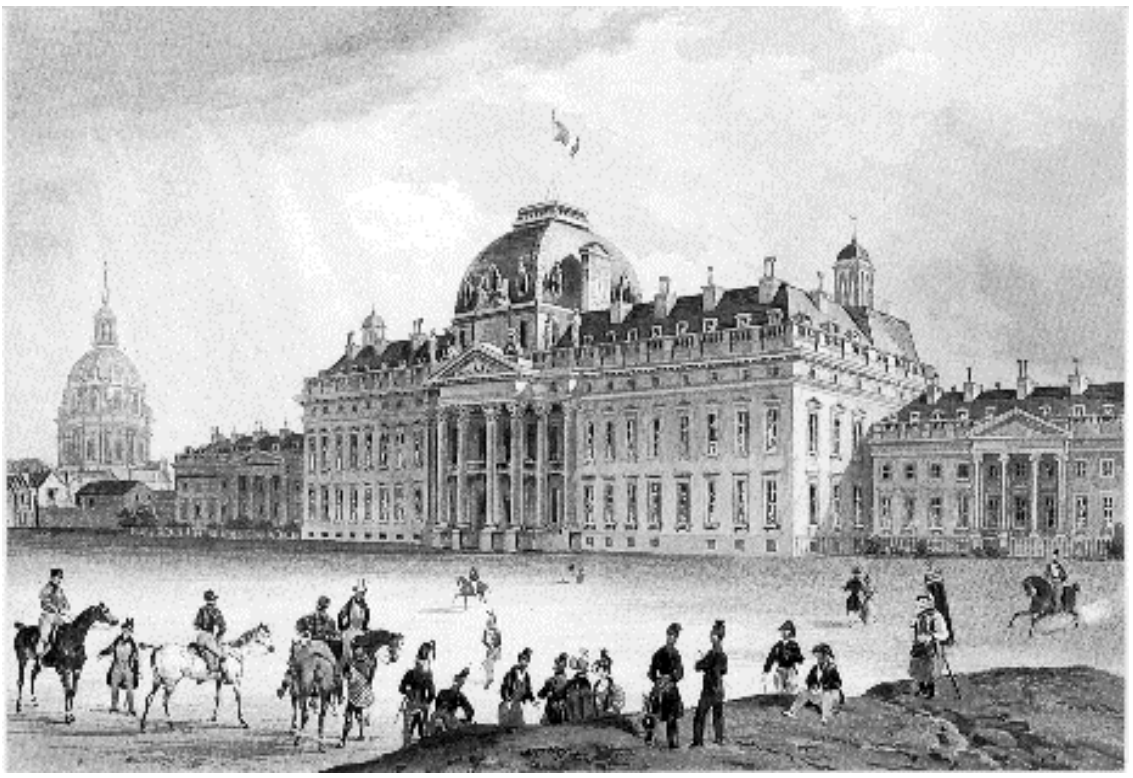
Collège Interarmées de défense
7ième promotion 1999-2000

Prédominance de l'information,

Complexité et Stratégie



Lieutenant-colonel C. LAVROFF (groupe D3)

FICHE DE PRESENTATION

1. Mémoire de stratégie

2. LCL (Air) Catherine (MAZET ép.) LAVROFF

3. 13 mars 2000

4. Groupe D3

5. Prédominance de l'information, complexité et stratégie

6. La prédominance de l'information et l'accroissement de la complexité caractérisent les futurs théâtres d'opération. La maîtrise des nouvelles menaces passe par l'adaptation des systèmes d'information.

7. Mots clefs : Révolution dans les affaires militaires , Guerre de l'information , Non linéarité , Imprédictibilité , Dominance par l'information, Prise de décision , Cadres de référence

Prédominance de l'information,

Complexité et Stratégie

Sommaire

1. Introduction

Les évolutions rapides de la technologie ont un impact si important sur les systèmes d'armes présents et futurs qu'il est nécessaire de bien analyser et percevoir les nouvelles approches que cela va induire sur la stratégie militaire. Pour cela on doit remonter quelques décennies en arrière pour saisir la manière dont ces changements ont été pris en compte jusque là au travers du concept de " Revolution in Military Affairs ". Cela conduit naturellement à identifier les caractéristiques essentielles de l'environnement des futurs théâtres d'opérations. A l'évidence il y a deux éléments majeurs à analyser de façon systématique : la prédominance de l'information et l'accroissement considérable de la complexité. La première est approchée en considérant toutes les formes identifiables de la guerre de l'information. Quant à la complexité, après avoir précisé ses principales caractéristiques, on peut montrer, en s'appuyant sur la pensée de Clausewitz, qu'il est justifié et pertinent de lui donner toute sa place dans la pensée stratégique militaire. Après une description de ces deux réalités fondamentales, on sera en mesure de s'intéresser à leur impact structurant sur le processus de prise de décision en stratégie.

2. Les révolutions dans les affaires militaires

2.1 Historique

La notion d'un potentiel révolutionnaire apporté par les nouvelles technologies militaires apparaît dans les écrits du soviétique N.V.Ogarkov dans les années 70 à 80. Quand les Américains, familiers avec les révolutions scientifiques, examinent à leur tour cette idée, ils focalisent eux aussi sur l'aspect technologique de la réforme et parlent de **"** Military Technical Revolution ".

Mais les analystes, tels qu'Alvin et Heidi Toffler, Andrew Krepinevich, Jeffrey Cooper, Michael Mazarr, perçoivent rapidement que le concept doit être élargi à une approche plus généraliste de " révolution dans les affaires militaires " (**RMA :** Revolution in Military Affairs), déclenchée par des nouveautés technologiques importantes et concomitantes, aptes à des applications militaires innovantes et à forte valeur ajoutée. L'essence d'une RMA n'est pas l'invention d'une nouvelle technologie, mais bien la découverte de méthodes innovantes pour organiser et optimiser son emploi.

Ce concept a fait flores au lendemain de la Guerre du Golfe où l'efficacité des forces américaines s'est illustrée. Une révolution historique qui combinerait les apports de l'" ère de l'information " avec une doctrine et un entraînement appropriés, semblait pouvoir mettre un point final à la stratégie de la Guerre froide : on pourrait alors donner à l'outil militaire, certes plus ramassé mais très moderne, une efficacité sans précédent dans la défense des intérêts nationaux. Il y a en effet concomitance de l'apparition d'un potentiel et d'une certaine urgence, les forces militaires en constante diminution, pouvant être engagées dans deux conflits régionaux simultanément, pas

forcément sur le même théâtre. Cela explique l'encouragement apporté par des personnalités de haut rang de la Défense, comme l'amiral William A. Owens, à la réflexion novatrice et créatrice.

2.2 La RMA et son contenu

Dans la première phase de la RMA, un consensus s'est fait sur l'identification des besoins suivants :

- Furtivité et armement de précision tiré à distance de sécurité : c'est certainement l'aspect le moins révolutionnaire de cette première phase, puisque des armements mettant en œuvre ces technologies équipent déjà les forces.

- Systèmes de commandement, de contrôle et de renseignement performants : la capacité d'acquérir, d'analyser et de redistribuer l'information tout en la contrôlant et en la synchronisant, permet déjà de mener des opérations plus complexes sur un théâtre. Après maturation, elle devrait permettre de mener des opérations sur plusieurs théâtres en parallèle.

- Moyens de guerre de l'information : les analystes s'accordent pour considérer l'information, non plus seulement comme un moyen de contrôle opérationnel, mais comme un capital de plus en plus stratégique. C'est un changement radical de la pensée, dans le droit fil de l'approche macro-économique des Toffler. Selon eux, la " première vague " du développement humain était essentiellement agricole et a donc conduit à des guerres de conquête de territoire ; la " deuxième vague ", dominée par la production industrielle, a connu des guerres d'usure visant à ruiner les ressources de l'adversaire ; la " troisième vague " cherchera logiquement à éroder ou détruire les moyens adverses de collecte, de traitement, de stockage et de distribution de l'information. En effet, au fur et à mesure que les forces armées deviennent dépendantes de l'information, leur vulnérabilité à la guerre de l'information s'accroît, principalement face à la menace d'un ennemi de niveau comparable. Toutefois on ne peut pas déjà affirmer que la guerre de l'information ait acquis ses lettres de noblesse comme méthode de guerre en elle-même. Elle est encore considérée comme un adjuvant des moyens conventionnels, au mieux comme un démultiplicateur de forces.

- Moyens non léthaux : Ils pourraient s'attaquer à la réduction des pertes humaines et des dégâts collatéraux, bien mieux que la recherche de la précision des frappes. Chris et Janet Morris les appellent des " armes de protection massive ", qu'elles soient électromagnétiques, cinétiques, chimiques, acoustiques, optiques… Elles seraient utilisées pour dissuader et désarmer, en protégeant les non-combattants. Dans un contexte politique où les pertes humaines sont de moins en moins tolérées, l'utilisation d'armes non léthales pourrait offrir une alternative à l'emploi de forces militaires classiques. On peut imaginer qu'une force multinationale d'interposition ou de maintien de la paix aurait là un moyen efficace de désamorcer la crise au plus bas niveau de violence.

2.3 Analyse diachronique du concept de RMA

Quand est-ce qu'une RMA se produit ? Quel est son cycle de vie ?

Même si la RMA en cours a suscité de brillantes analyses, on trouve peu de discours stratégiques tentant de la replacer dans son contexte global, théorique et historique. En effet, si tout le monde admet l'intérêt de poser des questions de portée plus globale, l'approche normale consiste à assurer la continuité de l'environnement de sécurité et de faire rentrer la RMA dans les contingences de la programmation. Le concept et la théorie sont en général sous-estimés au profit de la politique d'action.

Pourtant l'élaboration d'un concept est primordial : œuvre collégiale, impliquant une large communauté d'intellectuels, elle se base sur la formulation d'hypothèses qui sont débattues, testées, confirmées ou rejetées.

On distingue des RMA " mineures " (l'organisation des armées napoléoniennes, par exemple) et des RMA " majeures " incorporant des changements fondamentaux, à la fois dans les domaines social, économique et politique (naissance de l'ère industrielle, par exemple). Une RMA " mineure " peut être contrôlée et canalisée par ceux qui la comprennent ; une RMA " majeure " ne peut pas être contrôlée : les stratèges doivent y répondre et s'y adapter. L'accroissement de l'efficacité au combat, objet de la RMA, est cumulatif : il est intense pendant de brefs épisodes (révolutions) séparés par de plus longues périodes d'évolutions. Mais c'est une notion qui reste intrinsèquement relative et qui doit être appréciée par rapport à l'ennemi, réel ou potentiel. De plus, elle n'implique pas nécessairement une utilisation accrue de la puissance militaire comme instrument stratégique.

Il semble que les RMA apparaissent selon un schéma cyclique : phase initiale de stabilité, suivie d'une initialisation, puis d'une montée en puissance jusqu'à atteindre une masse critique, puis d'une phase de consolidation et de mise au point de réponses et enfin d'un retour à une phase de stabilité.

Une RMA commence quand le potentiel latent dans les changements technologiques, conceptuels, politiques, économiques et sociaux, est reconnu et utilisé pour accroître l'efficacité au combat. Pour franchir ce pas, la motivation peut provenir d'une défaite, d'une perception d'infériorité ou de déclin par rapport aux capacités d'autres acteurs. Ceux qui déclenchent la révolution jouent avec l'incertitude car le résultat n'est jamais connu d'avance. Rappelons-nous la situation d'urgence et d'exclusion diplomatique dans laquelle se trouvaient les Révolutionnaires français en 1794 avant de recourir à la levée en masse qui sauva la Nation. Une chose est de percevoir la nécessité d'une RMA, autre chose est de la mener à bien d'une façon appropriée et équilibrée.

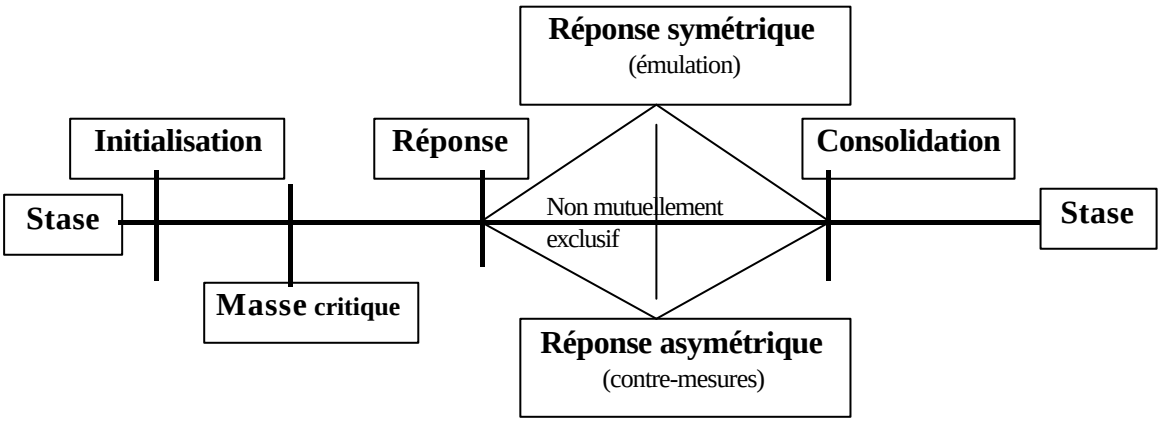
L'initialisation d'une révolution requiert des " révolutionnaires " comme Charles De Gaulle, B.H. Liddell Hart, J.F.C. Fuller… Les RMA sont conduites par les forces armées qui tolèrent les visionnaires, et qui les accréditent au moment approprié.

Mais même dans ce cas, il est bien rare qu'un schéma directeur n'émerge sans de nombreux ratés et atermoiements. Cette phase de mûrissement des nouveaux concepts, organisations et technologies placent les forces armées en état de relative faiblesse, opportunité le plus souvent ignorée ou sous-estimée par ses adversaires.

La période qui précède ou suit immédiatement le point de masse critique est potentiellement conflictuelle, soit parce que les adversaires ont pris conscience du danger et veulent s'y opposer, soit parce que ce nouveau pouvoir cherche à s'exercer à titre de test.

La percée effectuée finit toujours par susciter des réponses de la part des autres états : réponses symétriques, asymétriques ou mixtes. A la suite de leur quasi-défaite par la " Blitzkrieg " allemande en 1941-42, les Soviétiques adoptèrent la même méthode pour finalement battre les maîtres à leur propre jeu. La stratégie de " guerre par le peuple " développée par Mao ou Giap est une illustration de réponse asymétrique à une force supérieure.

A un moment donné, la progression de la RMA se ralentit puis cesse. Soit parce que l'équilibre militaire est atteint et satisfait le pouvoir politique ; soit parce que les coûts ou les risques ne sont pas justifiés par les bénéfices visés. On entre alors dans une phase de stabilité où l'amélioration de l'efficacité dépend alors de l'entraînement des forces.



On constate de nos jours, principalement du fait de la prégnance des moyens de communications, une accélération du cycle des RMA.

2.4 Les options stratégiques des Etats-Unis d'Amérique

Trois options stratégiques se présentent donc pour les Etats-Unis :

- Mettre la RMA en sommeil pour consolider les capacités militaires acquises. On pourrait penser raisonnablement que la poursuite de la RMA peut être dangereuse et que les coûts et risques engendrés dépassent les avantages escomptés.

  ⇒ On risque en effet que l'efficacité acquise ne s'applique pas à l'ennemi futur le plus probable : en effet la RMA actuelle, en portant l'accent sur les frappes à distance de sécurité, sans effet collatéraux, peut-elle répondre à l'ensemble du spectre des menaces, et en particulier aux organisations cellulaires terroristes fondues dans la population ?

  ⇒ Un autre risque inquiétant serait le développement de réponses asymétriques en contre-mesure aux avancées de la RMA, ou par peur de la part de pays actuellement non hostiles : nouvelles armes bactériologiques ou chimiques, ou bien nouvelle arme dont l'émergence annihilerait d'emblée la supériorité militaire acquise.

  ⇒ Sur le plan politique, la poursuite de la RMA présente deux dangers. Placer la capacité militaire comme facteur prédominant de la puissance nationale est tentant en période de ralentissement économique mais l'histoire a montré qu'une telle supériorité n'est jamais pérenne. Enfin, la supériorité acquise menace les alliances, remettant ainsi en cause les liens de confiance et de stabilité.

- Poursuivre la trajectoire entreprise. Cette décision serait profitable pour trois raisons :

  ⇒ un gain appréciable d'efficacité au combat a été acquis par rapport à des adversaires de niveau moyen ;

  ⇒ l'acquisition de capacité de tir de précision à distance de sécurité, en minimisant les dégâts collatéraux, facilite pour le politique l'usage de l'outil militaire qui devient ainsi plus dissuasif ;

  ⇒ enfin, la RMA devrait empêcher les Etats-Unis de perdre leur suprématie militaire ; les développements technologiques ne sont que les aspects les plus simples d'une telle réforme ; la reformulation et l'adaptation des doctrines, des organisations et de l'entraînement est un processus beaucoup plus laborieux, dans lequel certains autres états se sont eux aussi engagés.

- Orienter la révolution dans de nouvelles directions. Dans ce cas la stratégie, et non pas la capacité technologique, doit être le maître-mot. Les dirigeants doivent absolument se poser la question " que voulons-nous que l'armée du futur soit capable de faire ? " plutôt que celle-ci " Qu'est-ce que la technologie émergente va permettre à notre armée du futur ? ". Un moyen d'y parvenir est d'examiner les objectifs stratégiques et les menaces attendues.

⇒ Si l'Etat prône l'engagement et le soutien actif des systèmes politiques et économiques ouverts, alors il faut forger une force de projection avec une réelle capacité à durer sur le terrain. La stratégie militaire combinera alors des frappes à distance avec une occupation du territoire et des actions de reconstruction de la Nation s'appuyant sur des armes non léthales.

⇒ Au contraire, si l'Etat mène une politique de désengagement politique et militaire, la stratégie sera celle de frappes de défense courtes et dissuasives ; la capacité de frappe à distance sera toujours requise, puisque les alliés n'assureront plus de bases arrière, mais il n'y aura plus d'occupation du terrain.

⇒ Enfin, à mi-chemin du spectre, la charge pourrait être partagée avec les alliés, idée séduisante quand le coût d'entretien d'une gamme complète de capacités militaires devient rédhibitoire pour de nombreuses nations.

Quand on réfléchit aux menaces potentielles, il faut là aussi raisonner en terme de spectre.

⇒ A un bout du spectre, on trouve des forces armées, ou coalitions, de niveau militaire comparable. La projection de puissance sera alors préférée à la projection de forces. Des mesures de protection limiteront la prolifération de la connaissance applicable au domaine militaire. Finalement, la ligne de partage entre compétition et hostilités, entre paix et guerre, sera ténue.

⇒ Puis on trouve des agresseurs régionaux aux capacités militaires moins développées, dotés éventuellement d'armes de destruction massive.

⇒ Puis se présentent des menaces " sub-nationales ", milices ethniques ou mouvements terroristes, qui ne sont pas négligeables car " nichées " éventuellement dans certains créneaux technologiques (guerre de l'information, par exemple).

⇒ Enfin au bout du spectre, se trouvent les organisations criminelles de tous types, recourant à la violence, à la subversion économique, au terrorisme écologique etc…Pour s'y opposer, les unités combattantes devront être très petites et flexibles, aptes à répondre à des menaces s'étendant du niveau le plus bas de la technologie au plus élevé. Mais surtout des forces non militaires seront requises en grand nombre, constituées d'experts, de policiers, de scientifiques, dotées d'équipements de protection individuels et rompues à la " psychotechnologie ". On voit qu'à cette extrémité du spectre , les armes tirées à distance de sécurité et la domination de l'espace sont d'un piètre secours.

Toutes ces menaces seront potentiellement à traiter dans l'avenir. Il faut donc les affecter d'un coefficient de priorité qui déterminera sur quel type de technologie militaire porter l'accent, le nombre de systèmes requis, les spécifications pour une opération de longue durée, les relations avec les organisations non militaires de sécurité, etc…

2.5 Poursuivre la RMA

Quels avantages voient les analystes à poursuivre la RMA ?

- C'est d'abord de faire des forces militaires un outil plus facile d'emploi pour les politiques dans un contexte social où les pertes humaines ne sont plus acceptées par l'opinion publique ; nous avons évoqué, par exemple, l'avantage de moyens non léthaux pour désamorcer une crise au plus bas niveau d'intensité.

- C'est aussi un moyen pour les Etats-Unis de repousser l'émergence d'une puissance militaire de niveau comparable. Le coût d'acquisition et de maintien d'un tel niveau de capacité est d'ores et déjà dissuasif pour les pays compétiteurs et doit le rester.

- Le développement de la RMA appelle une deuxième phase, pour le moins :

  ⇒ la recherche de la précision des frappes, basée dans un premier temps sur l'emploi d'armes " intelligentes ", pourrait s'orienter vers la robotique, la domination de l'espace, la non-léthalité, la " psychotechnologie " et la " cyberdéfense ".

  ⇒ la recherche de coordination, basée dans un premier temps sur la communication des systèmes, pourrait s'orienter vers la " nanotechnologie ", dispersion de milliers de petites machines intelligentes, capables, de façon autonome, de collecter du renseignement et de prendre des décisions.

  ⇒ la recherche de l'adéquation de l'organisation, basée dans un premier temps sur la constitution de forces conjointes et de coalitions " ad hoc ", pourrait évoluer vers une organisation hyperflexible, voire l'utilisation d'un essaim de petites armes intelligentes capables de coloniser une cible (concept du " fire ant warfare " de Martin Libicki).

On comprend, à l'éclairage de telles anticipations, que la plupart des analystes estiment que le monde militaire n'en est qu'à l'aube de ses transformations.

2.6 Synthèse et réflexions sur l'intégration de la RMA

Une synthèse sur le sujet de la RMA peut être effectuée en considérant les trois dimensions de la pensée stratégique :

- La dimension verticale est celle du temps : elle s'attache à spéculer sur le futur et à équilibrer les objectifs à court et long terme. Celle-là est bien prise en compte par la RMA en cours.

- La dimension horizontale s'attache à intégrer et synchroniser les différents types de pouvoir en un effort collectif à un instant donné. Peu d'intellectuels ont encore exploré les liens d'une

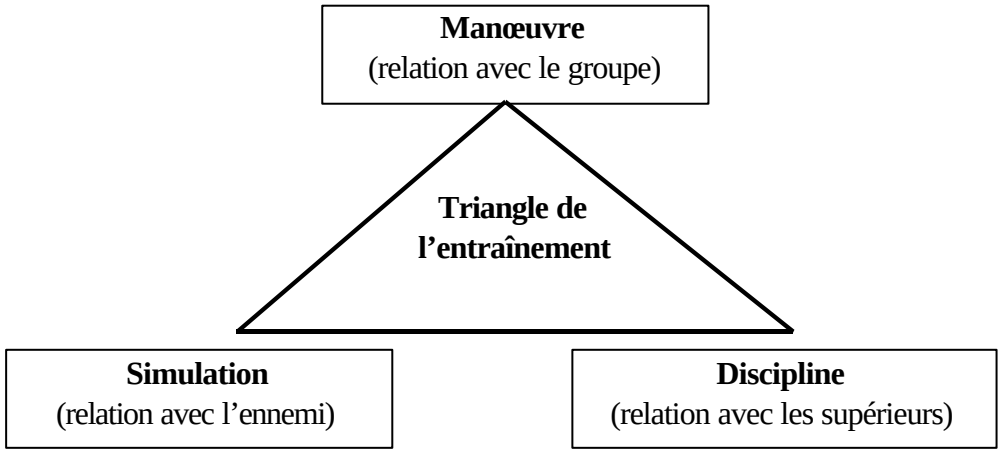
puissance militaire remodelée sous l'effet de la RMA avec les pouvoirs économique, diplomatique et politique.

- La troisième dimension est normative et émet des préférences et des jugements de valeurs sur le monde futur, non pas tel qu'il est accessible, mais plutôt tel qu'il est préféré. Cette réflexion est absente pour le moment. Là réside le véritable enjeu si l'on veut que la RMA conduise à un progrès plutôt qu'à de simples changements.

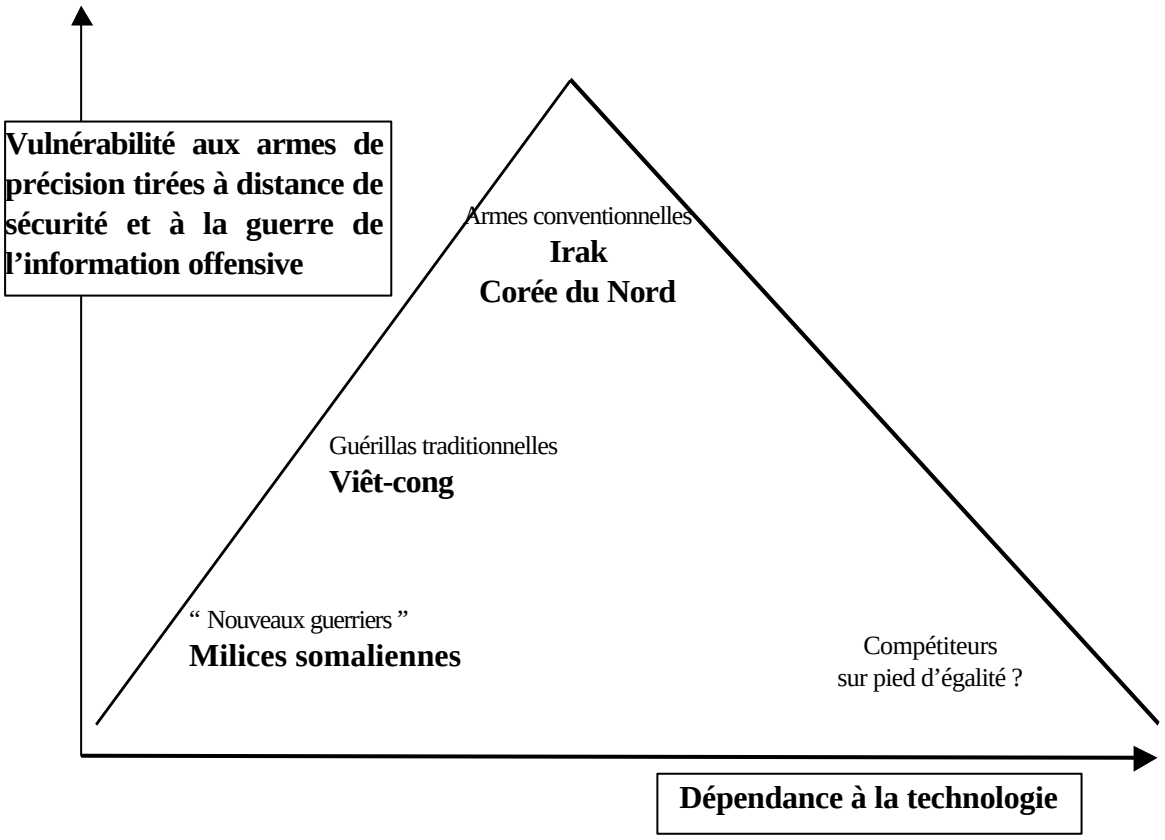
La RMA est donc à la croisée des chemins : pour faire le bon choix stratégique, le ministère de la défense américain (DoD) doit continuer à raffiner la théorie des révolutions militaires, encourager la créativité en son sein, voire l'institutionnaliser. Il doit aussi élargir le débat au public averti et aux dirigeants politiques en le replaçant au niveau des objectifs nationaux.

Dans le domaine des hypothèses à examiner, la crainte que suscite la RMA chez les autres états, ainsi que la coopération entre alliés sont des thèmes de réflexion majeurs.

Il faudra aussi identifier les effets secondaires pour chaque option ; par exemple, dans l'hypothèse d'une manœuvre et d'un entraînement focalisés sur un terminal d'ordinateur, qu'adviendrait-il des valeurs traditionnelles de discipline et de bravoure ? Seraient-elles encore nécessaires ? L'utilisation des techniques psychologiques contre l'ennemi, combattant ou non, outil également applicable à la résolution de problèmes domestiques, pose aussi un certain nombre de questions d'ordre éthique.



Enfin, pour ne pas se laisser déborder par une menace prise à la légère, il faut envisager une réponse pour toute menace du spectre. C'est la leçon tirée de la politique d'endiguement du communisme qui a développé à outrance la puissance nucléaire et le bombardement stratégique au détriment de toute aptitude à la contre-guérilla et à la projection sur des théâtres de crise régionaux.



3. L'âge de l'information

3.1 La problématique

Pour illustrer les difficultés que posent l'étude de cette question on va s'appuyer sur la parabole du télescope empruntée à Martin Van Creveld dans " Command in War ".

On s'intéresse ici au volume de données requis par les Américains pour la gestion de la guerre du Vietnam. A l'initiative de McNamara et Westmoreland, la mode était alors aux statistiques

comme outil d'aide à la décision : l'avalanche quotidienne des messages, ne pût-elle être lue, devait du moins être quantifiée ; comme devaient l'être aussi le nombre d'accrochages et celui des pertes humaines de chaque côté, mais aussi le pourcentage de la population dans les zones " pacifiées ", le nombre de kilomètres de routes et de voies fluviales praticables, le nombre de tonnes de riz achetées sur les marchés urbains, etc… Ces données étaient traitées pour fournir des rapports quotidiens au commandement, tâche dont les ordinateurs s'acquittèrent fort bien. Cependant une grave pathologie de l'information se développa, caractérisée par un retard à la disponibilité de l'information, un renforcement de la centralisation due à l'incompréhension des échelons intermédiaires, des décisions aux effets non maîtrisés, une pression accrue sur le terrain pour fournir encore plus de données, des données de plus en plus douteuses et inadaptées… La seule décision valable que cette approche statistique obtint jamais, fut que les Etats-Unis ne gagneraient pas une guerre d'attrition et que de rajouter des troupes sur le terrain ne servirait à rien.

On s'avisa alors de ce moyen rapide et très flexible qu'est l'hélicoptère pour déplacer le commandement d'un point à un autre et lui donner une vue d'ensemble du champ de bataille. Le chef du bataillon pouvait ainsi observer la compagnie engagée dans un accrochage et demander à son chef de rallier sa fréquence radio. Le chef de la division, ou celui du corps faisait de même…. On découvrit là une sorte de télescope omnidirectionnel tellement puissant qu'il paralysa l'action qu'il était sensé diriger.

Un autre palliatif consista à puiser à la source des médias. Les journalistes partageaient avec le commandement la même méconnaissance du théâtre où ils ne se rendaient que très brièvement, à l'occasion de tel ou tel événement dramatique. Mais libres de toutes statistiques et de toute supervision, ils pouvaient opérer rapidement, préférant le spécifique et le sensationnel au détriment d'une vision globale. Ils constituèrent donc eux aussi un télescope particulièrement directionnel et efficace, mais dont le remarquable pouvoir de focalisation était aussi le principal défaut.

La morale de cette parabole est que les statistiques et la technique constituent des formes abstraites et ambiguës du savoir humain et ne peuvent en aucun cas se substituer à une connaissance approfondie de l'environnement.

Pour appréhender cet environnement on dispose aujourd'hui de tout une panoplie de capteurs.

3.2 La gamme de capteurs

Les avancées technologiques ont enrichi la palette des différents capteurs. Un typologie possible se définit comme suit :

- Les capteurs à grande distance de sécurité, principalement spatiaux, mais aussi sismiques et acoustiques.

- Les capteurs à courte distance de sécurité, tels que les drones dotés de moyens d'observation, multispectrale, à micro-ondes passifs, radars à synthèse d'ouverture, et

d'écoute électronique ; des radars de surface ou des bouées côtières peuvent aussi être équipés de tels moyens.

- Les détecteurs sur le terrain, qu'ils soient acoustiques, gravimétriques, biochimiques ou optiques.

- Les détecteurs de systèmes d'armes, infrarouge, radar ou lidar.

Cette liste illustre l'ampleur de la tâche de ceux qui doivent collationner, recouper et fusionner ces différentes sources de renseignement. Elle suggère aussi la difficulté de ceux qui voudraient leurrer les systèmes de renseignement sur toute l'étendue de leur gamme.

3.3 Qu'est-ce que la " guerre de l'information " ? (Information warfare : IW)

Le concept de " guerre de l'information " prend racine dans le fait indiscutable que l'information et les technologies de l'information concernent de plus en plus la sécurité nationale au sens large et la guerre en particulier. L'information devient une source de pouvoir que l'on peut acheter, vendre ou échanger avec ceux qui reconnaissent sa valeur, voler et protéger.
Il est donc admis que les formes de guerre futures seront caractérisées par la bagarre, sous toutes ses formes, pour le contrôle des systèmes d'information et l'acquisition de la " dominance par l'information " (voir § 3.8).

On peut se poser la question de savoir si l'IW va reléguer les formes plus traditionnelles de la guerre à l'arrière plan ? Alors que le concept d'attaque des systèmes d'information adverses gagne en crédit, on assiste à la mutation des architectures vers des systèmes de plus en plus distribués et redondants. Le bénéfice de l'IW n'est donc pas encore confirmé. Assiste-t-on à l'avènement d'un nouveau médium de conflit né du bourgeonnement de l'infrastructure globale de l'information ? Ou bien n'est-ce simplement qu'une opportunité de pression supplémentaire offerte par le développement des technologies de l'information ?

Définir l'IW est comme, pour un aveugle, de découvrir la nature de l'éléphant : celui qui touche sa patte dira que c'est un arbre ; celui qui touche sa queue dira que c'est une corde ! Les manifestations de l'IW sont ainsi diversement perçues. Peut-être même n'y a-t-il pas d'éléphant mais seulement un arbre et une corde qui aspirent à le devenir ?

3.4 Taxinomie

Dans l'état naissant de cette science, la taxinomie proposée par Martin C. Libicki (Institute for National Strategic Studies) est généralement adoptée :

- **La guerre du commandement (" command-and-control warfare " : C2W)** :

Historiquement, on a toujours chercher à supprimer le chef militaire. **“ Frapper l’ennemi à la tête ”** signifie aujourd’hui s’attaquer aux centres de commandement pour désorganiser durablement les opérations. Malgré le danger évident qu’elle entraîne, la centralisation du commandement est un mal souvent nécessaire pour l’harmonisation des éléments de situation entre les différents acteurs et une bonne distribution des messages. Cependant, la technologie confère à ces points névralgiques une furtivité qui ne cesse de s’accroître : *réplication*[1] des données sur des sites dispersés, masquage des émissions radio-électriques, utilisation de la visioconférence et du *whiteboarding*[2], alimentation électrique photovoltaïque, *centres de backup*[3] permettant une reprise délocalisée, etc…

La fragilité de ces nouvelles architectures distribuées réside maintenant dans les flots de données qu’elles exploitent : ils requièrent des lignes de communication à haut débit et redondantes. De nos jours, il faut donc **“ couper le cou de l’ennemi ”** en le privant de ses liaisons stratégiques. La C2W a le rôle de les repérer et d’occuper le potentiel de l’ennemi à d’incessantes actions de reconfiguration.

- **La guerre du renseignement (“ intelligence-based warfare ” : IBW)** :
  Il s’agit du renseignement glané en cours d’opération, informations de ciblage et évaluation des dommages essentiellement.

  Contrairement aux effets masqués de la C2W, **l’IBW offensive** débouche sur le tir d’une cible. Son intérêt croît avec le nombre des capteurs du champ de batailles, capables d’alimenter les conduites de tir de façon fiable et précise et quasiment en temps réel. De nos jours, le capteur, l’opérateur et l’arme ne sont plus localisés sur la même plate-forme : ils sont reliés par le réseau qui est capable d’assurer la traçabilité et le fusionnement de toutes les informations pertinentes. Ce gain qualitatif du renseignement permet au commandement non seulement de coordonner mais aussi d’assurer la cohérence de la bataille et des plans (“ *situational awareness* ”[4]). Il suggère aussi la réorganisation des réseaux du renseignement et leur ramification vers les échelons subordonnés, voire les systèmes d’armes eux-mêmes. L’avenir de l’IBW offensive est promis à un vaste chantier, celui de l’automatisation du fusionnement des données, reposant sur le développement de l’intelligence artificielle.

  Quand à **l’IBW défensive**, on perçoit la difficulté de son rôle car aucun moyen de leurrage n’est efficace sur l’étendue de la gamme des capteurs. De plus le coût d’un missile est acceptable s’il est tiré contre un JSTARS mais il ne l’est plus contre une myriade de capteurs bon marché. Enfin le point d’application de la contre-attaque doit être judicieux pour mettre hors d’état le système plutôt qu’un seul de ses éléments. Le recours au piratage informatique (§ « hackerwar » HW ci-dessous) peut être préférable à la destruction physique.

---

[1] Les principaux éditeurs de logiciels de bases de données ont conçu ce nouveau mécanisme permettant, après mise à jour d’une donnée sur un site autorisé, la recopie à l’identique de la nouvelle valeur sur un ensemble préétabli de sites “ abonnés ” à cette donnée.

[2] Cet anglicisme désigne un outil de communication, souvent associé à la téléconférence parce qu’il permet d’illustrer ses propos à l’aide de l’écriture et du dessin.

[3] Un centre de backup désigne une structure dotée de moyens de sauvegarde et de restauration de systèmes d’information.

[4] Cet anglicisme intraduisible évoque l’acuité de la perception que l’on peut avoir de la situation grâce à la plus-value qu’apporte le traitement de l’information.

- **La guerre électronique (“ electronic warfare ” : EW)** : L’EW traite de techniques opérationnelles, radioélectricité ou cryptographie, dans le but de dégrader les supports de transmission de l’information.

  Dans le domaine de la **lutte anti-radar**, on se protège en séparant l’émetteur, cible des missiles anti-radiation, du récepteur. Pour assurer la survie du système, on multiplie et dissémine les dispositifs d’émission et de réception ; la complexification des signaux d’émission et des algorithmes de réception gardent un temps d’avance sur celle des brouilleurs.

  L’EW **contre les communications** est plus délicate car elles recourt à des techniques difficiles à brouiller ou à intercepter, (évasion de fréquence, élargissement du spectre, codage CDMA…), couplées à la compression numérique et à la redondance des transmissions. La localisation des émissions est souvent contrariée par un environnement électronique saturé. Les systèmes adverses se protègent en élargissant la gamme de leurs capteurs et en ménageant un “ tuilage ” des zones de couverture.

  Si l’intérêt de protéger sa propre vision de la réalité tout en tentant de dégrader celle de l’adversaire reste évident, le mythe de la **cryptologie** va s’affadir avec la disponibilité de technologies à clés publiques et privées comme le DES (Digital Encryption Standard) facilitant l’encryptage. Casser un code ou falsifier un message va devenir de plus en plus coûteux et improductif.

- **La guerre psychologique (“ psychological operations ” : PSYOPS)** : elle traite de l’information comme moyen de guerre s’exerçant sur l’esprit humain, et non plus sur les ordinateurs qui le supportent. Il y a quatre catégories de PSYOPS :

  Les opérations psychologiques **contre la volonté nationale** conjuguent - Thucydides en témoigne - le gant de velours et la main d’acier. Le départ peu glorieux des Américains de Somalie est un exemple patent de l’effet parfois décisif d’une telle manipulation. L’utilisation de satellites à diffusion directive (DBS) permet à tout groupuscule de se faire entendre d’une très large audience sans lui en demander l’autorisation, et à un coût de plus en plus accessible. Mais la manipulation de masse est difficile car elle doit traverser les filtres culturels de chaque communauté : une manipulation plus ciblée, par l’intermédiaire de micro-opérateurs collectant et modifiant à leur convenance l’information pertinente pour la société visée, pourrait bien succéder au “ phénomène CNN ”. Contrairement aux idées reçues, l’ubiquité de la télévision n’en fait pas un outil facilement utilisable en PSYOPS. Mais elle peut contribuer à créer l’événement souhaité, comme certains films à succès récents l’ont montré. Statistiquement, cette technique est assurée du crédit d’une partie de la société ciblée, quel que soit son degré de sophistication.

  Les opérations psychologiques **contre les troupes** adverses exploitent deux thèmes traditionnels : la peur de la mort et le potentiel de ressentiment du front envers les arrières. Le niveau d’équipement technique des forces est suffisant pour assurer la faisabilité de la communication avec les troupes déployées sur le terrain. La gageure est d’atteindre l’individu lui-même. Par exemple, le persuader que s’il est détecté, il n’a aucune chance de survivre, l’amènerait à détruire lui-même son matériel de guerre. L’interpeller nominativement, lui ou ses

proches, par voie télévisée au cœur de son unité, pourrait être un puissant moyen de pression individuelle. Les gigantesques capacités de stockage permettant aujourd'hui la traçabilité de chaque individu dans sa vie quotidienne, rendent ce scénario tout à fait plausible.

Les opérations psychologiques **contre le commandement** adverse visent à le désorienter et à l'induire en erreur, en lui fournissant de fausses informations relatives aux capacités et aux intentions de l'ennemi, ou en utilisant l'effet de surprise.

Les opérations psychologiques peuvent-elles susciter et exploiter **les conflits de cultures** ? La notion même de culture n'est pas acceptée par toutes les nations dont certaines ne reconnaissent que des normes de comportement social et politique. Celles-là prônent la liberté de choix et de commerce des produits culturels est sont donc peu perméables à la " Kulturkampf ".

- **Le piratage informatique** et les attaques logicielles contre les systèmes d'information **(" hackerwar " : HW)** : il s'agit ici des systèmes autres que ceux de commandement et de contrôle concernés par le C2W. La HW peut aussi être différentiée entre HW défensive et HW offensive.

  Le débat autour de la **HW défensive** porte sur la responsabilité du DoD dans la sauvegarde des systèmes non militaires. Il est vrai qu'un ordinateur sans connexion vers le monde extérieur est parfaitement protégé mais parfaitement inutile aussi ! La sécurité a un coût, ce qui explique que la liste des systèmes déclarés d'importance vitale pour le pays, soit restreinte. De plus, à l'instar des voies ferrées en campagne, les réseaux non protégés entre ordinateurs suscitent peu d'opérations de sabotage. La pire menace est l'accès frauduleux sans incident qui trompe l'attention des administrateurs de systèmes. Il est cependant plus facile pour un responsable de sécurité de tester les failles de son système contre l'intrusion que pour le pirate informatique de faire le même test ! Mais il n'y gagnera pas l'aura de mystère que le public accorde aux pirates ! Il y a donc bien une réalité du phénomène qui peut être qualifié de guerre quand des actions concertées s'attaquent à des systèmes d'information commerciaux, en provoquant une perturbation suffisante pour interpeller le pouvoir politique. Cela s'apparente au mode d'action terroriste, ou à la guerre économique. Mais l'effet n'est pas assez probant pour que l'Etat cède à ce chantage. La HW défensive est une tâche quotidienne essentielle, même pour les systèmes non vitaux, dans laquelle la responsabilité individuelle des administrateurs de systèmes, et non pas celle de l'Etat, est engagée.

  Le débat autour de la **HW offensive** porte sur l'opportunité de son emploi ; à l'instar de la guerre bactériologique, est-on sûr de maîtriser l'antidote avant de lancer l'attaque ? En temps de paix, les intérêts des nations sont tellement interdépendants que la HW est inutilisable, mais il serait impardonnable de ne pas s'y préparer pour le temps de crise.

- **La guerre économique** et le contrôle du commerce de l'information **(" information economic warfare " : IEW)**. Elle peut prendre deux formes : le blocus de l'information et l'impérialisme de l'information.

Etablir un **blocus de l'information** suppose que l'on attaque un pays vraiment dépendant de ses flots entrant et sortant d'information. Pendant encore longtemps, peu de pays seront vraiment menacés. Le pays attaquant doit quant à lui être relativement insensible aux actions de rétorsion de même nature. En dépit du blocus, le pays attaqué peut conserver l'accès à l'information sous la forme d'imprimés ou de CD-ROM et continuer à commercer. Il perd cependant le bénéfice du temps réel et, en étant banni de *l'infosphère*[5], il compromet sa compétitivité commerciale. Contrairement à un blocus sur les échanges de marchandises, celui-ci peut être mis en place avec peu de risque de violence ou de contournement. Il est établi en coupant les lignes de communication physiques, en brouillant les lignes hertziennes, et en suspendant les services publics par satellites. Mais il n'est pas possible de dissuader les chaînes privées de communication par satellites et les réseaux de téléphonie mondiale de profiter de cette opportunité lucrative. Les pays sont cependant plus sensibles que l'on ne le croit à la privation de services fournis par l'extérieur car de nombreux secteurs de leur économie font souvent appel à l'expertise de consultants étrangers.

En constatant que les pays rivalisent pour la domination de certains secteurs économiques stratégiques, on admet la menace d'un **impérialisme de l'information**. En effet, les industries à forte valeur ajoutée tirent leur prospérité du cercle vertueux dans lequel elles se développent : main d'œuvre qualifiée et motivée, acquisition de compétences de haut niveau, accès aux sources d'information dans les domaines technologiques de pointe… Ces pôles – il s'agit d'ailleurs souvent de corporations multinationales à caractère de moins en moins national - se défendent de pratiquer l'impérialisme et préfèrent reconnaître des " avantages comparatifs ".

- **La guerre cybernétique (" cyberwar " : CW).**
  Le **terrorisme de l'information** vise à dévoiler publiquement le contenu des fichiers de données nominatives à usage confidentiel (santé, achats, …). Ce n'est pas tant la crainte de la compromission qui fera réagir les victimes que l'incapacité des pouvoirs publics à s'y opposer.

  Les **attaques sémantiques** passent inaperçues dans l'exploitation courante du système. Elles sont ainsi capables de fraudes financières ou, par l'introduction de données factices en réponse aux sollicitations d'un serveur, de production de résultats invalides en sortie d'analyse. Des précautions adaptées, signature électronique et surveillance humaine, doivent être développées pour protéger ce genre de système.

  La **guerre simulée** remplacera-t-elle un jour la guerre réelle ? Idéalement, livrer une guerre par simulation pour montrer à l'ennemi qu'il va perdre, pourrait le dissuader de s'y engager. Pour que le système de simulation soit crédible, les adversaires seraient tenus de décrire avec exhaustivité les caractéristiques, performances et concepts d'emploi de leurs systèmes réciproques. Une telle honnêteté serait le plus sûr gage de paix ! La simulation demeure appropriée pour les opérations qui se déroulent en dehors de la scène des combats : utilisation

[5] L'infosphère est un néologisme suscité par la prolifération des applications commerciales des technologies de l'information ; elles ont pour effet direct de créer une communauté mondiale d'usagers qui ont le privilège d'être reliés par des réseaux voix-données-images permettant une communication en temps quasi-réel ; la non disponibilité de ces applications est dès lors un facteur d'exclusion.

des systèmes d'information et des armements transhorizon par exemple. L'entraînement à la détection en environnement réel est aussi un domaine d'application de la simulation.

Enfin, en considérant la réalité du pouvoir du monde virtuel véhiculé par Internet, pourquoi ne pas envisager des **guerres virtuelles** entre des agents ou des coalitions de cybernautes, mandatés pour l'appropriation de biens ou de services bien réels.

3.5 Les formes irréductibles da la guerre de l'information

Ces sept formes ne sont que peu couplées. Certains aspects de l'IW sont vieux comme le monde : frapper l'ennemi à la tête, le duper par toutes sortes de procédés, utiliser des moyens psychologiques...

D'autres sont plus récents : l'EW s'est imposé pendant la Deuxième Guerre mondiale ; l'automatisation récente des centres de commandement a créé une nouvelle vulnérabilité ; l'évolution de la société civile vers la dimension virtuelle laisse envisager de beaux jours pour les pirates informatiques, la guerre économique et cybernétique.

Les structures de commandement conjoint se partagent les responsabilités des différentes formes militaires de l'IW de la manière suivante :

- La C2W est assignée à la cellule J3 (opérations) de l'état-major interarmées.
- La conception et la protection des moyens de commandement et de contrôle reste du domaine de compétence de la cellule J6.
- L'IBW dans sa partie relative à la connaissance du champ de bataille échoit naturellement à la cellule J2 (renseignement).
- La connaissance de l'architecture des systèmes adverses, nécessitant une vue à long terme, est du ressort de la cellule J5 (planification) .

La supériorité dans l'IW va à celui qui sait profiter au mieux de ses systèmes d'information et qui, en conséquence, en comprend mieux les faiblesses. Si ces systèmes confèrent effectivement à leur utilisateur la supériorité dans les domaines C2W, IBW et EW, ils le placent aussi dans une position de dépendance, et donc de vulnérabilité par rapport aux menaces PSYOPS, HW et CW.

Une caractéristique de l'IW est que personne ne peut prouver que telle action pourrait être, ou ne pas être, un succès, ni même définir ce que le succès d'une action signifie dans ce contexte.

En conséquence l'IW reste encore essentiellement défensive. De plus certaines actions offensives ne seraient tout simplement pas réalisables dans le cadre restrictif des règles d'engagement auxquelles les forces sont assujetties.

Une autre caractéristique de l'IW est qu'elle n'est pas un jeu à somme nulle, c'est-à-dire que la maîtrise de l'un des adversaires dans ce domaine n'exclut généralement pas les progrès de l'autre (sauf en de rares occasions comme le brouillage ou la concurrence pour l'accès aux moyens de communication). Si la notion de supériorité dans le domaine de l'information est acceptable, celle de suprématie n'est pas plus pertinente que dans le domaine de la logistique.

En corollaire, les spécialistes de l'IW doivent bien comprendre que leur raison d'être n'est pas de lutter contre leurs homologues " d'en face ". Ils ont la responsabilité d'acquérir la connaissance précise et fiable des systèmes d'information de l'adversaire, qui seule permet la conduite de l'IW : quels sont leur architecture physique et même logicielle, le degré de dépendance des processus de décision, les structures de commandement, l'infrastructure de communication... ?. Le meilleur moyen d'acquérir cette connaissance est de participer dès le temps de paix à la conception et à la mise en œuvre des systèmes, et de faciliter leur interconnexion avec les systèmes nationaux. Une politique commerciale favorable à l'acquisition de logiciels et de matériels communs, associée à l'offre de services et d'ingénierie, assurera une standardisation de facto de l'infrastructure globale de l'information. Enfin, il faut être convaincu qu'une IW conduite sans tenir compte du mode de prise de décision et du contexte culturel de l'adversaire est vouée à l'échec.

De façon plus générale, si l'IW consiste à avoir une meilleure connaissance du champ de bataille de l'ennemi, il faut garder à l'esprit qu'une donnée n'a pas de valeur si on ne peut l'incorporer à une structure conceptuelle porteuse de sens ; mais les meilleures structures ne sont que des abstractions du monde réel ; l'important est d'être conscient du degré de dangerosité que ce biais introduit dans la perception. L'IW produira donc des résultats très différents d'un commandant d'opération à un autre, en fonction de leur style propre de prise de décision.

Il serait logique d'envisager un corps de " guerrier de l'information " capable de gérer le cycle de l'information depuis son capteur jusqu'au système d'armes. Ils seraient chargés de développer et d'organiser les éléments du système, de les surveiller, de maintenir leur intégrité, d'interpréter leurs produits et de les acheminer. Ce corps contribuerait notablement à la C2W, l'EW et à la HW. Mais les formes civiles de l'IW, telles que la PSYOPS et l'EW, dépassent largement la portée du DoD et les capacités d'acquisition de connaissance d'un tel corps, aussi large soit-il.

Si l'on considère les formes de blocus de l'information et de cyberdéfense comme encore largement prématurées, si l'on considère que la HW, bien que réelle, est largement exagérée, si l'on répartit les formes de l'EW sur les domaines qu'elle peut supporter (par exemple C2W, IBW), trois formes demeurent : C2W, IBW et SPYOPS ; chacune d'elles pouvant être appréhendée comme une discipline séparée.

3.6 Les aspects juridiques de la guerre de l'information

Le développement de l'IW suscite de nombreuses interrogations relatives au droit international ; elles pourraient bien compliquer la tâche de ceux qui exécutent ou répondent à des attaques contre les systèmes d'information.

Depuis la fin de la Guerre froide, les nations occidentales souhaitent subordonner tout engagement militaire à un mandat d'une coalition internationale ou de l'Organisation des Nations Unies. Ils leur est donc indispensable de pouvoir persuader les autres nations que leurs actions sont légales et que celles de leurs ennemis ne le sont pas.

Un autre intérêt évident à promouvoir le droit international, dans le domaine particulier de l'IW, est qu'il contribue à la stabilité générale et à la protection des systèmes d'information stratégiques.

Le droit international consiste essentiellement en un droit " conventionnel " et en un droit " coutumier ". Le droit conventionnel résulte des traités et autres protocoles d'accord entre les nations, qui sont alors liées à leurs engagements selon le principe du " pacta sunt servanda ". Le droit coutumier résulte de la pratique régulière et cohérente des états (" opinio juris "), ou du consensus autour d'un texte normatif d'intérêt collectif. En exemples, on citera le statut traditionnellement protégé des diplomates ou la revendication historique des trois miles nautiques d'eaux territoriales. Mais il n'existe aucun moyen universel pour décider de ce qui est reconnu ou non par le droit international coutumier.

Même quand les normes légales sont bien établies, la pratique contraire de certains états qui les méprisent contribue à amoindrir leur force et à altérer leurs principes. D'autant plus aisément qu'aucune police internationale n'est chargée d'en imposer l'application. Le droit international, en effet, est plus proche d'un arrangement contractuel entre personnes privées que du corpus contraignant du droit national.

D'un point de vue légal, les anciennes formes de l'IW, telles que le camouflage, le brouillage, la coupure des lignes téléphoniques …, ne posent pas de problème particulier, comme d'ailleurs les attaques contre les systèmes militaires d'observation.

Mais le développement des technologies de l'information, principalement celles des ordinateurs, des télécommunications et des réseaux, a fait place à de nouvelles formes de combat et de dommages, qui ne nécessitent pas de pénétrer physiquement dans le pays de l'ennemi. Les systèmes électroniques ou d'information, dont les états sont de plus en plus dépendants, deviennent des cibles particulièrement attractives. A usage dual par nature, ils ne permettent plus la distinction aisée entre cibles militaires et civiles.

De telles nouveautés remettent en cause le droit international sous trois angles :

- Les dommages provoqués, (perturbation de systèmes d'information, corruption de données mémorisées, transmission de données manipulées…), sont immatériels et s'apparentent mal aux dégâts que causent les guerres conventionnelles.

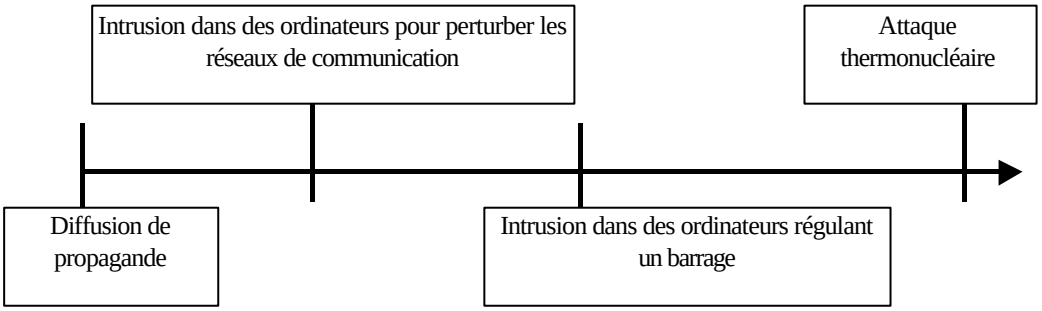
- La capacité des signaux à traverser des réseaux internationaux remet en question la notion de souveraineté nationale territoriale qui veut que chaque nation ait l'autorité exclusive sur les événements qui se déroulent à l'intérieur de ses frontières.

- Il est difficile de qualifier les cibles de l'IW de " militaires " (donc généralement légitimes) ou de " civiles " (donc généralement interdites). Des attaques visant des cibles principalement

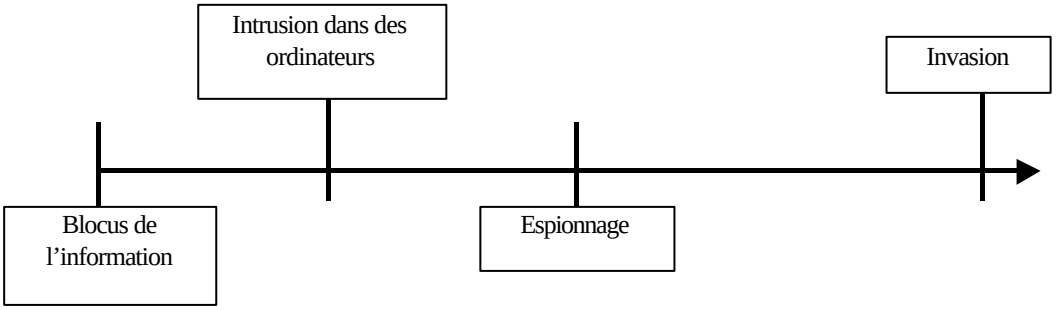
militaires peuvent engendrer des conséquences sur des systèmes civils connectés. De plus, les dommages provoqués ne sont pas susceptibles de relever du droit humanitaire qui protège les non-combattants.

Trois graphiques illustrent l'étendue du spectre des actions de guerre et montrent bien la difficulté à situer les actions d'IW dans ce continuum :

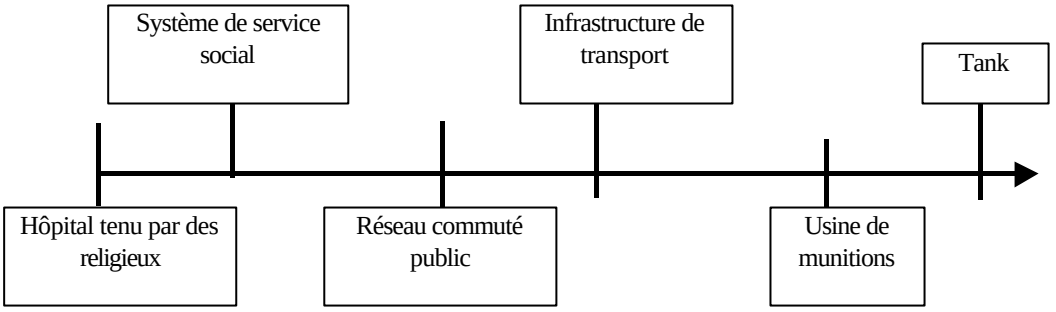
- Sur l'échelle du **pouvoir de destruction physique**, où placer la limite entre la guerre et la paix et comment déterminer que telle action est compatible, ou non, avec le droit international ?



- Sur l'échelle de **gravité de l'intrusion**, quand y a-t-il violation des frontières nationales ?



- Sur l'échelle de **l'ambiguïté du caractère militaire ou civil** des cibles, où placer la limite entre légitimité et illégitimité ?



En fait, le droit international existant laisse assez de latitude à l'expression de l'IW sous toutes formes de techniques et de circonstances.

Par exemple, c'est l'Union internationale des télécommunications (ITU) qui régit les télécommunications internationales par câble ou ondes radio. Mais il est peu probable que cette organisation puisse s'opposer aux activités de l'IW, particulièrement en temps de guerre. Historiquement, sa raison d'être a été le développement du télégraphe et, ce qui reste sa mission aujourd'hui, la promotion de l'interopérabilité et la réduction des interférences. Mais elle n'a pas autorité pour imposer l'exécution de ses décisions. L'IUT est plus un organisme de coordination qu'un organisme de régulation. Un contrevenant manque à ses obligations contractuelles, mais ne commet en aucun cas un acte de guerre justifiable d'une répression par la force.

Dans le domaine de l'espace, le texte fondamental régissant son utilisation est le traité multilatéral de 1967 (" The Outer Space Treaty "). Il prescrit la liberté d'exploration et le droit d'exploitation sur la base de l'égalité des états, mais il proscrit la mise en orbite terrestre d'armes nucléaires ou de toutes les sortes d'" armes de destruction massive ". Le traité de 1979 concernant la Lune (" The Moon Treaty "), n'autorise que les activités pacifiques, tout en leur appliquant les mêmes restrictions. L'accord de 1971 relatif à l'organisation internationale de télécommunications par satellites (INTELSAT), et la convention de 1976 pour l'organisation internationale de satellites maritimes (INMARSAT) se limitent au principe de non discrimination entre les nations utilisant leurs services.

Aucun de ces textes ne s'oppose aux activités de l'IW faisant usage de satellites. Ils ont eu le mérite d'instituer la norme de l'utilisation pacifique de l'espace et d'empêcher une course aux armements en orbite. Mais il est indéniable que l'espace a été, et est encore, utilisé à des fins militaires. La surveillance spatiale est légale et commune ; l'espace est couramment traversé de signaux militaires pour la communication, la navigation et le guidage des armes. Les activités de l'IW, le plus souvent non léthales et non physiquement intrusives, pourraient de même être

qualifiées de “ pacifiques ”. Ses partisans pourraient aussi alléguer que le satellite n’est qu’un conduit utilisé par une arme qui se trouve effectivement à terre.

La pratique des états, source d’une partie du droit international coutumier, est elle-même permissive vis à vis des actions de l’IW. Elle tolère la surveillance spatiale alors que le droit national qualifie l’espionnage de criminel ; les câbles sous-marins sont systématiquement sectionnés pendant les guerres ; le brouillage et les ruses de guerre sont considérés comme des procédés légitimes.

La neutralité d’un pays n’est pas réputée enfreinte dès lors que ses réseaux de communications ou ses ordinateurs sont utilisés dans une attaque visant un pays tiers. Si cela était le cas, l’état neutre pourrait être légitimement la cible d’actions de rétorsion.

Le droit humanitaire, lui non plus, n’apporte pas de contraintes explicites à l’IW ; son principe de base, la protection des non-combattants, condamne l’attaque non justifiée de cibles civiles. Les “ objectifs militaires ” sont les cibles dont la nature, la localisation, ou l’usage contribuent à l’action militaire ou celles dont la destruction apporte un avantage militaire manifeste. Les armes employées doivent permettre au tireur de distinguer les cibles civiles des objectifs militaires. Enfin la programmation et l’exécution des attaques doivent respecter la règle de proportionnalité entre les dommages civils et les objectifs militaires atteints. L’usage de la force doit être en rapport avec l’importance du différend (“ jus ad bellum ”) ; les actions doivent être en rapport avec leurs objectifs et les pertes humaines qui sont susceptibles d’en découler (“ jus in bellum ”). Au regard du droit humanitaire, les attaques seront donc jugées bien plus sur leurs effets que sur leurs méthodes : la perturbation intentionnelle d’un système de contrôle aérien provoquant le crash d’un avion de ligne serait certainement condamnée ; mais le sabotage d’un système de sécurité sociale ou la divulgation de données nominatives confidentielles sont peu susceptibles de violer les lois de la guerre.

La propagande, la manipulation d’images, les émissions captieuses, dans la mesure où elles encouragent la guerre civile, voire le génocide, peuvent être illégales.

Si la ruse est admise en temps de guerre, la perfidie, (feindre une trêve ou une blessure, usurper le statut civil, …) est réprouvée. De même, l’interdiction de revêtir l’uniforme de l’ennemi est une norme requise par les lois de la guerre pour différencier les troupes qui s’affrontent. Ces obstacles moraux ne sont plus pertinents lorsqu’il s’agit d’attaques contre des systèmes d’information.

L’usage de l’IW en temps de paix pose un problème de définitions : peut-elle être qualifiée de “ guerre ”, d’“ acte de force ” ou d’“ agression ” ? Si oui, l’IW devient un outil illégal en temps de paix ; l’emploi de la force en défense est alors justifié, et pourra constituer une réponse proportionnée à l’attaque. Si non, le droit humanitaire ne s’applique pas et les dommages causés aux civils ne sont pas un obstacle du point de vue légal. Une agression caractérisée, quant à elle, permet d’en appeler au Conseil de sécurité des Nations unies.

La surveillance aérienne a historiquement été restreinte par la notion de souveraineté de chaque état dans son propre espace aérien. Le droit international a choisi de considérer la surveillance spatiale, pourtant de même nature, comme une activité libre et universelle de l’espace. Cette

extension n'est ni évidente ni logique; mais les états contestateurs n'ont aucun moyen de s'y opposer. Les développements technologiques n'auraient-ils pas entraîner l'IW hors des voies légales coutumières ? Il est vrai que les dommages infligés ne sont pas de ceux que les lois de la guerre s'attachent à limiter.

La Charte des Nations Unies interdit la menace ou l'usage de la force contre l'intégrité territoriale ou l'indépendance politique d'un état. Récemment, l'Assemblée générale a rejeté la proposition d'élargir la sémantique du mot "force " pour inclure par exemple des mesures économiques coercitives, comme l'embargo sur le pétrole de 1993. Les intentions des auteurs de la Charte ont été réaffirmées dans plusieurs déclarations de l'Assemblée générale : les droits de souveraineté ne doivent pas être aliénés par la force ou " toute autre forme de coercition ". Il reste à prouver qu'une attaque d'IW viole ces droits souverains.

Les nations peuvent s'infliger des coups réciproques, (embargos, espionnage économique, fermeture d'un canal, …), sans qu'ils soient reconnus comme agressions ou actes de guerre. Un blocus naval et une attaque de l'IW ont tous deux des effets désastreux sur l'économie d'un pays ; pourtant le premier sera considéré comme action de force agressive car il est exécuté par des militaires et comporte une menace physique ; tandis que le second peut être exécuté par des civils et n'est pas physiquement envahissant ou destructeur.

3.7 La légalité de la réponse à la guerre de l'information

La problématique légale de la réponse à l'IW est toute aussi complexe que celle de l'attaque.
La première difficulté est d'identifier l'attaque elle-même, en particulier quand elle ne survient pas en période de tension, car ses effets sont similaires à ceux d'un bogue logiciel ou d'une mauvaise manipulation.

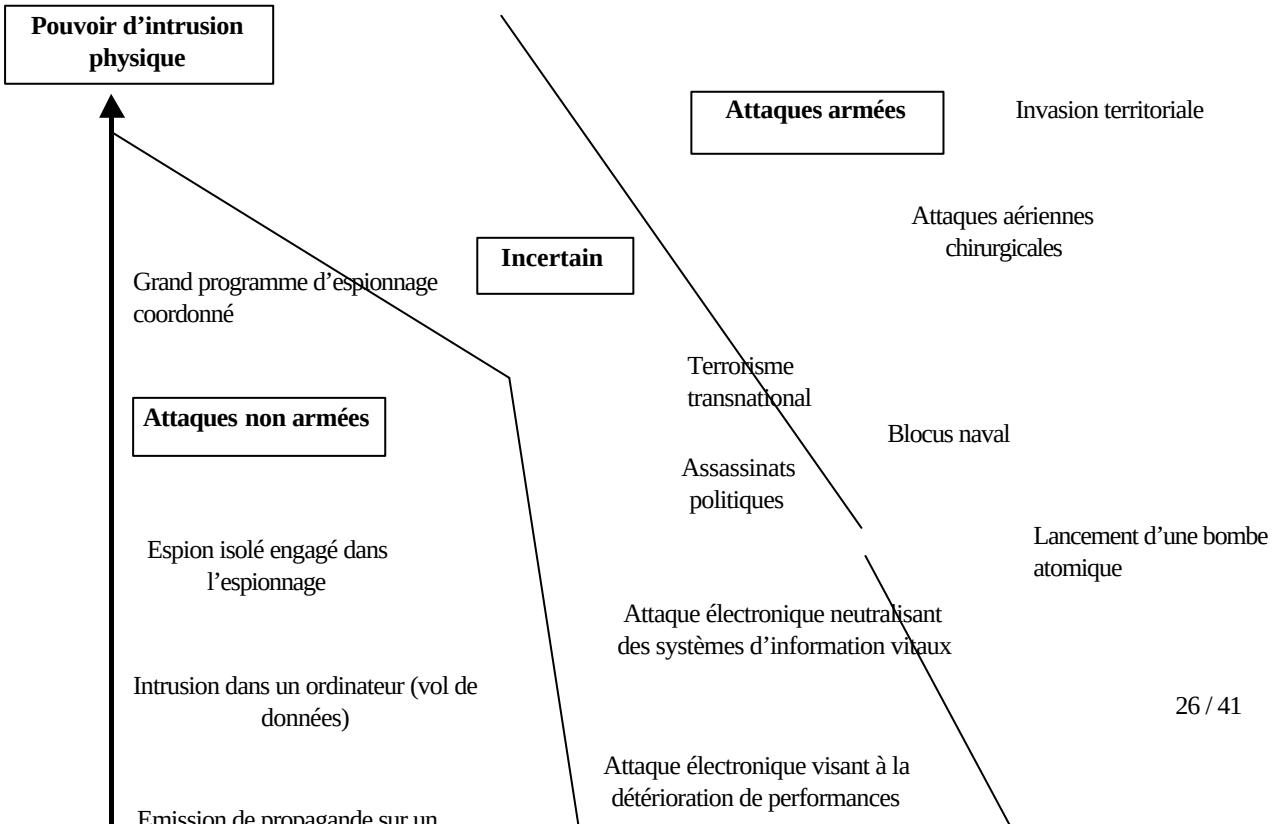
La deuxième est de pouvoir enquêter sur la provenance de l'attaque : si les électrons traversent librement les réseaux internationaux, les agents nationaux ne peuvent pas lancer unilatéralement une poursuite à l'étranger. De plus les pirates informatiques s'ingénient à brouiller leur pistes en traversant plusieurs pays et en masquant leur identité. L'étendue et la disponibilité des équipements nécessaires à l'IW permettent aux terroristes qui les utilisent de s'affranchir du support d'un état protecteur ; de toutes façons, une accusation de complicité dans ce domaine peut être déniée en toute plausibilité.

Une troisième difficulté vient du fait que la coopération internationale pour la lutte anti-IW ne présente aucun caractère obligatoire, en l'absence de traité. Un refus de coopération n'est même pas suspect, bon nombre de pays étant simplement réticents à dévoiler leurs capacités ou leurs vulnérabilités dans le domaine des systèmes et des réseaux. Une investigation menée sans la collaboration officielle des pays traversés, bien que n'étant pas illégale au regard du droit international, pourrait, si elle était découverte, placer son auteur dans une situation diplomatique et politique délicate.

Une quatrième difficulté est liée à l'extradition des coupables : cette possibilité n'existe que si un traité spécifique lie les deux états en stipulant l'éventail des crimes qui, à la condition qu'ils soient reconnus de part et d'autre, justifient une extradition. Encore faut-il parer les clauses d'exemption, par exemple pour certains crimes à motivation politique, permettant aux états d'argumenter leur refus. En effet, la crainte d'éventuelles représailles, ou une politique d'encouragement au développement des technologies de l'information pourraient conduire certains gouvernements à ne pas vouloir pénaliser les attaques d'IW.

Enfin le droit de réponse dépend de la qualification de l'attaque : une réponse armée ne peut être envisagée qu'en réponse à une " agression armée " selon les termes de la Charte des Nations Unies ; mais nous avons vu combien il est difficile de prévoir si telle action sera qualifiée d'" acte de guerre ", d'" agression " ou d'" usage de la force ". En dehors de ces cas, toute réponse présenterait le risque de justifier une action de légitime défense dans le cadre de l'article 51 de la Charte. Il faut aussi se garder de créer des cas de jurisprudence pouvant constituer des entraves légales pour l'avenir. La proportionnalité de la réponse est, elle aussi, très subjective ; elle dépend de l'identification d'une cible pouvant être estimée d'une valeur comparable au préjudice subi.

Cette discussion montre bien l'ambiguïté du droit international au regard des activités de l'IW qui ne peuvent que se développer dans un futur proche ; les pays possédant une avancée dans le domaine des technologies de l'information ont l'opportunité d'initialiser les normes qui pourraient préfigurer de futures lois internationales. Cependant ils trouveront plus prudent de laisser le jeu mondial opérer la régulation et l'arbitrage nécessaires. Ils pourraient aussi agiter le spectre des dangers de l'IW : ce serait une initiative contre-productive perçue comme un frein au développement de puissances concurrentes. Il est pourtant de leur responsabilité de promouvoir la coopération dans la lutte anti-IW et la criminalisation des attaques de systèmes d'information.



Attaque électronique
causant la panne
d'un barrage

Une loi ne constitue pas une panacée et ne remplace pas la vigilance et la préparation. Elle canalise, malgré tout, le comportement des nations et des individus et contribue aux efforts diplomatiques pour désamorcer les crises ou en atténuer les effets.
Il est donc de l'intérêt des nations d'étudier et de faire évoluer la panoplie juridique avant d'être confrontées à une situation d'urgence.

3.8 La Dominance par l'Information (Information dominance : ID)

Le pouvoir grandissant de l'information apporte une connotation hiérarchique aux termes suivants : infériorité, parité, supériorité, suprématie et dominance. La terminologie de la doctrine doit refléter, en choisissant le terme approprié, le niveau effectivement requis pour l'accomplissement de la mission.

La notion de supériorité est basée sur des mesures quantitatives, telles que le ratio d'attrition : par exemple, on pourra dire qu'un ratio de 55-45 est synonyme de supériorité et qu'un ratio de 95-5 est synonyme de suprématie.

La notion de dominance est qualitative et globale ; elle prend en compte l'effet de synergie existant entre plusieurs pôles de supériorité.

La dominance par l'information peut être définie comme étant l'acquisition de la maîtrise dans la génération, la manipulation et l'exploitation de l'information, sur toute sa gamme et dans l'espace-temps opportun. Elle suppose que l'on a atteint le seuil de connaissance de "l'infosphère " qui offre, plus qu'un avantage sur l'adversaire, la liberté d'action.

La dominance de l'information recouvre trois capacités :

- le **commandement et le contrôle**, qui reposent sur la connaissance de la localisation des forces amies dans le champ de bataille (le " où "), éventuellement complétée de celle de leur état de fonctionnement, de façon à exécuter une opération au moment souhaité et le plus rapidement possible (le " quand ").
  Le pilote de chasse américain John Boyd a illustré ce concept en proposant le concept de la boucle OODA : Observer le champ de bataille, s'Orienter dans ses limites, Décider de l'action à mener et Agir. Le vainqueur sera celui qui est capable de parcourir ce cycle le plus vite.
  En conséquence, des efforts d'investissement portent actuellement sur l'équipement des mobiles et des hommes en moyens de localisation. Mais il faut être conscient que la conjonction des moyens de communications, des capteurs et des systèmes d'armes est plus importante que l'existence individuelle des bâtiments, aéronefs ou sous-marins qui les emportent. Elle permet la coordination des moyens et la transmission des ordres d'opération en temps réel, et par là, une plus grande efficacité et économie des moyens.

- le **renseignement**, qui a traditionnellement le rôle d'informer le commandement sur la taille, la localisation et les intentions des forces ennemies. La technologie permet maintenant de localiser des plates-formes isolées en temps réel et avec une précision métrique et de fournir l'information directement au combattant et à son système d'armes. Cela a été illustré par l'attaque des chars sur la route de Khafji, détectés par le JSTARS (Joint Surveillance, Targeting, and Reconnaissance System aircraft).
  La capacité à voir et frapper un ennemi à des distances de plus en plus grandes a été et reste le principal souci de ce que l'on a appelé aux Etats-Unis la Révolution dans les Affaires Militaires (RMA). La première phase de ce projet s'est consacrée à l'étude des munitions guidées de précision (PGM) : guidage laser, signatures radar ou infrarouge, bombardement sur coordonnées... Si l'on admet que l'on sait frapper un ennemi que l'on a vu, il faut donc convenir que la suprématie consiste à voir l'ennemi : les capacités à détecter et identifier les forces ennemies, à déterminer avec précision leur position et leur cap, seront donc au cœur des préoccupations de la deuxième phase de la RMA.

- la **guerre de l'information**, qui s'attaque aux système d'information adverses, rarement pour les détruire, mais plutôt pour les ralentir, les tromper ou les fausser. Plus l'information est au cœur des systèmes militaires, plus l'IW apparaît logiquement comme une capacité militaire indispensable. Elle est cependant difficile à maîtriser pour six raisons :
  ⇒ 1- percer des systèmes adverses de plus en plus étendus et complexes requiert des ressources d'intelligence, humaine principalement, considérables ;
  ⇒ 2- la prolifération des logiciels et moyens de cryptage, et la chute de leur prix, rendent les moyens de redondance et de défense contre l'IW plus accessibles ;
  ⇒ 3- en conséquence, le succès en IW est hasardeux et opportuniste ;
  ⇒ 4- les dégâts infligés ne sont pas toujours visibles et peuvent être masqués ou feints ; leur évaluation (BDA) est donc sujette à caution ;
  ⇒ 5- l'IW étant systématiquement associée à l'idée de leurrage, elle peut difficilement être utilisée comme une arme de dissuasion ;
  ⇒ 6- priver l'adversaire de ses moyens de commandement peut nuire à la mise en œuvre des conditions de cessez-le feu ou d'armistice.

La " Joint Vision 2010 " américaine se propose d'atteindre, pour les opérations combinées du 21ième siècle, la dominance " tous azimut " (" full spectrum dominance "). Cette ambition exige que le niveau de qualité des traitements de données et de l'information dépasse le seuil de la supériorité. L'IW pourrait devenir un facteur clé de prévention ou d'apaisement des hostilités si elle sait convaincre l'adversaire qu'il ne peut pas gagner.

Cela dit, il faut garder à l'esprit que la dominance par l'information est une capacité toute relative, pour trois raisons :

1- L'acquisition de la dominance aérienne peut clouer la force aérienne adverse au sol ; mais la dominance par l'information ne garantit aucunement la paralysie des systèmes d'information adverses.

2 - Dans un conflit, les besoins en information ne sont pas équivalents des deux côtés ; en Somalie, les Etats-Unis avaient la dominance de l'information au niveau tactique (détection à grande distance) mais ne l'ont jamais atteinte au niveau opérationnel et politique.

3- Comme l'affirmait déjà Sun Tzu 2500 ans avant notre ère, la connaissance la plus importante que l'on peut apporter sur le champ de bataille est d'abord celle de soi (que veut-on, pourquoi, et à quel prix), et ensuite celle de l'autre ; ce sont ces éléments-là qui forgent la stratégie ; une mauvaise stratégie peut rarement être sauvée par une suprématie de l'information au niveau tactique.

Finalement, et conformément à la pensée de Sun Tzu, l'apogée de l'art militaire est de vaincre sans combattre, d'arriver à convaincre le parti adverse de la justesse de nos vues et de le rallier à nos intérêts. L'histoire présente peu de cas de résolution de conflits dans ces termes. Mais les valeurs occidentales se répandent universellement et conduisent à un statu quo faisant abstraction de la force, basé sur l'adhésion aux règles de droit, au respect de la liberté de commerce, au renforcement des droits de l'homme... La " dominance par l'idéologie ", peut-être synonyme de " la fin de l'Histoire ", serait la forme achevée de la dominance par l'information.

4. L'approche militaire de la complexité

4.1 Introduction

La seconde évidence qui s'impose aujourd'hui est l'accroissement considérable de la complexité. L'étude effectuée au paragraphe précédent en est une illustration convaincante. Il est donc naturel de chercher à mieux qualifier cette notion. Le caractère intrinsèque le plus important qui peut être identifié est, en tout premier lieu, la non-linéarité du comportement des systèmes complexes. Après avoir explicité cette notion, on aborde la manière dont elle s'inscrit dans la pensée stratégique.

4.2 De la non-linéarité

Ce néologisme, comme beaucoup d'autres mots tels que " asymétrie " ou " déséquilibre ", sous-entend que la linéarité est la norme et que la vérité réside dans ce qui est simple (stable, régulier et logique) plutôt que dans ce qui est complexe (instable, irrégulier et illogique).
Cette tournure d'esprit typiquement occidentale, est un héritage des Classiques grecs ; elle conduit à une idéalisation de la réalité environnante sensée se plier aux règles intuitives et à un comportement attendu. On voit quelle marge d'erreur elle peut introduire dans nos perceptions.

La guerre froide a duré quarante années pendant lesquelles nous avons vécu et lutté dans un monde bipolaire où les interactions, limitées à celles des deux principaux acteurs, l'URSS et les USA, restaient dans un système essentiellement linéaire.
La supériorité historique des USA dans les domaines industriel et technologique a constitué un deuxième facteur de durabilité de ce système linéaire. En effet, elle a autorisé une stratégie d'attrition à travers des déploiements massifs de forces à chaque engagement. La force écrasante a tendance à linéariser un conflit en limitant les effets non linéaires.

La météorologie, les turbulences de fluides, la combustion, la rupture ou le flambage, l'évolution biologique, les réactions biochimiques dans les organismes vivants, l'hystérésis des systèmes électroniques offrent des exemples de phénomènes non linéaires.
Dans un système non linéaire, il n'y a pas de proportionnalité des sorties par rapport aux entrées ; le système n'est pas additif : il n'est pas quantitativement la somme de ses composants, ni qualitativement descriptible à partir de ses constituants ; il n'est pas " réplicable " car à partir de mêmes causes, on n'obtient pas les mêmes effets. Par conséquent la connaissance d'une petite partie du système ne peut pas être extrapolée par un changement d'échelle : le système n'est pas prédictible à la façon des systèmes linéaires.
Bien que des solutions analytiques aient été utilisées depuis des siècles pour aborder ces problèmes, leur étude a été relativement limitée jusqu'à l'avènement d'ordinateurs offrant des techniques numériques de résolution.
Il est vrai que les techniques de résolution d'équations linéaires ont atteint un degré de sophistication tel qu'elles sont devenues à la fin du dix-neuvième siècle l'outil préféré non seulement des mathématiciens mais aussi des physiciens ; c'est ainsi que les études des ondes de surface, des vibrations de faible amplitude et des faibles gradients de température se sont accommodées de telles approximations.

La " théorie du chaos " notamment, met en évidence la sensibilité des systèmes non linéaires aux conditions initiales, bien que ce soit déjà le cas pour les systèmes déterministes. Des différences infimes en entrée peuvent produire des résultats tellement différents que le comportement peut être attribué au hasard ; d'où le terme de " chaos ". Le premier exemple de système instable a été rencontré dans la météorologie des années 60. Le mathématicien Edward Lorentz, en utilisant dans son modèle un système de trois équations différentielles du premier ordre, a pu dire qu'un battement d'aile de papillon de ce côté-ci du monde pouvait provoquer une tempête de l'autre côté. Cet effet provient du fait que les variables ne peuvent pas être isolées l'une de l'autre : leur interaction dynamique est une des caractéristiques du système non linéaire.

Ce qui est nouveau c'est que les ordinateurs ont permis une approche numérique de la non-linéarité et des problèmes d'instabilité qui captent aujourd'hui l'intérêt tant des scientifiques que des profanes. De formidables capacités graphiques leur ont permis de visualiser et d'expérimenter ces phénomènes.

La non-linéarité est à la fois une menace et une opportunité : elle génère des instabilités, des discontinuités, des synergies et des imprédictibilités. Mais elle se fait le champion de la flexibilité, de l'adaptabilité, du changement dynamique, de l'innovation et de la réactivité. D'où l'intérêt de l'étudier dans le cadre de la guerre, quand le faible recherche les angles morts du fort pour les exploiter, ou essaie d'affecter le contexte politique pour retourner à son avantage les conditions du conflit. L'habitude de la linéarité a émoussé notre sens de l'imagination, ce qui est devenu une fragilité par rapport à l'adversaire.

4.3 De l'auto-adaptation

Une plus grande appréhension de la complexité de la réalité pourrait nous aider à construire des systèmes plus robustes, capables de s'auto-réorganiser, qui minimiseraient la durée de la surprise et de l'adaptation aux changements des circonstances. Ces systèmes dits " adaptatifs complexes " sont nés de l'étude du comportement de systèmes vivants pour tenter de modéliser des états de conscience artificielle.
Il est intéressant d'énumérer leurs caractéristiques essentielles qui comportent 4 propriétés et 3 mécanismes :

Propriété 1 : **agrégation** :
Il y a émergence d'agents complexes, constitués par l'agrégat d'agents de plus bas niveau ; ces macro-entités possèdent une signification propre qui n'aurait pas pu être prédite à partir de leurs composants élémentaires.

Propriété 2 : **non linéarité** :
Cette caractéristique provient de l'existence de plusieurs variables dont l'agrégat présente un comportement plus compliqué que la simple somme ou moyenne.

Mécanisme 1 : **repérage** :
C'est la capacité à marquer l'appartenance des agents à des familles hiérarchisées que l'on peut ainsi filtrer, spécialiser ou coordonner. Ce marquage est rémanent même si l'agent qui le porte est en continuelle évolution.

Propriété 3 : **effet démultiplicateur** :
Les flux au travers du réseau ne sont jamais constants ; ils se reconfigurent, se recyclent, voire s'éliminent d'eux-mêmes, en fonction de l'expérience accumulée dans le temps. La

capacité à marquer les agents permet d'envisager la sélection de ceux dont les interactions sont favorables au système et l'éradication de ceux qui provoquent des dysfonctionnements.

Propriété 4 : **diversité** :
La communauté des agents est en permanence renouvelée pour s'adapter au besoin sans pour autant générer des agents polyvalents et uniformes qui conduiraient le système sur la voie de l'équilibre et donc de la stagnation. Les agents doivent être raisonnablement diversifiés, aptes à la mise en concurrence et à la coopération pour la recherche d'un effet démultiplicateur et le recyclage des ressources.

Mécanisme 2 : **adaptation dynamique de la structure interne** :
Le système est capable de repérer des motifs répétitifs dans le flot d'entrée, d'auto-adapter sa structure interne pour faire face à l'évolution et d'anticiper les événements futurs. On distingue deux types de modèles internes : le " tacite " qui prescrit une action dans un but recherché implicite, et le " déclaré " qui rend compte explicitement des explorations de ses alternatives. Les deux existent souvent simultanément dans les systèmes complexes.

Mécanisme 3 : **auto-apprentissage** :
Les systèmes complexes sont capables de détecter dans une scène complexe les éléments déjà testés et expérimentés individuellement ; ils ont donc une aptitude à sélectionner et apprendre des éléments de comportement pour les réutiliser plus tard dans une grande variété de combinaisons, à la manière d'un jeu de mécano.

4.4 Clausewitz, la non-linéarité et l'imprédictibilité de la guerre

En dépit de nombreuses lectures, interprétations et controverses, l'œuvre maîtresse inachevée de Carl Von Clausewitz (1831), " De la guerre ", continue à intriguer ses exégètes en offrant une théorie de la guerre qui réfute les caractères mêmes d'une théorie : la simplification, la généralisation, la prédiction parmi d'autres.

Les admirateurs de " De la guerre " s'accordent à dire que jamais traité n'a décrit la complexité de la guerre avec plus de réalisme. Sa difficulté de compréhension, pourtant, suggère plusieurs explications. Clausewitz, qui révisait continuellement son travail, n'aurait pas eu le temps d'y intégrer l'état élaboré de ses réflexions au delà du chapitre 1 du livre 1. Une deuxième explication tient évidemment à la distorsion des interprétations engendrée par le recul du temps, et au défaut, généralisé chez les lecteurs, de " conscience historique ". Enfin, on peut penser que les désaccords proviennent moins de nos changements d'interprétation que de ceux que la guerre elle-même a connus.

Les aspects de " De la guerre " relatifs à la nature humaine, à l'incertitude, à la politique, aux calculs rationnels, sont éternellement valides. Tous les autres aspects de la guerre ont été profondément changés par la technologie et de façon irréversible. Notre réalité est qualitativement différente de celle de Clausewitz.

Mais certains termes et concepts nouveaux nous permettent de réviser notre lecture de Clausewitz : son œuvre est sous-tendue par une intuition très nette et convaincue du phénomène que nous qualifions aujourd'hui de " non-linéarité ". La non-linéarité est inhérente à chaque guerre ; conduire une guerre provoque la transformation de sa physionomie, dans un rapport qui ne peut être prédit. Clausewitz comprend que la recherche de solutions analytiques ne convient pas au problème de la guerre et que notre aptitude à prévoir le cours d'un conflit est très limitée. Il s'oppose d'ailleurs en cela à ses homologues contemporains Heinrich von Bulow et Antoine-Henri de Jomini. Cela explique la déception des analystes de " De la guerre ", à la recherche de solutions prédictives.

La guerre est-elle un phénomène non linéaire pour Clausewitz ?
Dans le chapitre 1 du livre 1, Clausewitz entraîne le lecteur dans trois descriptions de plus en plus sophistiquées, toutes très empreintes de non-linéarité.
L'interaction est inhérente à la guerre. Ce n'est pas une simple séquence des intentions et des actions de chaque camp, mais le système dessiné par des intentions mutuellement hostiles et des actions conséquentes et simultanées. Clausewitz l'illustre par l'image de lutteurs (" Zweikampf ") dont la position contournée des corps ne peut être obtenue sans l'application de contre-forces et de contre-poids.

La connaissance du contexte politique dans lequel se déroule un conflit ne suffit pas pour en déduire la réaction des protagonistes : il existe entre eux comme une masse de matériau inflammable qui peut produire une combustion aux effets complètement disproportionnés à leurs causes. La connaissance des paramètres quantifiables de la logistique et de l'armement ne suffit pas pour prédire le régime comportemental du système. Que la guerre soit un instrument de la politique ne signifie pas qu'il soit immuable, pas plus que ne l'est la politique elle-même. La guerre s'adapte en même temps que ses visées, lesquelles s'adaptent aux moyens choisis, lesquels modifient le cours de la guerre. La relation fins-moyens s'adapte en permanence.

Plus loin, Clausewitz définit la guerre comme étant une remarquable trinité composée : 1- de la force aveugle de la violence et de la haine, 2- du hasard et de la probabilité subis et générés par le commandant et son armée, 3- de la subordination de la guerre à la politique du gouvernement. Ces trois pôles sont trois variables interagissantes, comparables à trois aimants qui maintiennent en équilibre un objet. La démonstration confirme que la trajectoire d'un pendule placé entre trois aimants est imprédictible et impossible à reproduire à l'identique.
Ces métaphores montrent bien le parti pris de l'auteur d'abandonner la recherche de la simplicité et de la certitude analytique dans le domaine de la guerre. Il pressent que c'est un processus dynamique qui ne peut être séparé ni de son contexte ni du hasard, et qui doit donc s'accommoder de complexité et de probabilité.

La non-linéarité dans " De la guerre " se manifeste au travers de l'imprédictibilité :

- L'imprédictibilité due à l'interaction : Dans le chapitre 3 du livre 2, Clausewitz considère que l'étude de la guerre ne relève ni d'une science, ni d'un art, car elle ne s'applique ni à un objet inanimé, ni à l'esprit humain, mais à un objet animé qui réagit. De plus cette réaction n'est pas ponctuelle ; c'est une dynamique mettant en jeu des forces psychologiques dont les effets

n'ont pas la même résonance chez le vaincu et chez le vainqueur. Les règles ne sont pas les mêmes pour tous, comme au jeu d'échecs ; elles s'attachent même à être imprédictibles. La guerre peut être théorisée qualitativement et en termes généraux pour permettre une meilleure compréhension, mais pas avec le degré de détail qui permet la prédiction.

- L'imprédictibilité due à la " friction " : Pour Clausewitz, la " friction " dans la guerre est ubiquiste et endémique ; le premier sens qu'il donne à ce terme est celui utilisé couramment en physique et en thermodynamique ; il rend compte de la résistance physique, de la dissipation de chaleur accompagnant chaque action, et entraînant une perte d'énergie et de performance. Cette " friction " militaire peut être réduite par l'entraînement, la discipline, les inspections, … Le deuxième sens est celui lié au " brouillard " enveloppant l'information et qui engendre des délais, des distorsions et des pertes de signal utile.

- L'imprédictibilité due au hasard : Pour Clausewitz, aucune autre activité humaine n'est autant liée au hasard que celle de la guerre. L'approche probabiliste n'est pas recevable car les tirages ne sont pas équiprobables comme au jeu de dés. Clausewitz préfère d'ailleurs l'image du jeu de cartes où chaque joueur a le loisir d'étudier ses adversaires. Une deuxième forme du hasard est celle des macroeffets amplifiés et disproportionnés par rapport aux microcauses. Cette manifestation est en revanche plus fréquente dans la guerre où les causes sont souvent anciennes et imparfaitement connues. Enfin une troisième forme de hasard est due à l'aveuglement de l'esprit humain, inapte à comprendre l'univers dans sa globalité sauf à fractionner la complexité sur le modèle de la mécanique newtonienne.

Clausewitz ne soutient pourtant pas que la linéarité n'ait pas sa place dans la guerre. Elle y est présente mais reste une exception, comme dans le monde réel, qui doit donc être systématiquement assortie des conditions restrictives qui la bornent. Dans " De la guerre ", la linéarité est étroitement imbriquée dans un environnement général de non-linéarité. Même quand Clausewitz se réconcilie avec les analystes en préconisant l'attaque des centres de gravité de l'ennemi (" Schwerpunckt ") comme étant le cœur de son pouvoir et de sa motricité, il dépasse l'idée de l'attaque des forces proprement militaires pour englober aussi celles d'ordre moral et communautaire.

La guerre et la politique ne sont pas deux variables séquentielles parce que pouvoir et violence sont intrinsèquement dépendants. Il n'y aura jamais deux guerres identiques. De telles intuitions ont pu souvent déconcerter les lecteurs de " De la guerre ". Le corpus constitué aujourd'hui autour des phénomènes non-linéaires permet à ceux qui veulent atteindre à une meilleure compréhension de la guerre, de le redécouvrir avec profit .

5. Application à la prise de décision stratégique

5.1 Introduction

La prise en compte du concept de RMA, comme l'évidence d'un accroissement de la complexité des environnements dans lequel l'action militaire peut être amenée à s'exercer ne doit pas nous détourner de la réflexion sur ce qui nous sert à penser la stratégie. Ainsi on est conduit à se préoccuper de l'organisation et du développement des outils appropriés, qu'on désignera par " cadres de référence " et qui prennent en compte les nouvelles situations et les concepts qui s'y rattachent.

5.2 L'environnement stratégique

Le but de la stratégie de sécurité nationale est de fixer et d'atteindre des objectifs qui, dans le long terme, assureront un haut niveau de sécurité à la Nation et à ses citoyens. Elle s'inscrit donc dans un processus itératif et permanent qui balaye l'environnement stratégique, en élabore l'évaluation, conçoit des objectifs et formule des plans à long terme pour les atteindre.

Les questions que l'on doit se poser sur l'environnement stratégique sont les suivantes :

- Qui sont nos principaux concurrents ?
- Quelle est la compétitivité de notre organisation à long terme ? Pourquoi ?
- Qu'est-ce qui peut favoriser notre compétitivité à long terme ou, au contraire, lui être défavorable ?
- Que contiennent nos plans à long terme pour contourner les obstacles et exploiter nos avantages ?
- Peut-on anticiper des problèmes majeurs de ressources pour le futur ?
- Peut-on prévoir des menaces vitales pour le long terme ?

Cette revue stratégique pour les vingt ans à venir est extraordinairement difficile à mener. Elle nécessite un certain sens de l'histoire qui permette l'élaboration d'un cadre de référence (voir §5.3 infra) dont la pertinence historique devra être en permanence testée et ajustée par rétroaction. L'établissement d'un ordre nouveau recherche un accroissement coordonné du bien-être de la Nation avec celui de la communauté mondiale.

Les décisions stratégiques ont des conséquences à long terme et gagent d'importantes ressources. Elles couvrent de longues périodes et coûtent cher. Elles s'inscrivent dans le contexte de l'état final recherché mais aussi d'éventuels autres états non recherchés mais générés par le mode d'action. Une option politique peut déclencher une réaction en chaîne de causes et d'effets étalée sur plusieurs années, dont les effets indirects n'avaient pas été prévus.

Entre la conception traditionnelle de la stratégie des vainqueurs de la Première guerre mondiale, imposant de lourdes sanctions aux vaincus et celle déployée par Marshall pour le règlement de la Deuxième guerre mondiale, il y a une évolution qualitative évidente.
C'est d'autant plus le cas que la décision implique des cultures différentes, des systèmes complexes ou très dynamiques.

Dans le domaine économique en particulier, l'équilibre du système monétaire est si délicat et sa sensibilité aux pressions inflationnistes est telle qu'il semble que toute action soit dangereuse et que l'immobilité soit de mise. Prenons l'exemple de la taxation des gains en capital. Une taxation

élevée pourrait décourager les cessions d'investissements en vue de faire du bénéfice, donc ne serait pas favorable à la réduction des déficits. On pourrait supposer, au contraire, qu'une baisse de la taxation favorise la vente des actions et donc fasse chuter le marché. Mais ce raisonnement est-il plus fondé ?

Il y a de nombreuses barrières à la pertinence des décisions d'ordre stratégique. Certaines sont d'ordre humain ; elles incluent le jugement subjectif du stratège et ses enjeux personnels : peur de l'échec, risques liés à la carrière, perte de popularité…
D'autres sont liées à l'environnement :

- il est dynamique voire **volatile ;**
- il est **incertain** voire impossible à prédire ;
- il est **complexe** par la diversité des problèmes à appréhender.
- il est **ambigu** par l'hétérogénéité et la multiplicité des facteurs en entrée du système, encore compliqués par le contexte culturel.

Nous désignerons par l'acronyme **VICA** les environnements caractérisés par ces quatre aspects : volatilité, incertitude, complexité et ambiguïté.

La prise en compte d'un tel environnement n'est donc pas à la portée d'un individu isolé, d'autant plus que la décision devra souvent s'accommoder d'une situation de crise ou de stress.
En effet toutes les sociétés et organisations rivalisent pour l'accroissement de leur richesse et de leur pouvoir. Même quand une alliance comme l'OTAN se noue, c'est bien pour obtenir un avantage compétitif par rapport à une autre alliance. Le monde est par nature une arène où s'affrontent des intérêts contradictoires pour l'allocation de ressources limitées. Sur le champ de bataille, c'est l'avantage en terme de supériorité et de pérennité technologique qui est en jeu, au delà de la destruction des systèmes d'armes en présence. La gageure est de comprendre le sens du changement au plus tôt et de bâtir la stratégie adaptée dans un délai compatible avec la réalisation et le maintien des avantages compétitifs visés. De plus, ceux-ci sont souvent obtenus par surprise et au terme de manœuvres dilatoires, ce qui ne fait que confirmer l'incertitude de l'environnement " VICA ".

Les marchandages et plaidoyers des différents partenaires donnent à la décision la forme d'une négociation pour la recherche d'objectifs communs par des chemins acceptables par tous. Sans ce minimum de consensus, tout espoir d'effort collectif est illusoire. La démarche doit assurer que tous les points de vue en compétition aient été entendus et doit établir entre eux les priorités.

Les décisions du niveau opérationnel peuvent encore être le fait d'un seul individu. Plus on se situe haut dans la hiérarchie, plus le travail s'effectue de façon collégiale et doit prendre en compte la disparité des idéologies, des personnalités et des organisations impliquées. La négociation et le compromis sont la norme. De plus ces décisions ne sont jamais finales et doivent être réévaluées de façon récurrente. Enfin, elles requièrent une plus grande quantité d'informations, aussi bien qualitatives que quantitatives et doivent donc utiliser des techniques de gestion sophistiquées.

L'écueil le plus évident d'une approche par la négociation est le nivellement de la réflexion par le plus petit dénominateur commun, dû aux rivalités de pouvoir. L'art de la décision stratégique est

de fédérer les intérêts en compétition dans des objectifs communs contextuels et non plus structurels.

Pour y parvenir, les atouts du décideur seront de développer les aptitudes suivantes :

- aptitude à naviguer dans des contextes complexes : les problèmes sont souvent mal définis, inédits ou impliquant des organisations complexes.
- aptitude à un management protéiforme apte à s'adapter aux différents systèmes de valeurs des acteurs internes ou externes à l'organisation.
- aptitude à s'adapter à l'environnement : le dirigeant doit analyser le lien de son organisation avec l'environnement, formuler, mettre en œuvre et évaluer la politique d'adaptation de l'un à l'autre.
- aptitude à un leadership charismatique pour motiver l'action collective.

5.3 Les organisations auto-adaptatives

La survie d'une organisation dépend de son aptitude à capter l'environnement, à l'analyser et à interargir avec lui.
L'organisation est un assemblage de composants connexes agissant dans un but commun et assurant le contrôle cybernétique du système ainsi constitué : entrées, processus de transformation, sorties, boucle de rééquilibrage du système.
Mais l'organisation est un système ouvert sur son environnement, confronté aux tactiques de la compétition, aux innovations technologiques, aux contraintes législatives et économiques, aux évolutions sociales et éthiques. Elle doit réagir aux menaces et aux opportunités.

Face à un flot de données et à un environnement de type VICA, le dirigeant a trop souvent le réflexe de solliciter ses compétences personnelles d'analyse et d'interprétation, toujours suspectes de partis pris. Il faut donc développer une fonction d'interprétation de l'environnement pour une prise de décision stratégique meilleure et plus rapide.

Développer ce concept conduit à promouvoir des organisations dites " auto-adaptatives ", prônant l'amélioration de la performance par le retour d'expérience. Elles se caractérisent par deux aptitudes :

- leur capacité à auditer l'efficacité de leurs procédures internes par rapport aux exigences de l'évolution externe et dans les limites de leur métier de base : d'où la nécessité d'acquérir une parfaite connaissance des compétences, d'analyser les procédures et de rechercher leurs plus-values, de montrer la contribution de chaque membre de l'organisation à la " vision d'entreprise ".

- leur capacité à cumuler des expériences aptes à répondre quantitativement et qualitativement à des changements de l'environnement. Pour cela, les dirigeants doivent institutionnaliser l'acquisition de connaissance comme un processus permanent et non pas comme une réponse ponctuelle. Toutes les sources de connaissance peuvent être exploitées : publications, analyses de produits, programmes de recherche, projets de démonstration, revues de performance...

L'essentiel est que la phase d'acquisition de connaissance soit suivie d'une phase de distribution de l'information. Les dirigeants ont une responsabilité capitale dans la facilitation de cette circulation de l'information entre les différentes divisions de l'organisation. L'investissement dans ce domaine peut porter sur le capital humain par la formation à ce type de compétences, mais il peut aussi prendre la forme d'un système référentiel à la taille de l'organisation, facilitant l'accès et le partage de l'information.

Ce système d'information suppose la mise au point d'une procédure de recueil de l'expérience :

- pour l'enregistrement des expériences organisationnelles pertinentes en matière d'objectifs stratégiques,
- la recherche d'expériences organisationnelles,
- l'application de ces expériences à la prise de décision stratégique.

Ce processus est souvent problématique dans les organisations, fortement dépendantes de la volonté et des capacités individuelles de leurs membres, et donc vulnérables au renouvellement du personnel. C'est au dirigeant de formaliser ce processus et d'expliquer que la performance de cette mémoire organisationnelle, à l'instar de celle des humains, s'améliore quand elle est régulièrement exploitée.

5.4 Les cadres de référence comme outil de décodage de l'environnement

La doctrine du Pentagone semble bien en être restée à l'emploi d'une puissance militaire massive malgré la disparition de l'Union Soviétique alors que toutes les disciplines militaires expérimentent de nouvelles organisations et méthodes " high-tech " de guerre.

Son cadre de référence n'a pas encore été adapté au changement du contexte géostratégique mondial. Constituer un cadre de référence consiste, à partir d'une collection de données disparates décrivant une situation problématique, à établir leurs liens logiques et formuler le problème en évaluant toute sa signification et son étendue. Un cadre est une sorte de décodeur qui permet à ses utilisateurs de comprendre une réalité qui, sans lui, n'aurait pas de cohérence. Il présente l'avantage d'être un guide de compréhension commun à tous, qui peut aussi être imposé ou délibérément appris. Certains cadres nous sont familiers : l'âge, le milieu professionnel, les codes de conduite dictés par la religion ou l'éthique… Il est évident qu'un cadre représente la perception de son auteur, avec les limites et les influences de son expérience et de sa culture. Un cadre établi pour la même collection de données par une autre autorité serait tout à fait différent.

Dans leur livre " Reframing Organizations ", Bolman et Deal proposent quatre cadres pré-fabriqués et prêts à l'usage : le cadre structurel, le cadre politique, le cadre des relations humaines et le cadre symbolique.

Le cadre **structurel** montre comment une organisation doit être bâtie pour atteindre ses objectifs : responsabilités, connexions, mécanismes…

Le cadre **politique** décrit la composition sociale de l'organisation , la diversité des valeurs et des comportements pour chaque communauté d'intérêts, la rivalité pour le partage des ressources, le rôle de la négociation.

Le cadre **des relations humaines** insiste sur la réciprocité des échanges entre les employés et l'organisation qui les emploient, pour satisfaire les attentes des deux parties sans excès d'exigence, ni paternalisme. La pyramide à cinq degrés du psychologue Abraham Maslow rappelle, qu'outre les besoins primaires, physiologiques et de sécurité, l'organisation sociale ne doit pas négliger les besoins plus élaborés que sont le désir d'appartenance au groupe, la soif d'estime, individuelle et collective, et enfin le besoin de développement personnel.

Le cadre **symbolique** s'attache à traduire le sens des événements à l'aide de symboles empruntés à la culture de l'organisation dont la perception commune sert à réduire l'incertitude et l'ambiguïté des événements, à faciliter la prédiction et la direction.

L'un de ces cadres peut être plus adapté que les autres pour l'étude de certains problèmes particuliers ; mais il est en général recommandé d'appliquer successivement l'ensemble de ces cadres de façon à obtenir le cadre de référence optimal.
Le stratège sera donc tour à tour architecte (cadre structurel), catalyseur (cadre des relations humaines), avocat (cadre symbolique), prophète et poète (cadre symbolique).

6 Conclusion

Inéluctablement tous les systèmes militaires seront amenés à intégrer des systèmes d'information plus ou moins sophistiqués. Cette évolution fait naître de nouvelles possibilités mais aussi de nouvelles menaces, difficiles à cerner. L'évolution technologique très rapide et le caractère non linéaire des réponses aux actions menées conduisent à rechercher la dominance de l'adversaire par l'adaptation ou l'évolution, plutôt que par la maîtrise des aléas d'un univers dont la prédictiblité est faible. L'adaptation requiert d'être innovant, mais avant tout d'être diversifié dans nos possibilités offensives et défensives. L'évolution et l'adaptation des systèmes d'armes devraient, dans la perspective d'une approche européenne de la Défense, trouver les réponses politiques et financières appropriées, dans un cadre de référence coopératif.

7 Bibliographie

Strategy and the Revolution in Military Affairs: From Theory to Policy
Steven Metz and James Kievit
Strategic Studies Institute, US Army War College, Carlisle Barracks,
Pennsylvania 17013-5050, 27June 1995

What is Information Warfare?

Dr Martin C. Libicki
NDU, ACIS Paper 3, August 1995
Washington DC: Institute for National Strategic Studies, 1995

Defensive Information Warfare
DR. David S. ALBERTS
Director, Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS)
National Defense University, NDU Press Book, August 1996

Information Warfare and Deterrence
by Gary F. Wheatley and Richard E. Hayes.
NDU Press Book December 1996

Information Warfare and International Law
Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo
National Defense University Press

Coping with the bounds : speculations on nonlinearity in military affairs
Tom Czerwinski
Document NDU

Clausewitz, Nonlinearity and the Unpredictability of War
Alan D. Beyerchen
International Security, 17:3 (Winter, 1992), pp. 59-90.

Command in War
Martin Van Creveld
Harvard University Press, Cambridge, MA, 1987

Command and Control at the Crossroads
Thomas J. Czerwinski
Parameters, Autumn 1996: 121-132.]

Information Dominance
Dr. Martin C. Libicki
Strategic Forum, Number 132, November 1997

Strategic Leadership and Decision Making,
text developed by the Industrial College of the Armed Forces

War and Anti-War: Survival at the Dawn of the 21st Century.
Toffler, Alvin and Heidi.
Boston: Little, Brown, 1993

Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advise.
George, Alexander L.,

Boulder: Westview Press, 1980.

Reframing Organizations: Artistry, Choice, and Leadership.
Bolman, L. G., and T.E. Deal. 1991.
San Francisco, CA: Jossey-Bass Publishers.

Comprendre la stratégie
Contre-amiral (CR) Jean-Marie MATHEY
Ed. Economica, 1995

Traité de stratégie
Hervé Couteau-Bégarie
Economica, 2ème Edition 1999

La stratégie de l'action
Général André BEAUFRE
Editions de l'Aube