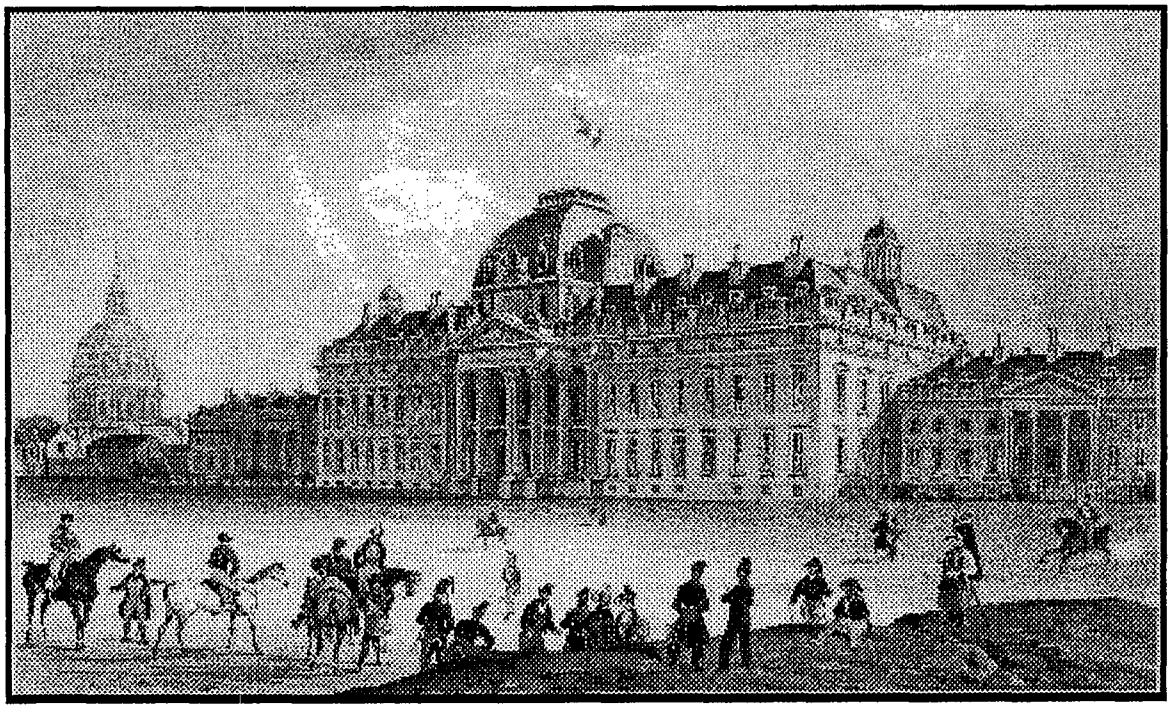
Collège Interarmées de Défense

CID



SESSION 1997 - 1998
MEMOIRE DE STRATEGIE

"UNE STRATEGIE DE L'INFORMATION EST-ELLE CONCEVABLE ? "

« N'ignorer rien de ce qui se passe chez eux.
Ne soyez surpris de rien »

Sun Zi.

SOMMAIRE

Introduction.

« Etre au coeur d'une mutation profonde n'en facilite pas la compréhension ni l'analyse. L'entrée dans la société de l'information, qui vient à la suite de la société industrielle et en bouleverse les données, constitue une révolution culturelle, économique et sociale sans précédent car elle touche simultanément toutes les parties du monde et toutes les activités. »

Ainsi débute le rapport d'information au Sénat de la mission commune d'information sur l'entrée dans la société de l'information, présidé par M. Pierre LAFFITTE, faisant vraisemblablement référence au concept énoncé par Alvin Tofler dans ses ouvrages *The Third Wave*[1] et *War and Antiwar*[2].

De fait, si l'information occupe depuis longtemps une place centrale dans les sociétés occidentales marquées par une recherche de productivité et de rationalisation qui suppose la détention et la bonne utilisation de l'information, l'accélération récente de l'innovation technologique et sa mondialisation donne un nouvel éclairage à cette donnée.

A ce constat, s'ajoute celui du changement de la « donne stratégique » auquel nous assistons depuis la fin du monde bipolaire et qui nous a fait passer d'une menace directe, monolithique et clairement identifiée, à un ensemble de menaces diffuses et multiformes.

Ces deux évolutions majeures constituent les facteurs incontournables qui nous imposent, pour le moins, un renouveau dans notre réflexion stratégique. Le *Livre blanc* de 1994 a apporté une première réponse à cette réflexion, mais il n'a traité que du deuxième constat, et plus particulièrement des menaces, sans considérer l'ampleur de l'évolution stratégique induite par la place prise par l'information.

1 The Third Wave, Alvin Tofler, 1980.
2 War and Antiwar, Alvin Tofler, 1990.

Lancé par les Etats-Unis dés le début des années 90, le concept de l'« *Information Warfare* » a donné lieu outre-Atlantique à une importante littérature et se trouve actuellement en Europe au centre d'un grand nombre de réflexions. Aussi, si il n'est plus utile de démontrer la pertinence d'un tel sujet, il demeure néanmoins essentiel de valider désormais la proposition selon laquelle la guerre de l'information ne constitue pas seulement un nouveau mode d'action mais un véritable concept traduisant une stratégie globale.

Afin d'étayer cette thèse, ce mémoire redéfinit tout d'abord le concept général de la guerre de l'information, puis il examine le concept américain plus élaboré de la *Strategic Information warfare*[3] (SIW) pour enfin établir les fondements de cette nouvelle stratégie.

[3] la guerre de l'information stratégique.

I. La guerre de l'information : un nouveau concept.

« Nous vivons dans un âge qui est conduit par l'information. Les percées technologiques (...) sont en train de changer le visage de la guerre et la manière de la préparer. »

William Perry[4].

La guerre de l'information est en France, comme dans beaucoup d'autres pays, un sujet de réflexion et une préoccupation de très grande actualité, et ce, non seulement pour les Armées mais aussi pour tous les organismes qui s'intéressent de près ou de loin à la Défense.

Toutefois, la guerre de l'information est souvent mal connue et le concept mal défini. Si les Armées conçoivent bien l'importance que revêt l'information dans les crises ou les conflits présents ou à venir, et que nombre de bureaux des états-majors s'occupent d'information, celle-ci n'est malheureusement que très peu perçue dans sa globalité. Il n'en demeure pas moins vrai que les ressources humaines et financières mises en place par un petit nombre de pays dans ce domaine permettent d'affirmer que sinon la guerre de l'information, au moins son concept est devenu une réalité.

Il convient donc, tout d'abord, d'établir une approche de définition de la guerre de l'information, puis d'en élaborer la typologie, pour enfin, chercher à en dégager les évolutions récentes.

A. Une approche de définition.

Synthétisant à la fois un concept américain et une grille de lecture utilisée en interne au ministère de la Défense, la guerre de l'information peut être définie comme une action ou une somme d'actions, offensives et défensives, visant à acquérir et conserver la supériorité informationnelle dans le cadre de la stratégie militaire ; ces actions s'exerçant pour l'information, contre l'information et par l'information. Laissons pour l'instant le concept de la supériorité informationnelle qui sera étudié plus en détail dans la partie consacrée à la stratégie de l'information américaine, et penchons-nous sur les trois formes que revêt la guerre de l'information.

B. Typologie de la guerre de l'information.

Comme le rappelle H. Coutau-Bégarie, « disposer de l'information, en priver l'autre par la maîtrise de l'espace électromagnétique circumterrestre devient déterminante »[5]. Le premier type de la guerre de l'information, la guerre pour l'information, est essentiellement celle du renseignement. Il s'agit là non seulement de capter le plus grand nombre possible d'informations sur l'ennemi, son environnement géopolitique, économique et militaire, - et si possible un plus grand nombre que lui - mais aussi et surtout de pouvoir exploiter ces informations, c'est-

[4] *Secretary of Defense.*

5 Hervé Coutau-Bégarie, *Introduction à la stratégie, la guerre du Koweït*, CID, 1997-1998, p.116.

à-dire d'avoir la capacité de les traiter dans le temps et l'espace où ces informations sont encore pertinentes. En effet, comme il est dorénavant communément admis, « trop d'informations tue l'information », et se doter d'une réelle capacité de traitement de l'information est désormais indispensable à la mise en place d'un outil de défense cohérent. Confronté à cette nécessité d'accroître le volume d'informations disponible, il est également indispensable de neutraliser le système des capteurs adverses et de réduire la « signature » de son propre dispositif. Cet aspect est la cause de l'intérêt croissant que montrent les puissances pour la furtivité de leurs équipements.

Le deuxième type de guerre de l'information est la guerre contre l'information. C'est à la fois le domaine de la guerre électronique et celui des actions plus classiques sur les centres de commandement. Ce type de guerre de l'information ne se limite pas à interdire à l'ennemi tout accès à l'information, mais également à se prémunir contre les attaques ennemies sur notre système informationnel. Ces attaques ressemblent en premier lieu à celles que l'on connaît en matière de guerre électronique (intrusion, brouillage, déception et neutralisation), et de tactique générale (frapper à la tête de l'adversaire). Elles sont complétées, en deuxième lieu, par des techniques plus modernes issues du monde des pirates informatiques, ou *hackers*, et qui permettent des attaques beaucoup plus fines.

Le troisième type de guerre de l'information est la guerre par l'information. Elle englobe, d'une part, la bataille médiatique, et d'autre part, l'action psychologique. Ce type de guerre est très difficile à mener car il est paradoxal : le succès d'une campagne médiatique repose sur la transparence, la véracité des informations et l'habituelle crédibilité de l'organisme responsable de la communication, alors que la réussite d'une action psychologique s'appuie sur la technique de manipulation de l'information, voire sur la désinformation, c'est-à-dire sur l'art du mensonge. Ces deux domaines de la guerre par l'information requièrent des hommes imaginatifs et réactifs, rompus également à la psychologie et aux techniques de l'information mais dont les buts et les moyens sont très différents. Enfin, tous ces acteurs ont des caractères et des motivations sensiblement différents puisque les uns travaillent à la lumière des médias alors que les autres oeuvrent le plus souvent dans l'ombre de l'anonymat.

C. Les évolutions récentes.

A première vue, la guerre de l'information ne semble pas très novatrice. Chercher à détruire les centres de commandement de l'adversaire, tromper sa perception des éléments déterminants du champ de bataille, gêner son système d'information, mener des actions psychologiques..., tout cela avait déjà été établi par les stratèges les plus anciens.

L'un des aspects les plus nouveaux est l'accroissement du volume disponible des éléments nécessaires à la prise de décision. La puissance des technologies employées permet d'intégrer un grand nombre de données jusqu'alors ignorées par manque de temps ou par manque de moyens d'acquisition et de traitement. La conquête de la vitesse et son accélération ont atténué désormais la notion de distance et de durée. *A contrario*, en l'absence d'information ou plutôt d'information convenablement traitée, le décideur n'a qu'une alternative : « parier » - c'est-à-dire agir sans avoir les éléments nécessaires à la prise de décision - ou ne rien faire. Dans les deux cas, on voit le danger d'une telle situation.

Un autre aspect novateur est la possibilité de modifier non seulement l'information reçue par l'adversaire, ce que l'on pratique depuis longtemps par des opérations de déception ou des actes de guerre électronique, mais aussi de pouvoir manipuler le système d'information de l'adversaire, c'est-à-dire le contenu et le contenant (*software* et *hardware*) et ce, sans qu'il s'en aperçoive.

Enfin, l'aspect le plus révolutionnaire est la conception d'une stratégie qu'autorise désormais la guerre de l'information. En effet, dans ce cadre, l'information n'est pas uniquement une arme militaire. Elle est un élément fondamental non seulement pour la connaissance des forces armées de l'ennemi, au sens large, mais aussi pour la connaissance et la maîtrise de l'adversaire dans sa globalité, c'est-à-dire sur le plan économique, politique, culturel et militaire. Réussir à lier ces différents domaines, à les ordonner et à en tirer les meilleurs principes permet, sous réserve que l'on s'applique simultanément le même processus, de concevoir une véritable stratégie. Mais nous reviendrons sur ce sujet par la suite.

Donnée désormais fondamentale et déterminante pour toute activité humaine, l'information et sa maîtrise sont devenues incontournables pour qui veut être puissant. Cependant, l'étendue de son champ d'application et son caractère transverse en font une réalité d'une complexité infinie et par conséquent d'un contrôle difficile. Cette réalité réclame donc une réflexion globale très poussée et la mise en oeuvre de technologies émergentes. Le concept de la guerre de l'information existe donc, mais actuellement, selon les meilleurs spécialistes du sujet, une vingtaine de pays seulement sont en mesure de mener des recherches dans ce domaine, et parmi eux, seuls les Etats-Unis semblent être parvenus à un niveau expérimental.

II. Le concept de la stratégie de l'information aux Etats-Unis.

« A cause de son impact potentiel, la guerre de l'information, doit devenir un instrument important de la politique nationale... Cela appelle un grand débat public. »
Vice Amiral Arthur Cebrowski[6].

Les Etats-Unis sont entrés de plain pied dans une ère caractérisée par une croissance accélérée du rôle de l'information, par la multiplication des sources et des moyens de propagation de l'information. Ils appellent cette nouvelle ère, l'âge de l'information[7]. Il y a cependant un décalage entre les réalisations et les concepts. Si le projet *Force XXI*[8] a été initié pour reconfigurer les forces de l'Armée de terre afin qu'elles soient aptes à affronter la guerre à l'âge de l'information, au niveau conceptuel, ce stade est désormais dépassé. Il semble même que le concept de la guerre de l'information lui-même ait été dépassé, pour aboutir à celui de la stratégie de l'information, sans que ces termes soient explicitement employés. « *On est passé des notions d'arms control, de guerre électronique, de renseignement et d'opérations psychologiques, de C4I, qui étaient des matrices de l'Information age Warfare, à*

[6] Vice Amiral Arthur Cebrowski, Directeur du *Command, Control and Communication* au Pentagone.
[7] *Information age warfare.*
[8] Nouvelle doctrine d'emploi de l'armée de terre américaine en cours de définition et prenant en compte les plus récentes technologies en matière d'information.

quelque chose de beaucoup plus vaste, puisque sont ajoutées des opérations contre les attaques logicielles imprévues, la guerre pour le contrôle de l'information économique, ou encore la guerre dans l'espace virtuel du combat. »[9] Ce concept, qui a reçu le nom d'*Information Dominance*[10], affirme qu'il est possible de maîtriser son environnement en maîtrisant l'information. Car connaître les faits et gestes d'un adversaire permet d'anticiper ses mouvements. Pour les américains, ce concept peut s'appliquer à tous les domaines : politique, économique, social, militaire, etc., et devenir ainsi la *Strategic Information Warfare*. Pour les militaires américains, l'information est désormais considérée comme la cinquième dimension de l'espace du champ de bataille aux côtés des dimensions terre, air, mer et espace.

Avant d'étudier plus profondément le concept de la *Strategic Information Warfare*, il est nécessaire d'analyser ce que recouvre la notion de guerre de l'information pour les stratégistes américains.

A. L'information comme système d'armes.

L'étude de la doctrine américaine de la guerre de l'information se fondera sur le livre « *What's Information Warfare ?* »[11] du Dr. Martin C. Libicki qui est l'un des principaux chercheurs de l'*Institute for National Strategic Studies* à la *National Defense University* et qui fait donc référence en la matière.

Pour Martin C. Libicki, il n'y a pas une guerre de l'information qui serait un instrument unique pour faire la guerre, mais sept types distincts de guerres :

- une guerre concernant le commandement et le contrôle (*Command & Control Warfare, C2W*), c'est-à-dire les centres de commandement et leurs liaisons horizontales et verticales. Sur le plan défensif, il s'agit, d'une part de ne pas se faire repérer et donc d'être furtif, et d'autre part de mettre en place des moyens suffisamment redondants pour que la neutralisation d'un maillon du réseau n'empêche pas la totalité du système de fonctionner. Dans ce domaine, c'est l'organisation plus que les méthodes de travail qui doit être changée. Sur le plan offensif, ce concept comprend la destruction physique des moyens de commandement ennemi ;
- une guerre s'appuyant sur le renseignement (*Intelligence-Based Warfare*) qui consiste à connaître, duper, perturber, neutraliser ou détruire les capteurs du système d'information ennemi par la mise en place de ses propres capteurs sur toute la profondeur du champ de bataille. Sur le plan offensif, le problème est, d'une part de pouvoir faire face à la multiplicité des capteurs ennemis, et d'autre part d'avoir la capacité de traiter la masse des informations recueillies. En mode défensif, la solution adaptée est le leurrage, c'est-à-dire par l'émission d'une image électronique, faire prendre pour vrai ce qui est faux et pour réel ce qui est virtuel ;
- une guerre électronique (*Electronic Warfare*) qui intéresse les moyens communications et les radars. Dans ce domaine, les menaces et les

[9] *La Revolution in Military Affairs, état des lieux*, Réunion du CIRPES, 8 décembre 1995, p.14.
[10] Domination par l'information.
[11] *What's Information Warfare ?* Martin C. Libicki, Center for Advanced concepts and Technology, Institute for National Strategic Studies, National Defense University, août 1995.

protections sont du même type que dans la guerre s'appuyant sur le renseignement ;

- des opérations psychologiques (*Psychological Warfare*) dans lesquelles l'information est utilisée pour décourager, pacifier ou perturber les forces adverses c'est-à-dire les volontés nationales, les commandants et leurs troupes. Dans ce domaine, les modes d'action restent encore très largement prospectifs ;
- une guerre de piratage (*Hacker War*) dans laquelle les processeurs et autres procédés automatisés du système sont dégradés, modifiés ou espionnés par le biais d'un accès illicite aux ordinateurs permettant d'utiliser les caractéristiques propres du système pour qu'il s'attaque lui-même. Ce domaine est certainement le plus fermé car il englobe des actes illégaux et illégitimes comme des attaques même en temps de paix contre les réseaux de tout type (bancaires, électriques, données administratives...). Cependant, malgré le faible niveau de connaissance que nous avons de l'état d'avancement des travaux sur ce sujet, ce n'est plus seulement de la fiction. Ainsi que E. Paige l'affirme : « Nous avons une capacité offensive mais nous ne pouvons en parler. »[12] Sur le plan défensif, cette guerre de l'informatique traite des moyens de protection contre la menace, de détection des attaques et des réactions appropriées.
- une guerre cybernétique (*Cyber War*) qui reste pour l'instant au stade expérimental et prospectif et qui, selon les auteurs, ne recouvre pas toujours la même réalité. Ce type de guerre regrouperait, pour certains spécialistes, la guerre par simulation, qui permettra de façon virtuelle d'anticiper sur le dénouement du conflit et montrera sa vanité pour l'ennemi, et selon d'autres spécialistes, la guerre par systèmes informatiques très intégrés interposés (systèmes cybernétiques incluant de la robotique et de l'intelligence artificielle).
- une guerre de l'information économique qui participe du concept très actuel de l'intelligence économique. Agissant de l'extérieur, ce type de guerre consiste, soit à bloquer le système d'information ennemi, soit à le contrôler afin de parvenir à le dominer. Il semble évident que ce type de guerre menace davantage les pays ayant atteint un haut niveau technologique informationnel. Cependant, ce sont ces mêmes pays qui sont en mesure de se protéger le plus efficacement. Dans ce domaine, les Etats-Unis considèrent détenir deux avantages déterminants : ils sont *leaders* sur le marché des systèmes informatiques et aucun pays ne possède suffisamment d'emprise sur leur système d'information.

Après ce tour d'horizon du champ d'application de la guerre de l'information américaine, quelques remarques peuvent être faites quant à sa comparaison avec le concept français. Les américains ont une vision plus globale du domaine de la guerre de l'information alors que dans le même temps, les différents types de guerre de l'information sont mieux définis. Cela tient sans doute au fait que la recherche dans ce domaine est plus avancée aux Etats-Unis qu'ailleurs et surtout qu'y trouvant son origine, elle y a davantage mûri. Elle y occupe aussi un plus grand nombre d'organismes, sans qu'il y ait pour l'instant, et ce, là comme ailleurs, un organisme qui coordonne l'ensemble des activités du domaine. On notera,

[12] E. Paige, Secrétaire Assistant du Pentagone pour le C4I, Washington Technology, 22 juin 1995.

enfin, qu'en France, la communication est une compétence considérée comme relevant du domaine de la guerre de l'information, ce qui n'est pas le cas outre-Atlantique où ne figure que la guerre psychologique.

B. La *Strategic Information Warfare.*

La nouvelle donne stratégique se caractérise par la coexistence de plusieurs types de guerres - guerre classique, guerre civile, guérilla, guerre économique, guerre idéologique... - et par conséquent de plusieurs types d'adversaires - armées, rebelles, milices, mafias, sectes... Il en résulte qu'une défense militaire, en plus de ces compétences conventionnelles, doit être en mesure d'agir sur un adversaire plus furtif, immergé dans la société civile et utilisant des technologies non létales mais efficaces.

Constatant le bouleversement provoqué par l'avènement de l'âge de l'information et l'existence de cette nouvelle donne stratégique, les Etats-Unis ont conduit une analyse stratégique qui a abouti aux conclusions suivantes :

- la compétence informatique nécessaire pour s'introduire dans les réseaux est à la portée d'un grand nombre de pays ; une attaque peut donc venir de n'importe où,
- les réseaux ne reconnaissent pas les frontières et s'interconnectent de façon de plus en plus transparente ; n'importe quel pays est donc attaquable (même les Etats-Unis) et il est difficile de savoir d'où vient l'attaque et qui la mène,
- les technologies de l'information sont particulièrement bien adaptées à l'élaboration d'objets virtuels ; donc ce qui semble réel n'est peut-être qu'un leurre,
- ces technologies sont furtives ; il est donc difficile de savoir que l'on est attaqué,

Pour les américains, la guerre de l'information devient conceptuellement stratégique puisque des adversaires potentiels peuvent essayer d'attaquer des objectifs politiques, sociaux, économiques et militaires, en tentant d'endommager le système informationnel du pays. Il leur semble, de plus, vain de vouloir éradiquer toute menace dans ce domaine car l'information est de plus en plus omniprésente et accessible par tous. Il vaut donc mieux considérer cette situation comme une nouvelle contrainte dans l'utilisation des systèmes d'information, et chercher à en minimiser les effets.

A partir de cette constatation, le Pentagone a d'abord établi le principe selon lequel la meilleure protection consiste à dominer l'information sous toutes ses formes, c'est le principe de l'*Information Dominance*. Il a ensuite élaboré successivement les doctrines de la *Military Technoligical Revolution*[13] (MTR en 1991-1993) et de la *Revolution in Military Affairs*[14] (RMA en 1994-1995). Celles-ci définissent dans la théorie ce que devra être une armée adaptée aux conflits du XXI[e] siècle.

[13] la révolution technologique militaire.
[14] la révolution dans les affaires militaires.

Comme on peut l'observer, les Etats-Unis ont pu, à partir des derniers conflits et des plus récentes innovations techniques, définir un nouvel environnement stratégique. Ce travail s'est déroulé sur plus de cinq ans et n'a abouti pour l'instant qu'à l'ébauche d'un concept stratégique. L'objectif à atteindre est maintenant moins flou, mais si les moyens à mettre en place pour y parvenir sont à peu près inventoriés, ils ne sont pas, loin s'en faut, clairement définis. Si les Etats-Unis restent pionniers et leaders dans ce domaine, ils n'ont officiellement pas fait le « vrai saut » stratégique qui consisterait à passer d'une conception où l'information a une valeur stratégique à celle où toute stratégie repose sur l'information.

III. Les fondements d'une stratégie pour le XXIè siècle.

« La guerre doit correspondre entièrement aux intentions politiques et la politique s'adapter aux moyens de guerre disponibles. »

Clausewitz[15]

Pour répondre à la question « une stratégie de l'information est-elle concevable ? », il convient tout d'abord d'adopter une définition de la stratégie.

Selon le Général Poirier, la stratégie est « l'ensemble des opérations mentales et physiques requises pour calculer, préparer et conduire toute action collective finalisée, conçue et développée en milieu conflictuel. » Le Général Beaufre reste assez prés de cette définition en affirmant que la stratégie est « l'art de la dialectique des volontés employant la force pour résoudre leur conflit. » On retiendra pour l'étude, la définition donnée en synthèse de ces deux approches par Hervé Coutau-Bégarie dans son *Introduction à la stratégie* : « l'art de la dialectique des volontés en milieu conflictuel », c'est-à-dire pouvoir imposer sa volonté à autrui par la guerre.

A. Pour un concept stratégique élargi.

Utiliser l'information comme instrument pour « calculer, préparer et conduire toute action collective » afin d'imposer sa volonté est tout à fait pertinent et ne demande pas de développement particulier. En revanche, il y a loin de l'emploi de l'information à l'usage de la force. On pourrait donc affirmer, à la lumière de ces définitions, que l'information étant incompatible avec la force brutale, il n'y a pas de stratégie de l'information possible. De la même manière, il n'y aurait pas de stratégie économique possible puisque imposer sa volonté économique ne requiert pas l'usage des armes.

La raison de cette inéquation en est peut-être la définition restrictive que l'on donne au syntagme « milieu conflictuel ». En effet, désormais, la guerre de l'information, malgré son nom, dépasse largement le cadre étroit de l'usage de « la force pour résoudre un conflit. »

Restreindre la notion de conflit à celle de l'usage de la force armée, c'est penser en stratège de la guerre froide, c'est-à-dire ignorer les stratégies indirectes. Si les Etats se doivent de réfléchir à la manière de conserver leur puissance, voire pour

[15] Clausewitz, *De la guerre.*

certains de l'instaurer ou de la rétablir, et ce, aux dépends d'autres Etats, désormais, le recours à la force armée n'est plus le seul moyen d'y parvenir. Depuis que les organismes internationaux interdisent la guerre, les Etats ont dû avoir recours à d'autres moyens que celui de la lutte armée pour maintenir leur puissance et le meilleur moyen qu'ils aient trouvé est l'influence, qu'elle soit économique, politique ou culturelle. Si l'instrument privilégié de cette influence a souvent été l'argent, c'est maintenant l'information qui joue ce rôle de facteur de puissance, car maîtriser l'information, c'est connaître ses concurrents actuels et ses adversaires potentiels tout en pouvant leur imposer une image améliorée de soi-même.

Dans cette perspective, la notion de stratégie de l'information rejoint celle de Rémy Martinot-Leroy : « La stratégie de l'information [est] l'art de la modification des pans de perception de l'environnement de l'adversaire au moyen de messages visant, in fine, à affaiblir sa volonté et partant, son comportement stratégique puis politique. »[16] Ainsi, nous vivons dans un monde conflictuel, dans lequel l'information est une arme d'influence qui ne tue pas mais qui permet d'imposer sa volonté.

B. Stratégie générique ou haute stratégie ?

Selon les stratégistes, on distingue principalement trois types de stratégies : la petite stratégie, la stratégie générique et la haute stratégie. La petite stratégie s'apparente davantage à de la tactique opérative qu'à de la véritable stratégie ; elle ne sera donc pas étudié dans ce mémoire. En revanche, il s'agit de déterminer si une stratégie de l'information participe de l'une ou l'autre, voire des deux autres catégories.

La stratégie générique est une stratégie dans laquelle l'outil stratégique est prédominant. La stratégie nucléaire, par exemple, consiste à imposer sa volonté de défense par la possibilité d'utiliser l'arme atomique, les autres outils que peuvent être les forces conventionnelles n'étant constitués que pour fournir un appoint tactique. Dans ce cadre, il semble qu'il est concevable de faire de l'information un des outils primordiaux pour imposer sa volonté. C'est le principe même de *l'Information Dominance* américain. Maîtriser, ou du moins dominer la sphère informationnelle mondiale, peut être le but principal et suffisant d'une puissance pour vaincre la volonté d'une autre puissance. De ce point de vue, il existe donc une stratégie générique de l'information.

Pour sa part, la haute stratégie est celle qui engerbe toutes les autres stratégies. Avec la fin du monde bipolaire, nous sommes passés d'une stratégie directe (l'ennemi était désigné), réelle (les plans et les armes existaient) et de non-action (on ne souhaitait pas avoir à agir) à la nécessité de rétablir, en complément à cette première stratégie, une stratégie indirecte (d'influence), virtuelle (les électrons sont furtifs et éphémères) et d'action (elle est permanente). « Tout miser » sur l'information pour imposer sa volonté dans un cadre stratégique élargi autorise ces deux stratégies. Elle intègre même toutes les stratégies, celle de dissuasion, d'action et d'influence. Alors que la stratégie de dissuasion ne connaît que la défensive, la stratégie de l'information permet l'offensive (stratégie d'influence et d'action) et, *a fortiori* la défensive (stratégie de dissuasion), comme on a pu le voir

[16] Rémy Martinot-Leroy, *Thèse de DEA : une stratégie de l'information est-elle concevable ?*, p.47.

dans le développement concernant le concept américain de la guerre de l'information. La stratégie de l'information peut donc être, à terme, également une haute stratégie.

Poursuivant le raisonnement à l'extrême, la stratégie de l'information serait même la stratégie suprême puisque comme l'écrit Sun Zi « remporter cent victoires en cent combats n'est pas ce qu'il y a de mieux ; soumettre, l'ennemi sans combattre est ce qu'il y a de mieux. »[17]

C. Les principes de la guerre au service de la stratégie de l'information.

Les principes de la guerre, tels que les ont énoncés Clausewitz et Foch, et quels que soient les termes employés par d'autres auteurs, semblent maintenant faire partie des invariants du vocabulaire stratégique. Ainsi, il est possible de prétendre que si la stratégie de l'information respecte ces principes, celle-ci est concevable. D'ailleurs, plus elle amplifie ces principes, plus elle devient préférable à d'autres stratégies. Or, on constate que dans le cadre de la stratégie de l'information, les principes de la guerre sont, non seulement d'une étonnante modernité, mais aussi qu'ils s'adaptent exactement au contexte élargi de la stratégie de l'information et sont de la plus grande pertinence pour aider à la décision et à la conduite de l'action.

Le premier principe, celui de la liberté d'action, est indissociable de la stratégie, car sans liberté d'action, il n'y a pas de « dialectique des volontés » possible. L'information donne un surcroît de liberté d'action en apportant la meilleure connaissance possible du champ stratégique et en perturbant celle de l'adversaire. La stratégie de dissuasion ne confère, ni aux stratèges, ni aux politiques, une liberté d'action suffisante, puisqu'elle les enferment dans un processus logique n'offrant pas de véritable alternative.

Le deuxième principe, l'économie des forces et son corollaire, la concentration des moyens, retrouve toute sa signification dans une stratégie de l'information. En effet, celle-ci peut, tout d'abord, être une stratégie du faible au fort. Former des hommes aux techniques de l'information (informatique, communication...) et acquérir un début de système informationnel est moins coûteux et plus rapidement efficace que de se forger une armée puissante, *a fortiori*, si l'on veut que cette armée dispose d'un arsenal nucléaire. Elle peut aussi permettre, ensuite, une bascule des forces et donc une concentration des efforts plus facilement, plus rapidement et plus furtivement qu'une stratégie classique.

Enfin, le troisième principe de la guerre, celui de la sûreté des voies de communication est parfaitement revalorisé dans une stratégie de l'information puisque, comme nous l'avons vu précédemment, l'une des catégories de la guerre de l'information est l'établissement et la protection d'un système d'information.

Partant des principes de la guerre, la stratégie de l'information apparaît comme une stratégie non seulement concevable, mais supérieure. Cependant, la considérer comme une stratégie réalisable à court terme serait précipiter les choses. D'une part, il y a encore loin du concept à l'objet, et d'autre part, tous les

[17] Sun Zi, *L'art de la guerre*, Economica, Paris, 1995, p.105.

pays n'étant pas rentrés dans l'âge de l'information, les guerres conventionnelles, et avec elles les stratégies classiques d'action, ne sont pas mortes.

Pour aller plus avant dans la réflexion stratégique, il faut maintenant développer le niveau stratégique que réclame l'information considérée comme matière première primordiale. Ce niveau stratégique ne peut se développer de façon pertinente que si l'on admet dorénavant que la notion de conflit ne s'applique plus uniquement aux oppositions directes armées, mais plus globalement à tous les affrontements ou concurrences ayant pour objectif la destruction ou la neutralisation d'un adversaire. Le concept de la stratégie de l'information est concevable, à quelque niveau stratégique où l'on se situe ; aux stratèges de lui donner davantage de corps.

Conclusion.

« C'est dans le domaine de la guerre de l'information au sens large, imposant une grande maîtrise du temps et de l'espace, que ce conflit [la guerre du Golfe] entre pleinement dans la catégorie des guerres du XXIè siècle. »[18] Il semble en effet que la guerre du golfe a marqué l'émergence du concept de la guerre de l'information et de son développement. Sept ans plus tard, le concept a beaucoup évolué, engerbant, pour les puissances qui s'y intéressent, la plupart des domaines d'action qui ont à traiter de l'information.

La France comme beaucoup d'autres puissances mène une réflexion dans ce domaine. Des organismes comme la FED[19], l'IHEDN[20] et le CHEAr[21] conduisent des travaux dans ce sens et diffusent régulièrement des rapports et des écrits des meilleurs spécialistes du sujet. Les bureaux d'études et de prospectives des états-majors (EMAT, DRM...) cherchent également à donner un contenu à un concept de la guerre de l'information. Mais il n'existe pas véritablement d'organe fédérateur de ces réflexions et encore moins d'action concrète. Le gouvernement français, considérant, après une longue interrogation, ce domaine comme de la première importance pour le pays, a mandaté le SGDN[22] pour coordonner les actions ressortant de l'intelligence économique. A l'instar du Sénat, il a récemment pris en compte le défi que représentent la maîtrise de l'information et de ses technologies, mais il n'a pas encore pris conscience de l'importance stratégique de cette maîtrise pour la défense de notre société, de notre culture et de nos intérêts. Car l'information agit désormais dans tous les domaines d'intérêt d'une nation. A ce titre, la guerre de l'information doit donc faire partie de la stratégie globale de notre pays. Cela suppose deux postulats. Il faut, d'abord, redonner à la réflexion stratégique sa vraie place et la confier principalement aux

[18] Hervé Coutau-Bégarie, *Introduction à la stratégie, la guerre du Koweït*, CID, 1997-1998, p.56.
[19] Fondation pour les Etudes Stratégiques.
[20] Institut des Hautes Etudes de Défense.
[21] Centre des Hautes Etudes de l'Armement.
[22] Secrétariat Général de la Défense Nationale.

militaires qui s'en sont vu écartés en raison d'une stratégie de dissuasion naturellement subordonnée aux politiques. Car, de même qu'il est du ressort du politique de définir les buts politiques, il est du ressort des militaires de proposer aux responsables politiques les stratégies disponibles pour mener à bien cette politique. Ensuite, il faut renforcer la réflexion des Armées sur ce concept et, tout en restant attentif à l'évolution des technologies de l'information, mettre en oeuvre sans attendre des organismes orientés non seulement vers la réflexion mais aussi vers l'action.