Les conséquences organisationnelles de la numérisation du champ de bataille

Par Betsy ANNEN
Chercheur associé au CEREMS

Janvier 2006

"*Un outil ne vaut que par la main qui l'anime*".
Maréchal de Lattre de Tassigny

Introduction

Engagée par les Etats-Unis dans les années 90, la Transformation s'inscrit dans l'exacte continuité de la Révolution dans les Affaires Militaires (RMA) et conjugue les progrès de la précision et de l'information. La Transformation repose en effet sur l'idée que le différentiel technique crée un différentiel d'efficacité. A cet égard, un des facteurs déterminants de la Transformation est l'usage intensif des nouvelles technologies destinées à remplacer peu à peu la puissance de feu des grands équipements par une intelligence électronique reliée en réseau, du combattant à l'état-major. L'introduction de ces nouvelles technologies de l'information est le fruit de méthodes d'abord explorées par les entreprises telles que l'ouverture des structures hiérarchiques, l'interconnexion des capteurs et des décideurs, l'accélération des processus décisionnels ou l'auto-synchronisation.

Si les nouvelles technologies constituent un vecteur nouveau d'efficacité, leur rôle n'en est pas moins paradoxal : tout en aidant à relever certains défis de l'intervention sur le terrain, elles introduisent des complexités inédites qu'il devient impératif de saisir voire de pallier. Une numérisation mal maîtrisée peut en effet rapidement devenir contre-productive.

Ainsi, de nombreuses interrogations sous-jacentes guident actuellement les réflexions sur la prochaine étape de la Transformation : jusqu'où peut-on pousser le processus de numérisation du champ de bataille ? Quelle est la place de l'initiative humaine dans une guerre « info-centrée » (Network Centric Warfare) ?

I) Les effets de la numérisation de l'espace de bataille (NEB).

Supériorité informationnelle

La numérisation de l'espace de bataille (NEB) procure aux combattants, aux chefs et aux états-majors **une connaissance en temps quasi-réel de l'évolution de la situation**. La NEB repose donc sur la notion de connectivité à savoir la synchronisation quasi-instantanée de fonctions (détecter, transmettre, agir) géographiquement séparées, induisant de fait un rétrécissement de l'espace. Les sources d'information sont légions : le fantassin, la section, la division, l'avion de combat, le drone, le satellite etc. peuvent tous jouer à un moment ou à un autre le rôle de capteurs, reliés entre eux et au commandement par un réseau informatique crypté. La NEB apporte ainsi à chaque rouage une « compréhension situationnelle » (situational understanding) qui va au-delà d'une perception immédiate de la situation par une interprétation des intentions des forces ennemies et une prise en considération des hypothèses d'action parmi tous les éléments de l'espace de bataille.

La NEB est donc un **multiplicateur d'efficacité** en ce sens qu'elle permet une accélération de la prise de décision, évite une déformation de l'information et renforce la

liberté d'action. En effet, la maîtrise du temps précipite le processus décisionnel qui permet de surpasser l'ennemi par un rythme d'opérations plus soutenu. Par ailleurs, les ordres et les informations en provenance directe du théâtre d'opération ne sont plus transmis en cascade mais sont communiqués directement. Enfin, la numérisation de l'espace permet au chef de commander au cœur de l'événement grâce à un PC tactique très mobile, léger et concentrant tous les flux d'informations utiles puis de diffuser ces mêmes informations à la totalité des zones d'évolution de plus en plus larges des forces terrestres.

L'usage d'interfaces informatiques a donc pour objectif d'affirmer une **supériorité informationnelle** potentiellement décisive, par l'acquisition, le traitement et l'exploitation de toutes informations utile à la mission. Cette supériorité est supposée réduire au maximum l'incertitude et donc les risques d'erreur militaire en maximisant la rapidité et l'efficacité.

Verticalité et horizontalité

La NEB s'appuie sur un outil complexe, le **C4ISR** (commandement, contrôle, communications, computers, intelligence (renseignement), surveillance et reconnaissance). Il s'agit d'un « système de systèmes » qui intègre tous les réseaux du champ de bataille dans une architecture globale. Chaque élément de cette structure fait l'objet d'un groupe distinct d'unités, d'analystes et de commandements dont l'intercommunication est indispensable à la bonne marche des opérations militaires.

Il en résulte donc **un système communicationnel à deux sens** : 1) un système traditionnel de communication verticale des échelons supérieurs vers les échelons inférieurs et vice versa (d'amont en aval et d'aval en amont) 2) un système nouveau de communication horizontale, d'une unité à une autre, d'un commandement à une unité, d'une unité à un commandement, d'un commandement à une unité.

II) Les bouleversements du commandement

L'aplatissement des lignes hiérarchiques

La NEB modifie donc profondément la guerre qui devient « réseau centrée » (*Network Centric Warfare* – NCW) où la boucle entre détection, décision et action entre les systèmes d'armes et les donneurs d'ordres est considérablement raccourcie. La diffusion ultra rapide et transversale de l'information comporte le risque d'un **affranchissement de la hiérarchie**, colonne vertébrale des armées. Par exemple, la mise en place de messageries électroniques induit une notion d'échange transverse d'informations qui s'oppose à la structure pyramidale du commandement.

Si la structure hiérarchique peut être court-circuitée de la base vers le commandement, elle peut également être mise à mal par le commandement lui-même. Le chef peut être tenté de ne pas respecter **le principe de subsidiarité** qui veut que le responsable sur le terrain est mieux à même de décider, dans les limites du périmètre qui lui a été défini, ce qu'il doit faire que son supérieur, éloigné des réalités du combat.

Le syndrome « Big Brother »

Cette possibilité de contourner les échelons intermédiaires par les deux extrémités de la chaîne de commandement peut déboucher sur une **déresponsabilisation** globale de tous les échelons inférieurs et donc de paralysie du système : d'un côté, les échelons d'exécution ont l'impression que le commandement, soudainement omniscient et omnipotent est le seul à pouvoir prendre des décisions grâce à la vue d'ensemble que lui offre la NEB. S'ajoute à cela la crainte implicite d'être constamment scruté ce qui annihile

toute liberté d'action et tout esprit d'initiative. De l'autre côté, le commandement peut être incité à imposer directement aux échelons inférieurs le détail de leurs manœuvres.

Dans les deux cas, le raisonnement est erronée et dangereux puisqu'il est impossible de transmettre par écrans interposés des facteurs autant décisifs qu'impalpables tels que le moral des troupes.

Ce même risque peut être transposé à l'articulation entre **le monde politique** et le commandement militaire puisque les politiques, bénéficiant d'une masse considérable d'informations, peuvent être tentés de priver la sphère militaire de sa nécessaire liberté d'action afin d'obtenir des résultats tant rapides que visibles.

Une conséquence inévitable de la logique de réseau ?

Ces boucles courtes de décisions contreviennent certes à la culture de subordination militaire mais certains exercices, organisés par le CDES (Commandement de la doctrine et de l'enseignement supérieur de l'Armée de Terre) notamment, ont montré l'opportunité offerte par les nouvelles technologies de créer des groupes de forces transversaux de circonstance. Ces groupes *ad hoc*, tout en respectant les trois phases élémentaires de l'action (conception, mise en œuvre, exécution), sont parfois plus efficaces pour mener des opérations ciblées.

L'estompement du rôle charismatique du chef ?

Les nouvelles possibilités de gestion de l'information qu'offrent les NTIC peuvent amener le chef à être de plus en plus éloigné de ses hommes, à ne communiquer avec eux qu'indirectement. Le concept novateur de « **Reachback** » qui consiste à maintenir dans un PC « sanctuaire » les fonctions qui ne sont pas indispensables sur le théâtre confirme cette évolution. La confiance dans le système est telle que les capacités numériques sont amenées à remplacer le lien physique entre l'exécutant et son chef. Cela ne va-t-il pas dans le sens d'une diminution l'ascendant moral du chef, trop éloigné de la réalité du terrain et du quotidien de ses hommes ?

III) Les limites techniques du « tout technologique »

Le ralentissement du processus décisionnel

Paradoxalement, la montée des nouvelles technologies dans l'espace de bataille est susceptible de ralentir le processus décisionnel. En effet, le désir de **diminuer au maximum la part d'incertitude** peut conduire le chef à attendre la dernière information pouvant réduire autant que faire se peut la part de subjectivité de ses décisions. Cet abus de confiance dans le système entrave considérablement la prise de décision et incite les chefs à oublier que la prise de risque est inhérente à toute opération militaire.

Par ailleurs, tout aussi paradoxalement, on pourrait penser que les progrès technologiques de la NEB entraînent une réduction considérable des effectifs en éliminant les intermédiaires, les messagers etc. Au contraire, de nouvelles fonctions, liées au traitement de l'information, font leur apparition.

La vulnérabilité des infrastructures et des réseaux

La mise en réseau des commandements et le lien direct établi avec leurs troupes provoquent une complexité organisationnelle où **la fiabilité de la transmission** tient un rôle primordial. La première difficulté consiste donc à protéger les infrastructures de communication (ordinateurs, satellites, radars, fibres optiques). En cas de destruction, d'endommagement ou de capture des infrastructures digitales, tout le réseau s'en trouve

désorganisé : les troupes sont coupées de leurs commandements ; le combat se fait « à l'aveugle ».

Cette dépendance du combattant à la technologie est d'autant plus inquiétante que **les réseaux sont *a priori* vulnérables**. Ils peuvent être attaqués par des agressions physiques ou par l'exploration du système, l'écoute et le décryptage ce qui permet d'exploiter la ressource informationnelle adverse à son profit. De simples programmes suffisent à désorganiser l'ensemble (virus, « vers », « bombes logiques », « chevaux de Troie » etc.). Ce risque est d'autant plus sérieux que l'attaquant est difficile à identifier du fait de son extériorité au champ de bataille ou parce qu'il est usager interne au réseau. Il faut donc organiser une protection de l'information lors de sa transmission mais également une préservation du réseau lui-même.

Aussi, plus la dépendance du soldat à la technologie sera forte, plus l'infrastructure technologique constituera une cible prioritaire par rapport au soldat.

Les effets de la surinformation

La surinformation représente le risque d'un débordement par un flux incessant et indistinct d'informations. Il devient inutile de disposer d'un grand nombre d'informations s'il est impossible de distinguer rapidement et sûrement l'information décisive de l'information triviale. La supériorité informationnelle n'a donc de sens que si la prolifération de l'information ne paralyse pas la prise de décision.

IV) Perspectives : Les NTIC ne sont qu'un outil au service de l'homme.

Recentrer la guerre sur le facteur humain.

Les retours d'expérience américains sur la guerre en Irak soulignent tous la nécessité de se garder d'une dépendance absolue de l'homme à la technologie. Les Etats-Unis ont en effet dû faire face à certaines déconvenues : les réseaux ont parfois été saturés (notamment à cause des flux d'information distribués sans discernement au plus bas niveaux) malgré l'emploi d'une cinquantaine de satellites ; les unités ont rencontré des problèmes d'interopérabilité technique au sein de la coalition etc. Plus ponctuellement, un missile « Patriot » a frappé un « Tornado » britannique, un A10 a attaqué un convoi britannique qui portait toutes les marques d'identification et enfin, les éléments de pointes de l'US Army et du Marines Corps se sont combattus de part et d'autre du Tigre parce que leurs postes radios n'étaient pas compatibles.

Il apparaît donc nécessaire de prendre conscience des limites du tout technologique, d'en tempérer la montée par un **recentrage de la vision stratégique sur le facteur humain**. L'analyse humaine reste un maillon essentiel de l'art de la guerre qui ne peut se résumer à une science, même poussée, de la technologie. Deux impératifs doivent guider le commandement et l'action des combattants : comment transmettre la bonne information à la bonne personne au bon moment ? Et, comment traduire le plus rapidement possible la complexité des faits en ordres simples ? La stratégie se nourrit nécessairement de l'expérience des chefs et n'est donc pas réductible aux nouvelles technologies, incapables de prendre en considération des éléments de contingence pure.

La valorisation de nouvelles fonctions

Pour limiter au maximum les éventuels dysfonctionnements d'une diffusion en réseau de l'information, il est envisageable de valoriser davantage voire de créer de nouvelles fonctions. Ainsi, afin de garantir et de renforcer l'**expertise relative à la sécurité de l'information et des réseaux**, il serait bienvenu (notamment dans les pays européens) de développer la filière « expert SSI » (Sécurité des Systèmes d'Information), trop souvent ramenée à un sous-domaine du management des systèmes d'information.

Afin de gérer les effets de surinformation au niveau du commandement, les Etats-Unis privilégient la mise en place d'**opérateurs techniques** permettant aux chefs de prendre le recul nécessaire à la conduite des travaux d'état-major sans être accaparés par la gestion de l'information. Il semble également nécessaire d'identifier de nouveaux postes stratégiques afin d'assurer une **veille informatique permanente**. Par exemple, au cours de l'exercice Aigle 99 de l'Eurofor, une cellule « Intelligence Management Cell » (IMC) a été instaurée afin de fluidifier le traitement de l'information.

Cohabitation de deux structures décisionnelles

Il ne fait aucun doute que la structure pyramidale, parce qu'elle permet de conserver une cohésion et une cohérence indispensable, reste essentielle au bon fonctionnement des armées. Il faudrait donc **superposer deux structures**, une fonctionnelle qui permet d'aller directement au « nœud décisionnel » en cas d'urgence et une hiérarchique destinée à assurer la cohérence d'ensemble et la normalité. L'introduction des processus collaboratifs en réseau ne doit pas remettre en cause les structures hiérarchiques mais les valoriser par exemple en favorisant les regroupements d'experts qui fournissent des analyses bien plus complètes qu'auparavant.

De nouveaux outils

Des nouvelles technologies peuvent également émerger certaines parades, certains **outils d'aide à la décision**. Il est envisageable d'instaurer un premier de tri de l'information grâce à des filtres, des mécanismes de synthèse ou d'élimination de l'information non pertinente. Des indicateurs agrégeant certains types d'information sont également à l'étude pour aider les décideurs à conserver leurs capacités de synthèse. Des procédures plus rigoureuses peuvent également être mises en place comme l'instauration d'un format court pour la transmission des ordres d'opération.

Conclusion

Les réflexions actuelles sur le processus de Transformation, nourries des retours d'expériences d'Irak et d'Afghanistan, se recentrent sur la place de l'initiative humaine, mue par une intelligence non reproductible par la technologie, aussi avancée soit-elle. De nouvelles orientations se dessinent : d'une part, de nombreuses recherches sont menées sur le renforcement de la sécurité des systèmes et la mise en place de procédure de fonctionnement en cas de panne totale (ou d'attaque) des réseaux ; d'autre part, il devient impératif d'actualiser la formation des combattants qui sont désormais amenés à cumuler diverses compétences techniques de pointe et à se familiariser avec des techniques de management en réseau. Il n'en reste pas moins que le combattant doit maîtriser les outils technologiques non pas au détriment des méthodes "traditionnelles" de combat mais en concordance avec celles-ci.

Bibliographie

Sur le processus de Transformation en général

▪ CIMBALA, Stephen J. « Transformation in Concept and Policy », *Joint Force Quaterly*, n°38, 3 ème trimestre 2005.

▪ CDEF (Centre de Doctrine d'Emploi des Forces), « La Transformation : jusqu'où ? », *Héraclès,* n°4, juillet-août 2004.

▪ BRAILLARD, Philippe et MASPOLI, Gianluca, « La 'Révolution dans les Affaires Militaires' : paradigmes stratégiques, limites et illusions », *Annuaire Français des Relations Internationales,* 2002.

▪ HOOKER, Richard D. Jr., McMASTER, H. R. et GREY, Dave « Getting the Transformation right », *Joint Force Quarterly,* n°38, 3 ème trimestre 2005.

Approches nationales du processus de Transformation

▪ CDEF (Centre de Doctrine d'Emploi des Forces), «La France dans le concert de la Transformation », *Doctrine*, numéro spécial, septembre 2005.

▪ DORMAN, Andrew « Transformation and the United Kingdom », *Joint Force Quaterly,* n°37, 2 ème trimestre 2005.

Sur l'introduction des nouvelles technologies sur le champ de bataille

▪ BEZACIER, Gérard, « Soldier Centric Network », *Héracles*, n°9, juin 2005.

▪ DE NEVE, Alain, « Guerre d'Irak (20 mars – 1er mai 2003) : réseaux, infodominance et révolution dans les affaires militaires », *Cahiers du RMES*, n° 2, décembre 2004.

▪ FORGUES, Pierre (Colonel), « Le commandement et la guerre réseau-centrique », *Revue militaire canadienne*, été 2001.

▪ NACHEZ, Eric, « L'impact de la numérisation de l'espace de bataille sur la culture des officiers d'état-major », *Le Casoar*, n°176, janvier 2005.

▪ NOYER, Jean-Marc, *Guerre et Stratégie*, Les Cahiers du Numérique, vol. 3, n°1 – 2002.

▪ PERROW, Charles, « Difficulties with Network centric Warfare » (Chapitre 10), *Information Assurance : Trends in Vulnerabilities, Threats and Technologies*, Working Paper, Janvier 2005

▪ THOMAS, Thimothy L., « Infosphere Threats », *Military Review*, septembre-octobre 1999.

▪ THORNTON, Robert, « Technologie and Transformation : Implications on the Company Commander », *Armor*, Janvier-Février 2005.

▪ TOOMEY, Christopher J., (Lieutenant-colonel – US Army), « C4ISR in the Stryker Brigade Combat Teams », *Military Review*, Mai-Juin 2003.

▪ WALLACE, William S. (Général de corps d'armée – US Army), « Network-Enabled Battle Command », *Military Review*, Mai-Juin 2005.

▪ WASILIEWSKI, Jean-Marc (Lieutenant-colonel), « Les conséquences inattendues de le numérisation », *Objectif Doctrine*, n°18, octobre 2002.

Sites Internet

▪ Combined Arms Research Librairy / Command and General Staff College - http://www.cgsc.army.mil/carl/ (certaines sources en accès restreint)

▪ Defense Technical Information Center (DTIC) - http://stinet.dtic.mil/

▪ Military Domain Search Engine - http://call-search.leavenworth.army.mil/

▪ Official website of US Department of Defense - http://www.defenselink.mil/transformation