientifique, AFRL/IF) ; au docteur Warren Debany, à Mike Wessing et John McNamara, conseillers techniques de la division, ainsi qu'à toutes les autres personnes qui ont participé à la préparation de cet article, y compris Scott Adams, Carson Bloomberg, Tim Busch, le colonel Matthew Caffrey Jr., USAFR, Joe Caroli, Steven Drager, Steven Farr, Dan Fayette, Joe Giordano, Rick Hinman, Richard Jayne, John Lemmer, le docteur Mark Linderman, le docteur Richard Linderman, le docteur Mark Minges, le docteur Thomas Renz, Dave Legare, William McQuay, Richard Metzger, le docteur Don Nicholson, Paul Oleski, E. Paul Ratazzi, le docteur John Salerno, Scott Shyne, le lieutenant Justin Sorice, Clare Thiem, Derryl Williams, Dave Williamson et Bill Wolf.

disposition des commandants à tous les niveaux. Certains observateurs sont convaincus que d'ici 2010 « les planificateurs d'opérations [aériennes et spatiales] disposeront d'une quantité incroyable d'informations sur l'état des objectifs. Ils ne sauront jamais tout mais la quantité d'informations qu'ils recueilleront sur l'ennemi sera incomparablement supérieure à ce qui était le cas lors des guerres du passé. Grâce à ces informations, les commandants orchestreront les opérations avec une fidélité et une rapidité sans précédent. Ils bénéficieront des progrès révolutionnaires réalisés dans les domaines du transfert, du stockage, de la reconnaissance et du filtrage de l'information pour diriger des attaques extrêmement efficaces presque en temps réel. »¹ Aux dires de certains, un tel scénario s'est déjà matérialisé, posant les fondations de la transformation de la guerre.

Cette transformation au sein des Forces armées s'effectue de la guerre plateforme centrique classique à la Guerre réseau centrique (*Network-Centric Warfare* – NCW), qui prend en considération les comportements humains et organisationnels et est basée sur de nouvelles méthodes de réflexion et d'application de ces concepts aux opérations militaires.² Elle se définit comme un concept d'opérations adapté à la supériorité informatique qui produit un accroissement de la puissance de combat par la mise en réseau de capteurs, de décideurs et d'exécuteurs permettant d'obtenir une connaissance partagée, une rapidité de commandement accrue, une accélération de la cadence des opérations, une plus grande létalité, une meilleure survie et un certain degré d'auto-synchronisation.³ Un schéma conceptuel de la guerre réseau centrique mettrait en lumière certains de ses éléments ou modules principaux (Fig. 1). Il est également possible d'imaginer une vision réseau centrique du Commandement et contrôle (*Command and Control* – C2) dans le contexte des travaux menés antérieurement sur les concepts de commandement et contrôle (Fig. 2).

Les progrès cruciaux accomplis dans la technologie de l'information liée à la guerre, qui constituent la fondation des opérations réseau centrées, ont leur origine dans les laboratoires militaires, qui fournissent un ser-

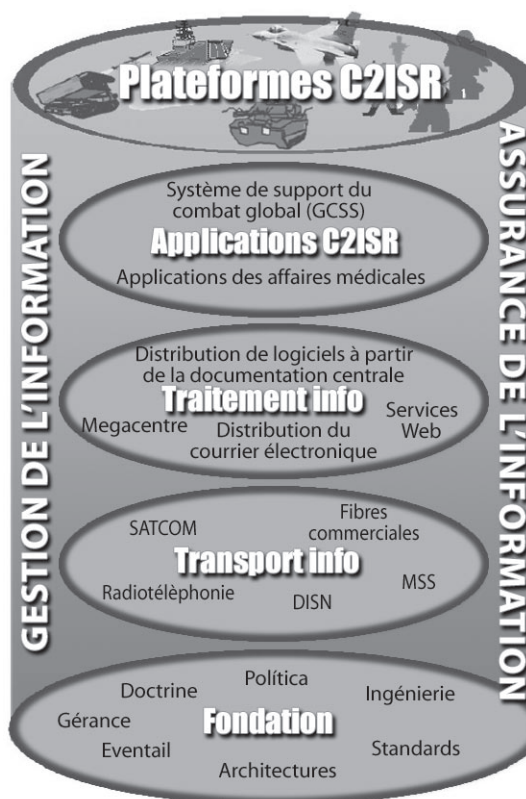


Figure 1. Éléments de la guerre réseau centrique. (Cette figure, de même que les figures 3–20, est reproduite à partir de sources de la Force aérienne.)

vice essentiel aux Forces armées en transformant les technologies de base de l'information en applications de combat. Bien que le Centre de commandement/contrôle et de renseignement-surveillance-reconnaissance de l'Armée de l'Air de la base de Langley, en Virginie, soit chargé des opérations de Commandement, contrôle, communications, Computers, renseignement, surveillance et reconnaissance (*Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance* – C2ISR) de l'Armée de l'Air depuis plus d'un demi-siècle, la direction de l'informatique du Laboratoire de recherches de l'Armée de l'Air (AFRL/IF) situé à Rome, dans l'état de New

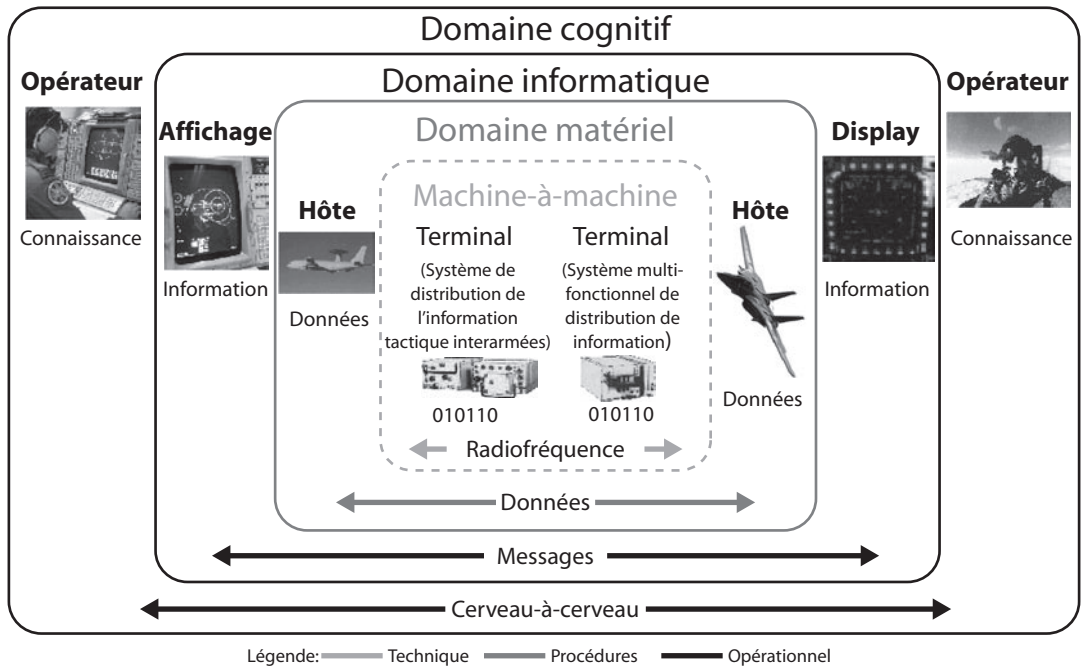


Figure 2. Domaines de la guerre réseau centrée. (Illustration présentée lors de la réunion d'information tenue à Hanscom AFB, Massachusetts, les 5 et 6 février 2003 ; sujet : Technologie de l'information pour la guerre réseau centrée : Une réunion de la semaine de l'intégration ESC – *Electronic Systems Command* (Commandement des systèmes électroniques).

York, a étudié et développé des technologies qui ont contribué à la révolution informatique. L'ordinateur électronique, le circuit intégré, le stockage et la recherche d'information, ainsi que l'Internet, pour ne citer que quelques exemples évidents, ont bénéficié de la recherche effectuée ou conduite par les scientifiques et les ingénieurs travaillant à Rome. En outre, les technologies AFRL se sont introduites, et continuent de le faire, dans les mondes aussi bien militaire que commercial, où elles transforment littéralement les opérations, les méthodes et même les modes de pensée (c'est-à-dire, contribuent aux changements doctrinaux).

Compte tenu du fait qu'*information* et *technologies de l'information* ont souvent des significations différentes pour différentes communautés, il est important de comprendre les

distinctions qui pourraient survenir. Le mot *information* est couramment utilisé pour se référer à divers points du spectre d'information qui convertissent les données en connaissances.⁴ Information a, par conséquent, différentes significations suivant le domaine dans lequel on opère. Par exemple, David S. Alberts et d'autres ont identifié trois domaines – matériel, informatique et cognitif – qui décrivent et définissent chacun l'information différemment.⁵ Le fait fondamental reste toutefois que l'information est le résultat du placement d'observations individuelles dans un contexte significatif d'une sorte ou d'une autre. Sur la base de cette distinction, l'*information* est définie en fonction de son application ou, plus précisément, du domaine dans lequel elle sera exploitée. En conséquence, les milieux commerciaux et universitaires ne traitent pas

l'information de la même manière que leurs homologues militaires.

A côté de la distinction entre les domaines que nous venons de décrire, il existe un certain nombre de raisons pour lesquelles le développement des technologies de l'information diffère entre les milieux militaires et industriels/universitaires. Par exemple, le moteur du marché commercial est le profit ou le taux de rendement de l'investissement, pas les performances générales du système. En outre, dans le monde commercial, l'utilisateur final d'un nouveau produit est devenu l'« essayeur pilote ». Dans un environnement de combat, où la découverte d'une erreur peut littéralement couler un navire, cette méthode est inacceptable. De même, bien qu'une erreur de conception puisse entraîner de nombreux réamorçages quotidiens d'un système commercial, la répétition de telles anomalies dans un système militaire peut se traduire par des blessures voire des morts. Par exemple, lors de *Operation Enduring Freedom*, le système utilisé par cinq soldats américains pour guider un engin « intelligent » se réamorça et inséra à leur insu dans le système la position dans laquelle ils se trouvaient au lieu de celle de l'objectif. En conséquence, l'engin se guida sur leur position au lieu de celle de l'objectif sélectionné. La vérité est que les applications militaires demandent des performances supérieures avec des cycles de base et un coût réduits par rapport aux applications non militaires. Enfin, les technologies commerciales mettent surtout l'accent sur la capacité de calcul (par ex. en fabriquant des calculateurs, ordinateurs, etc. plus puissants) alors que les applications militaires le mettent plus sur les moyens d'action annexes (par ex. évaluation de la planification d'une campagne et EBO – *Effects-Based Operations* (Opérations basées sur les effets)). Il est clair qu'il existe un besoin appréciable de technologie de l'information spécifiquement militaire, même lorsque de tels systèmes ne satisfont pas les critères de rentabilité ou de taux de rendement de l'investissement qui prévalent dans le secteur commercial. C'est ici qu'intervient vraiment l'utilité de l'AFRL/IF.

Efforts de recherche en matière de technologie de l'information

L'AFRL/IF cherche à transformer les opérations militaires en développant une science et une technologie des systèmes informatiques orientées vers les besoins propres à la Force aérienne. L'utilisation de méthodes commerciales lui permet d'augmenter pour un coût raisonnable le potentiel des systèmes terrestres, aériens, Internet et spatiaux de la Force aérienne. Les domaines généraux de l'investissement en science et technologie incluent la fusion des informations de haut niveau, les communications, les EBO, les environnements collaboratifs, les infrastructures d'information répartie, la modélisation et la simulation, les agents intelligents, l'assurance de l'information, la gestion de l'information, ainsi que les systèmes informatiques et les bases de données intelligentes. L'obtention de résultats fructueux dans ces domaines offre les options de moyens d'un coût raisonnable qu'exige la suprématie informatique de la Force aérienne et sa supériorité dans l'air et dans l'espace. Afin de fournir ces moyens, la AFRL/IF concentre ses efforts dans trois domaines principaux – connaissance planétaire, planification et exécution dynamiques, entreprise d'information planétaire – qui s'appuient sur sept domaines à orientation technologique : exploitation de l'information, fusion et compréhension de l'information, gestion de l'information, architectures d'ordinateur évoluées, cyber opérations, connectivité aérienne et spatiale, commandement et contrôle (C2).

Exploitation de l'information

Compte tenu de la menace croissante posée par le terrorisme international, l'utilisation et l'exploitation potentielles de la technologie de l'information facilement accessible par nos adversaires imposent aux Etats-Unis de continuer à investir dans les technologies de protection et d'authentification des systèmes d'information numériques destinés aux Forces armées et à la défense du territoire. C'est dans ce but que l'AFRL/IF est à la pointe de la recherche et du développement dans le domaine de la technologie de l'intégration des données numériques.

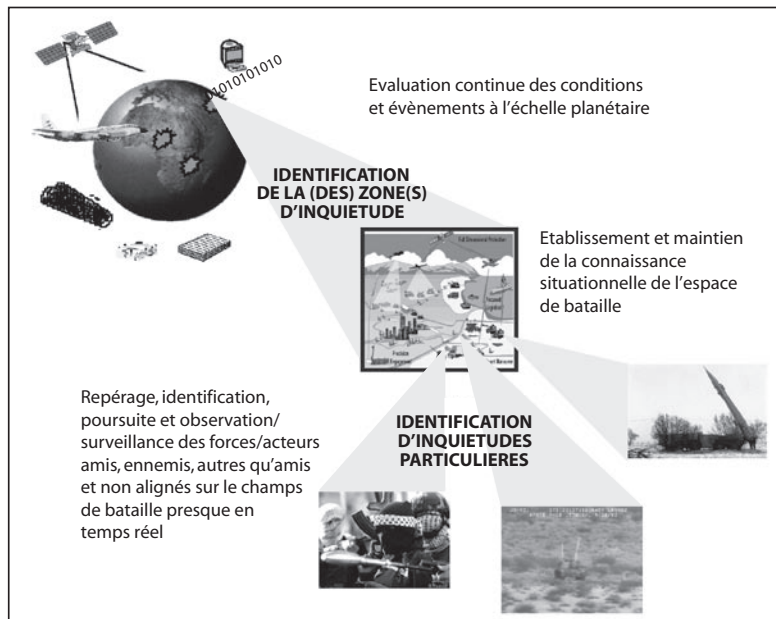


Figure 3. Fusion 2+

Le travail de la direction dans des domaines tels que le masquage d'information, la stéganographie, le tatouage numérique, la stéganalyse et la criminalistique informatique amélioreront grandement la capacité des combattants à exploiter les systèmes de l'ennemi tout en apportant une plus grande sécurité pour garantir qu'aucun adversaire ne peut accéder aux systèmes américains et alliés.

Fusion et compréhension de l'information

Que se passe-t-il ? Qui est l'adversaire ? Que prépare-t-il ? De telles questions sont abordées dans le domaine naissant de la fusion 2+ ou connaissance situationnelle (Fig. 3). Au cours de la décennie écoulée, le terme *fusion* est devenu synonyme de connaissance tactique ou de l'espace de bataille une fois que les hostilités ont commencé. A ce titre, le travail s'est concentré sur l'identification des objets, le suivi des algorithmes et l'utilisation de multiples sources afin de réduire l'incertitude et de maximiser la couverture. Alors que des crises toujours plus nombreuses se déroulent dans le monde entier, des décisions stratégiques intelligentes doivent être

prises *avant* le déploiement des moyens limités à disposition. Afin d'évaluer les intentions de l'adversaire et l'impact stratégique possible, nous avons considérablement élargi le champ de la fusion pour prendre en considération la connaissance de la situation stratégique et la technologie de l'information nécessaire pour la prendre en charge.

Le plan directeur stratégique du commandement spatial de la Force aérienne déclare que « la première priorité consiste à *protéger* nos systèmes spatiaux nationaux vitaux pour qu'ils soient à la disposition de tous les combattants quand et où ceux-ci en ont besoin » (accent mis dans l'original).⁶ Cette protection inclut également la possibilité de réparer les dommages causés par des anomalies très diverses susceptibles d'affecter les systèmes spatiaux en orbite. Dans le cadre du programme Picosat de l'Agence de la défense pour les projets de recherche avancés (*Defense Advanced Research Projects Agency* – DARPA), l'AFRL/IF a lancé le plus petit satellite du monde – le Contrôleur sur pico-satellite à microsystèmes électromécaniques (*Micro Electro-Mechanical*

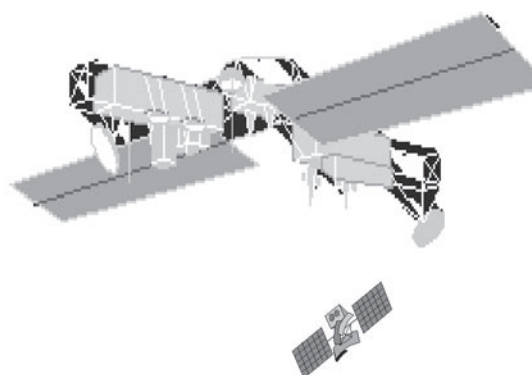


Figure 4. InfoBot

Systems-Based Picosatellite Inspector – MEPSI – depuis la navette spatiale en novembre 2002, réalisant ainsi le travail préparant à la mise en œuvre d’un potentiel naissant de protection et/ou de dépannage extérieur des satellites. L’*InfoBot* (Fig. 4) est un robuste dispositif extérieur qui reçoit, traite, corrèle et distribue l’information de manière fiable, sans ambiguïté et avec rapidité. Ce concept ouvre la voie à de nombreux moyens naissants tels que le dépannage ou la protection internes.

La protection de l’espace exige la mise en garde contre les possibles menaces (d’origine aussi bien naturelle qu’humaine) pesant sur les systèmes spatiaux alliés, la réception des rapports de possibles attaques contre des satellites et la synchronisation des Etats-Unis et des autres

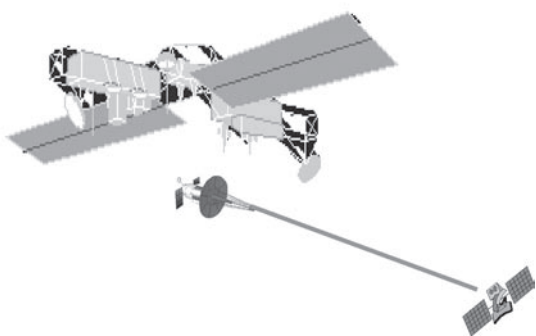


Figure 5. « Bestiole de combat » de l’espace

propriétaires ou opérateurs, ainsi que le guidage des forces chargées de réagir à une menace. Pour satisfaire ces besoins, les systèmes spatiaux doivent être dotés de capteurs internes destinés à détecter les attaques et à signaler rapidement les anomalies ou évènements suspects. Le principal objectif de ces « bestioles de combat » (Fig. 5) serait d’offrir un potentiel de réaction rapide permettant de neutraliser des menaces imminentes qu’il est impossible d’éviter par d’autres moyens conventionnels (par ex. manœuvres orbitales, blindage, etc.) d’une manière peu coûteuse mais efficace.

Gestion de l’information

L’essence de l’Info sphère de l’espace de bataille interarmées (*Joint Battlespace Info sphère – JBI*) (Fig. 6) consiste en un « espace d’information » interopérable à l’échelle planétaire qui intègre, regroupe et diffuse intelligemment les informations pertinentes sur l’espace de bataille pour contribuer à l’efficacité de la prise de décision. L’Info sphère fait partie d’un système de gestion de l’information de combat à l’échelle planétaire établi pour offrir aux utilisateurs individuels à tous les niveaux de commandement des informations adaptées à leurs responsabilités fonctionnelles particulières. La JBI regroupe toutes les informations nécessaires au soutien des combattants et de leurs missions, et leur permet d’obtenir et d’intégrer des données provenant de sources très diverses en touchant un

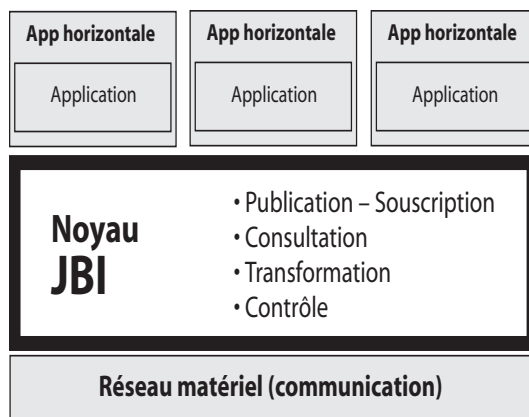


Figure 6. Infrastructure de l’Info sphère de l’espace de bataille interarmées

écran, de regrouper ces informations et de les distribuer sous la forme appropriée et avec le degré de détail demandé par les utilisateurs à tous niveaux. La JBI opère vraiment de système à systèmes dans la mesure où elle sert les utilisateurs à tous les échelons, depuis le poste de commandement éloigné jusqu'au soldat dans son trou. Elle se distingue en termes d'organisation, de processus et d'usage de l'infrastructure de communications qu'elle emprunte et des systèmes d'applications utilisateur qu'elle sert.

La JBI est un « lieu », indépendant des systèmes de commandement, contrôle, communications, computers et renseignement, surveillance, reconnaissance en service, où les informations peuvent être regroupées. Les tentatives de gestion de l'information se sont jusqu'ici articulées autour de systèmes, c'est-à-dire que, en développant un système (que ce soit de communications ou d'applications utilisateur) offrant une capacité donnée, les développeurs décidaient des méthodes de définition, d'organisation, de manipulation, de stockage et de transport de l'information en se basant sur celles qui étaient optimales pour le système particulier en cours de développement. Ces systèmes propres à une application optimisaient l'information sur la base des besoins de stockage et d'accès du logiciel, des magasins de données (bases de données) et de l'interface utilisateur prévue du système. En conséquence, les systèmes de communication étaient optimisés en fonction du routage, de la bande passante, du débit et de la vitesse de transfert. La gestion de l'information basée sur ces optimisations s'est avérée très préjudiciable à l'interopérabilité – c'est-à-dire la capacité des systèmes à *échanger* et *utiliser* des informations et des services. La JBI joue le rôle d'un « niveau information » qui exploite la discipline de la gestion de l'information en éliminant l'actuel environnement d'information « à niveaux rigides » et en le remplaçant par des espaces d'information interopérables, gérés logiquement, largement répandus et sécurisés qui encouragent la diffusion de l'information à tous ceux qui en ont besoin. La JBI fournira les réponses à de nombreuses questions importantes. D'où proviennent les données ? Qui en a besoin ? Quelle est leur priorité ? Les données sont-elles « intéressantes » ? Puis-je me fier à elles ? Doivent-elles

être transformées, regroupées ou intégrées à d'autres informations ? Qui peut y avoir accès ?

Le Système gestionnaire de réseau multi domaine (*Multidomain Network Manager – MDNM*) (Fig. 7) permet aux administrateurs système de surveiller plusieurs domaines de sécurité (par ex. Etats-Unis uniquement, coalition, non classifié) simultanément sur un même ensemble de terminaux. Il permet d'obtenir une image COSE du réseau, des vues hiérarchiques des domaines de sécurité, une unité de limite sécurisée pour accès à l'information réseau et une réduction de l'empreinte d'exploitation. Selon certaines estimations, le système permettra une économie de personnel de 10 à 25 pourcent, maintiendra les coûts à un niveau raisonnable (moins de 10 000 dollars par installation) et permettra une détection des attaques multi niveau propre à la guerre de l'information ainsi qu'une capacité de réaction. Au sein d'un centre d'opérations aérienne et spatiale, par exemple, le MDNM aurait pour effet net une réduction significative du nombre d'administrateurs système nécessaires pour surveiller les divers domaines de sécurité 24 heures sur 24 pendant toute l'année et une surveillance collective du système pour détecter des intrusions antagonistes.

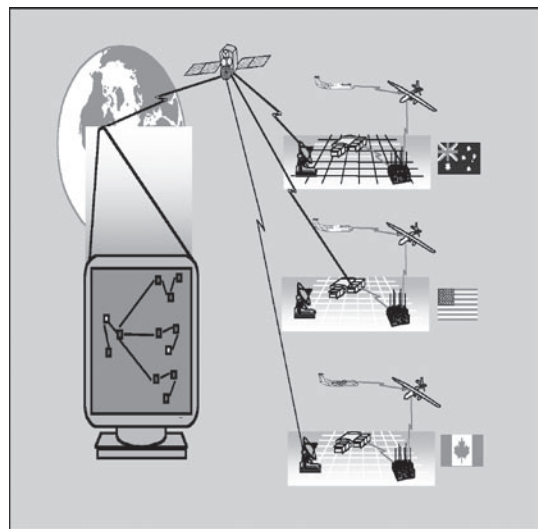


Figure 7. Gestionnaire de réseau multi domaine



Figure 8. Jview

Une interface de programmeur d'applications, *Java View* (Jview) (Fig. 8), est conçue pour réduire le temps, le coût et l'effort associés à la création d'applications de visualisation informatique ou de l'interface de visualisation d'une application. Jview permet d'importer, d'afficher et de fusionner plusieurs sources d'information simultanée. Qu'est-ce que cela veut dire pour le combattant ? Imaginez une très haute résolution sur un écran plat installé dans un F-15 ou un B-2 ou sur le viseur du fantassin.

La nouvelle doctrine d'opérations réseau centrées du Ministère de la défense (*Department of Defense – DOD*) demande l'application des technologies de l'information et de la simulation pour permettre au combattant d'opérer dans un univers de réseaux informationnels synergiques et intégrés de connaissance qui intègre l'information aérienne et spatiale. Les chefs de mission doivent assimiler un volume énorme d'information, décider et réagir rapidement, ainsi que quantifier les effets de ces décisions en dépit de l'incertitude. La recherche menée par l'AFRL sur l'environnement d'aide à la décision collaborative décentralisée (Fig. 9) offre un cadre de collaboration *indépendant des applications* constitué d'outils intégrés, de technologies de l'information et de services de collaboration adaptatifs visant à apporter une aide améliorée à la décision, un partage de la connaissance et des moyens de



Figure 9. Aide à la décision collaborative décentralisée

contrôle des ressources. Ces technologies permettront à du personnel, des processus et des ressources géographiquement dispersés de travailler ensemble avec une efficacité et un rendement supérieurs afin de créer les produits destinés aux entreprises de défense décentralisée de l'avenir (par ex. gestion tactique collaborative, planification des réactions aux crises et antiterrorisme).

Une information en temps opportun sur les forces ennemies, les forces amies et les conditions du champ de bataille est particulièrement cruciale pour les équipages des avions de combat dont la situation sur le champ de bataille change rapidement. Le démonstrateur de technologie évoluée de Connaissance situationnelle commune (*Common Situational Awareness – CSA*) (Fig. 10) permet le développement et la démonstration de l'architecture de système d'information embarqué néces-



Figure 10. Connaissance situationnelle commun

saire pour aider les équipages surchargés en traitant, sélectionnant et affichant les informations disponibles. Le programme CSA, qui vise plusieurs plateformes de mission et aéronaves des forces d'opérations spéciales, intégrera les informations reçues des systèmes embarqués et exploitera les bases de données de renseignement et produits d'imagerie déportés pour offrir une image cohérente de l'espace de bataille à l'équipage. La conception de la CSA inclut trois éléments clés : connectivité, architecture modulaire intégrée et interface équipage/système.

Architectures informatiques évoluées

Le moteur de la croissance de la technologie de l'information au vingt-et-unième siècle sera la technologie informatique évoluée résultant du développement et de la mise en application de paradigmes de traitement de l'information qui aujourd'hui apparaissent originaux. Les progrès accomplis dans le domaine de la technologie de l'information offriront des avantages considérables aux combattants, qui doivent non seulement faire face à l'ennemi sur le champ de bataille mais également lutter pour assimiler le volume énorme de données qu'ils reçoivent de nombreuses sources. Les futurs systèmes d'information incluront des sous-systèmes d'informatique biomoléculaire et quantique (Fig. 11) qui incorporent des mécanismes de stockage et de traitement des données dont la densité d'enregistrement et les performances, telles que puissance et

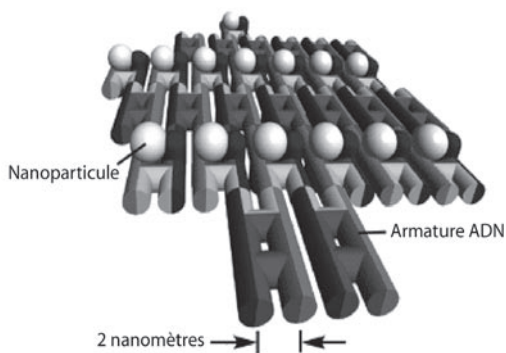


Figure 11. Informatique biomoléculaire et quantique

vitesse évaluées et mesurées par métrologie informatique, surpassent largement ce que permettent les technologies de pointe actuelles, qui utilisent les puces électroniques. Ces systèmes d'information seront vraisemblablement des systèmes hybrides à architecture informatique biomoléculaire/silicium, quantique/silicium ou biomoléculaire/quantique/silicium. Ils pourront traiter l'information plus vite ainsi qu'acquérir de nouveaux attributs qui permettront de progresser encore plus rapidement vers des systèmes informatiques encore plus rapides et intelligents.

Les systèmes spatiaux actuels utilisent la technologie des années 70 et 80 sous la forme de microprocesseurs 286/386/486/586. Toutefois, la connexion de systèmes de commandement et contrôle, de capteurs et d'armes via une « intégration horizontale » exige une capacité de traitement rapide des données-image brutes aussi bien nouvelles qu'acquises précédemment. Une communauté diverse et décentralisée d'analystes du renseignement et de décideurs sur le champ de bataille a besoin de cette capacité pour permettre à ses membres de prendre les mesures appropriées sur la base de ces analyses. L'AFRL/IF travaille en collaboration avec ses directions sœurs – Capteurs (AFRL/SN) et Véhicules spatiaux (AFRL/VS) – sur l'ordinateur spatial de la prochaine génération (Fig. 12). Imaginez un superordinateur de bord de la classe des Cray qui offrirait une puissance de traitement suffisante

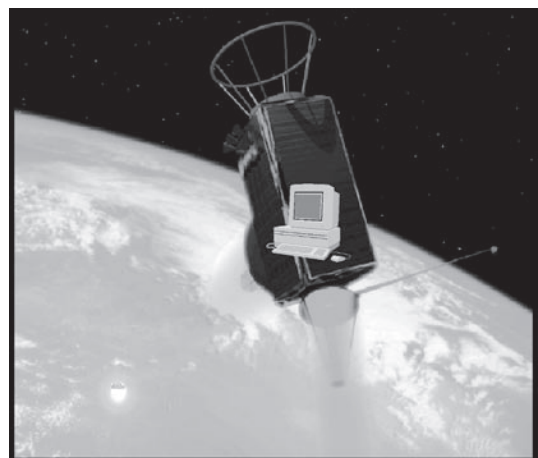


Figure 12. Ordinateur spatial de la prochaine génération

pour que jusqu'à la moitié de la capacité de la station de contrôle terrestre d'un satellite puisse résider dans un même astronef. Cet ordinateur spatial augmentera la capacité de traitement d'un satellite pour la faire passer de millions (10^6) d'opérations par seconde à un trillion (10^{12}) d'opérations par seconde en 2006. Les stations de contrôle terrestre pourront profiter d'une capacité allant jusqu'à un quadrillion (10^{15}) d'opérations par seconde en 2010. Une telle capacité s'accompagne d'avantages significatifs pour la communauté spatiale : réduction de l'empreinte, réduction significative des frais d'exploitation et de maintenance, et possibilité de visualiser, traiter, exploiter et diffuser directement l'information sur l'ensemble d'un théâtre d'opérations, sans devoir solliciter une station fixe de contrôle terrestre.

Cyber opérations

Les agents logiciels intelligents permettent le contrôle et la « surveillance » du cyberspace. Ces entités logicielles encapsulées ont leur propre identité, état, comportement, enchaînement de messages de commande et capacité à dialoguer et communiquer avec d'autres entités, y compris le personnel, d'autres agents et les systèmes hérités. Etant essentiellement des « cyber véhicules », qu'on appelle souvent « Info véhicules » (Fig. 13), ils opéreraient dans le cyber domaine un peu comme les véhicules aériens et spatiaux le font dans l'atmosphère.

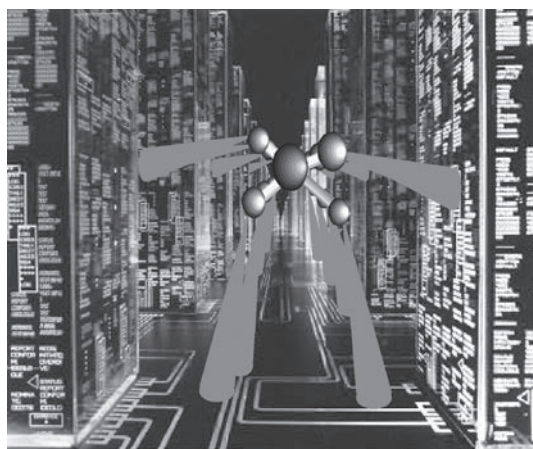


Figure 13. Infocraft

Connectivité aérienne et spatiale

La réalisation d'un environnement opérationnel parfaitement sûr et non-interceptable exige le transfert sécurisé de l'information au moyen de canaux dominés par les effets quantiques – c'est-à-dire la Distribution de clés quantiques (*Quantum Key Distribution – QKD*) (Fig. 14). Dans la plupart des cas, le bruit quantique joue un rôle essentiel dans le développement d'une voie de transmission mais de récents travaux employant un comportement limitant les quanta indépendamment du bruit apportent une contribution majeure à l'assurance de l'information. En collaboration avec le Bureau de la recherche scientifique de la Force aérienne, l'AFRL/IF se penche actuellement sur trois problèmes importants qui empêchent l'établissement d'un canal quantique : rapport signal-bruit, contrôle du canal et maintien de débits exploitables.

L'établissement en temps opportun de la connectivité des réseaux de communications est crucial pour le succès et la survie des Forces américaines dans les environnements de la guerre moderne. Les récents conflits ont démontré le besoin d'un déploiement rapide et d'une prompt réaction aux scénarios qui changent constamment. Une prise de décision efficace et dynamique devient impossible sans communications locales (par ex. radio portable, réseaux de transmission de données câblés ou sans fil et réseau hertzien point à point) et à grande distance (par ex. à haute fréquence ou par satellite) adaptées et fiables à l'intérieur comme à l'extérieur de l'espace de bataille. L'adaptation de la technologie de la radio commerciale et des Réseaux locaux (*Local Area Network – LAN*) permet actuellement l'établissement de réseaux IP (*Internet Protocol*) de transmission de données à grande vitesse dans les positions avancées. Le terminal de Télécommunication par satellite (*Satellite Communications – SATCOM*) sur véhicule (Fig. 15) est relié à un routeur IP qui fournira la connectivité Internet à un réseau local sans fil composé d'ordinateurs portatifs utilisés dans plusieurs véhicules circulant derrière le véhicule passerelle. Au cours des deux dernières années, plusieurs activités telles que les manœuvres *Warrior* et *Global Patriot* qui se dé-

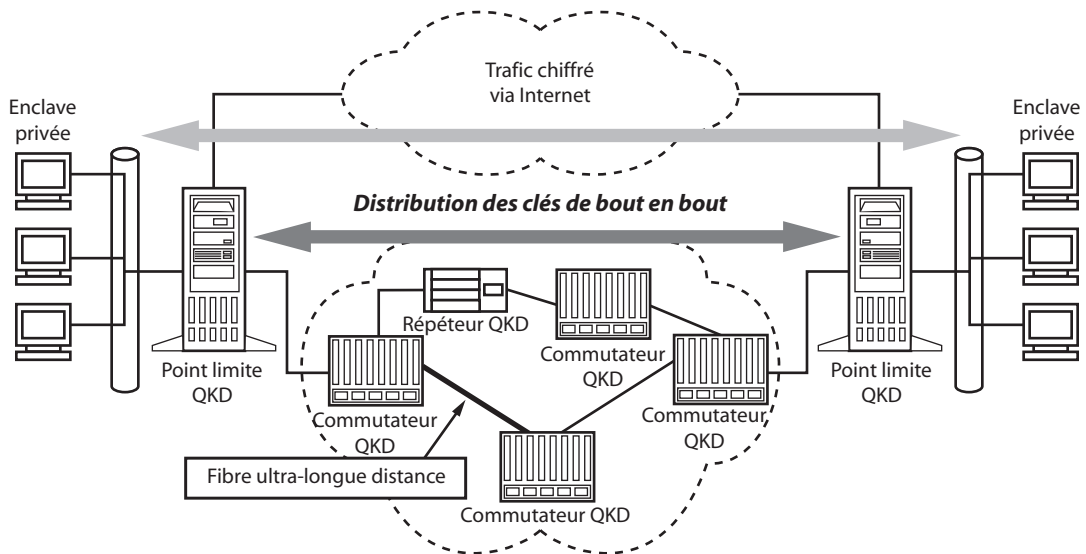


Figure 14. Distribution de clés quantiques

roulèrent à Fort Drum, dans l'état de New York, ont inclus des démonstrations du terminal mobile SATCOM de l'AFRL.

Les réseaux locaux commerciaux sans fil aux normes industrielles, tels que ceux qui sont conformes à la norme 802.11 de l'Institut des ingénieurs électriciens et électroniciens (*Institute of Electrical and Electronics Engineers – IEEE*), donnent aux Forces armées une chance non négligeable d'adapter une technologie

largement répandue et peu coûteuse à des applications difficiles, coûteuses ou impossibles à mettre en œuvre avec les réseaux câblés standard ou les systèmes de communication militaires traditionnels (Fig. 16). Ces normes, qui ont connu un succès extraordinaire permettent d'obtenir des vitesses de liaison allant jusqu'à 54 millions d'octets par seconde sur des distances allant de plusieurs centaines de mètres à plusieurs dizaines de kilomètres, au



Figure 15. Ka-band (satellite à large bande de transmission) mobile satcom en mouvement



Figure 16. Réseau sans fil du commerce amélioré pour les opérations militaires

moyen d'un matériel qui s'intègre de façon transparente à la vaste majorité du matériel informatique du commerce actuellement utilisé par nos forces. En dépit du potentiel remarquable de cette technologie, son utilisation présente de nombreux risques dans la mesure où les réseaux opèrent dans des bandes de fréquences non autorisées, peuvent être aisément brouillés, n'offrent pas d'authentification mutuelle, utilisent des protocoles de gestion non sécurisés, emploient des algorithmes de chiffrement faibles et défectueux, sont faciles à surveiller et sont dépourvus de système de détection d'intrusion, pour ne citer que quelques uns de leurs points faibles.

Cette technologie semble au premier abord totalement inadaptée à une utilisation dans des environnements critiques à haute assurance tels que ceux dans lesquels se déroulent la plupart des opérations militaires. Il est heureusement possible de réduire ou d'éliminer complètement la plupart des risques liés à l'utilisation de réseaux à la norme IEEE 802.11. L'une de ces solutions utilise le point d'accès tactique protégé de l'AFRL, dont le noyau est un éventail de services de base à la norme IEEE 802.11 qui utilise un point d'accès disponible

dans le commerce comme pièce maîtresse. Les stations clientes étant également basées sur un matériel IEEE 802.11b non modifié, on peut ainsi tirer un avantage maximum d'une technologie peu coûteuse disponible dans le commerce. Plusieurs approches et technologies différentes sont combinées pour former un système afin d'atténuer les risques inhérents et d'améliorer l'assurance de l'information sur ce réseau. En outre, des mécanismes de plus haut niveau tels que les réseaux privés virtuels, les coupe-feu, le filtrage d'adresse de destination, un chiffrement robuste et l'authentification mutuelle complètent ces sécurités de plus bas niveau pour offrir une solution complète d'assurance de l'information basée sur des stratégies de défense en profondeur.

Le projet de Langages évolués de transmission et d'affectation des nouvelles technologies s'appliquant aux communications internationales et à la prolifération des formes de signaux alliées (*Advanced Transmission Languages and Allocation of New Technologies for International Communications and the Proliferation of Allied Waveforms* – ATLANTIC PAW) (Fig. 17) représente un effort international regroupant les Etats-Unis, l'Allemagne, la France et le Royaume-Uni et visant à permettre

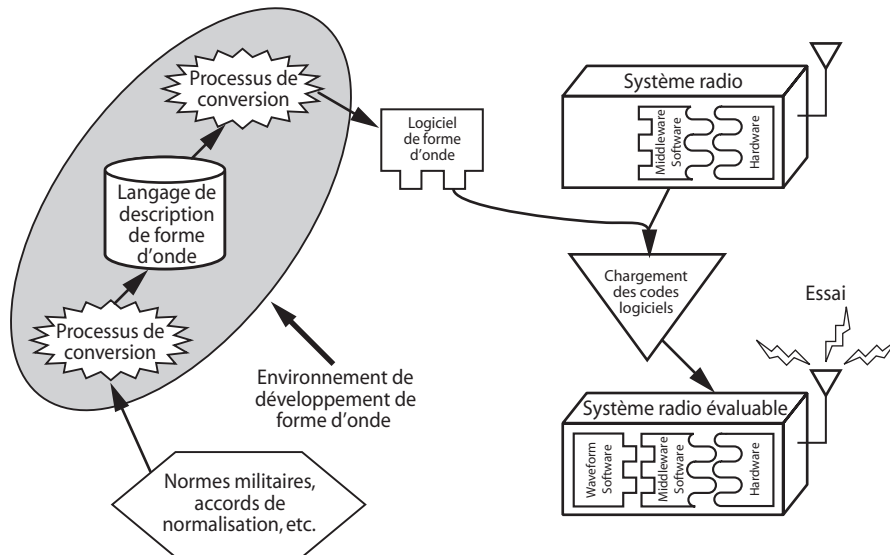


Figure 17. ATLANTIC PAW

l'interopérabilité des moyens de communication sans fil multinationaux. Le programme vise à démontrer la portabilité d'un logiciel de forme d'onde radio sur des plateformes matérielles radio indépendantes. L'approche de l'accomplissement de la transportabilité d'un logiciel de forme d'onde nécessite la formulation coopérative d'un langage de description des formes d'ondes pour capturer sa fonctionnalité et d'un environnement de développement de formes d'ondes pour convertir cette description en un logiciel de forme d'onde radio opérationnel.

Les liaisons de transmission de données aéroportées, qui constituent un élément clé de notre structure de commandement et contrôle, sont essentielles pour permettre à nos Forces armées d'accomplir leur mission et de survivre. La transformation du potentiel de combat par l'exploitation de technologies réseau centrées exige une restructuration spectaculaire et abordable de ce potentiel. Le programme de Technologie des réseaux de choix des objectifs tactiques et des moyens de traitement (*Tactical Targeting Network Technology – TTNT*), financé par la DARPA, a pour objet le développement, l'évaluation et la démonstration de technologies de communication rapidement reconfigurables, abordables, robustes, interopérables et évolutives conçues spécialement pour prendre en charge les applications naissantes de choix des objectifs et des moyens de traitement en réseau conçues pour maintenir la menace qu'on exerce sur les objectifs fugaces. Les expériences de laboratoire et les essais en vol initiaux ont déjà indiqué que la conception de la TTNT peut dépasser les espérances.

Les missions spatiales américaines et les services tels que le contrôle du lancement dans l'espace à la demande et l'entretien courant des véhicules spatiaux en orbite exigent un accès à la demande au satellite pour mener des opérations en temps réel. Les principaux goulets d'étranglement du soutien spatial incluent les limites et contraintes affectant la disponibilité, l'opérabilité et la souplesse des antennes à réflecteur qui assurent les liaisons entre les véhicules spatiaux et les centres d'opérations spatiales au sol. Une antenne originale à balayage électronique sous dôme (Fig. 18) en cours de mise au point – rendue possible par une technologie de modules

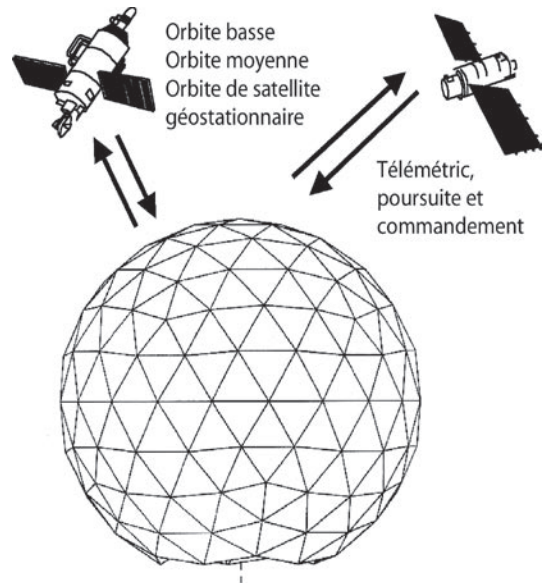


Figure 18. Antenne à balayage électronique sous dôme

émetteurs/récepteurs novatrice et d'un coût raisonnable – atténuera le goulet d'étranglement. Elle satisfera en outre les besoins de transformation de la Force aérienne grâce à de nouvelles capacités en termes d'accès simultané multi bande ; de multifonctionnalité programmable et d'exécution de mission intégrée.

Commandement et contrôle

L'engagement pris par la Force aérienne de relever les défis de demain se manifeste dans un grand nombre de ses activités de transformation. Afin de leur donner un cadre, elle adopte une mentalité EBO pour la guerre de manœuvre et le combat aériens et spatiaux. La stratégie aérienne et spatiale décrit la synchronisation dans le temps et dans l'espace de la Force aérienne et spatiale qui permet d'atteindre les objectifs souhaités. Dans la même logique, les EBO guident la Force aérienne et spatiale tout en représentant un moyen d'exprimer la stratégie aérienne et spatiale permettant au commandant de l'élément aérien et spatial de la Force interarmées d'atteindre ces objectifs de haut niveau en utilisant des moyens létaux ou non. Cela suppose la maximisation des avanta-

ges asymétriques de la Force aérienne et spatiale afin de créer les effets souhaités au bon endroit et au bon moment. L'AFRL a mis en place une Démonstration de technologie évoluée (*Advanced Technology Demonstration – ATD*) pour mettre au point de nouveaux moyens de mise en œuvre des EBO. Les processus actuels de planification, d'exécution et d'évaluation des opérations militaires utilisent des approches orientées cibles et objectifs qui n'incluent pas l'évaluation dynamique de campagne et ignorent les considérations d'opportunité, les niveaux direct et indirect d'efficacité, ainsi que l'analyse de système de choix automatisé des objectifs et des moyens de traitement lors du développement de la stratégie. La démonstration de technologie évoluée d'EBO de l'AFRL/IF met l'accent sur l'élaboration d'outils d'évaluation de campagne et de développement de stratégie afin de combler les vides existants.

Cela fait des années que la Force aérienne s'efforce de découvrir une approche de l'évaluation de campagne plus générale que le « zoom arrière » de l'évaluation des dégâts causés par les bombardements. L'Outil d'analyse causale (*Causal Analysis Tool – CAT*), conçu pour effectuer une évaluation dynamique de campagne aérienne dans les conditions générales d'incertitude, utilise l'analyse bayésienne (une méthode statistique qui tient compte des informations recueillies antérieurement pour déterminer des probabilités) de modèles causaux temporels aléatoires sans demander aux analystes d'avoir des connaissances mathématiques spéciales. Le CAT met l'accent sur le support pour la modélisation de notions causales (aléatoires) telles que la synergie, la nécessité et la suffisance. Développé comme outil d'analyse des plans de campagnes aériennes du type opérations orientées effets, le CAT est un élément crucial de l'outil de développement de stratégie qui permet d'évaluer le plan orienté effets en partant de son élément d'élaboration.

D'après le général William Wallace, qui commandait le Vème Corps de l'Armée de Terre lors de *Operation Iraqi Freedom*, « L'ennemi que nous combattons est différent de celui auquel nous faisons face lors de nos jeux de guerre », ⁷ une déclaration qui démontre clairement que nous devons rechercher des méthodes améliorées

de jeux de guerre dans l'ensemble du Ministère de la défense. A cette époque d'opérations basées sur les effets et de transformation, les jeux de guerre doivent évoluer en conséquence pour favoriser une représentation adaptée non seulement de la doctrine et des systèmes américains mais également de ceux de l'ennemi. Les jeux de guerre doivent être adaptatifs, souples et objectifs. L'AFRL/IF prend actuellement des mesures collaboratives initiales pour mettre au point cette nouvelle méthode de jeux de guerre avec pour double objectif de simuler la victoire et de la faire se matérialiser – plus rapidement, avec moins de pertes et de dommages collatéraux. Pour atteindre ces objectifs, l'AFRL/IF développe la capacité de concevoir un Jeu de guerre de troisième génération (*Third-Generation War Game – 3GWG*). Incorporant trois axes cruciaux supplémentaires – cycles de décision, facteurs humains et effets opérationnels – le 3GWG complète les jeux de guerre de deuxième génération qui modélisent avec succès l'attrition, le mouvement et la logistique (Fig. 19). Les 3GWG contribueront en outre à former les décideurs en les aidant à prendre de meilleures décisions.

Le chef militaire doit pouvoir vivre dans l'avenir en comprenant l'impact que les décisions

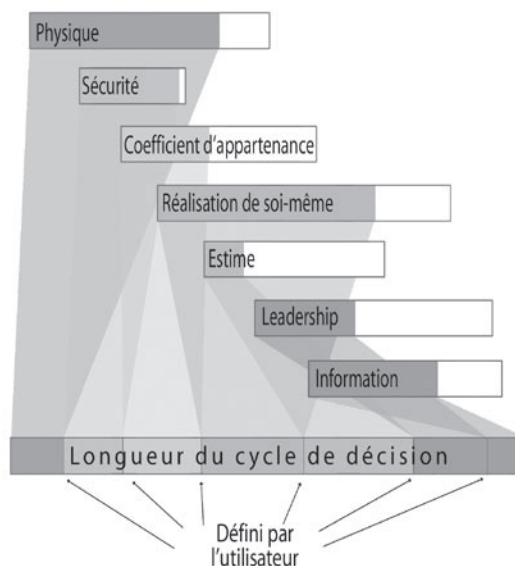


Figure 19. Jeux de guerre pour les combattants du siècle prochain

prises aujourd'hui auront sur l'espace de bataille de demain. Plus il ou elle est gradé(e), plus il ou elle doit pouvoir voir loin dans l'avenir. A tous les niveaux, les commandants prennent continuellement des décisions et choisissent des lignes de conduite en se basant sur leur compréhension du monde et leur capacité à prévoir les résultats des actions envisagées. Cette capacité apparaît habituellement après des années d'entraînement, avec l'acquisition d'une vaste expérience des combats et à l'issue d'un processus rigoureux de sélection. Toutefois, même les tacticiens expérimentés ne peuvent envisager que deux ou trois lignes de conduite possibles pour toutes les situations, à l'exception des plus simples. Pour arriver à la Connaissance prédictive de l'espace de bataille (*Predictive Battlespace Awareness* – PBA), il est nécessaire d'aborder de nombreux problèmes techniques complexes ; en outre, pour la Force aérienne, la PBA doit faire face aux changements de culture, d'organisation, d'architecture et de technologie. Un des éléments essentiels de la PBA est une capacité de simulation qui permet au commandant de pouvoir mieux visualiser les futurs possibles créés par les décisions militaires. Cette capacité de simulation peut prendre de nombreuses formes mais elle a été surnommée l'espace de bataille synthétique interarmées (Fig. 20). Les cinq à sept prochaines années verront l'apparition d'une technologie qui offrira une capacité de simulation synchronisée réaliste au combattant.

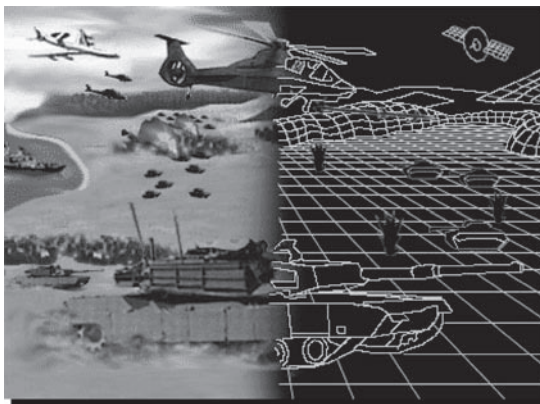


Figure 20. Espace de bataille synthétique interarmées

Récapitulatif

La technologie de l'information a non seulement amélioré la connaissance situationnelle des commandants mais également accru la complexité de l'environnement de prise de décision. L'obtention de résultats fructueux dans ces domaines offre les options de moyens d'un coût raisonnable qu'exigent la suprématie informatique de la Force aérienne et sa supériorité dans l'air et dans l'espace. La direction de l'informatique du Laboratoire de recherches de la Force aérienne reste à la pointe de la transformation des technologies de l'information en moyens de combat. L'AFRL/IF s'engage à poursuivre la transition de la science et de la technologie qui offrent des moyens de combat cruciaux dans des domaines tels que le renseignement d'origine électromagnétique, l'imagerie, le renseignement mesuré, la fusion de l'information, la gestion de l'information, l'informatique évoluée, les cybers opérations, ainsi que le commandement et contrôle – c'est-à-dire les domaines cruciaux de la technologie de l'information qui assisteront le combattant de l'avenir. La direction s'engage également à poursuivre le développement de la suprématie informatique qui soutient la connaissance à l'échelle planétaire en faisant circuler l'information dans l'environnement de l'entreprise d'information planétaire articulé essentiellement autour de réseaux commerciaux pour permettre la planification et l'exécution dynamiques du plan de bataille du commandant.

Notes

1. Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (La guerre de l'avenir : Une évaluation des campagnes aérospatiales en 2010), (Maxwell AFB, AL: Air University Press, janvier 1996), xx–xxi.

2. La transition de plateforme centrée à réseau centrée n'est que le début d'une transformation vers des niveaux plus élevés de guerre. Les auteurs croient que les prochaines étapes de l'évolution feront passer la guerre du mode information centrée au mode connaissance centrée.

3. David S. Alberts, John J. Garstka, et Fredrick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (La guerre réseau centrée : Développement et renforcement de la supériorité informatique), 2^{ème} édition. (Washington, DC: *CHSR Cooperative Research Program [CCRP]*, février 2000), 2.

4. David S. Alberts et autres, *Understanding Information Age Warfare* (Comprendre la guerre à l'ère de l'informatique), (août 2001 ; réimpr., Washington, DC: CCRP, juillet 2002), 16, <http://www.iwar.org.uk/iwar/resources/ccrp/UIAW.pdf>.

5. Ibid., 16-29.

6. *United States Space Command, Long Range Plan, Avril 1998* (Commandement spatial des Etats-Unis, plan à long terme), chap. 5, «*Control of Space*» (Contrôle de l'espace),

<http://www.fas.org/spp/military/docops/usspac/lrp/ch05a.htm>.

7. Julian Borger, Luke Harding et Richard Norton-Taylor, «*Longer War Is Likely, Says US General*» (Une guerre prolongée est vraisemblable, déclare un général américain), *Guardian Unlimited*, 28 mars 2003, <http://www.guardian.co.uk/Iraq/Story/0,2763,924497,00.html> (accès du 19 janvier 2004).

AIR & SPACE POWER CHRONICLES

Le site de

Air & Space Power Journal et Chronicles Online Journal

<http://www.airpower.maxwell.af.mil>

Visitez les sites des autres éditions

• *Air & Space Power Journal – Arabe*

<http://www.airpower.maxwell.af.mil/apjinternational/aspjarabic.html>

• *Air & Space Power Journal – Espagnol*

<http://www.airpower.maxwell.af.mil/apjinternational/aspjesp.html>

• *Air & Space Power Journal – Français*

<http://www.airpower.maxwell.af.mil/apjinternational/aspjrench.html>

• *Air & Space Power Journal – Portugais*

<http://www.airpower.maxwell.af.mil/apjinternational/aspjpor.html>