COLLEGE INTERARMEES

DE DEFENSE

EPO N° B05

ETUDE PARTICULIÈRE À OPTION

FORCES SPÉCIALES ET GUERRE DE L'INFORMATION

SOUS LA DIRECTION DE L'ICA FONTENILLE

MEMBRE DU COMITÉ **CDT PICHENE** (AIR)
MEMBRE DU COMITÉ **LCL MAILFERT** (AIR)
MEMBRE DU COMITÉ **LTCDR AMEYE** (ROYAL NAVY)
MEMBRE DU COMITÉ **CBA BEVILLARD** (TERRE)
MEMBRE DU COMITÉ **CBA VINCENT** (TERRE)

4° PROMOTION 1996 - 1997

TABLE DES MATIERES

FORCES SPECIALES
ET
GUERRE DE L'INFORMATION

INTRODUCTION

For decades to come...
many of the best military minds
will be assigned to the task
of further defining the components of knowledge warfare,
identifying their complex inter-relationship
and building the "knowledge models"
that yield strategic options.

Alvin & Heidi TOFFLER,
War and Anti-war: Survival at the Dawn of the twenty-first Century.

Car la guerre de l'information n'est manifestement pas une guerre comme les autres... Certains ont affirmé qu'elle constituait la guerre du troisième type, après un type de guerre qualifié de "guerre agraire" et un autre de "guerre industrielle".

Mais la guerre de l'information comporte d'autres spécificités qui n'ont pas grand-chose à faire avec la guerre dans le sens classique de

son acception, autrement dit le conflit armé. Cette guerre d'un type nouveau doit-elle être l'apanage des forces spéciales? Rien n'est moins sûr, et les différents aspects de la guerre de l'information ont des spécificités telles qu'une analyse est nécessaire pour définir lesquels sont déjà pris en compte dans nos concepts de guerre conventionnels, et lesquels doivent nécessiter des efforts particuliers de la part des forces dites classiques ou de la part des forces dites spéciales.

La guerre de l'information a déjà été le sujet de nombreux ouvrages. Elle englobe en réalité plusieurs disciplines recouvrant des domaines aussi divers et éloignés que la guerre électronique peut l'être de la guerre psychologique. Ces deux concepts, eux-mêmes génériques, font pourtant partie des domaines de la guerre de l'information.

L'étude menée dans les pages qui suivent a pour objet de tenter de définir les rôles que peuvent avoir les forces spéciales dans les différents concepts que recouvre la guerre de l'information, et parallèlement, de définir ce qui relève spécifiquement des autres composantes de forces, c'est à dire les forces classiques, qui ont déjà dans leur panel de missions des disciplines directement liées à la guerre de l'information.

Enfin, dans une optique plus orientée vers la prospection mais néanmoins complémentaire, cette étude tentera de montrer dans quels domaines relevant de la guerre de l'information les forces spéciales peuvent voir mis à leur portée des champs d'engagement nouveaux.

Le cadre de cette étude particulière à option a été délibérément restreint aux forces spéciales françaises. Cependant, les missions des forces spéciales américaines et britanniques, avec leurs doctrines d'emploi, ont également fait l'objet de recherches dans le cadre de cette étude.

Ces recherches ont servi à titre d'information, mais aussi à titre de comparaison avec des concepts d'emploi déjà existants. Elles ont aussi permis de fournir des orientations possibles pour nos forces spéciales nationales, tout en essayant d'éviter de réinventer des champs d'engagement qui auraient déjà fait l'objet d'études, de développement, ou d'améliorations dans le cadre de concepts non envisagés en France, ou utilisés dans un passé récent puis abandonnés, mais qui pourraient ou devraient être réhabilités.

Il est apparu au cours des recherches menées dans le cadre de cette étude, que les doctrines et concepts d'emploi des forces spéciales anglo-saxonnes étaient beaucoup plus accessibles. Elles ont offert une intéressante ouverture aux novices que nous étions en la matière. Du côté national l'accès à une information écrite est resté très restreint. Fort heureusement, ce manque de données a été compensé par des contacts directs et fructueux avec des responsables des forces spéciales.

Cette étude s'articule en trois parties. Dans un premier temps ont été passés en revue les différents aspects que peut revêtir la guerre de l'information, afin de fournir un support à la réflexion, suffisamment exhaustif et détaillé pour ne laisser dans l'ombre aucun domaine. Dans un deuxième temps, les différents rôles possibles des forces spéciales ont été déclinés à la lumière de ces différents domaines, pour définir ou expliciter leurs attributions dans les disciplines qui leur sont propres. Enfin, dans une troisième partie, les rôles des autres composantes de forces dans certains domaines de la guerre de l'information ont permis de compléter les attributaires des différentes disciplines. Et, en orientant finalement la fin de cette étude vers des perspectives, les champs d'engagements nouveaux pour les forces spéciales françaises ont été mis en évidence, éventuellement à la lumière des concepts d'emploi des *special forces* anglo-saxonnes.

Note: un certain nombre de sigles anglo-saxons a été utilisé, pour dénommer en particulier les différentes disciplines de la guerre de l'information, afin de conserver une standardisation avec la terminologie en vigueur.

1 - LA GUERRE DE L'INFORMATION

Le concept de guerre de l'information est suffisamment récent pour que l'on s'attarde à lui donner une définition. Plusieurs spécialistes l'ont fait, américains pour la plupart, en tentant de regrouper de la manière la plus exhaustive possible tous les modes d'action envisageables au sein d'un même catalogue. Cette méthode a conduit le plus souvent à y faire figurer des actions ou des modes d'actions encore mal définis ou dont la compréhension est réservée à quelques initiés. De plus, certaines des fonctions ne relèvent pas du domaine strictement militaire ou ne font pas partie de la stratégie française, en particulier dans le domaine économique.

L'approche de Stephen Hardy (Journal of Electronic Defense, 1996) est la suivante:

« Une arme dite intelligente devient ignorante lorsqu'elle est privée d'informations sur sa cible, et stupide lorsqu'elle dispose d'informations erronées. »

Sur le fondement de cette constatation, il propose une première définition de la guerre de l'information: science permettant d'éviter sa propre ignorance tout en rendant l'adversaire aussi stupide que possible.

En 1992, la définition suivante a été adoptée par le Secrétariat à la Défense américain, branche Command, Control, Communication and Intelligence (OASD/C3I):

« La guerre de l'information est l'ensemble des actions visant à procurer la supériorité en matière d'information, en agissant:

- sur les informations,
- sur les processus à base d'information,
- sur les systèmes d'information de l'ennemi,

tout en protégeant ses propres informations, processus et systèmes. »

Martin C. Libicki a, lui, examiné les fondements de ce nouveau concept dans un essai paru sous le titre "What is Information Warfare?"[1], et proposé sept fonctions fondamentales:

COMMAND AND CONTROL WARFARE (C^2W)
INTELLIGENCE BASED WARFARE (IBW)
ELECTRONIC WARFARE (EW)
PSYCHOLOGICAL WARFARE (PSYW)
HACKER WARFARE
ECONOMIC INFORMATION WARFARE (EIW)
CYBERWARFARE

[1] "What is Information Warfare?", Martin C.Libicki, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995.

1.1 - COMMAND AND CONTROL WARFARE (C^2W)

C'est l'ensemble des opérations qui visent à détruire, ou au moins neutraliser, les moyens de commandement et de contrôle de l'ennemi, que ce soit au niveau de la tête (*antihead*), ou de ses réseaux (*antineck*).

Le champ d'action s'étend de la capture ou de la suppression de la tête elle-même (tireurs d'élite), à la destruction de son poste de commandement et de ses moyens de contrôle grâce aux armements de précision à guidage terminal. Les coupures des réseaux de communication et des lignes de ravitaillement des PC font également partie de cette catégorie.

Cependant, ce sont non seulement les systèmes de commandement plus que les chefs eux-mêmes qui seront visés; les technologies de redondance et la dispersion font que l'on peut estimer que les centres de commandement seront encore plus protégés dans l'avenir. Le maillage des liaisons s'étend également davantage et les nouvelles techniques permettent de mener des opérations avec un minimum de flux d'échange de données.

1.2 - INTELLIGENCE BASED WARFARE (IBW)

Le combat fondé sur les capacités de renseignement fait appel à la conception et à la protection de systèmes capables de rechercher le renseignement pour une parfaite connaissance du champ de bataille.

La baisse des coûts de l'électronique au service du renseignement permet d'optimiser plus encore le développement des systèmes de *targetting*.

La furtivité mise à part, les moyens classiques de se soustraire à ce mode d'action, comme le camouflage, deviennent inefficaces.

1.3 - ELECTRONIC WARFARE (EW)

La guerre électronique recouvre un large spectre de types d'actions, qui vont de la guerre antiradar à la guerre anti-communications et à la cryptographie.

La destruction des radars de surveillance ou de conduite de tir par des missiles antiradar, et le brouillage continu sur toute une zone de combat sont des actions militaires désormais courantes. Cependant émission et réception seront de plus en plus séparées sur le terrain: la survivabilité de ces systèmes bipolaires sera supérieure à celle des systèmes monolithiques.

Du fait de l'étalement du spectre, de l'évasion de fréquence, des antennes directionnelles très précises, les communications passeront. Donc l'efficacité des actions de guerre électronique dans ce secteur sera de plus en plus limitée.

En matière de cryptographie les nouvelles techniques de chiffrement donnent l'avantage à ceux qui font les codes plutôt qu'à ceux qui cherchent à les casser.

1.4 - PSYCHOLOGICAL WARFARE (PSYW)

Les actions de guerre psychologique visent à utiliser l'information comme un moyen de changer les modes de pensée de l'ennemi. Ce moyen peut également être appliqué à nos propres modes de pensée amis. Il doit aussi permettre de convaincre ceux qui n'ont pas (encore) choisi leur camp.

Elles sont dirigées soit vers la nation, soit vers les troupes, soit vers le commandement.

Par exemple, le bombardement intensif des positions irakiennes avant l'offensive terrestre a joué un rôle décisif au plan psychologique.

Les images de CNN montrant le corps dénudé d'un pilote d'hélicoptère traîné par le véhicule d'une milice en Somalie ont transformé l'opinion américaine. On peut estimer que le général Farah Aidid a ainsi gagné la guerre de l'information.

Dirigées vers les troupes, ces actions sont destinées à décourager, dissuader, démobiliser. Elles sont aujourd'hui de plus en plus faciles à mettre en oeuvre grâce au développement des moyens de communication, par satellites ou par réseaux herziens.

Cependant l'efficacité des manoeuvres de déception de la part du commandement reste aujourd'hui encore difficile à apprécier.

Un dernier secteur de la guerre psychologique, mais cette fois-ci à très grande échelle est ce que l'on pourrait nommer la guerre des cultures ou *Kulturkampf.* Ce mode d'action a un impact destructeur sur les cultures et sur les individus ou est ressenti comme tel... quand il est déjà tard pour réagir. Par exemple, les importations américaines (hamburger, jeans, films hollywoodiens) sont souvent considérées en France, pays attaché à son patrimoine culturel, comme des vecteurs de standardisation du comportement.

1.5 - HACKER WARFARE

C'est l'ensemble des opérations de piratage informatique (pénétration des systèmes, piratage des fichiers, des banques de données, virus informatiques) par des spécialistes appelés *hackers*.

Les sociétés et les systèmes économiques sont très vulnérables par leur dépendance croissante aux réseaux informatiques, mais les systèmes peuvent être sécurisés par une protection efficace.

Lors d'un symposium tenu à Washington le 6 juin 1995, le directeur du C4 (*Command, Control, Commmunication and Computers*) à l'état-major des armées américaines, a chiffré à un milliard de dollars les

budgets nécessaires à la protection des ordinateurs militaires américains pour la seule année 1996...

1.6 - ECONOMIC INFORMATION WARFARE (EIW)

Ce domaine, qui fait partie intégrante de la guerre économique que se livrent les pays sur un nouveau champ de bataille, fait appel à toutes les techniques en matière de renseignement, d'informatique, de protection du secret industriel ou technologique. L'espionnage économique est devenu un objectif stratégique. La capacité de connaître avant les autres les évolutions d'un marché ou les initiatives d'un concurrent se traduit très rapidement par une augmentation du chiffre d'affaires, ou au contraire par des pertes abyssales.

Cependant, peu de pays sont à l'heure actuelle très dépendants de flux d'information importants. Certes, le commerce et la guerre impliquent tous deux la compétition, mais le commerce n'est pas toujours la guerre.

1.7 - CYBERWARFARE

Pouvant être traduit par guerre dans le cyberespace[2], ce concept repose sur les possibilités qu'offrent désormais les ordinateurs et les réseaux modernes de communication comme l'Internet. On peut y espionner, y dérober des informations, y violer l'intimité des citoyens et y dissimuler des entreprises criminelles.

Quatre types d'actions peuvent être distingués: le terrorisme informatique, le piratage informatique transparent, la guerre par simulateur interposé et la guerre dite de Gibson (*Gibson warfare*).

Le terrorisme informatique a pour cibles les banques de données personnelles, les fichiers contenant des informations à caractère privé; l'objectif final peut être le chantage, le harcèlement ou d'autres formes de pression.

Le piratage informatique transparent est également dénommé attaque sémantique. A la différence du piratage classique qui provoque des pannes, un système victime d'une attaque sémantique fonctionne apparemment correctement mais fournira des réponses différentes de la réalité en jouant sur la sémantique des mots. Les cibles privilégiées sont tous les systèmes assistés par ordinateur pour la prise de décision et utilisant des informations en provenance de capteurs de toute nature.

La guerre par simulateur interposé est un concept qui passionne les Américains. Il est fondé sur la volonté et la possibilité d'éviter le combat et le sang versé en prouvant à l'ennemi qu'il ne peut que perdre, simulation à l'appui. Le côté attractif de la technologie de simulation aujourd'hui réside dans ses capacités de présenter le champ de bataille avec le point de vue de tous les acteurs du théâtre. Cependant, ce type

[2]"Guerres dans le Cyberespace", Jean Guisnel, Editions Découvertes, 1995.

d'affrontement n'est pas la panacée et paraît même n'avoir de pertinence qu'entre adversaires de niveaux technologiques comparables.

La dénomination *Gibson warfare* provient du nom de William Gibson, auteur de "Neuromancer", ouvrage de science-fiction dans lequel les bons et les méchants sont des personnages virtuels capables de se battre à l'intérieur des systèmes informatiques, à l'image des héros du film de Walt Disney "TRON"... Même si ce concept peut paraître ésotérique ou réservé à quelques surfers audacieux, et ne pas mettre en péril les intérêts d'une nation, c'est une des facettes de la guerre de l'information du futur.

2 - ROLE DES FORCES SPECIALES DANS LA GUERRE DE L'INFORMATION

2.1 - ORGANISATION DES FORCES SPÉCIALES EN FRANCE

Ces forces interarmées sont structurées en 3 cercles :

a) Le premier cercle:

Il est composé d'unités dépendant du COS en permanence.

Ces unités sont:

- 1° RPIMa: 1er Régiment Parachutiste d'Infanterie de Marine, (Armée de Terre),
- Commandos marines: 4 classiques + 1 spécialisé (Marine Nationale),
- CPA 10: Commandos Parachutistes de l'air (Armée de l'air),
- DOS/H: Division Opérations Spéciales d'Hélicoptères (hélicoptères de manoeuvre de type Super Puma pour les opérations de CSAR à Aix-les-Milles, ainsi que les équipages sélectionnés),
- DOS/ATT: Division Opérations Spéciales / Avions de Transport Tactique, actuellement équipée d'un C 160 rénové + un second en commande (Armée de l'air),
- EOS: Escadrille des Opérations Spéciales appartenant au 4° RHCM de Pau (ALAT),
- LOG: éléments logistiques internes,
- état-major (création été 1997).

b) Le deuxième cercle:

Il se compose d'unités aux structures et aux missions proches de celles des opérations spéciales, qui sont affectées occasionnellement au COS en fonction de ses besoins.

- GCP: Groupements Commandos Parachutistes (ex CRAPS) en provenance des effectifs organiques des régiments parachutistes de la 11ème Division Parachutiste,

- 13° RDP: Régiment de Dragon Parachutiste (Direction du Renseignement Militaire).

c) Le troisième cercle:

Il s'agit des directions et unités aux missions propres, qui peuvent participer ponctuellement avec une partie de leurs moyens aux missions dévolues aux opérations spéciales.

- GSIGN: Groupement de Sécurité et d'Intervention de la Gendarmerie Nationale constitué par :
  - l'EPIGN: Escadron Parachutiste d'Intervention de la Gendarmerie Nationale,
  - et le GIGN: Groupement d'Intervention de la Gendarmerie Nationale,
- DRM: Direction du Renseignement Militaire,
- DGSE: Direction Générale de Sécurité Extérieure,
- DGA: Direction Générale de l'Armement.

Cadre d'emploi:

	RENSEIGNEMENT		ACTION
ETRANGER, renseignement fermé*	**DGSE**	⇐COS⇒	**DGSE**
ETRANGER, renseignement ouvert*	**DRM**	⇐COS⇒	**DRM**
TERRITOIRE NATIONAL	**GSIGN**	⇐COS⇒	**GSIGN**

Le COS interagit sur tous les théâtres, avec la DGSE, la DRM ou le GSIGN, selon l'organisme employé.

* On parle de renseignement fermé ou ouvert, selon le degré de dissimulation dont est affectée l'opération (mise en place ou non d'un paravent, personnels en civil ou en uniforme...).

2.2 - LA COMMUNICATION OPÉRATIONNELLE SPÉCIALE (COSPE) DES FORCES SPÉCIALES FRANÇAISES

2.2.1 - Pourquoi l'élaboration d'une COSPE ?

Cette nouveauté est relative étant donné le précédent historique.

Sans remonter trop loin dans l'histoire, on peut voir dans l'expédition de Bonaparte en Egypte (fin du XVIII^{ème} siècle), une opération

militaire innovatrice compte tenu de l'accompagnement d'un contingent de scientifiques et d'hommes de lettres ayant reçu pour mission d'analyser, étudier et comprendre un nouveau milieu dans tous ses domaines (historique, géographique, économique, politique, humain, etc.). Ce contingent a largement influencé en bien la perception de la France par les autochtones, contrebalançant ainsi les effets mitigés de la campagne militaire.

La communication spéciale a été développée et employée avec succès par les Britanniques pendant la guerre des Boers (fin du XIX^{ème} siècle) en Afrique du Sud, ainsi que pendant leurs campagnes de décolonisation (première moitié du XX^{ème} siècle, notamment en Birmanie avec le Major Wingate et ses célèbres *Chindits*).

En France, après la défaite de Dien Bien Phu, l'état-major des armées, profitant de l'expérience acquise par toute une génération d'officiers, appliqua des méthodes de communications spéciales au cours des "opérations de maintien de l'ordre" en Afrique du Nord de 1954 à 1962.

Une instruction provisoire sur l'emploi de l'arme psychologique (TTA 117) fut approuvée par le Chef d'état-major général des Forces armées en juillet 1957.

Le contexte médiatique peu propice et les conséquences politiques qui firent suite à la décolonisation de l'Algérie en 1962, ont, depuis, fait abandonner ce savoir-faire (le TTA 117 est censé avoir été détruit en 1988).

Cependant, la multiplication des conflits dits de "gestion de crise", faisant intervenir les forces armées dans des contextes complexes où les facteurs politiques, économiques, sociaux et humains ont des rôles décisifs, a montré les limites des forces classiques pour remplir ces nouvelles missions.

La France a été impliquée dans certaines opérations (au Tchad et au Liban, en particulier) qui ont montré, par leur contexte, l'insuffisance d'un traitement uniquement réalisé par des moyens militaires. Ce phénomène s'est accru avec l'intervention en ex-Yougoslavie et dans la zone d'influence française en Afrique (Rwanda, RCA...).

Grâce à la communication opérationnelle spéciale, le COS offre au CEMA des solutions d'alternative diverses et souples. On peut ainsi élargir les capacités de traitement avancé d'un théâtre en menant simultanément des actions armées et des actions d'influence et en s'attachant à les combiner.

Les américains mettent déjà ce concept en pratique de façon très actuelle, car USSOCOM (United States Special Operations Command) mène une action "psyops" au Rwanda depuis avril 1995, s'inscrivant ainsi en amont de la possibilité d'un conflit de basse intensité et dans une logique définie par leur commandement.

Face aux rumeurs et aux désinformations diverses et agressives menées à l'encontre de nos forces engagées, cette solution d'alternative douce permet donc de mieux prendre en compte une situation locale et d'offrir ainsi des capacités d'actions graduées avant un engagement armé possible.

2.2.2 - Concept de la COSPE

a) Généralités:

Les actions d'influence menées le plus en amont possible d'une opération extérieure s'intègrent dans la logique de traitement avancé menée par le Commandement des Opérations Spéciales sur le terrain. Elles permettent de participer à:

- une inversion du processus de crise,
- une meilleure gestion de la crise,
- une accélération de la sortie de crise.

b) Définition:

Les actions de communication opérationnelle spéciale sont des actions d'influence capables de modifier l'opinion, les sentiments et le comportement de cibles choisies (population, belligérants, ressortissants) et, ainsi, d'orienter l'environnement humain dans un sens favorable à la réalisation des objectifs d'une opération en cours.

c) Buts:

La cellule COSPE contribue à la légitimation de l'action entreprise tout en oeuvrant pour:

- obtenir la neutralité des populations et de certains belligérants et, au mieux, leur adhésion aux finalités poursuivies par les forces engagées,
- conduire les opérations nécessaires pour réduire les capacités et le moral de l'adversaire.

Ainsi les objectifs principaux de la communication opérationnelle spéciale sont les suivants:

Vis-à-vis de la population:

- la rassurer en lui faisant connaître les raisons de notre présence,
- légitimer auprès d'elle l'action entreprise par nos forces ou par des partis alliés,
- obtenir sa neutralité voire son adhésion,
- la désolidariser des mouvements extrémistes en la préservant de toute forme de déstabilisation.

Vis-à-vis des belligérants:

- lutter contre la désinformation,
- atténuer, voire décourager, toute intention belliqueuse à l'encontre de nos forces,
- surprendre l'adversaire par des actions de déception ou de diversion,
- être en mesure de réduire les capacités et le moral de l'adversaire, en affichant notamment une détermination sans faille.

Vis à vis des ressortissants:

- être en mesure de leur transmettre des consignes ou conduites à tenir en vue de les rassurer, les informer et organiser leur évacuation.

2.2.3 - Emploi

a) Les actions d'influence menées sur le terrain au niveau local d'un théâtre sont intégrées à la stratégie de communication voulue par le CEMA et menées sous son commandement opérationnel. Dans le cadre d'une action militaire multinationale, où nos personnels sont insérés dans une organisation internationale (OTAN, UEO, OUA, etc.), les directives locales établies avant l'élaboration des messages d'influence sont communiquées au CEMA pour avoir son aval.

Ainsi, dans le cadre de la mission de communication opérationnelle spéciale réalisée en Bosnie, les trois officiers insérés à l'état-major de la S.FOR à Sarajevo et l'équipe de liaison et de contact placée sous le commandement tactique de la F.M.N.S.E. à Mostar rendent compte à l'adjoint COS du COMFRANCE de toutes les orientations prises dans ce domaine. A Bangui la mission COSPE est directement aux ordres de l'adjoint COS.

b) Ces actions sont complémentaires mais essentiellement différentes de celles confiées au Service d'Information et de Relations Publiques des Armées. En effet, il importe de ne pas impliquer le SIRPA dans une démarche opérationnelle, qui pourrait irrémédiablement nuire à son image de marque actuelle.

c) Ces messages sont élaborés en liaison avec les différents bureaux (B1, B2, B3, B4) ou composantes de la force (unités présentes, DRM, etc.), afin de pouvoir bénéficier de points de situation les plus précis possibles. Les actions de la communication opérationnelle spéciale sont également analysées en liaison avec les spécialistes de l'expertise civile spéciale (E.C.SPE), qui bénéficient d'un réseau d'influences locales liées à des intérêts d'ordre économique ou institutionnel.

2.2.4 - Moyens mis en oeuvre

La mise en oeuvre des personnels et des moyens doit être faite en fonction d'une reconnaissance spécifique (effets à produire, types de messages possibles, sources d'information à prendre en compte, etc.) et de spécialités reconnues.

a) les personnels interarmées d'active et de réserve appartiennent à des modules adaptables à chaque situation:

- une Equipe de Liaison et de Contact (E.L.C) chargée, d'une part de procéder à des actions d'évaluation dans le but de capter, directement sur le terrain, auprès des cibles choisies, les rumeurs et les désinformations, leurs sources et leurs effets, et d'autre part d'évaluer l'impact des actions menées et de participer directement à des actions d'influence (contacts, distribution de productions...).

Les hommes qui la composent sont choisis parmi les cadres les plus expérimentés des unités du 1° cercle et représentent un volume de 5 à 10 personnels,comprenant:

- un à deux réservistes spécialistes de la communication spéciale,
- des techniciens.

b) les matériels utilisés sont variés:

- station mobile de radiodiffusion,
- tracts,
- affiches,
- autocollants,
- haut-parleurs (montés sur véhicules).

Cette liste n'est évidemment pas exhaustive et ont peut envisager des produits comme ceux employés durant les campagnes médiatiques politiques (chemisettes avec flocage, petits fanions, affiches sur support publicitaire standard...)

Le choix de la mise en oeuvre combinée ou non de ces moyens dépend de chaque situation et du type d'informations à diffuser (informations de fond, factuelles, de crise ou d'alerte).

2.2.5 - Exemples

- Dans le Golfe: les Américains ont déployé la totalité de leur chaîne de communication spéciale pour orienter l'opinion publique irakienne en amont et en parallèle de l'opération Desert Storm. Leur action visait aussi à saper le moral des forces armées irakiennes, notamment en parachutant des tracts annonçant les futurs bombardements, leurs effets et incitant les soldats à se rendre avant, afin d'avoir la vie sauve.

Ces tracts étaient diffusés en irakien et en anglais, beaucoup comportaient des petits dessins et des schémas facilement compréhensibles. L'attitude à adopter pour se rendre était particulièrement bien expliquée.

- Au Cambodge: la communication spéciale visait, d'une part, à marginaliser les Khmers rouges tout en renforçant la crédibilité du prince Sihanouk et des partis reconnus officiellement et, d'autre part, à encourager la population à participer en masse au référendum. Cette action était menée essentiellement par les bataillons mandatés, n'ayant pas forcément tous les savoir-faire requis.

De plus, leur action était entravée par la juxtaposition de contingents originaires de différentes nations aux politiques étrangères parfois divergentes (cf. le différend entre l'Australie et la France).

- En République Centrafricaine, la COSPE française, forte de l'expérience acquise au Rwanda, a mis en oeuvre une station radio ("radio Azur"), à très forte audience, permettant de calmer les esprits d'une population désorientée tout en faisant passer les messages voulus

par le commandement français. Ceci accompagne les actions de COSPE classiques.

- Au Rwanda:

Cas français: ce fut la première expérimentation sur un théâtre d'opération de la composante COSPE. Quoique disposant initialement de peu de moyens, son action a été déterminante notamment pour entraver les effets pervers des diffusions haineuses de la radio "des mille collines".

Cas US: depuis le retrait français, un contingent américain spécialisé en communication spéciale a pris le relais et maintient une présence discrète mais efficace pour mettre en oeuvre la politique voulue par les Etats-Unis.

- En ex-Yougoslavie: des équipes de COSPE étaient souvent envoyées en précurseur des bataillons classiques. Elles ont assuré des missions d'information, voire de sécurité, dans des endroits totalement isolés.

2.2.6 - Limites

Au plan financier, la COSPE, outre les équipements lourds comme les stations radio ou les imprimantes de campagne, doit pouvoir disposer de fonds liquides pour pouvoir acheter les informations nécessaires et fidéliser quelques individus sélectionnés pour constituer les réseaux de communication occasionnels.

En ce qui concerne les moyens techniques, une panoplie classique déjà citée au préalable peut être définie. Toutefois, il serait judicieux de disposer de moyens autonomes ou de contrats préétablis auprès d'entreprises compétentes afin de disposer au plus vite des moyens nécessaires. Il faut aussi disposer de moyens aptes à servir en campagne, donc particulièrement rustiques et fiables.

La doctrine est actuellement en cours d'élaboration. Elle devrait être avalisée par le chef d'état-major des armées. On peut craindre que les réminiscences du conflit algérien (1962), fassent hésiter le haut commandement à officialiser une telle doctrine. Son bien-fondé, les limites fixées ainsi que le nouvel esprit qui l'inspire devraient objectivement lever toutes réticences.

2.3 - LES AFFAIRES CIVILES AU SEIN DES FORCES SPÉCIALES FRANÇAISES

En cours de mise en place au sein des forces spéciales, la partie "affaires civiles" va maintenant être évoquée de façon beaucoup plus succincte compte tenu de son caractère encore évolutif et très spécifique, car essentiellement économique et un peu moins militaire.

2.3.1 - Pourquoi l'élaboration d'un volet "affaires civiles"

- Une nouveauté:

Avant même le déploiement de leurs forces dans le Golfe, les américains avaient mis en place une cellule "civil affairs" dont une des missions était clairement de préparer la signature de contrats dans tous les domaines, avec les différents partis en présence, au profit des sociétés américaines.

- Le besoin actuel:

Dans le contexte de guerre économique que se livrent les pays au niveau international, les gouvernements cherchent naturellement à aider leurs entreprises nationales en se servant du marché potentiel de reconstruction ou de développement que peut offrir un théâtre d'opérations.

On considère aujourd'hui que, depuis la Guerre du Golfe, près d'un million d'emplois ont pu être créés aux Etats-Unis grâce à ce type d'action.

2.3.2 - Le concept des affaires civiles

a) Définition:

Il s'agit d'engager au sein des forces projetables, une cellule ayant des compétences économiques, juridiques et financières, capable d'effectuer des expertises et de pénétrer les milieux économiques des pays situés sur le théâtre d'opérations, en vue de pouvoir réaliser un "retour sur investissement". Cette équipe, envoyée avant la crise cherchera à trouver une ou plusieurs solutions (non nécessairement militaires) permettant le cas échéant de résoudre cette crise le plus tôt possible.

b) Buts:

Les objectifs principaux de la cellule affaires civiles sont les suivants:

- effectuer une expertise poussée sur le terrain afin d'établir un état des lieux dans tous les domaines essentiels,
- nouer des relations d'un niveau stratégique en vue d'établir un "carnet d'adresses" regroupant les principaux intervenants dans les secteurs clés : politique, économique, culturel...,
- tenter de résorber la crise avant qu'elle prenne des proportions trop importantes,
- constituer un dossier comportant le maximum d'éléments pouvant servir au COMELEF en vue d'une résolution de la crise par moyens militaires.

2.3.3 - Emploi

D'un volume variable suivant le théâtre d'engagement, les équipes affaires civiles sont envoyées, dès que la situation sur le terrain le permet, après le déploiement de l'échelon militaire. Leur mission d'évaluation réclame quinze jours à un mois d'étude sur place avant l'établissement d'un dossier d'expertise adapté.

2.3.4 - Moyens mis en oeuvre

En matière d'affaires civiles, les forces spéciales s'impliquent surtout au plan humain. En effet, la qualité et la spécificité du personnel engagé dans ce type d'opération revêtent un caractère fondamental. Aussi, autour d'une structure composée de personnels d'active, il est largement fait appel à des spécialistes du secteur civil pris dans la réserve sélectionnée. Ces experts de réserve doivent tous posséder un haut niveau dans leur domaine de compétence et il est donc important de gérer ce réservoir avec le plus grand soin.

2.3.5 - Exemples

Actuellement, l'équipe "affaires civiles" du COS mise en place en ex-Yougoslavie expérimente avec succès ce concept, créant une véritable synergie avec les moyens militaires conventionnels pour participer à la guerre de l'information sur tous les fronts.

Il n'en demeure pas moins que l'avance prise par les Américains dans ce domaine reste considérable.

2.3.6 - Limites

En France, actuellement, les données recueillies restent en grande partie inexploitées car non acheminées vers les entreprises susceptibles d'être concernées.

Aussi le problème le plus criant reste l'absence d'un échelon de coordination interministériel au niveau du commandement pour constituer le lien entre le COS et les différents ministères de façon à répercuter les besoin du théâtre d'engagement.

3 - LES CHAMPS D'ENGAGEMENT NOUVEAUX POUR LES FORCES SPÉCIALES

Cette dernière partie de l'étude est une prospective des actions que pourraient mener les forces spéciales françaises dans les domaines inexplorés ou jugés encore futuristes au plan national. Avant de s'engager dans cet examen, il convient de cerner quels domaines de la guerre de l'information sont déjà couverts par les forces conventionnelles de nos armées.

3.1 - LES DOMAINES DE LA GUERRE DE L'INFORMATION RELEVANT DES FORCES CONVENTIONNELLES

Comme il a pu apparaître dès la première partie de cette étude, la guerre de l'information n'est pas un concept révolutionnaire sorti de la pensée prolifique d'un stratège de l'ère moderne. Depuis bien longtemps, les hommes ont pratiqué certaines formes de guerre de l'information, à plus ou moins haute dose et avec plus ou moins de succès. A l'époque de la guerre industrielle, les forces conventionnelles mènent usuellement plusieurs types de disciplines de la guerre de l'information, et ceci depuis quelques décennies.

Afin de pouvoir discerner les disciplines qui pourraient faire l'objet de domaines d'action nouveaux mais spécifiquement dévolus aux forces spéciales, il importe maintenant d'examiner quels domaines de la guerre de l'information sont dévolus ou au moins pris en compte par nos forces classiques.

3.1.1 - La lutte contre les systèmes de commandement et de contrôle

Tout d'abord, la lutte contre les systèmes de commandement et de contrôle (*Command and Control Warfare*, C^2W) est une discipline qui vise à frapper les systèmes de commandement. En ces termes, elle est partagée par tous les acteurs en présence, sur terre, sur mer et dans les airs et l'espace, car à l'évidence, les organes permettant le fonctionnement des postes de commandement sont les plus visés dans n'importe quelle crise, sans que l'on désigne en particulier la guerre de l'information pour s'appliquer à un mode d'action. C'est la guerre de l'information de Monsieur Jourdain, en quelque sorte...

L'action peut aussi être partagée entre des commandos du 1er cercle du Commandement des Opérations Spéciales, illuminant au laser un objectif devant subir une attaque de la part de forces classiques avec un armement à guidage laser.

Dans le futur, ce type de discipline de la guerre de l'information devrait toujours être d'actualité, même si les centres de commandement

parviennent à être mieux dissimulés, mieux durcis, ou plus dispersés et redondants. Le besoin de pouvoir les désigner pour objectifs (*antihead*), donc de les déceler, sera accru et plus ardu, de même que celui de mettre à mal les systèmes de transmissions de données (*antineck*) par lesquels les centres de commandement assurent leur fonctionnement.

Ce type de guerre de l'information entre aussi couramment dans les attributions des forces conventionnelles, quand il s'agit de supprimer des relais ou des antennes. Les flux de communications en tant que conduits, liaisons, "tuyaux" d'acheminement de l'information, sont beaucoup moins aisés à traiter, car ils ne se présentent que rarement sous la forme d'objectifs justifiant une frappe, mais relèvent plutôt, comme cela a été explicité au cours de la deuxième partie, de l'action ponctuelle de commandos infiltrés. Dans tous les cas, ces flux et leurs noeuds de transmissions seront dans l'avenir de mieux en mieux dissimulés, de plus en plus miniaturisés, et de moins en moins vitaux.

3.1.2 - Le combat fondé sur les capacités de renseignement

En deuxième lieu, le combat fondé sur les capacités de renseignement (*Intelligence Based Warfare*, IBW) est également un champ d'action privilégié des forces conventionnelles. En effet, l'action de renseignement est permanente au sein de tous les types de forces, et chacun se doit de mettre tous ses moyens en oeuvre pour assurer un renouvellement permanent du renseignement. Cependant, le but avoué en termes de guerre de l'information devient la recherche des systèmes cachés de l'ennemi. Cette recherche est particulièrement complexe dans les spectres courants où opèrent satellites, avions de reconnaissance, et détecteurs divers, dans les domaines du visible ou des ondes radar. Il faut maintenant être capable de détecter des cibles de plus en plus petites, miniaturisées, et émettant de moins en moins. D'un autre côté, la baisse des coûts de l'électronique est favorable aussi à la recherche du renseignement, en ce sens qu'elle permet d'optimiser le développement et la multiplication des systèmes de *targetting*.

Dans ce domaine de la guerre de l'information, il apparaît de plus en plus illusoire de rechercher le camouflage, face à des détecteurs de plus en plus performants. Les seules actions d'une relative efficacité relèvent de la furtivité. Cette notion est encore à la fois confidentielle et relative, car elle ne peut concerner qu'une partie du spectre électromagnétique, et un système furtif dans une plage de fréquence peut se comporter comme un miroir dans une autre bande.

Dans l'IBW, les forces classiques et les forces spéciales ont chacune pour "tâche de fond" de recueillir le renseignement et de le recouper. Une unité comme la brigade de renseignement et de guerre électronique (BRGE) est un exemple d'élément de forces conventionnelles inscrit au troisième cercle des forces spéciales, et dont la mission est, entre autres, la détection puis l'analyse de systèmes ennemis dissimulés.

3.1.3 - La guerre électronique

C'est encore une discipline "implicite" de la guerre de l'information qui est pratiquée depuis plus d'un demi siècle... Elle se décline en trois domaines, les actions antiradar, les actions anti-communications, et la cryptographie.

En matière d'actions antiradar, les forces conventionnelles ont un rôle majeur à jouer, qu'elles ne remplissent pas véritablement en France. En effet, les armes antiradar sont rares, voire inexistantes, au moins pour ce qui est de leur efficacité réelle. Si les forces aériennes ont disposé d'un missile antiradar (l'AS 37 MARTEL, modernisé ADAM), cet armement n'est plus utilisable aujourd'hui. Il n'est pas prévu d'armement de remplacement dans un futur proche. Il faut donc éliminer ce type d'actions des attributions des forces conventionnelles, et en confier toute la responsabilité aux forces spéciales... Il est vrai que les actions antiradar n'auront probablement rien à voir dans le futur avec ce que l'on a pu en connaître au cours de la Guerre du Golfe, car là aussi, la miniaturisation des systèmes, l'accroissement de leur nombre, et la séparation des unités émettrices d'avec les capacités de réception rendront très délicate l'utilisation d'armements lourds comme les missiles cités plus haut. Il va sans dire que la tâche d'unités des forces spéciales chargées de les détruire n'en sera également que plus ardue...

En attendant, on ne peut que regretter l'incapacité des forces conventionnelles à assurer cette lutte, sauf à faire appel aux capacités de nos alliés en la matière, car les systèmes radars contemporains resteront encore pour un certain nombre d'années des objectifs de choix.

Les actions anti-communications ont probablement encore moins de chances de succès, du fait de l'étalement du spectre et de la "démocratisation" des appareils de communication à agilité de fréquence. De plus, il en est des communications comme des techniques de brouillage: il suffit de connaître la position de l'interlocuteur (ou du système à brouiller) et d'émettre à l'aide d'antennes à faisceau fin dans une direction précise, pour assurer une communication fiable car concentrée vers son récepteur mais discrète dans le reste de l'espace (ou un brouillage efficace pour son objectif mais ne gênant pas les systèmes amis).

Il y a fort à croire qu'il sera encore pour longtemps plus intéressant de tenter d'intercepter les communications de l'adversaire que de tenter de les brouiller ou de les interdire directement.

Enfin, dans le domaine de la cryptographie, la célèbre affaire des machines ENIGMA risque peu de se reproduire, ou ne durerait que peu de temps, tant les progrès en matière de chiffrement devancent la rapidité d'action des équipes et des systèmes capables de décrypter le contenu des communications.

Le bilan des capacités des forces conventionnelles dans la guerre de l'information se réduit à ces trois domaines, C^2W, IBW et EW. Les

champs d'engagement nouveaux des forces spéciales vont être étudiés dans ce qui suit.

3.2 - LES CHAMPS D'ENGAGEMENT NOUVEAUX POUR LES FORCES SPÉCIALES

Les champs d'engagement nouveaux peuvent être appréhendés en termes de besoin, de faisabilité, et d'aptitude à pratiquer de nouvelles formes de travail. Ces formes de travail sont peut-être encore pour nous, Français, du domaine de l'irréel, mais, dans la mesure où les Américains portent à certains aspects de la guerre de l'information un intérêt certain, nous risquons de nous mettre à l'écart des champs d'action du futur, si nous ne nous sentons pas déjà sensibilisés.

Parmi les champs d'engagement nouveaux, nous avons distingué dans un premier temps ceux pour lesquels un développement existe déjà, et qui ont fait l'objet de la deuxième partie. Ces domaines relèvent du court terme. Par ailleurs, nous avons tenté dans un deuxième temps de trouver dans quelles disciplines plutôt "futuristes" des orientations nationales pouvaient être envisagées.

3.2.1 - Le court terme: ce qui est réalisable

Ce qui est réalisable est complémentaire de l'organisation de la COSPE telle que présentée dans la partie 2.

Dans un premier temps, il s'agit d'améliorer l'existant.

Les moyens mis en oeuvre pour la COSPE sont trop limités pour être déployés ne serait-ce que dans deux théâtres simultanément. Aussi cet objectif doit être atteint pour satisfaire aux buts fixés par le Livre blanc et aux réalités des interventions extérieures françaises.

Outre une seconde station mobile de radiodiffusion, une imprimerie autonome devrait être mise sur pied.

L'effectif en personnel qualifié doit être accru, notamment le nombre de réservistes spécialistes de la COSPE après sélection. Ce personnel doit ensuite être "fidélisé", la cible étant de pouvoir inclure à chaque niveau opérationnel, à partir de l'unité élémentaire, une composante COSPE. Notons que les Etats-Unis parviennent à détacher sept personnels spécialisés par unité élémentaire engagée sur un théâtre.

Dans un deuxième temps, il faut élargir l'éventail des moyens.

Des équipements peu coûteux existent et seraient fort utiles pour les objectifs visés par la COSPE.

Ainsi une imprimante de campagne aérotransportable permettrait une autonomie de diffusion adaptée au contexte d'une intervention de moyenne durée.

Des artifices plus originaux doivent être utilisés tels les banderoles tirées par des avions (ou ULM) "publicitaires", les tracts avec slogans ou dessins ciblés employés massivement, des affiches collées ,

etc., en fait une véritable campagne "militaro-publicitaire" doit être montée pour chaque opération.

Troisièmement, il faut donner toute sa dimension au domaine économique.

Les interventions militaires françaises résultent de plus en plus de carences économiques et d'insuffisances des autorités locales à assurer les besoins vitaux des populations. Le traitement de la crise ne sera efficace et définitif que si la dimension économique est prise en compte dès la conception de l'opération. La cellule "affaires civiles" de l'état-major engagé ne doit plus uniquement régler les litiges que ne manque jamais d'entraîner une opération. Elle doit, parallèlement aux acquis militaires sur le terrain, participer au redressement économique de la zone sinistrée. Qui plus est, cela renforcera l'influence de notre pays de façon durable et confortera nos intérêts. Pour schématiser, cet état d'esprit qui vise à appliquer le slogan "gagnant-gagnant" est de mise puisque les populations victimes du conflit voient leur sort amélioré et notre pays voit sa position renforcée et ses intérêts développés.

Outre le renforcement de la cellule "affaires civiles" il convient d'inculquer un état d'esprit général aux cadres militaires impliqués dans l'opération pour qu'ils aient tous, à leur différent niveau, la volonté de participer au redressement économique de la zone sinistrée.

Dans un quatrième temps, c'est cet état d'esprit qui est le maître mot de l'effort à fournir pour être compétitifs dans le domaine de la guerre culturelle, le *Kulturkampf.*

La question primordiale que nous devons nous poser, en tant que Français, est de savoir si nous sommes en mesure d'exercer ce genre d'activité de standardisation du comportement, et par le biais de quels vecteurs notre action peut être la plus efficace. En effet, il semble illusoire de tenter de combattre sur le même terrain que les Américains, c'est à dire de chercher à s'imposer face aux grands vecteurs comportementaux habituellement promus par les Etats-Unis. En revanche, nous avons certains atouts à mettre en valeur, et certains champs d'action à développer, même s'il ne paraît pas à première vue évident de pouvoir rencontrer de grands succès dans ces domaines.

La deuxième question est de savoir où les forces spéciales peuvent intervenir dans cette démarche, qu'on pourrait qualifier de "publicité pro-nationale implicite multi-théâtres".

Peu de réponses viennent aisément à l'esprit, et hormis les notions de francophonie et d'exception culturelle qui relèvent plus de traditions de politique extérieure et de représentation, il n'est pas évident de cerner des champs d'application pour les forces spéciales!

Cependant il s'agit bien d'une guerre culturelle, qui n'est que le reflet de l'attitude socio-politique d'un pays. La Constitution des Etats-Unis est un exemple de la propension des Américains à défendre ardemment le droit au choix en matière de culture. Mais ce choix est ensuite une obligation latente qu'ils s'imposent et cherchent ensuite à imposer. La démarche française est différente. Les Français n'ont pas de choix culturels à faire, il sont déjà "installés" dans une culture qu'ils cherchent seulement à défendre... La différence fondamentale est là:

quand les cultures nationales fortes et anciennes, comme en France ou au Japon, restent sur leurs acquis, les Américains présentent une mentalité de pionniers, et ont une stratégie culturelle offensive.

Lorsque Français ou Canadiens se plaignent de l'envahissement culturel de leurs pays, les Etats-Unis considèrent ces plaintes comme des entraves aux libertés commerciales et refusent de considérer ces réticences comme légitimes.

En métropole, les forces spéciales n'ont pas de rôle déterminant à jouer en la matière. Sur les théâtres extérieurs, partout où la COSPE est représentée, cette forme de guerre culturelle doit être menée, avec nos moyens et à notre niveau. En ce sens, il s'agit plus, comme nous l'avons vu ci-dessus, de résistance aux formes d'imposition de l'*American cultural way* que d'offensive proprement dite. L'effort à fournir est donc un véritable endoctrinement (ou même un "contre-endoctrinement" préventif!), pour savoir résister à la *cultural warfare* menée par les Etats-Unis dès qu'ils sont représentés sur un théâtre.

3.2.2 - Le moyen terme: ce qui est envisageable

Les techniques de piratage informatique et le terrorisme informatique:

Quelques définitions s'imposent:

PHREACKER: terme né aux Etats-Unis, qui désigne les adeptes du sport consistant à utiliser son ordinateur pour arracher, au coeur des systèmes de gestion des comptes clients des grandes sociétés de télécommunication, les codes d'accès qui leur permettront de téléphoner gratuitement.

HACKER: le piratage téléphonique est, du strict point de vue de la technicité requise, très en deçà du *hacking*, pratiqué par le *hacker*, auquel il convient de préférer le terme de pirate: ce dernier désigne aujourd'hui celui qui sait mettre en route l'ensemble des opérations consistant à forcer les accès d'un ordinateur distant, et désormais, pour l'essentiel, via l'Internet. La plupart du temps, les pirates n'ont pas d'intention frauduleuse et agissent pour la beauté du sport. Ce sont des experts du monde informatique, aux compétences souvent exceptionnelles .

CRACKER: les plus méchants des pirates, souvent appelés *crackers*, cherchent à détruire ce qui peut l'être: effacer des fichiers, implanter des "bombes logiques".

Les autorités françaises ont pris ces affaires très au sérieux et la gendarmerie comme la police nationale disposent de quelques spécialistes. Outre les équipes de la DST qui travaillent sur ces questions, mais bien souvent dans le but de repérer des talents pour les "retourner", la préfecture de police de Paris dispose du SEFTI (Service d'enquête des fraudes aux technologies de l'information), créé en février 1994, et la police judiciaire nationale de la BCRCI (brigade de recherche et de répression de la criminalité informatique). La loi Godfrain de 1988 a marqué le véritable coup d'arrêt, en France, des intrusions dans les

systèmes d'ordinateurs. La DGSE et surtout la DST sont passées maîtresses dans l'art de retourner ces "espions", pour lesquels les tribunaux n'ont guère de sympathie . Ainsi, ils sont priés de mettre leurs talents de délinquant informatique au service de la France, et de travailler pour les services secrets. Cependant, les détails manquent sur les affaires impliquant les services français. Les services secrets allemands, le BND (*Bundesnachrichtendienst*), sont également très férus de ces techniques.

Pour ce qui est de la protection des ordinateurs, ce sont les services techniques du ministère de la Défense, le GESSI (Groupe d'évaluation de la sécurité des systèmes d'information), appartenant au CELAR, qui assurent pour les divers organismes gouvernementaux, les recherches en la matière. Les ingénieurs de l'armement qui s'y trouvent sont les meilleurs experts français en matière de cryptosystèmes, de protection des réseaux et de discrétion des ordinateurs.

Le piratage informatique transparent (ou attaques sémantiques):

Chargés d'organiser la protection des ordinateurs du Ministère de la Défense, les ingénieurs du CELAR ont mis au point des "chevaux de Troie" qui, comme leur nom l'indique, sont de petits programmes dissimulant des capacités indésirables, parfois extrêmement dommageables pour l'ordinateur qui les accueille, et ce sans que l'utilisateur s'en aperçoive (programme "femme de ménage").

Ainsi il apparaît que la fonction *hacker warfare* soit prise en compte et maîtrisée par les services spéciaux du Ministère de l'Intérieur, qui dispose aujourd'hui des méthodes et du personnel qualifié, formé par des organismes comme l'EIREL (Ecole Interarmées du Renseignement et d'Etudes Linguistiques) ou le CESD (Centre d'Etudes Scientifiques de Défense). Les liens entre le contre-espionnage et les armées sont plus étroits que par le passé. C'est la logique du renseignement, désormais incontournable qui les rapproche. Aussi, on peut considérer que si ce domaine constitue pour les forces spéciales un champ d'engagement nouveau, elles ne peuvent s'y investir que par une coopération étroite avec le Ministère de l'Intérieur et la DRM, et au travers des structures déjà existantes.

La guerre par simulation:

En dehors de la simulation classique, grâce à laquelle il est possible d'empêcher une attaque ennemie en lui faisant craindre la défaite (par armes conventionnelles ou nucléaires), il existe la "guerre simulée" qui, comme nous l'avons vu, est une façon d'éviter la guerre en prouvant à son ennemi, à l'aide de simulateurs et de démonstrateurs, qu'il ne peut que la perdre. Il faut donc être convaincant et faire en sorte que l'ennemi n'ait pas de doute sur notre volonté et sur la capacité de nos moyens.

Il faut par conséquent être en mesure non seulement de lui offrir une simulation de ce que pourraient être les combats mais également de lui faire une démonstration réelle des possibilités de nos armes.

Ponctuellement, nous sommes capable de mener avec succès ce type de combat. Cela a d'ailleurs déjà été fait en ex-Yougoslavie, où, pour obtenir l'évacuation d'une zone par un des belligérants, celui-ci s'est vu offrir une démonstration de la précision et de l'efficacité de notre artillerie sur des carcasses isolées.

Cette façon de procéder peut évidemment s'étendre à tout un théâtre d'opération. Mais actuellement, les simulateurs servent principalement à l'entraînement des combattants et il parait encore difficile de reproduire de façon réaliste une guerre avec tous ses aléas. Quant aux démonstrateurs, il est presque toujours possible de prouver à un éventuel ennemi, la capacité de notre armement.

De toutes façons, les forces spéciales ne pourraient évidemment pas, à elles seules, contrôler les nombreux domaines que réclame ce type de guerre. Elles ne pourraient que participer, à court ou moyen terme, à la guerre psychologique qu'il serait nécessaire de mener en parallèle à une *simulation warfare*.

Gibson warfare:

En ce qui concerne la *Gibson warfare*, on peut admettre que les techniques mises en oeuvre ne relèvent pas, pour l'instant, des compétences des forces spéciales. Ce type de guerre ne présente donc pas, à moyen terme, un champ d'engagement nouveau pour celles-ci.

CONCLUSION

Dans un contexte mondial en grande mouvance, le concept de guerre de l'information est lui-même singulièrement sujet à se "tentaculariser", vers des domaines qui peuvent être complètement étrangers les uns avec les autres. En matière de guerre de l'information, il est aujourd'hui impossible de ne pas faire référence aux techniques employées par les Etats-Unis, et d'examiner de façon comparative ce qui est fait ici ou ailleurs, et ce qui n'est pas fait. C'est la démarche qui a été entreprise dans ce document qui ne prétend pas avoir fait le tour de la question, eu égard aux nombreuses facettes que présente le sujet.

L'examen des techniques de guerre de l'information a montré l'étendue des disciplines concernées, et fourni un éclairage de leur contenu. Si certaines de ces disciplines sont déjà largement employées par toutes nos forces armées, d'autres formes de guerre de l'information nous semblent encore relever complètement de la science fiction. Du côté des forces spéciales, une organisation récemment revue et un effort de promotion de la communication opérationnelle spéciale permettent actuellement et pour les années à venir de s'attaquer aux problèmes

rencontrés sur les théâtres d'opération potentiels où seraient amenées à agir nos forces.

Du côté des forces conventionnelles, la guerre de l'information est plutôt une guerre anti-systèmes d'information, dans les domaines de guerre électronique par exemple. Ces aspects n'innovent pas particulièrement, mais l'effort de développement, tant dans la définition des armements futurs que dans les techniques d'emploi de nos forces conventionnelles, doit tenir compte des évolutions technologiques des systèmes de détection et des nouvelles doctrines de combat que permet l'emploi des armes intelligentes, et qu'imposent la notion de "zéro mort" et la prise en considération de l'opinion publique.

Enfin, du côté des forces spéciales, les champs d'engagement nouveaux sont limités par les moyens, en matériel et en personnel. Les orientations prises en matière de communication opérationnelle spéciale sont cependant prometteuses. Il ne faut pas se disperser vers des techniques de guerre de l'information qui nous sont encore complètement étrangères et dans lesquelles nous nous dépenserions sans résultat. Les efforts consentis dans le domaine des affaires politico-militaires doivent être poursuivis car il apparaît que c'est bien en appréhendant fermement les problèmes de cet ordre que nous pourrons promouvoir de façon efficace et durable l'économie, la culture et les intérêts français.
