1997-1998

CBA PRIGENT ERIC

C4

UNE NOUVELLE STRATEGIE :

LA STRATEGIE DE L'INFORMATION

BIBLIOGRAPHIE :

- **Information age warfare** : Military review. september-october 1997.
- **The revolution in military affairs** : prospects and cautions.(Earl Htilford, JR) Defense issues (June 1995)
- **Toward a Better Intelligence Community Relationship**. (Defense issues, volume 10, Number 73)
- **DoD'S Fundamental Challenges in an Uncertain Future** (Defense issues, Volume 13, Number 4)
- **Digitization in task force XXI** (Defense Issues)
- **Retaining the edge on Current and Future Battlefields** (Defense Issues, Volume 10, Number 85)
- **Embedded training Concept** (Tradoc Pamphlet 35)
- **Revue de la Defense Nationale** (janvier 1998)
- **Une nouvelle stratégie pour le renseignement** : (Amiral Pierre Lacoste)
- **« La guerre dans le cyber-espace »** (Jean Guisnel)

De quoi s'agit-il ?

Au XXI° siècle, le défi majeur lancé à l'habileté des politiques et des stratèges est de priver l'adversaire potentiel d'accéder aux informations vitales pour lui et indispensables à la conduite des opérations, tout en conservant en permanence un avantage décisif dans ce même domaine. Le but de cette dernière manoeuvre est donc bien de gagner la bataille de l'information.

Ainsi, au même titre que les stratégies maritime, aérienne ou terrestre qui font elles mêmes partie d'une grande stratégie plus globale, on peut maintenant parler de la stratégie de l'information.

Une stratégie nouvelle pour le XXI°siècle :

la stratégie de l'information

Lancée par la guerre du golfe qui a validé, si ce n'est consacré, les technologies militaires des années 80 (furtivité, précision à longue portée, importance du C3I, observation par satellite et gestion électronique de l'information), la « Révolution in Military Affairs » ouvre aux Etats-Unis « l'ère de l'information » qui consacre à son tour la dominance informationnelle.
Cette dernière est considérée, en France, au mieux comme un gadget américain, ou au pire, comme un complot, destiné à attirer dans une compétition gagnée d'avance les puissances de second rang. Aussi, prudemment, on préfère parler dans notre pays de la « maîtrise de l'information ».
Le général Elie, directeur de la DRM, dans le numéro de la revue « Défense nationale » de janvier 1998 insiste, cependant, sur le fait que la maîtrise de l'information est une nécessité stratégique.

Cependant, cette maîtrise de l'information, qui recouvre toutes les formes du renseignement, englobe la prévention des crises et la domination tactique sur le champ de bataille, la guerre psychologique et les moyens électroniques du renseignement, n'est considérée, jusqu'à aujourd'hui, que comme une stratégie indirecte.

Pourtant, dès maintenant, le renseignement et la maîtrise de l'information sous toutes leurs formes s'imposent en tant que stratégie à part entière.

En effet, un conflit constitue un ensemble unique ; ce n'est pas la guerre sur mer, sur terre, ni dans les airs, ni même dans l'espace ou maintenant dans ce qu'il est convenu d'appeler le cyber-espace. Par les armes et grâce à des manoeuvres dans plusieurs environnements géographiques, les belligérants cherchent à se procurer l'avantage stratégique. L'objectif est le même : atteindre ou s'emparer du centre de gravité stratégique de l'adversaire ou de la coalition.

Aujourd'hui, le défi majeur lancé à l'habileté des politiques et des stratèges est de priver l'adversaire potentiel d'accéder aux informations vitales pour lui et indispensables à la conduite de la bataille, tout en conservant en permanence un avantage décisif dans ce même domaine. Le but de cette dernière manoeuvre est donc bien de gagner la bataille de l'information.
Ainsi, au même titre que les stratégies maritime, aérienne ou terrestre qui font elles mêmes partie d'une grande stratégie plus globale, on peut maintenant parler de la stratégie de l'information.

Afin de mieux comprendre la nécessité de cette dernière, il paraît tout d'abord nécessaire de faire un bilan de la situation dans le secteur de l'information en cette fin de siècle, avant de définir, dans une deuxième partie, cette stratégie, ses besoins, ses enjeux et les formes qu'elle pourrait revêtir.

1° PARTIE : Bilan de la situation actuelle dans le domaine de l'information :

Quand on s'intéresse à la guerre de l'information, il est normal de se retourner vers les Etats-Unis, car ce sont les militaires américains qui ont inventé INTERNET, voilà un quart de siècle, lors de la conception de leur réseau ARPANET. Des organismes comme la *National Security Agency* s'y sont investis totalement, au point de ne plus rien ignorer de ce qui se passe sur le réseau.
Installée à Fort-Meade, la NSA compte aujourd'hui plus de 40 000 employés, elle intercepte pratiquement tout ce que les ondes radioélectriques peuvent porter. La NSA est aujourd'hui au coeur du renseignement mondial, car l'extraordinaire explosion des moyens de communications électroniques ne laisse pratiquement plus aucune bribe de l'activité intellectuelle, politique, industrielle, militaire ou commerciale humaine à l'écart. Tous les services de renseignement se servent des communications *on line* pour aller interroger, partout, des bases de données qu'ils explorent grâce à des moyens informatiques aux capacités stupéfiantes. A l'âge numérique, voler des informations peut se faire simplement par l'interception des données en un point quelconque, qu'elles soient stockées ou en transit.
Mais la naissance des réseaux communicants planétaires s'est doublée de l'émergence de nouveaux outils de protection de l'information : des moyens de cryptage aptes à protéger les communications sur le réseau ont été diffusés, gratuitement, et les services de renseignement du monde entier se battent actuellement pour que cette évolution soit contrée. Ce sera l'un des enjeux primordiaux du moyen terme.
Les différentes époques de la guerre ont toujours été marqués par l'introduction d'armes et/ou de doctrines nouvelles. L'information et son traitement ont déjà commencé à bouleverser les rapports de force sur la planète et constituent indiscutablement la nouvelle révolution de cette fin de siècle.

Personne ne peut plus ignorer l'importance de systèmes de commandement intégrant, lors de la bataille, les informations recueillies par tous les *senseurs* possibles : Images, renseignements radioélectriques, surveillance des flux transnationaux d'information, gestion adaptée des chaînes de transmissions du commandement, surveillance des réseaux, autant d'impératifs qu'il n'est désormais plus question de négliger pour un état souverain. Ces systèmes permettent aussi de forger les opinions publiques en contrôlant les images et les nouvelles à la source et en orientant l'information de masse vers des buts conformes à ceux des chefs de guerre.

Mais le changement fondamental n'est pas dans l'apparition des nouvelles techniques d'information, mais plutôt dans la manière dont il en est fait usage. En effet, la perception de l'information ne s'est modifiée que récemment, pour sortir du seul domaine de l'espionnage et des systèmes de communication. L'information est ainsi devenue un domaine à part entière dans la défense.
L'information n'est donc plus uniquement perçue comme une aide à la décision au profit des responsables politiques.
Elle fait irruption sur le champ de bataille comme une arme à la disposition du chef interarmes, qui doit alors définir dans ce domaine un mode d'action. Il doit planifier et

mettre en oeuvre une véritable stratégie, car il s'agit pour lui de conserver dans ce domaine un avantage crucial sur l'ennemi avant, pendant, et même après les opérations militaires.
Ainsi, dès le début du déclenchement de l'opération « *DESERT SHIELD* », l'une des innovations technologiques majeures a été apportée, côté américain, par les systèmes de traitement de l'information et la mise au point de nouveaux réseaux, dont en particulier le DSNET2, ultraprotégé par le transfert par paquets des informations numérisées les plus sensibles jusqu'au plus bas niveau de la hiérarchique du champ de bataille. Les analystes des services de renseignement militaires américains disposaient en temps réel des informations mondiales, afin d'anticiper les actions inamicales, de discerner et d'analyser les tendances politiques. Les stratèges américains ont désormais intégré cette problématique, les réseaux font aujourd'hui partie de leur culture profonde et les technologies de l'information entrent massivement dans l'arsenal militaire. Avec un âge de l'information parvenu à maturité, une forme de guerre vraiment révolutionnaire va émerger. Dès lors qu'un adversaire potentiel aura accès à de multiples systèmes d'information, la guerre se conduira virtuellement, à la vitesse de la lumière et sur des distances considérables.

La domination du cyberespace, selon certains, pourrait rendre moins probable l'emploi des forces conventionnelles et de la puissance de feu. La guerre de l'information et donc la guerre tout court, pourra se gagner sans combattre ou même se perdre après la bataille.
L'information électronique s'affirme donc, non seulement comme une arme et une pièce maîtresse d'une stratégie globale, mais devient elle-même sujet d'une stratégie particulière.
Pour les militaires, il s'agit donc de découvrir ou d'inventer une nouvelle catégorie de stratégie.

2° PARTIE : La stratégie :

Si aux Etats-Unis la réflexion a déjà donné naissance à une véritable stratégie débouchant sur une volonté de se donner les moyens matériels et humains pour gagner la guerre de l'information, en France toute vision offensive de la question est proscrite : on se contente de se protéger.

Les spécialistes français de la sécurité des systèmes d'information peuvent sans nul doute protéger les informations d'intérêt national avec une grande efficacité, mais une stratégie uniquement défensive ne concède que rarement l'avantage sur le champ de bataille. Ensuite la règle d'efficacité maximale, dans la protection du secret, est désormais l'exploitation rapide de l'information et non sa classification et son rangement dans un coffre : toute information non exploitée rapidement est une occasion d'action perdue !!

La stratégie de l'information ne peut donc qu'être résolument offensive.

Aussi, pire que de ne pas avoir le matériel ou les moyens, c'est le manque d'imagination, d'enthousiasme, de vision, de croyance, le doute, qui sont les principales entraves au développement d'une telle stratégie.
En effet, le rythme inégalé des innovations technologiques, la fin de la guerre froide et la réduction des budgets de défense impliquent non seulement des changements

fondamentaux dans la manière d'envisager les conflits, mais amènent de fait les politiques et les responsables militaires à adapter de nouveaux concepts opérationnels et à revoir l'organisation des armées. Ils doivent ainsi non seulement se préparer à affronter de nouvelles formes de guerre qu'ils ne comprennent pas toujours, mais aussi à changer ce qu'ils pensent et surtout comment ils pensent.

Pour définir une stratégie, il faut, tout d'abord, bien connaître l'ennemi et les formes des menaces qu'elle est supposée affronter. Le renseignement est ainsi par nature la quintessence de la guerre de l'information.

Or, les menaces des vingt prochaines années sont difficiles à cerner et se caractérisent par leur caractère nouveau, varié et volatile.
Le livre blanc écrit en 1994 ne prend sans doute pas assez en considération certaines formes de menace qui se sont affirmées depuis.
En effet, si les scénarios décrits dans ce livre blanc demeurent d'actualité, bien qu'on sous-estime sans doute actuellement, la probabilité d'un conflit de grande intensité, les risques et les menaces inhérents à la prolifération d'armes de destruction massive, nucléaires, chimiques ou bactériologiques, se font plus pressants en cet fin de siècle qu'il n'y a cinq ans.
Les menaces liées au terrorisme international, au crime organisé et au trafic de drogue se font plus précises et ne peuvent plus être ignorées et passées sous silence par les responsables de la défense nationale.
L'ennemi ne peut donc être défini avec précision et la menace est beaucoup plus globale qu'on ne l'avait envisagée jusqu'alors. Les barrières entre renseignement tactique et stratégique sont plus floues, le renseignement d'intérêt militaire y perd même son sens au profit d'un renseignement plus large et tout azimut, ce qui place naturellement la guerre de l'information et, donc le renseignement, en première ligne.

Classiquement, le but du renseignement de théâtre est de faire en sorte que le chef interarmes dispose, en temps réel de toutes les informations disponibles qui lui donnent une vision d'ensemble du champ de bataille. Ce rôle du renseignement est encore renforcé, mais il n'est plus suffisant.

En effet, pour gagner la guerre de l'information, le chef interarmes ne peut plus se satisfaire de connaître la situation tactique de l'ennemi avec précision, il doit être sûr de posséder, dans le domaine de l'information, la supériorité et l'avantage à chaque instant sur ses adversaires.

Les applications de l'info-war vont de la prévention des crises à la domination tactique sur les champs de bataille, en passant par la guerre psychologique et les moyens électroniques du renseignement. Elles doivent permettent d'obtenir l'effet de surprise et, réciproquement, d'en priver l'adversaire.
Pour cela, le chef de guerre doit s'assurer que ses propres systèmes d'information soient effectivement bien protégés. Il doit être en mesure d'attaquer et de semer la confusion dans les systèmes d'information de l'ennemi, et enfin être alimenté par un juste flux d'informations de qualité.
Le projet de l'armée américaine « Army vision 2010 », affiche la volonté de rendre le champ de bataille transparent pour elle et opaque pour ses adversaires.
Alors que de telles assertions semblaient saugrenues en Europe, les Etats-Unis

prenaient une avance démesurée. Une école spécialisée s'est mise en place et a accueilli dès août 1995, les premiers officiers venus se former spécifiquement à la guerre de l'information.

La stratégie de l'information débute donc bien en amont d'un conflit, car c'est dans le domaine technique que les progrès sont les plus stupéfiants.
Les états-majors doivent ainsi mettre en place une véritable politique de recherche et d'acquisition des matériels nécessaires, en se tenant toujours informés des progrès réalisés et des nouvelles possibilités offertes, en particulier par les réalisations dans le secteur civil.
Pour être en mesure d'accompagner ces dernières, il est nécessaire, par exemple, de standardiser les interfaces et d'utiliser les standards commerciaux, quand cela est possible, pour permettre une évolution des systèmes à moindre coût.
Pour cela faut-il encore faire preuve d'imagination, de créativité, d'anticipation, posséder les infrastructures, planifier et gérer la dépense d'énergie de nos équipes de recherche qui ont la dure tâche de résoudre des problèmes techniques ardus et, enfin, posséder des crédits conséquents pour la recherche et le développement.
Les progrès se font surtout sentir dans l'observation aérienne, l'imagerie spatiale et surtout les interceptions électroniques et la cryptographie. Les satellites optiques, infrarouges et les radars les plus perfectionnés obtiennent des résultats spectaculaires.
Au-delà des moyens de recherche proprement dits, c'est surtout au niveau du traitement et de l'exploitation des informations que l'on peut parler d'une véritable révolution. Les américains disposent dès maintenant, par exemple, d'un internet tactique qui promet déjà de révolutionner le monde des communications, en accroissant de manière formidable le nombre de communications numériques possibles. Les extrapolations sur la guerre future évoquent désormais, comme une évidence, l'existence d'un champ de bataille numérique où tous les systèmes d'information amis communiquent entre eux.
Le défi actuel pour les armées est donc de transformer leurs dispositifs de communication en système, et de passer ainsi d'une organisation de type hiérarchique à un dispositif plus ouvert, permettant aux systèmes d'information de communiquer entre eux et de donner, en un temps record, le maximum de renseignements sur le champ de bataille.
Les discussions actuelles, qui peuvent paraître encore bien ésotériques, entre les tenants de la technique du « pull » ou du « push », pour la distribution de l'information, dissimulent en fait un débat de fond, car cela concerne notre philosophie et l'organisation du commandement.
Pour simplifier, nous aurions, d'un côté, les modernes, les Américains, partisans de la plus grande fluidité de l'information au profit du plus grand nombre, contre les anciens, les Français, qui conserveraient une vision classique de l'information : « le chef est propriétaire de *son* information et c'est lui qui INFORME ses subordonnés. ». A terme, c'est l'organisation du commandement qui sera bouleversée par l'évolution des techniques.
Toute la difficulté consiste à adapter notre manière de penser et de faire. La révolution des esprits doit accompagner et même précéder les mutations technologiques.
Nous pouvons donc employer le terme de stratégie, car il ne s'agit pas d'une simple politique d'équipement. Cette dernière doit s'accompagner de véritables opérations

de renseignement, destinées à connaître les possibilités des autres armées, amies ou ennemies probables, leurs matériels et leur politique en ce domaine, avec toujours le souci de conserver l'avantage sur elles.

Si la volonté et une bonne dose d'imagination créatrice sont paradoxalement nécessaires dans le domaine technique, elles sont, par contre, indispensables en ce qui concerne les ressources humaines sans lesquelles la guerre de l'information ne pourra être gagnée.

Dans un article de la « Revue de la Défense Nationale » qui traite de l'intelligence économique, son auteur Eric Denegé, énumère un certain nombre de nouveaux métiers liés au renseignement, qui devraient se développer et des plus anciens qui évolueront rapidement :
« Les spécialistes de la documentation au sens large (bibliométrie, infométrie, archivage), les spécialistes de la recherche technique et de l'interrogation des bases de données, qui opéreront en premier lieu sur internet (on peut déjà parler de webint), les spécialistes des télécommunications et des systèmes d'information, les spécialistes de la sécurité informatique, les spécialistes des sources humaines, les analystes et exploitants dans tous les domaines, les animateurs de la fonction intelligence. »
La collecte des informations n'est qu'une première étape, condition nécessaire mais non suffisante si elle n'est complétée par l'analyse et l'évaluation. L'analyse tient compte de la valeur de la source, des circonstances du recueil et du contexte général. Pour reproduire des évaluations, les différents services et états-majors doivent disposer d'experts, de bons connaisseurs des sujets traités, pouvant estimer, à leur juste valeur, la pertinence d'une question ou la crédibilité d'une information. Le professionnalisme réside à cet égard dans l'accumulation des connaissances de base, dans la mémoire à long terme. Ainsi, les banques de données actuelles deviendront progressivement des banques de connaissances, mettant à la disposition de chacun des archives d'une incroyable richesse. Le renseignement de nature opérationnelle, qu'il soit d'un niveau stratégique, opérationnel ou tactique, doit être exploité en temps réel par les responsables de l'action. Des spécialistes doivent donc être formés pour améliorer considérablement les capacités d'analyse, de comparaison et d'appréciation des informations en provenance de toutes sortes de sources de renseignement.
Paradoxalement, cette ère de l'information pour tous met donc l'accent sur le besoin en spécialistes de haut niveau qu'il faudra savoir motiver et conserver. Il s'agit, là encore, de former ses personnels d'une manière optimale, en cherchant à dominer les nations concurrentes dans leurs actions de formation.

C'est donc l'ensemble des décisions et des mesures humaines et matérielles, destinées à s'assurer la suprématie et l'avantage sur l'ennemi dans le domaine de l'information qui va constituer la stratégie de l'information.
Cette dernière se prépare bien avant la bataille.

CONCLUSION :

Ainsi, la « *RMA* » aux Etats-Unis, mais, plus généralement, les formidables progrès technologiques dans le domaine des télécommunications et des systèmes d'information, ont contribué à propager l'idée que l'information, démultiplicateur de puissance, serait la clé de la victoire sur les champs de bataille du début du siècle prochain.

Dès aujourd'hui, grâce aux énormes moyens financiers, techniques et humains engloutis dans ce qui peut apparaître à certains comme une nouvelle « IDS », prospective ou spéculation, la guerre de l'information est sur le point de forcer le destin et devenir réalité,
L'information, qui n'est encore perçue par les états-majors européens que comme une aide à la décision, s'impose pourtant sous nos yeux comme une véritable arme.
Nous ne sommes sans doute qu'au début de l'ère informationnelle et il est encore temps de réfléchir aux emplois possibles de cette nouvelle arme et d'en théoriser l'utilisation, afin qu'elle s'affirme comme une véritable stratégie.

Certains, enthousiastes, ont pu affirmer que la guerre était morte et que l'information s'affirmerait comme une arme de « non-guerre », en permettant aux états-majors de gagner les conflits avant un affrontement classique.
C'est sans doute aller un peu vite en besogne, car la guerre demeure par nature un subtile dosage d'objectifs politiques complexes, d'émotions humaines, de facteurs culturels et ethniques et de domination des techniques militaires. Les innovations technologiques, même si elles affectent profondément la nature et la manière de mener ces guerres, ne demeurent jamais que des outils.
De plus, la guerre de l'information, jusqu'à maintenant, demeure l'apanage des sociétés hautement développées disposant d'un très fort potentiel humain, technologique et financier. Ces pays ne sont pas à l'abri d'actions plus rustiques, comme le terrorisme. La guerre de l'information semble être très vulnérable dans ce dernier cas, et même receler de grandes fragilités, face à des menaces plus traditionnelles.