SCIENCES ET TECHNOLOGIES

175 STC 07 F
Original : anglais

Assemblée parlementaire de l'OTAN

TRANSFORMER LA GUERRE DE DEMAIN : CAPACITES RESEAUCENTRIQUES ET SYSTEMES SANS PILOTE

PROJET DE RAPPORT GENERAL

PIERRE CLAUDE NOLIN (CANADA)
RAPPORTEUR GENERAL*

Secrétariat international 14 août 2007

* Aussi longtemps que ce document n'a pas été approuvé par la Commission des sciences et des technologies, il ne représente que les vues du rapporteur.

TABLE DES MATIERES

I. INTRODUCTION

1. La transformation des forces et la révolution des affaires militaires n'est pas une démarche aussi évidente qu'on aurait pu le croire il y a quelques années encore. La mondialisation et l'essor des technologies de l'information, de l'informatique, des réseaux, des satellites et des technologies de précision ont toutes des implications considérables pour le secteur de la défense et de la sécurité. Les technologies modernes mises en œuvre lors des interventions militaires au Kosovo, en Afghanistan et en Irak ont permis aux militaires d'acquérir une précision et une cadence opérationnelle sans précédent et de gagner des guerres en l'espace de quelques semaines et non plus en plusieurs années, comme c'était encore le cas à une époque relativement proche. L'aspect de la haute technologie de la transformation militaire s'est avéré extrêmement prometteur et a incité certains pays à allouer une part importante de leur budget de la défense à des programmes tels que les capacités réseaucentriques (NEC)[1].

2. L'expérience récente des forces alliées en Afghanistan et en Irak a cependant montré que la haute technologie n'est pas la solution absolue. Si les nouvelles technologies ont un rôle déterminant lorsqu'il s'agit de gagner une guerre, elles semblent mal adaptées pour gagner la paix. Bien qu'elles soient parfois utiles, ces technologies ne sont pas la panacée lorsqu'il s'agit de lutter contre de petits groupes d'insurgés ou de maintenir l'ordre dans une zone après un conflit. On note une prise de conscience du fait que le processus de transformation militaire doit non seulement faire appel à des technologies de pointe, mais aussi accorder une place à des capacités anti-insurrectionnelles et de maintien de la paix. C'est ce qu'exprime d'ailleurs l'édition 2006 de la *Quadriennal Defense Review* aux Etats-Unis. Ces deux axes de transformation peuvent parfois être contradictoires. A titre d'exemple, on notera que les capacités réseaucentriques et les systèmes sans pilote devraient réduire sensiblement les besoins de déploiement de personnel dans les zones de conflit alors que les missions anti-insurrectionnelles auraient l'effet inverse.

3. Tout en tenant compte de cette dualité de la transformation militaire, le rapporteur a choisi de consacrer son rapport à la technologie militaire de pointe, un thème qui s'impose naturellement pour la Commission des sciences et des technologies. Le rapport traitera plus particulièrement de deux capacités naissantes de premier plan – les capacités réseaucentriques et les systèmes sans pilote – qui promettent de révolutionner la conduite des opérations militaires au XXI^{e} siècle. Les nouvelles technologies soulèvent une série de questions fondamentales pour les décideurs politiques : dans quelle mesure l'importance croissante de la sécurité de l'information va-t-elle affecter le fonctionnement des alliances militaires ? Ces évolutions vont-elles entraîner de nouvelles synergies d'efforts ou une fracture technologique sans précédent ? L'OTAN va-t-elle conserver sa raison d'être ou va-t-on plutôt s'orienter vers des coalitions entre partenaires de confiance ? Faudra-t-il assouplir ou durcir les politiques relatives au transfert de technologies ? L'Alliance devrait-elle développer ses propres capacités réseaucentriques et systèmes sans pilote ou cette tâche incombe-t-elle exclusivement aux Etats membres ? Les nouvelles technologies de pointe sont-elles essentielles pour la lutte contre le terrorisme ou offrent-elles encore de nouvelles possibilités aux terroristes ? Quelle sera l'incidence de ces technologies sur la hiérarchie de prise de décision militaire, vont-elles la rationaliser ou la perturber ? Les systèmes de combat autonomes seront-ils encore soumis à un contrôle humain ? Faudrait-il une convention internationale pour enrayer les risques de prolifération de ces technologies ? Toutes ces questions sont d'une importance capitale sur le plan politique et il est donc essentiel que le législateur suive de très près l'évolution des technologies relatives aux capacités réseaucentriques et aux systèmes sans pilote plutôt que de la considérer comme un problème exclusivement technique.

---

1 Nous utilisons dans le présent rapport l'appellation officielle de l'OTAN "capacités réseaucentriques" (*Network-Enabled Capability* – NEC) qui est aussi le titre du programme britannique en la matière. Certains pays utilisent d'autres termes, comme réseaucentricité, guerre réseaucentrique, défense réseaucentrée, opérations réceaucentriques, etc.

II. CAPACITES RESEAUCENTRIQUES

A. LA PROMESSE ET LES DEFIS DE LA RESEAUCENTRICITE

4. La réseaucentricité, expression militaire de l'ère de l'information, est un concept relativement neuf que l'on doit au vice-amiral de la marine américaine Arthur K. Cebrowski et à John J. Garstka, directeur adjoint de l'Office américain de la transformation des forces, et qui est apparu pour la première fois dans un article qu'ils ont publié en 1998 sous le titre *Network-Centric Warfare* : *Its Origins and Future*. La réseaucentricité n'est pas uniquement un partage d'informations entre différentes composantes des forces armées utilisant une technologie moderne. L'intérêt des capacités réseaucentriques (NEC) réside dans le fait qu'elles créent de la valeur ajoutée en conférant à tous les éléments de l'espace de combat un accès en temps réel ou presque au système d'échange d'informations, dissipant ainsi le "brouillard de la guerre". Les trois plus grands spécialistes des NEC, David S. Alberts, John J. Garstka et Frederick P. Stein définissent la réseaucentricité en ces termes :

> Un concept opérationnel rendu possible par la supériorité de l'information, qui génère une puissance de combat accrue découlant du réseautage des capteurs, des décideurs et des combattants en opération afin d'atteindre un état de connaissance commun de l'espace de combat, une vitesse supérieure de commandement, une cadence accélérée d'opérations, une létalité accrue, une surviabilité prolongée et une plus grande faculté d'adaptation par des boucles de rétroaction rapides. Pour l'essentiel, [la guerre réseaucentrique] transforme la supériorité de l'information en puissance de combat.[2]

5. Ainsi, les NEC consistent à la base à améliorer la capacité entre le capteur et le combattant (C4ISTAR – commandement, contrôle, communications, ordinateurs, renseignement, surveillance, acquisition d'objectif et reconnaissance) pour en faire un élément essentiel, plutôt que complémentaire, des capacités militaires. Tout comme dans le monde des affaires, les nouvelles technologies et une meilleure coordination des efforts produisent des "effets de masse" et optimisent l'efficacité des forces armées. A l'ère de l'information, celle-ci redéfinit les concepts de masse, manœuvre, puissance de tir et logistique.

6. Des rudiments de NEC ont déjà été testés lors de l'Opération *Liberté immuable* en Afghanistan et pendant la guerre en Irak. Toutefois, les NEC en sont toujours à leurs premiers balbutiements. Pour Terrence Morgan, directeur des Opérations réseaucentrées chez Cisco Systems, au stade actuel, le capteur et le combattant en opération sont trop éloignés l'un de l'autre : la largeur de bande est limitée en raison de points de passage obligé et de problèmes d'interopérabilité, l'infrastructure est trop hétérogène et complexe pour supporter le "prêt-à-l'emploi" et le temps nécessaire à la mise en service de "nouvelles" applications est beaucoup trop long.[3]

7. Outre l'aspect technique, les NEC nécessitent des changements révolutionnaires au niveau du commandement et du contrôle (C2). La structure hiérarchique traditionnelle du C2 n'est pas assez souple pour tolérer des situations dans lesquelles des commandants de rang inférieur auraient accès à toute l'information pertinente et seraient en mesure de prendre des décisions sans attendre les instructions de leurs supérieurs.

---

2. Network Centric Warfare: Developing and Leveraging Information Superiority, par David S. Alberts, John J. Garstka and Frederick P. Stein. – DoD C4ISR Cooperative Research program. 2e édition, 2000. p. 2.
3. Transformation, Netcentric Defense, Space and Security. Terrence Morgan, directeur des Opérations réseaucentriques chez Cisco Systems. Exposé présenté aux membres de la STC de l'AP-OTAN, San José (Californie), 15 juin 2006.

8. Plusieurs auteurs évoquent aussi les aspects négatifs de la réseaucentricité. Par exemple, Alfred Kaufman, de l'Institut des analyses de défense, souligne quelques conséquences préjudiciables du réseaucentrisme :

- la course incessante à l'innovation peut compromettre la sécurité ;
- prendre ses désirs pour une réalité est érigé en stratégie ;
- la bureaucratie prend le pas sur la dynamique de la guerre ;
- le commandement et le contrôle perdent leur dimension humaine ;
- les machines remplacent l'être humain ;
- une puissance excessive fait peu de cas de la diplomatie.

9. Certains, à l'OTAN, disent aussi craindre que, les capacités réseaucentriques permettant de mieux se rendre compte des activités des échelons inférieurs, les officiers supérieurs aient tendance à s'ingérer et vouloir s'occuper de points de détail, décourageant de la sorte l'esprit d'initiative des officiers de rang inférieur.[4] Pendant la visite de la délégation de la STC au Centre de guerre interarmées (JWC) de l'OTAN de Stavanger, en Norvège, le maréchal de l'air Peter Walker, directeur du Centre, a reconnu que les technologies émergentes telles que les capacités réseaucentrées et les systèmes sans pilote altèrent les chaînes de C2 traditionnelles puisqu'elles permettent à des commandants d'échelon stratégique d'intervenir dans des opérations d'échelon tactique. Le directeur du JWC a répondu que la tâche essentielle du Centre est de décourager ce genre de pratique et de débarrasser les commandants en chef des questions de détail pour leur permettre de se concentrer sur une vision plus large et sur des décisions à plus long terme.

B. LES PROGRAMMES NEC ET L'ALLIANCE

1. Etats-Unis

10. Les Etats-Unis sont le leader mondial incontesté et un pionnier du développement des NEC. Son programme de guerre réseaucentrique (*Network-Centric Warfare* - NCW) est au centre de la stratégie de transformation de l'armée américaine, comme l'annonçait la *Joint Vision 2020*. Selon l'ancien secrétaire adjoint à la Défense, Paul Wolfowitz, "notre aptitude à exploiter la puissance de l'information et des réseaux sera la clé de notre succès"[5]. Le programme NCW devrait être pleinement opérationnel pour 2012, avec un réseau unique de capteurs, de décideurs et de combattants en opération, armes et combattants connectés par protocole Internet (*Internet Protocol*–IP), et une perception et une connaissance partagées au niveau du commandement.[6]

11. Les principales capacités réseaucentriques américaines sont :

- Le *Secret Internet Protocol Router Network (SIPRNET)*. En fait, SIPRNET est un réseau Internet propre à l'armée américaine et le plus grand réseau du département de la Défense réservé à l'échange d'informations classifiées. Il est progressivement devenu l'élément central de la capacité de commandement et de contrôle de l'armée américaine. SIPRNET est très semblable à l'Internet dans la mesure où il utilise aussi des protocoles TCP/IP et des navigateurs de type courant pour accéder à des sites programmés en langage HTML. Tout comme l'Internet, il permet la communication au moyen de courriels, de forums ou groupes

4. Network-Enabled Capabilities – Issues and Implications, Dr. Linton Wells II, secrétaire adjoint principal à la défense pour l'intégration des réseaux et de l'information . – Exposé prononcé au 21e Atelier international sur la sécurité mondiale. Berlin, 7-10 mai 2004.
5. Voir Global Information Grid, sur le site Internet de la National Security Agency.
6. C2 Constellation, par Skip Liepman. - Military Information Technology. Volume 8, Issue 6. 17 août 2004.

de discussion et de connexions de poste à poste. Toutefois, SIPRNET étant une cible tout indiquée pour des intrusions hostiles, il fait l'objet d'une série de procédures de sécurité extrêmement rigoureuses. Tous ses utilisateurs doivent être approuvés, enregistrés et les mots de passe doivent être changés au moins tous les 150 jours. Un système similaire mais beaucoup moins surveillé, le *Nonclassified but Sensitive Internet Protocol Router Network* (NIPRNET), permet une interopérabilité homogène pour des applications d'appui au combat non classifiées, ainsi qu'un accès contrôlé à l'Internet. SIPRNET est un outil précieux et facile à utiliser, deux qualités fort appréciées par le commandement militaire américain. Toutefois, son accès de l'extérieur est, comme on peut le comprendre, très limité. Seuls les alliés très proches de l'Amérique – Britanniques et Australiens – peuvent y avoir accès, mais de manière temporaire et limitée, pendant certaines missions conjointes. L'information provenant du renseignement sur SIPRNET est systématiquement qualifiée de secrète et non divulgable à des ressortissants étrangers (S*ecret Not Releasable to Foreign Nationals* - NOFORN). Il est arrivé, en Irak, que les Britanniques ne soient pas autorisés à consulter ou copier des données du renseignement fournies par des agents britanniques après que celles-ci aient été intégrées à des données américaines conservées sur le réseau SIPRNET et marquées NOFORN.[7]

- Le *Global Information Grid (GIG)*. Le système GIG sera le plus grand réseau d'information au monde et constituera l'ossature des capacités réseaucentriques des Etats-Unis. Constitué à partir de technologies commerciales, il comportera des fonctions de traitement, de stockage, de gestion et de transport de l'information destinées à fournir un appui à toutes les missions et des fonctions liées à la défense, à la sécurité nationale et au renseignement. Les capacités du GIG pourront être consultées depuis tous les sites d'opérations : bases, postes, camps, stations, installations, plates-formes mobiles et sites déployés. Le GIG sera en interface avec les systèmes des alliés et des forces de coalition qui lui sont extérieurs. Des satellites de la prochaine génération fourniront quantité d'informations en temps réel à des plates-formes et systèmes d'armes déployés aux contours du champ tactique. Chaque mètre carré de la surface du globe aura son adresse IP, permettant ainsi un suivi réel de tous les acteurs du champ de bataille. Ce programme de 34 milliards de dollars devrait être terminé en 2011.[8] Grâce au GIG, les soldats américains en opérations ne seront plus tributaires de l'appréciation par une personne absente du lieu de combat du type d'information dont ils ont besoin.[9]

- *FBCB2-Blue Force Tracking*. C'est ce système satellitaire qui a permis de générer des images du champ de bataille pendant l'Opération *Liberté pour l'Irak* et qui a permis aux forces américaines et britanniques de se suivre mutuellement et de détecter les positions de l'ennemi.

- *LandWarNet*. Regroupe tous les réseaux des forces terrestres américaines, de la logistique des bases militaires à l'appui des forces déployées à l'avant. Il permet le traitement, le stockage et le transport de l'information sur un réseau intégré. Son principal support, le *Warfighter Information Network –Tactical* (WIN-T), qui a coûté 10 milliards de dollars, constituera l'ossature du réseau de communication de l'armée américaine et devrait assurer des capacités numériques C4ISR renforcées mobiles, sûres, « surviables » et homogènes. La première mise en service d'un WIN-T par l'armée est prévue pour 2008.

---

7. US Kept Spying Data from Blair, par. Sarah Baxter. - The Sunday Times. 1 octobre 2006.
8. Live GIG, par Tony Skinner. – Jane's Defence Weekly. 25 octobre 2006.
9. Voir Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, par Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. Décembre 2006.

- *FORCEnet* est l'équivalent du *LandWarNet* pour la marine. *FORCEnet* est une architecture intégrée de technologie de l'information qui reliera les capacités opérationnelles sur terre, en mer et en air.

- *ConstellationNet*, l'équivalent de *LandWarNet* et de *FORCEnet* pour l'armée de l'air américaine, stockera et fera circuler la voix, les données, l'imagerie et l'information vidéo et servira d'interface au GIG.

- Le *Joint Tactical Radio System (JTRS)* est un outil de communication essentiel pour les forces terrestres et aériennes et un programme crucial pour la transformation de l'armée américaine. Le JTRS est une classe de radios logicielles destinées à se substituer à une vaste gamme de radios militaires conventionnelles répondant à différentes normes et utilisant différentes fréquences fixes. Par l'utilisation d'une norme unique, le JTRS va fortement faciliter l'interopérabilité des forces interarmées et permettra la transmission d'un volume de données nettement accru. Il permettra non seulement la communication vocale, mais aussi le téléchargement instantané d'images vidéo et de données ainsi que la connectivité de réseau. Les troupes et plates-formes équipées du JTRS pourront se connecter au réseau de la même façon qu'un ordinateur portable peut capter un signal pour se connecter à l'Internet. Cependant, bien que le JTRS soit extrêmement prometteur, le *Government Accountability Office* du gouvernement américain souligne qu'une série de problèmes techniques et de gestion doivent encore être surmontés. A titre d'exemple, l'intégration de l'équipement radio dans des plates-formes de types différents et le respect de limites de taille, de poids et de puissance sont des problèmes en attente de solution depuis longtemps.[10]

2. Alliés de l'OTAN

12. En dehors des Etats-Unis, de tous les pays de l'OTAN, seuls le Royaume-Uni, l'Allemagne, la France et l'Italie considèrent la réseaucentricité comme une priorité de leurs efforts de transformation militaire. C'est le Royaume-Uni qui, avec sa *Network Enabled Capabilities Initiative*, a l'approche la plus conceptuelle. Ayant récemment achevé la phase initiale d'interconnexion, il prévoit d'atteindre la phase d'"intégration totale" en 2015 et celle de la "synchronisation totale" d'ici 2025. Le Royaume-Uni est aussi le seul allié à avoir participé à des opérations réseaucentrées, son corps expéditionnaire ayant pu avoir accès aux réseaux américains pendant la campagne en Irak. On peut citer en tant qu'exemples de ses capacités réseaucentriques les systèmes de communication numérique Bowman, Cormorant, DII *(Future Deployed*) et Falcon ; le système de communications par satellites militaires de la prochaine génération SKYNET 5 ; le véhicule aérien télépiloté (UAV) Watchkeeper affecté à des missions ISTAR ; le système de surveillance terrestre ASTOR et le système OPLOC conçu pour le guidage du personnel en opérations.

13. Pour la France, la réseaucentricité est plus un terme opérationnel que technologique. Le principal programme réseaucentrique français est la *Bulle Opérationnelle Aéroterrestre (BOA)* dont le principe repose sur l'action combinée d'un ensemble d'entités. Il s'agit d'un contrat de 129 millions de dollars confié à un consortium dirigé par Thales pour la conception et le développement de TACTIC3, un démonstrateur des technologies et architectures du combat aéroterrestre rapproché (fantassins, véhicules blindés, engins télépilotés et système de capteurs déposés mis en réseau par un système d'information et de communication). Le démonstrateur TACTIC permettra d'évaluer sur le plan opérationnel les gains capacitaires du concept BOA.[11] La France développe aussi un projet de capacité d'engagement coopératif appelé Capacité d'Engagement Multi Plates-Formes (CEMP) ainsi que le programme de tenue de situation multi

10. Restructured JTRS Program Reduces Risk but Significant Problems Remain. - US Government Accountability Office Report to Congressional Committees. septembre 2006.
11. La France octroie le marché démonstrateur BOA à Thales, Giat Industries Sagem Défense Sécurité – Communiqué de presse du Groupe Thales, 8 décembre 2005.

plates-formes TSMP. Thales travaille sur les systèmes d'information et de commandement de nouvelle génération SIC 21 et RIFAN (réseau Intranet des forces aéronavales) pour la marine française.[12] Une autre entreprise du secteur de la défense, *Sagem Défense Sécurité*, développe actuellement le système FELIN V1 et le réseau de communication du fantassin SITEL.[13]

14. Il y a quelques années, l'Allemagne a révisé sa stratégie militaire pour l'axer davantage sur les missions hors zone. Son programme réseaucentrique, *Netzwerkgestützte Operationsführung* (NetOpFü*)*, est une des pierres angulaires de ses efforts de transformation. Il vise à assurer un partage d'informations fiable, pertinent et en temps utile aux forces allemandes situées dans une zone de crise. L'Office fédéral de la technologie et de l'approvisionnement (BWB) est chargé de l'acquisition des capteurs, effecteurs et systèmes adaptables au réseau. Il est chargé par ailleurs d'intégrer différents systèmes dans un "système de systèmes" afin de dégager des effets de synergie.[14] L'Allemagne s'emploie à apporter une solution aux problèmes techniques que pose la définition d'une image opérationnelle commune pertinente basée sur les rôles (*Role-Based Common Relevant Operational Picture* - ROBOCROP) qui fournira au commandant du champ de bataille ainsi qu'au commandant du quartier-général les informations pertinentes permettant de prendre la bonne décision au moment voulu, en évitant un excès d'information. Elle met actuellement en service des systèmes de C2 et de gestion du champ de bataille extrêmement sophistiqués (FüInfoSys, FAUST, GIATS/DCRC), et répondant aux normes d'interopérabilité de l'OTAN, afin de permettre à l'armée allemande de participer à des opérations réseaucentrées de l'OTAN.

15. L'armée italienne a mis en chantier son initiative Forza NEC portant sur la numérisation de trois brigades d'armée d'ici 2014. La cheville ouvrière des forces réseaucentrées italiennes, le système SICCONA, combinera les communications et une capacité de tenue de situation avec des données relatives à la navigation et aux véhicules. Ce système, élaboré par un consortium emmené pas Finmeccanica, est au stade des essais. Il permettra l'acheminement des données du champ de bataille du poste de commandement au véhicule et, de là, par signal Wifi jusqu'à l'équipement personnel de chaque soldat.[15]

3. OTAN

16. Les capacités réseaucentriques deviennent le sujet à la mode au sein de l'Alliance et s'imposent comme un des éléments clés de sa transformation militaire. La déclaration du Sommet de Riga fait référence aux NEC et aux programmes qui leur sont associés en insistant sur la nécessité :

- de s'employer à développer une capacité en réseau de l'OTAN pour partager les informations, les données et les éléments du renseignement d'une façon fiable et sûre, qui ne retarde pas les opérations de l'Alliance, tout en améliorant la protection de nos systèmes informatiques clés contre les cyberattaques ;

- d'activer un centre de fusion des données du renseignement pour améliorer le partage des informations et des données du renseignement dans le cadre des opérations de l'Alliance;

- de poursuivre les progrès dans le programme de capacité alliée de surveillance terrestre (*Alliance Ground Surveillance* – AGS), en vue de parvenir à des capacités réelles de soutien des forces de l'Alliance.

---

12. Au service des marines du monde entier : La réponse de Thales aux défis de demain – Exposé du Groupe Thales à Euronaval 2006. Paris, octobre 2006.
13. Network Centric Warfare/BOA – site Internet de Sagem Défense Sécurité : www.sagem-ds.com/
14. The BWB Role in Transformation. – Military Simulation and Training magazine. février 2006.
15. Italy, Finland, France Focus on C2 Technologies, par Pierre Tran. Defence News. 4 juin 2007.

17. Le développement du système *NATO Network-Enabled Capability* - NNEC a été confié à des agences de l'OTAN situées à Norfolk (*ACT Information Superiority & NATO Network Enabled Capabilities Integrated Capability Team* - IS&NNEC) et à Bruxelles (Agence OTAN des C3-NC3A). L'équipe ACT prépare un cadre stratégique et une feuille de route en vue de moderniser les capacités conjointes de l'Alliance et de permettre à l'OTAN de constituer une force entièrement mise en réseau, tandis que la NC3A s'efforce d'arrêter des normes techniques et des gabarits pour les nouvelles architectures. L'amiral Sir Mark Stanhope, ancien Commandant suprême adjoint des forces alliées Transformation, a déclaré que la NEC "sous-tend tout ce que nous faisons [à l'ACT]".[16] Des agences de l'OTAN ont préparé une étude de faisabilité des NNEC qui constitue la base à partir de laquelle se définissent tous les critères auxquels l'Alliance doit répondre en tant qu'entité pour arriver à une capacité réseaucentrique. Reste encore à relever les défis de la mise en application et de la gouvernance.

18. Les NEC revêtent une importance particulière dans le cadre de la Force de réaction de l'OTAN (NRF), déclarée pleinement opérationnelle au Sommet de Riga, en novembre 2006. L'absence d'une architecture de réseau commune pourrait compromettre la viabilité de cette force multinationale tournante et, en particulier, sa capacité à opérer avec les forces américaines après chaque rotation. C'est pourquoi l'équipe ACT IS&NNEC a été chargée d'analyser les différences pendant chaque rotation semestrielle et de définir la capacité réseaucentrique commune de base de cette force de réaction.[17]

19. Les principaux programmes de l'OTAN liés aux NEC sont les suivants :

- *Alliance Ground Surveillance* (AGS). Un projet ambitieux de l'OTAN, d'une valeur de 4,24 milliards de dollars, qui se composera notamment de plates-formes avec et sans pilote de RSR et donnera aux commandants de l'Alliance une représentation complète, à l'échelle du champ de bataille, de la situation au sol en temps réel, y compris de nuit et par mauvaise visibilité. Ainsi, tout comme le programme AWACS de l'OTAN assure une tenue de situation dans les airs, l'AGS fournira une vision commune au sol. Une fois déployé, l'AGS devrait devenir une capacité essentielle pour les missions de coalition et, en particulier, pour la NRF. L'AGS devrait être pleinement opérationnelle d'ici 2013 et sera exploitée par l'OTAN qui en sera aussi le propriétaire.

- Le Système de commandement et de contrôle aérien (ACCS), un projet de 1,5 milliards d'euros visant à fournir un système C2 aérien unifié qui permettra à tous les alliés européens de l'OTAN de gérer de manière intégrée tous les types d'opérations aériennes au-dessus de leur territoire et au-delà. L'ACCS fera appel aux technologies les plus modernes et permettra aux pays membres de l'OTAN de s'adapter aux exigences des opérations réseaucentrées. L'ACCS offrira une capacité opérationnelle initiale d'ici quelques années.

- Parmi les autres programmes de l'OTAN, figurent la mise au point du *NATO Messaging System* (système de messagerie électronique intégrée sécurisé et fiable), de normes pour radios logicielles et la *Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition* (MAJIIC), un projet réunissant 10 pays membres de l'OTAN et destiné à arrêter des critères opérationnels, architecturaux et techniques en vue de l'utilisation commune de dispositifs RSR de coalition à des fins d'appui aux missions militaires.

20. Les agences de l'OTAN en charge de ces programmes travaillent en étroite collaboration avec le secteur privé par le truchement du *Network Centric Operations Industry Consortium* (NCOIC). Créé à l'initiative du centre de commandement de l'OTAN de Norfolk, ce consortium

16. Interview de l'Admiral Sir Mark Stanhope, DSACT. – Revue de l'OTAN. printemps 2005.
17. IS and NNEC ICT works to develop better interoperability standards, par le US Navy Chief Petty Officer Joel I. Huval. – ACT News. 12 janvier 2007.

regroupe 80 entreprises leaders dans le domaine aérospatial, la défense et les technologies de l'information et a pour but de tenir l'OTAN au fait de ce qui se passe dans le secteur industriel. Les missions essentielles du NCOIC consistent à adopter des normes communes publiques de procédures, échanger des meilleures pratiques, et à faciliter et encourager la collaboration pour permettre à l'industrie de développer des produits compatibles.

21. Plusieurs comités et forums ayant l'interopérabilité pour thème et fonctionnant sous l'égide de l'OTAN se montrent en général très productifs et constructifs. Comme Keith Hooey, le représentant du Canada à certaines de ces réunions, l'a déclaré aux membres de la Commission, les experts nationaux réussissent en général à trouver un consensus sur des recommandations portant sur des procédures opérationnelles, des architectures d'information et des technologies d'échange d'informations. L'attitude la plus constructive vient surtout des participants américains. Cependant, lorsque les experts tombent d'accord sur une façon de procéder, cela signifie en général qu'un ou plusieurs pays vont devoir réorienter un ou plusieurs importants programmes d'acquisition, ce qui suppose un coût élevé. Ils peuvent très bien accepter un changement d'orientation en principe, mais un engagement sur un calendrier précis est plus difficile à obtenir. Cela nécessite une volonté politique à l'échelon le plus élevé.

C. LES DEFIS TECHNOLOGIQUES ET POLITIQUES POUR LES NEC

1. Défis technologiques

22. Sur le plan technologique, pour pouvoir participer efficacement à des opérations réseaucentrées, il faut tout d'abord que les partenaires d'une coalition aient la technologie requise et, ensuite, qu'ils soient en mesure de se connecter aux réseaux de leurs partenaires. Même si les commandements militaires sont habilités à diffuser des informations pertinentes en temps utile, encore faut-il qu'ils aient les moyens techniques de le faire et sans ouvrir des fichiers sensibles non pertinents. Comme l'explique une étude, pendant les opérations des coalitions en Afghanistan et en Irak en 2003, l'US CENTCOM (Commandement central) a été confronté à plus de 84 réseaux différents dont 26 seulement avaient un niveau de sécurité suffisant. Dans ces conditions, l'interopérabilité et l'échange d'informations entre les partenaires de la coalition étaient souvent très lents et pratiquement inexistants.[18] Ce sont ces problèmes d'échange d'informations par exemple qui ont freiné la cadence opérationnelle des forces britanniques, incapables d'accéder à des systèmes d'acquisition d'objectifs américains tels que JSTARS et Global Hawk.[19]

23. Pour répondre à ces défis, la *Defense Information Security Agency* (DISA) américaine a récemment mis en service un *Combined Enterprise Regional Exchange System* (CENTRIXS) conçu pour permettre aux forces américaines d'échanger en mode sécurisé et intégré des informations opérationnelles et tactiques avec ses partenaires de coalition et de mission en Afghanistan et en Irak. CENTRIXS combine un ensemble de réseaux multilatéraux et bilatéraux et compte 77 pays participants. Le système compte plus de 26 000 utilisateurs répartis entre 150 sites dans le monde.[20] Il lui manque toutefois un système de sécurité intégrale et il n'est pas connecté à d'autres réseaux classifiés, ce qui explique que le transfert d'informations entre les réseaux nationaux et CENTRIXS nécessite d'autres infrastructures, comme des terminaux et des liens de communication.

---

18. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, par Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. Décembre 2006.
19. The NATO Response Force. Facilitating Coalition Warfare through Technology Transfer and Information Sharing. Jeffrey P. Bialos et Stuart L.Koehl. Center for Technology and National Security Policy, National defence University. September 2005.
20. DISA Leads Efforts for Multinational Information Sharing, par Miriam Moss. - The Grid, DISA journal. février 2007.

24. Au niveau stratégique opérationnel, les Etats-Unis ont constitué le réseau classifié "Griffin" destiné à faciliter la communication entre les planificateurs de défense par le biais de services de messagerie et de groupes de discussion sécurisés. Seuls quelques pays – les partenaires les plus proches des Etats-Unis et ceux qui se sont dotés de capacités réseaucentriques – peuvent avoir accès au réseau Griffin. Selon le secrétaire adjoint principal à la Défense (Intégration des réseaux et de l'information) Linton Wells II :

> "Nous devons abandonner les réseaux de coalition actuels comme CENTRIXS et Griffin au profit de véritables systèmes d'information multinationaux, mais cela exigera beaucoup de travail, à la fois pour concevoir les systèmes et élaborer les politiques de partage de l'information sur lesquelles ils reposeront."[21]

25. La connectivité n'est pas une difficulté en soi. Les technologies NEC reposent sur des normes utilisées dans le domaine civil. En fait, ces technologies sont principalement développées, non pas par des laboratoires militaires secrets, mais par des firmes commerciales comme Cisco Systems, Ericsson ou Boeing. Les militaires américains, et l'OTAN de plus en plus, utilisent les protocoles de l'Internet (TCP/IP) pour les fonctions de commandement, de contrôle et de communication. Il faut cependant qu'un acteur dominant arrête ces normes. Tout comme les fabricants de matériels et de logiciels informatiques savent parfaitement que leurs produits ne vaudraient rien s'ils n'étaient pas compatibles avec le système d'exploitation Microsoft Windows, les producteurs de technologies NEC doivent s'adapter au SIPRNET, le réseau national de la première puissance militaire mondiale.[22]

26. L'Agence OTAN des C3, responsable de la mise en œuvre des NNEC, propose une approche axée sur le service plutôt que sur la conception du système, c'est-à-dire plutôt qu'une architecture fermée du type boîte noire, passer à un "système de systèmes" permettant la connexion et l'interopérabilité de systèmes de conceptions différentes. Il nécessiterait une série de normes techniques non patrimoniales encore inexistantes. Cette formule permettrait de baisser le coût qu'auraient à supporter les pays de l'OTAN souhaitant participer à des opérations réseaucentrées parce qu'elle ne leur imposerait pas d'acquérir un équipement entièrement neuf. Toutefois, certains alliés, en particulier les nouveaux pays membres de l'OTAN, voient les choses différemment parce qu'ils partent pratiquement de rien, leurs technologies de C4ISR étant complètement dépassées ou tout simplement inexistantes. Ces pays doivent construire l'infrastructure de leurs systèmes de communication et d'information sur des bases entièrement nouvelles, ce qui pose beaucoup moins de problèmes de compatibilité.[23]

27. Une autre difficulté d'ordre technologique liée à la NEC vient du besoin croissant de fréquences radio à des fins militaires. Le spectre électromagnétique est un élément déterminant de la NEC et la communication sans fil est un facteur vital des opérations militaires modernes. Cependant, le spectre de fréquences est limité et doit être géré et coordonné avec soin si on veut éviter les goulets d'étranglement. Le problème est aggravé par le fait que la demande de fréquences émanant du secteur commercial connaît, elle aussi, une augmentation vertigineuse. Le département américain de la Défense a pris une série de mesures pour faire face à ce problème en encourageant le développement de nouvelles technologies de gestion du spectre,[24] et en revoyant les normes et critères régissant l'utilisation militaire du spectre. Quoi qu'il en soit, de

---

21. Network-Enabled Capabilities – Issues and Implications, par Dr. Linton Wells II, secrétaire adjoint principal à la Défense – Intégration des réseaux et de l'information - Exposé prononcé au 21e Atelier international sur la sécurité mondiale. Berlin, 7-10 mai 2004.
22. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, par Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. Décember 2006.
23. In NATO, Technology Challenges Yield to Political Interoperability Hurdles, par Robert K. Ackerman. – Signal, magazine of the Armed Forces Communications and Electronics Association. Février 2006.
24. Une solution technologique serait d'utiliser des radios cognitives qui émettent et reçoivent en "sautant" d'une fréquence à une autre, suivant qu'elles sont "libres" et peu utilisées.

nouvelles lignes directrices adoptées au niveau le plus élevé, et avec la participation de l'OTAN, s'imposent pour répondre aux besoins de fréquences des forces de coalition opérant en réseau. D'après Paige Atkins, de la *Defense Spectrum Organization* (DSO) américaine, l'enjeu est de trouver de nouvelles méthodes de partage du spectre entre les alliés : "l'environnement étant de plus en plus encombré, nous devons nous efforcer de mieux appréhender les moments où les systèmes n'utilisent pas des éléments du spectre afin de pouvoir les utiliser plus efficacement".[25]

28. La protection des réseaux est un autre défi technique d'une importance capitale. L'information étant à la base de la NEC, sa sécurité est primordiale. Il est très facile de modifier, ajouter, supprimer ou diffuser une information numérique. Les interférences malveillantes, les fraudes sur l'identité et la présence de personnes mal intentionnées dans le réseau constituent autant de menaces pour la sécurité. On peut donc comprendre que le secteur militaire américain, de plus en plus en réseau, s'inquiète des rumeurs selon lesquelles la Chine développerait une capacité de guerre cybernétique. Selon des responsables du Pentagone, la compétence de la Chine en matière de technologies de l'information, autrefois axée sur la défense de ses propres réseaux, a évolué pour se spécialiser dans l'attaque des réseaux des adversaires.[26] Le fait qu'elle soit en mesure de menacer des systèmes de satellites, d'une importance capitale pour les militaires américains, a été clairement démontré en janvier 2007 lorsqu'elle a utilisé une arme antisatellite contre un vieux satellite météorologique. Ainsi, l'enjeu majeur consiste à trouver une solution optimale qui permette un débit ininterrompu d'informations entre des entités et personnes autorisées tout en préservant l'intégrité du réseau.

29. Beaucoup de solutions technologiques sont proposées à cet effet. On peut, par exemple, adapter un logiciel ou marquer des données de manière à en limiter l'accès aux seules personnes autorisées. Par ailleurs, selon les types d'autorisations, toutes les personnes n'auraient pas les mêmes droits d'accès, selon qu'elles souhaitent lire, publier, modifier ou transmettre des informations. Les concepts de portail gardé et de pare-feu dynamique doivent obligatoirement être mis en avant si l'on veut une véritable interopérabilité opérationnelle. En outre, on peut dresser un ordre de priorités pour éviter le risque d'une surcharge d'informations. Le développement du GIG en tant que "système de systèmes" chapeautant l'ensemble en fait une cible de prédilection. Pour renforcer la sécurité de cette nouvelle architecture de réseau, la *National Security Agency* américaine a commencé la mise au point d'un élément d'assurance de l'information pour le GIG. L'information doit être marquée et cataloguée au moyen de métadonnées permettant aux utilisateurs de rechercher et d'obtenir, au moyen d'un modèle d'"acquisition intelligente" et de gestion, l'information dont il a besoin pour mener à bien sa mission. Pour cela, le GIG doit savoir où se trouve l'information et reconnaître l'utilisateur où qu'il se trouve. L'accès au système ne dépendra donc plus de l'endroit où il est demandé, mais il restera néanmoins limité compte tenu du degré de risque de cet endroit.[27]

30. S'il est important de suivre l'évolution des technologies de protection des réseaux dans le domaine commercial, Linton Wells II estime qu'il serait imprudent de s'en remettre aux seules technologies disponibles dans le commerce pour protéger les réseaux militaires, car il est peu probable que les forces du marché produisent des logiciels suffisamment élaborés pour résister à des attaques répétées d'agresseurs soutenus par des Etats et disposant de moyens financiers suffisants. En conséquence, il faudrait donc des solutions qui émanent des seuls pouvoirs publics pour remplir des fonctions particulières que ne proposera pas le secteur privé.[28]

---

25. Crowded Spectrum, par Peter A. Buxbaum. - Military Information Technology. Volume 11, Issue 1.1 février 2007.
26. Pentagon: China Developing Cyberwar Capability, par William Matthews. Defence News. 18 juin 2007.
27. Voir Global Information Grid: IA Defence-In-Depth Implementation. – site Internet de la National Security Agency.
28. Network-Enabled Capabilities – Issues and Implications. Dr. Linton Wells II, secrétaire adjoint principal à la Défense – Intégration des réseaux et de l'information – Exposé prononcé au 21e Atelier international sur la sécurité mondiale. Berlin, 7-10 mai 2004.

2. Défis politiques

31. Les experts techniques pourraient très vite se mettre d'accord sur des normes sur lesquelles fonder les NEC, mais cela ne répond pas au problème de la diffusion de l'information, problème persistant s'il en est. D'après Keith Hooey, on aurait même l'impression que les commandements des forces multinationales seraient plus disposés à partager des éléments d'information critiques, mais qu'ils en sont souvent empêchés par des considérations d'ordre politique. Pour pouvoir tirer pleinement parti des atouts des NEC, la négociation de politiques de diffusion en temps quasi réel s'impose.

32. Des responsables de haut rang de l'OTAN soulignent aussi l'importance de l'aspect politique et culturel de l'interopérabilité réseaucentrée. C'est par exemple le cas du directeur général de l'Agence OTAN des C3, M. Dag Wilhelmsen, qui a déclaré que les domaines politique et culturel présentent bien plus de difficulté pour la NEC que les architectures et normes techniques. A titre de solution, il proposait que l'Agence OTAN des C3 fasse office d'"agent cohérent impartial" pour aider les pays membres à trouver de bonnes solutions plausibles entre les systèmes nationaux et les infrastructures internationales.[29]

33. Le défi politique de la réseaucentricité se résume pour l'essentiel à une question de confiance entre les Etats-Unis et leurs alliés. Les forces armées américaines devenant de plus en plus réseaucentriques, la sécurité de leurs réseaux pourrait bien acquérir une importance supérieure à la coopération avec les alliés. Tant que les Américains n'auront pas une totale confiance dans leurs alliés, ils hésiteront à leur laisser l'accès à leurs réseaux militaires. Bien que l'Europe tire profit de la technologie américaine dans des programmes tels que le *Joint Tactical Radio System*, le *Global Hawk*, les MEADS ou dispositifs de vision nocturne, la liste des projets américains liés à la NCW et faisant l'objet de consignes de non-diffusion ou de diffusion limitée reste très longue : *Future Combat System* (FCS), *Future Battle Command - Brigade and Below* (FBCB2), *Blue Force Tracking* (BFT), *Army Field Artillery Tactical Data System* (AFATDS), *Warfighter's Information Network - Tactical* (WIN-T).[30]

34. Il semblerait toutefois que le gouvernement américain s'engage sur la voie d'un meilleur partage de l'information et de la technologie avec ses alliés. En juin 2007, par exemple, les Etats-Unis ont signé avec la France et le Royaume-Uni des accords qui feront date visant à assouplir sa politique en matière de transfert de technologie militaire. Les dirigeants américains semblent maintenant convenir que cette politique constituait un frein et mérite d'être adaptée. D'après le Lt-Gén. Jefferey Kohler, directeur de l'Agence de coopération en matière de défense et de sécurité du Pentagone, "la nécessité d'apporter des améliorations au processus [de transfert de technologies] est reconnue". De même, l'Association américaine des industries aérospatiales (AIA) exhorte le gouvernement à revoir sa politique. Dans une déclaration commune avec son homologue européenne ASD, l'AIA affirme que "une modernisation du système américain qui le rendrait plus prévisible, transparent et efficace relancerait les échanges commerciaux transatlantiques et stimulerait la coopération et l'interopérabilité entre amis et alliés".[31] Cependant, la question de savoir si une telle réforme trouverait un soutien suffisant au Congrès ne fait pas l'unanimité chez les experts.

35. Dans le monde unipolaire de la *Pax Americana*, les dirigeants américains vont de plus en plus se trouver confrontés à un dilemme critique : alors que, pour des raisons politiques, les

29. In NATO, Technology Challenges Yield to Political Interoperability Hurdles, par Robert K. Ackerman. – Signal, magazine of the Armed Forces Communications and Electronics Association. Février 2006.
30. The NATO Response Force. Facilitating Coalition Warfare through Technology Transfer and Information Sharing. Jeffrey P. Bialos et Stuart L. Koehl. Center for Technology and National Security Policy, National Defence University. Septembre 2005.
31. Focus on Cooperation, par Pierre Tran. Defence News, 25 juin 2007.

Etats-Unis auront encore besoin d'alliés pour leurs opérations militaires, l'efficacité de ces opérations risque d'être compromise lorsque s'y ajouteront les forces d'autres Etats. En d'autres termes, la question fondamentale pour les décideurs américains est de savoir si l'intérêt national des Etats-Unis sera mieux défendu et ses objectifs de politique étrangère mieux servis :

- en préservant leur suprématie militaire mondiale, au risque de perdre leurs partenaires, ou
- en recourant à des coalitions multinationales qui risquent de leur coûter leur suprématie militaire.

36. Ainsi, le développement de la NEC sera, de manière fortuite, lourd de conséquences pour l'intégrité de l'Alliance. La quête de la sécurité de l'information pourrait obliger les dirigeants américains à opter au coup par coup pour des coalitions de volontaires plutôt qu'à faire appel à l'ensemble de l'OTAN. L'expérience de la guerre en Irak a montré que les membres de l'OTAN peuvent avoir des conceptions fort différentes de la politique étrangère et de la stratégie de défense. Par conséquent, la diffusion d'informations sensibles à tous les Alliés pourrait sembler délicate, voire dangereuse, d'un point de vue américain. Officiellement, des documents de stratégie américains comme la *Quadriennal Defense Review* ou la *National Security Strategy* soulignent la nécessité d'une collaboration avec les Alliés ; pourtant, l'évolution de la situation a incité le secrétaire à la Défense de l'époque, Donald Rumsfeld, à déclarer que les Etats-Unis doivent "s'abstenir d'essayer de convaincre à tout prix d'autres de rejoindre une coalition si cela doit compromettre nos objectifs ou mettre en danger notre structure de commandement".[32] Comme le disait Paul T. Mitchel, les NEC "pourraient placer les Etats-Unis dans une impasse numérique très sécurisée".[33]

37. Il faut noter que d'autres pays de l'OTAN contingentent aussi le partage de l'information. L'Allemagne, par exemple, a livré récemment des appareils de reconnaissance Tornado à l'ISAF. Il s'agit d'un apport particulièrement précieux pour ce qui est du soutien aux forces de l'OTAN en lutte contre les insurgés talibans dans le sud de l'Afghanistan. Toutefois, l'Allemagne impose des limites à l'utilisation et la diffusion des informations récoltées. A cela s'ajoutent des contraintes d'ordre technologique : les Tornados n'ayant pas de liaison descendante air-sol, les données ne peuvent être récupérées et analysées qu'une fois les appareils revenus à leur base.[34]

III. SYSTEMES SANS PILOTE

A. LES PROMESSES ET LES DEFIS DES SYSTEMES SANS PILOTE

38. Bien que NEC et systèmes sans pilote représentent deux évolutions technologiques différentes, ils sont liés par un fort degré de cohésion. D'une certaine manière, la nouvelle technologie des drones constitue un prolongement physique des NEC. Les systèmes C4ISTAR réseaucentriques vont de plus en plus dépendre des véhicules aériens télépilotés (UAV) pour la collecte des données du renseignement et de la reconnaissance, voire pour l'attaque d'objectifs. En revanche, les véhicules sans pilote ne sont d'aucune utilité s'ils ne sont pas connectés au réseau. Les systèmes sans pilote devenant de plus en plus autonomes, il va nécessairement falloir les connecter à d'autres capteurs sur le théâtre d'opérations pour qu'ils puissent corriger eux-mêmes leur plan de vol pour pouvoir mener leur mission à bien. Les capacités réseaucentriques comme les systèmes sans pilote devraient réduire fortement le besoin de déployer des troupes et accroître leur surviabilité.

---

32. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, par Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. Décember 2006.
33. Ibid.
34. NATO Seeks More ISR for Afghan Combat, par David Pugliese. Defence News. 4 juin 2007.

39. L'apparition des technologies sans pilote, autonomes et robotisées est souvent considérée comme la nouvelle vague de la révolution technologique. Les plus grands noms de la technologie prédisent que le monde est à l'aube de l'ère des robots, comme le fait Bill Gates. Il compare l'état actuel de la robotique à celui des ordinateurs au milieu des années 1970, lorsque lui et Paul Allen lancèrent Microsoft. Bill Gates imagine que la robotique ouvrira "une ère nouvelle dans laquelle l'ordinateur ne sera plus uniquement sur nos bureaux et nous permettra de voir, d'entendre, de toucher et de manipuler des objets dans des lieux dont nous sommes physiquement absents". Il ajoute aussi que les systèmes autonomes "seront un élément central des systèmes de sécurité." Microsoft a d'ailleurs lancé Microsoft Robotics pour s'assurer une place de premier plan dans ce nouveau domaine qui devrait décupler d'ici 2025.[35]

40. D'un point de vue technologique, les systèmes "télépilotés" sont fort différents des systèmes "autonomes". Alors que chaque mouvement d'un véhicule télépiloté (ou inhabité) est contrôlé à distance et guidé par un servant formé à cet effet, les systèmes autonomes (ou drones) peuvent effectuer des tâches diverses, y compris éviter un obstacle et évaluer une situation, sans l'intervention ou avec une intervention minimale d'un opérateur installé en un autre lieu. Comme en ont témoigné des experts de BAE Systems, première firme européenne du secteur de la défense, devant les membres de la STC lors de la visite de la Sous-commission à Londres, les systèmes autonomes présentent des avantages incontestables par rapport aux systèmes télépilotés parce qu'ils supportent mieux les changements d'environnement et sont insensibles à la fatigue et à la lassitude. Mais la difficulté est de programmer un véhicule autonome de telle sorte qu'il puisse changer d'itinéraire lorsqu'il est confronté à un obstacle imprévu, tout en pouvant poursuivre sa mission. Une solution consiste à définir un "couloir" aérien dans les limites duquel le drone peut librement modifier sa trajectoire. Les experts de BAE Systems font remarquer que les Etats-Unis ont une avance certaine dans le domaine du développement et, en particulier, de la mise en service de véhicules télépilotés, mais que l'Europe comble rapidement son retard dans le domaine de la recherche-développement sur les systèmes autonomes. Le véhicule aérien télépiloté Corax de BAE Systems, par exemple, est totalement autonome et a fait la preuve de sa fiabilité. Il est aussi à noter que les systèmes aériens ne sont pas les seuls à gagner en autonomie. Israël a récemment déployé un système appelé "See-Shoot" le long de ses 60 kilomètres de frontière avec la bande de Gaza. Ce système, composé de capteurs et de tourelles de tir, sera au départ commandé par des opérateurs avant de fonctionner automatiquement à terme.[36]

41. On classe aussi les véhicules sans pilote en fonction du milieu dans lequel ils évoluent (aérien, terrestre, aquatique ou sous-marin). Les systèmes aériens sans pilote (*Unmanned Aerial Systems* – UAS) constituent de loin la catégorie la plus en avance et sont déjà fréquemment utilisés dans des opérations militaires. Les UAS sont des aéronefs pilotés à distance ou autopilotés pouvant emporter des caméras, des capteurs, du matériel de communication ou d'autres charges, létales ou non. Pendant des années, tous les types de véhicules aériens pilotés à distance ont été appelés véhicules aériens sans pilote (*Unmanned Aerial Vehicle* – UAV). Or, ce terme ne rend pas compte du fait que ces appareils ont besoin de stations de contrôle au sol, de liens avec des satellites et de dispositifs de communication. L'expression "systèmes aériens sans pilote" rend mieux compte de la complexité de l'ensemble du système.

42. On note à première vue que les UAS présentent de nombreux avantages :

- Avant tout, les systèmes sans pilote permettent d'épargner des vies puisqu'il n'y a plus de pilote à bord. Les UAS devraient dorénavant assurer les missions dites 3D (*dull-dirty-dangerous*, c'est-à-dire ennuyeuses, sales et dangereuses). L'utilisation de drones terrestres et subaquatiques est déjà très répandue dans les opérations de déminage.

35. A Robot in Every Home, par Bill Gates. - Scientific American. Janvier 2007.
36. Israel's Robo-Shooters, par Barbara Opall-Rome. Defence News. 4 juin 2007.

- Le fait de ne pas devoir déplacer des troupes et leur équipement présente des avantages logistiques évidents. Cela réduit d'autant les besoins de transport, de logement, de nourriture et de sécurité nécessaires à l'appui des troupes sur le théâtre d'opérations.
- Le coût constitue aussi un incitant majeur. Un chasseur F16 coûte 30 millions de dollars alors qu'un MQ-9 Reaper, dernier-né de la famille des drones de combat (UCAV) américains, doté d'une charge utile proche de celle du F16, ne coûte que 7 millions de dollars. De plus, les UCAV pourraient constituer une solution de rechange moins chère que certains programmes dispendieux d'avion de chasse auxquels participent actuellement des pays membres de l'OTAN (à titre d'exemple, un F35 Joint Strike Fighter coûte 100 millions de dollars et un F22 Raptor 200 millions de dollars , tandis qu'on estime le coût de l'UCAV X-45 à 40 millions de dollars).
- Leur endurance est aussi un atout. Les appareils de soutien aérien rapproché restent en général 30 minutes au-dessus du champ de bataille avant de devoir refaire le plein de carburant. Par comparaison, un MQ-1 Predator pourrait survoler la cible jusqu'à 24 heures. En revanche, ils ne peuvent pas être réalimentés en vol et sont extrêmement lents ; ils ont besoin de beaucoup plus de temps pour atteindre le théâtre d'opérations.
- Les UAS peuvent être modernisés plus fréquemment et pour un coût raisonnable, ce qui les rend nettement plus souples et attrayants que les appareils pilotés lorsqu'il s'agit d'affronter de nouvelles menaces. Les UAS ont déjà fait la preuve de leur efficacité contre les menaces asymétriques. A titre d'exemple, les Etats-Unis ont mis au point des UAV tactiques appelés BUSTER, d'un poids de 1,5kg, que les soldats en mission peuvent emporter dans leurs sacs pour les lancer afin d'obtenir une tenue de situation exceptionnelle du secteur.[37]
- Enfin, le fait de ne plus avoir de pilote à bord ouvre la porte à des innovations technologiques impensables auparavant. En fait, la présence d'un pilote humain impose des contraintes très strictes de taille, de forme, de vitesse, d'altitude et d'autres caractéristiques techniques propres à un aéronef.[38] Débarrassés de ces contraintes, les ingénieurs peuvent concevoir des machines sans rapport avec la conception que nous nous faisons des capacités et de l'aspect d'un aéronef. Les systèmes sans pilote existants vont du minuscule Wasp, qui pèse moins de 225 grammes pour 20 centimètres de long, au Global Hawk, d'un poids supérieur à 14 tonnes et d'une longueur de 15 mètres.[39]

43. Toutefois, des problèmes requièrent notre attention. Tout d'abord, une présence massive d'UAV dans des cieux encombrés complique sérieusement le contrôle aérien. Les altitudes inférieures à 900 m étant généralement encombrées d'hélicoptères, d'avions volant à basse altitude et d'UAV "aveugles", le risque de collisions existe et des collisions se sont d'ailleurs produites à trois reprises en Afghanistan depuis le début du conflit. D'après un rapport du service de recherche du Congrès américain, "le risque pour un UAV d'avoir un accident est actuellement 100 fois supérieur à celui d'un appareil piloté".[40] Le nombre élevé d'accidents des UAV a d'ailleurs amené les militaires américains en Afghanistan à inscrire sur leur fuselage un texte en arabe disant, qu'en cas de perte, une récompense serait offerte à quiconque les restituerait à leur propriétaire. Equiper les UAV de dispositifs d'évitement des collisions ou de transpondeurs est pratiquement impossible, sauf pour les plus grands. De ce fait, ils ne sont pas conformes à la législation civile et ne seraient donc pas autorisés à utiliser l'espace aérien civil. Par conséquent, le principal souci des ingénieurs, mais aussi le plus difficile du point de vue technique, est celui de la détection et de l'évitement des objets aéroportés.

---

37. Unmanned Aircraft Systems: Refocusing the Integration of Air & Space Power, par le Général Tom Hobbins, Directeur du JAPCC. NATO's Nations and Partners for Peace. Volume 52. II/2007.
38. The Evolving Capability of UAV Systems, par le Professeur Ian Poll. NATO's Nations and Partners for Peace. Volume 52. II/2007.
39. Unmanned Aircraft Systems: Refocusing the Integration of Air & Space Power, par le général Tom Hobbins, director du JAPCC. NATO's Nations and Partners for Peace. Volume 52. II/2007.
40. Unmanned Aerial Vehicles: Background Issues for Congress, par Elizabeth Bone et Christopher Bolkcom. – CRS Report. Avril 2003.

44. Un danger réel des UAV est leur utilisation en tant qu'arme par des terroristes. Ressemblant à bien des égards à des missiles de croisière et capables de voler à basse altitude, l'intrusion d'un UAS hostile est indétectable par les systèmes terrestres de contrôle, en particulier pour ceux de petite taille. En théorie, des groupes hostiles pourraient soit convertir un missile de croisière anti-navire pour lui permettre de survoler la terre ferme, soit convertir un petit avion en UAV armé. D'après le directeur général du renseignement des forces armées canadiennes, des groupes terroristes ont déjà acquis des aéronefs ultralégers et des deltaplanes.[41] De plus, les transferts d'UAV semblent être un point faible des régimes multinationaux de non-prolifération et de contrôle des exportations en vigueur. D'après un spécialiste de renom de la défense, Dennis Gormley, des UAV non armés peuvent être transformés en UAV armés par le simple fait de changer leur charge utile, ce qui veut dire qu'un UAV sans pilote acheté dans un but déclaré peut très facilement être transformé en arme.[42]

B. LE DEVELOPPEMENT DES CAPACITES SANS PILOTE DANS L'ALLIANCE

45. Des UAS militaires sont utilisés dans des missions de reconnaissance et du renseignement depuis les années 1950 et des fonctions plus complexes sont envisagées pour ces appareils, notamment des missions de combat, la détection d'ADM (armes de destruction massive), des parachutages d'urgence, etc. Les constructeurs d'UAV ont même commencé à travailler sur des applications civiles, comme la protection contre les catastrophes naturelles, la surveillance maritime et la détection des incendies de forêt.

46. Néanmoins, l'engouement que suscitent les aéronefs sans pilote est relativement récent. Au début des années 1990, le département américain de la défense voulait des UAS pour répondre à ses besoins de surveillance à portée réduite, courte portée et catégories d'endurance.[43] Les missions de portée réduite devaient avoir un rayon de 50 km et être effectuées par des petits UAS portables lancés à partir d'un peloton ou d'une section. La courte portée avait un rayon de 200 km, c'est-à-dire celle d'un UAS tactique, le modèle le plus répandu. Enfin, les UAS stratégiques assureraient les missions d'endurance, soit en mode haute altitude et longue endurance (HALE) ou moyenne altitude et longue endurance (MALE). Grâce à leur furtivité, leur vitesse, leur charge, leur prix et, parfois, des facultés d'autoréparation, ce sont les UAS stratégiques autonomes qui offrent le plus de perspectives pour la guerre aérienne. Il se peut que les UAS n'en soient encore qu'à leurs premiers balbutiements, mais on aurait tort de sous-estimer leurs capacités à long terme.

47. Un seuil technologique a été franchi à la fin des années 1990 et les UAS n'ont plus été considérés comme des jouets n'ayant leur place que dans des salons d'aéromodélisme télécommandé. Ils sont devenus incontournables pour toutes les armées se voulant modernes. Les systèmes sans pilote prennent une place croissante dans les forces armées, en particulier aux Etats-Unis. D'après l'étude "*Unmanned Systems Roadmap* 2005-2030" du département de la défense, "les aéronefs sans pilote se sont développés à tel point qu'il n'est plus nécessaire de leur chercher des missions spécialisées… Plutôt que de devoir se demander quelle mission on pourrait trouver pour un aéronef sans pilote, on se demande maintenant pourquoi on continue à confier la mission à un être humain". Le commandant de l'US Air Force en Europe, le général William T. Hobbins, a déclaré qu'entre 2000 et 2010, la part des aéronefs sans pilote dans le

41. Unmanned Air Vehicles as Terror Weapons: Real or Imagined? par Dennis M. Gormley. – Issue Brief, Nuclear Threat Initiative. Juillet 2005.
42. Deadly Arsenals. Nuclear, Biological, and Chemical Threat, par Joseph Cirincione, Jon B. Wolfsthal et Miriam Rajkumar. – Carnegie Endowment for International Peace, Washington D.C., 2005.
43. L'évolution des programmes de drones de combat aux Etats-Unis à l'aune de l'UAS Roadmap: quelles conséquences doctrinales et industrielles à l'échelle transatlantique ? par Alain De Neve - Cahiers du RMES, Vol. 2, No. 2, hiver 2005.

budget total de la force aérienne devrait passer de 4 à 31 %.[44] L'armée de terre prévoit à elle seule de disposer de 10 000 UAS d'ici 2011, contre 1 200 actuellement.[45]

48. On peut, par conséquent, s'attendre à une propagation de cette technologie : aujourd'hui, 32 pays développent plus de 250 modèles différents d'UAV ; des clients d'Europe, du Moyen-Orient, d'Afrique du Nord et d'Asie devraient absorber près de 40 % du marché mondial. Actuellement, 17 pays de l'OTAN possèdent plus de 25 modèles d'aéronefs opérationnels, pour un total de 3 600 aéronefs sans pilote en activité à l'OTAN, dont près de 3 000 (15 modèles) pour les seuls Etats-Unis.[46] Pour tenter de combler leur retard avec les Etats-Unis, plusieurs pays d'Europe, emmenés par la France ont lancé l'initiative multinationale EuroMALE UAV en 2002. Toutefois, l'enthousiasme de départ retombé, ces pays n'ont pas arrêté d'approche commune des critères technologiques de ces UAV et ont choisi de se concentrer sur leurs programmes nationaux.

49. La question des systèmes sans pilote a été discutée pour la première fois à l'OTAN en 2002, à l'occasion de la publication d'un Accord de normalisation OTAN (STANAG) sur les véhicules aériens sans pilote. De plus, les pays de l'OTAN se sont engagés à acquérir des systèmes HALE ou MALE en application de l'Engagement capacitaire de Prague. L'acquisition de l'UAV Global Hawk est par ailleurs envisagée dans le cadre du programme réseaucentrique *Alliance Ground Surveillance* (AGS) de l'OTAN. Ces initiatives revêtent une importance particulière parce que, ces dernières années, l'Alliance a eu beaucoup de mal à obtenir de ses pays membres des aéronefs sans pilote pour des missions de reconnaissance. D'après une étude publiée par le Centre de compétences en matière de puissance aérienne interarmées de l'OTAN (JAPCC), premier groupe de réflexion de l'OTAN pour le domaine spatial, l'OTAN aurait besoin d'une cinquantaine d'aéronefs HALE et d'une vingtaine de MALE. Bien que l'OTAN semble disposer d'un nombre suffisant d'appareils pour répondre à ces besoins, en réalité, les choses sont un peu plus compliquées. Tout d'abord, les Etats-Unis sont les seuls à disposer d'UAV HALE ; malgré l'Engagement capacitaire de Prague, les autres alliés ne se sont pas dotés de ces capacités. Quant aux aéronefs MALE, ces appareils existent sur le plan technique, mais l'OTAN n'étant pas le seul "client", en règle générale, ils ne sont pas disponibles quand elle en a besoin. D'après un responsable de l'OTAN, l'Alliance n'a qu'un accès "intermittent" aux UAV en Afghanistan.[47] En outre, l'OTAN ne dispose pas d'un contrôle au sol ni de systèmes de C2 suffisants et elle ne forme pas de personnel à l'interprétation des données émanant des UAV.[48]

50. Pour pouvoir remédier efficacement à ces problèmes, les experts du JAPCC suggèrent que l'OTAN :[49]

- crée un organisme qui aurait la responsabilité de toutes les activités de l'OTAN se rapportant aux UAV ;
- se dote de ses propres systèmes sans pilote pour faire en sorte qu'ils soient disponibles lorsque l'OTAN en a besoin pour des opérations ;
- encourage les alliés des Etats-Unis de l'OTAN à se doter d'UAV HALE ;
- ajoute des systèmes sans pilote à ses capacités C4ISTAR et réseaucentriques ;
- établisse une politique claire sur la question des UAV de combat, et notamment sur la défense contre les UCAV ennemis.

51. La constitution d'une flotte d'UAV propre à l'OTAN, sur le modèle de ce qui s'est fait pour les AWACS, pourrait sembler une option intéressante, mais elle serait très difficile à concrétiser, étant

---

44. COMUSAFE: unmanned aircraft key to future decision superiority par le Capt. Elizabeth Culbertson, US Air Forces in Europe Public Affairs. – Air Force Print News. 19 octobre 2006.
45. Voir Unmanned Aircraft Systems Roadmap 2005-2030. – Office of the Secretary of Defence. Washington, 2005.
46. Unmanned Aircraft Key to Future Operations, General Says. Par le Capt. Elizabeth Culbertson, US Air Forces in Europe Public Affairs. – Air Force Print News. 20 octobre 2006.
47. Plotting a Course, par Robert Wall. - Aviation Week & Space Technology. 4 décembre 2006.
48. Voir The Joint Air Power Competence Centre Flight Plan for Unmanned Aircraft Systems in NATO.
49. Ibid.

donné que les pays de l'OTAN préfèrent réaliser leurs propres programmes de défense. Selon le lieutenant-général Hans-Joachim Schubert, directeur exécutif du JAPCC, "le fait est que ces nations sont souveraines et ont leurs propres programmes. Si vous envisagez une acquisition, alors, la tendance en Europe est parfaitement claire". Par conséquent, la démarche de l'OTAN se concentre sur l'intégration des normes de communication et des méthodes de contrôle plutôt que sur les plates-formes.[50]

52. La question de savoir si l'OTAN devrait s'équiper de drones de combat (UCAV) est sujet à controverse. Actuellement, seuls les Etats-Unis disposent de drones de combat opérationnels. Des Predators américains armés de missiles Hellfire ont été utilisés en Afghanistan et en Irak pour détruire des cibles d'Al-Qaïda ou de mouvements rebelles. Les Predators, placés sous le contrôle de la CIA, ont également fait la une de l'actualité en novembre 2002 lorsqu'un de ces aéronefs sans pilote a tué six terroristes présumés d'Al-Qaïda au Yémen.[51] Les Européens ont, eux aussi, commencé à s'intéresser au développement ou à l'acquisition d'UCAV comme, par exemple, avec le projet multinational Neuron conduit par la France. Mais les efforts européens semblent assez timides, peut-être en raison de la controverse à laquelle donne lieu l'utilisation de machines semi-autonomes en tant qu'armes létales. Quoi qu'il en soit, les considérations morales ne pèsent généralement pas lourd face au progrès technologique et il est probable que, comme le pronostiquait le général Wolfgang Schneiderhan, chef d'état-major de la Bundeswehr allemande, les UCAV "constitueront un élément essentiel de la force aérienne du XXI^{e} siècle".[52]

53. Le problème de la limitation des bandes de fréquence se pose avec autant d'acuité pour les systèmes sans pilote, étant donné qu'ils sont davantage tributaires des communications sans fil que les systèmes pilotés. Par exemple, comme le souligne l'étude de l'OTAN, des problèmes de conflits de fréquences sont à l'origine de la perte de contact des forces britanniques avec leur UAV Phoenix, mettant ainsi en danger les forces terrestres britanniques.[53] De plus, les aéronefs télécommandés nécessitent des connexions parfaitement sûres, ce qui n'est pas toujours possible ; souvent, le contact avec des UAV a été perdu à cause de ce qu'on qualifie de "fratricide électronique" (interférences provenant de sources amies). Les experts de l'OTAN suggèrent de réserver une partie du spectre des fréquences aux UAV.[54] Le problème des fréquences revêt aussi une très grande importance lorsqu'on aborde la question de la faisabilité des véhicules terrestres sans pilote, supposés effectuer une série de tâches, dont des missions de reconnaissance et de surveillance, de déminage et de transport. Le guidage de ces véhicules commence à poser problème lorsqu'ils opèrent dans un environnement urbain densément bâti où le béton et l'acier des immeubles empêchent les communications radio.[55] La solution généralement proposée pour obtenir une parfaite interactivité réside dans l'intégration dans la "guerre réseaucentrique". Si les Etats-Unis sont sur le point d'arriver à cette situation, les armées européennes en sont encore très loin. Il faut souligner que cet état de choses ne peut que creuser le fossé technologique entre les deux rives de l'Atlantique et compromettre la mise sur pied d'opérations conjointes complexes.

54. L'OTAN a créé un groupe de travail chargé de la question de l'élaboration de normes pour les véhicules terrestres sans pilote. Les STANAG correspondants, qui devront être adoptés d'ici à 2008, devront faciliter l'interopérabilité des dispositifs de combat robotisés des alliés et partenaires de l'Alliance. Comme l'explique le président de ce groupe de travail, Frank Schneider, ces STANAG "devront permettre de connecter une caméra à haute résolution française à un robot suédois et de communiquer ses données à un autre véhicule militaire robotisé, par exemple." La

50. Interview du Lt.-Gén. Hans-Joachim Schubert. – Jane's Defence Weekly. 26 octobre 2006.
51. UCAV Update, édité par by Luca Bonsignore. NATO Nations and Partners for Peace. Volume 52. I/2007.
52. UV's – an indispensable asset in operations, par le général Wolfgang Schneiderhan. NATO Nations and Partners for Peace. Volume 52. I/2007.
53. Plotting a Course. Par Robert Wall. - Aviation Week & Space Technology. 4 décembre 2006.
54. Voir The Joint Air Power Competence Centre Flight Plan for Unmanned Aircraft Systems in NATO.
55. Multinational Robots. By Brooks Tigner. Defence News. 29 mai 2006.

position de l'Agence européenne de défense ne se limite pas à proposer une simple normalisation ; elle exhorte les ministères européens de la défense nationale à poursuivre ensemble la mise au point de technologies de la robotique et à mettre leurs ressources en commun.[56]

IV. CONCLUSIONS

55. Le développement des systèmes réseaucentriques et sans pilote soulève des questions qui vont bien au-delà du seul aspect technologique. L'aptitude à détecter, analyser, cibler et attaquer à distance des éléments du champ de bataille et à partager instantanément l'information requiert un réexamen complet des doctrines et de la philosophie militaires. Les conséquences de ces tendances ne peut que faire l'objet de spéculations. A titre d'exemple, une capacité réseaucentrée permettra aux responsables stratégiques, jusqu'à l'échelon du commandant en chef, de prendre des décisions, y compris de nature tactique. En revanche, le commandant sur le terrain percevra parfaitement la situation et sera en mesure d'agir sans instructions de ses supérieurs. Reste à savoir quel sera le résultat de ces deux tendances contradictoires, mais il va de soi que la procédure de prise de décision hiérarchique traditionnelle sera totalement remise en cause.

56. La réseaucentricité et les systèmes sans pilote contribuent déjà dans une large mesure à la supériorité militaire croissante des Alliés de l'OTAN et permettent ainsi de sauver la vie de nos soldats. Le rapporteur invite instamment les parlementaires de l'OTAN à prendre en compte les perspectives qu'ouvrent ces technologies dans la discussion des budgets de la défense, des structures des forces, et des politiques d'acquisition et de transfert de technologies dans leurs parlements nationaux.

57. Cependant, il ne faut pas croire que ces systèmes soient la panacée qui résoudra tous les problèmes. Bien que certains enthousiastes, comme Robert Finkelstein, professeur à l'Ecole de management et de technologie de l'Université du Maryland, prédisent que "bien avant la fin du siècle, il n'y aura plus personne sur le champ de bataille"[57], on note une tendance aussi marquée à souligner l'importance des facteurs humains et culturels nécessaires pour obtenir l'adhésion de la population. L'utilisation de systèmes sans pilote (et autonomes, en particulier) comme véhicules de combat soulève aussi de délicates questions d'ordre moral.

58. Bien que l'aspect politique de ces problèmes, qui fait l'objet de ce rapport, soit le plus pertinent, d'autres démarches s'imposent par ailleurs afin de favoriser l'élaboration de normes techniques communes et de mécanismes de protection pour les réseaux comme pour les systèmes sans pilote. La question de la limitation des bandes de fréquence nécessite une attention particulière de l'OTAN.

59. La mise au point d'un système efficace de partage de l'information entre les partenaires d'une coalition est très importante à l'ère de l'informatique. Certains auteurs pensent qu'il est impossible de surmonter les problèmes que pose la réseaucentricité pour le bon fonctionnement d'alliances militaires. Pour Paul T. Mitchel, "une interopérabilité homogène est impossible. L'information est un élément vital de l'avantage concurrentiel qu'offre la guerre réseaucentrique et ne peut être compromise par des procédures automatiques de divulgation".[58] Toutefois, s'il y avait une réelle volonté politique, les pays de l'OTAN pourraient arriver à une solution pratique. Comme le disait le président du comité militaire de l'OTAN, le général Harald Kujat, "si vous n'arrivez pas à fonctionner ensemble, vous êtes non seulement moins efficaces, mais vous risquez de faire échouer votre mission et de mettre en danger la vie de vos soldats. Il ne suffit pas d'être une coalition de volontaires, il faut aussi être une coalition interopérable".[59]

---

56. Ibid.
57. War of the Machines, par Yuki Noguchi. – Gulfnews.com. 27 février 2004.
58. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, par Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. Décembre 2006.
59. The Collection of Statements – site Internet du Joint Air Power Competence Centre website.