

**ETUDE PARTICULIERE A OPTION
GROUPE B07**

LCL BOURASSEAU Groupe B6
LCL RICHEL Groupe B1
CDT LEPOIX Groupe B4
CDT PATRY Groupe B3
CDT HERNOUST Groupe B4

**Politique à adopter
face aux technologies civiles
dans le domaine des communications.**

Directeur de recherche : LCL MAISETTI (EMAT/BCSF/TRS)
Responsable du comité : CDT HERNOUST

Session 1998/1999

1. INTRODUCTION	1
2. REFLEXIONS SUR LA DUALITE CIVILO MILITAIRE	2
2.1 DEFINITION DE LA DUALITE CIVILO MILITAIRE	2
2.2 LES SPECIFICITES MILITAIRES	2
2.3 LE ROLE PREPONDERANT DU CODE DES MARCHES PUBLICS	3
2.3.1 <i>L'expression du besoin</i>	3
2.3.2 <i>La gestion des programmes</i>	3
2.3.3 <i>Les évolutions nécessaires</i>	4
2.3.4 <i>Conclusion</i>	4
2.4 DUALITE ET NOTION DE SYSTEME	4
2.5 L'ACHAT SUR ETAGERE	5
2.5.1 <i>Nécessité d'être pérenne</i>	6
2.5.2 <i>Nécessité d'être interopérable</i>	6
2.5.3 <i>Nécessité d'être robuste</i>	6
2.5.4 <i>Nécessité d'être intégré à un porteur</i>	7
2.6 L'ASSEMBLAGE DE SOUS SYSTEME	7
2.7 SERVICE DUAL OU EXTERNALISATION	8
2.8 CONCLUSION.....	8
3. LES SYSTEMES D'INFORMATION ET DE COMMUNICATION (SIC)	10
3.1 LES SYSTEMES DE COMMUNICATION (SC)	10
3.1.1 <i>Les systèmes de communication militaires</i>	10
3.1.2 <i>Les services attendus</i>	12
3.1.3 <i>La dualité dans un nouveau contexte technologique et budgétaire</i>	12
3.1.4 <i>Ensembles fondamentaux</i>	13
3.1.5 <i>Les réseaux support</i>	13
3.1.5.1 Niveau stratégique.....	13
3.1.5.2 Niveau opératif.....	13
3.1.5.3 Niveau tactique	14
3.1.5.4 Les réseaux support de combat de l'avant	14
3.1.5.5 Les réseaux locaux (SI).....	14
3.1.6 <i>Le « Noyau dur » de télécommunications militaires</i>	14
3.2 LA COMPOSANTE SATELLITAIRE.....	15
3.2.1 <i>Besoin satellitaire militaire à l'usage des forces projetées</i>	15
3.2.2 <i>Le « noyau dur » satellitaire</i>	15
3.2.3 <i>L'offre commerciale</i>	16
3.2.4 <i>Utilisation de l'offre commerciale</i>	16
3.2.5 <i>Limites de l'offre commerciale</i>	17
3.2.6 <i>Une étude de coût intéressante</i>	18
3.3 LA COMPOSANTE TERRESTRE.....	19
3.3.1 <i>Le besoin opérationnel</i>	19
3.3.2 <i>Intérêt et limites de la dualité</i>	19
3.3.3 <i>L'exemple du programme PR4G</i>	20
3.3.4 <i>Les réseaux radio-mobiles civils</i>	20
3.3.5 <i>Internet</i>	21
3.3.6 <i>Externalisation des télécommunications d'infrastructure</i>	21
3.4 LES SYSTEMES D'INFORMATION :	22
3.4.1 <i>Le besoin militaire</i>	22
3.4.2 <i>Les difficultés engendrées par la dualité</i>	23
3.4.3 <i>Les avantages de la dualité</i>	24
3.4.4 <i>Un exemple de dualité dans le domaine des SI</i>	24
3.4.5 <i>Les différents niveaux de dualité dans les SI</i>	25
4. LA SECURITE DES SYSTEMES D'INFORMATION	26
4.1 UN DISPOSITIF JURIDIQUE GRACE AU CODE PENAL DE 1992	26
4.2 DES MENACES EN CAS DE COOPERATION.....	26
4.3 LE RECOURS A L'EXTERNALISATION DANS CE CADRE JURIDIQUE	26
4.4 LA VULNERABILITE DES ENTREPRISES CIVILES	27

4.5 LA SECURITE DES SYSTEMES D'INFORMATION VUE PAR THOMSON-CSF	27
4.6 LE PROBLEME DE LA CRYPTOGRAPHIE.....	28
5. LES LIMITES DE LA DUALITE	29
5.1 LES RISQUES DE PERTE DE L'INDEPENDANCE NATIONALE	29
5.2 LES LIMITES POLITIQUES	30
6. CONCLUSION.....	32

1. Introduction

Depuis la fin de la guerre froide, l'industrie de l'armement est en pleine restructuration. Deux facteurs concomitants ont initié puis rendu inéluctable cette révolution industrielle :

- l'éloignement de la menace soviétique qui a eu pour conséquence la réduction drastique des budgets militaires,
- la montée en puissance de l'Europe économique, et la volonté manifeste des gouvernements européens de concurrencer l'industrie des Etats Unis.

Face à une industrie américaine qui, ne se satisfaisant pas d'un marché national important, s'est restructurée afin de mieux s'imposer à l'exportation, l'industrie européenne de Défense doit réagir si elle veut survivre et rester compétitive. Elle doit rester innovante, performante et rentable.

Cependant, si le budget de Défense est en forte diminution, certains marchés civils sont eux à forte croissance, citons les télécommunications et l'informatique. Ces marchés sont portés par le développement de technologies de pointes financées par les retombées économiques importantes. L'industrie de la Défense n'est plus la seule source d'innovations techniques. La téléphonie mobile, le multimédia deviennent des secteurs innovants au même titre que le programme nucléaire militaire au début des années soixante.

Dans un tel contexte, il est donc naturel de rationaliser les efforts en associant étroitement, lorsque cela est possible, les recherches et les développements civils et militaires afin de minimiser les coûts de production et d'optimiser les investissements.

Mais les deux mondes, civil et militaire, ne répondent pas aux mêmes lois, aux mêmes contraintes. Même si le concept de technologie duale s'impose aux esprits pragmatiques désireux de réaliser des économies de temps, de moyens et donc d'argent, il ne peut être une réponse universelle et idéale aux besoins de la défense.

Le but de notre étude est de définir une « politique à adopter face aux technologies civiles dans le domaine des communications ».

Pour cela nous précisons, dans une première partie, ce qu'est la dualité civilo-militaire. Cette étude nous permettra de détacher les avantages et les inconvénients majeurs du recours à la dualité dans les programmes d'armement.

Ces généralités étant admises, nous illustrerons, dans les parties suivantes notre propos en choisissant deux secteurs d'activités liés aux télécommunications de la défense :

- Les systèmes d'information et de communication,
- Le chiffre.

Pour chacun de ces domaines, nous proposerons une étude ciblée sur des réalisations existantes ou à venir en nous efforçant de faire ressortir le besoin militaire les contraintes et les avantages de la dualité sur le plan opérationnel, technique et financier. Enfin, dans une dernière partie, nous définirons les limites du recours aux technologies duales.

2. Réflexions sur la dualité Civilo Militaire

2.1 Définition de la dualité civilo militaire

Plusieurs définitions de la dualité peuvent être trouvées dans différents documents. Citons à titre d'exemple le plan prospectif à trente ans qui présente la dualité comme suit :

« une technologie duale est une technologie civile utilisée (ou qu'il serait judicieux d'utiliser) dans le militaire »

Cette définition a le mérite de la concision mais elle est trop générale, puisqu'elle recouvre aussi bien le composant électronique civil employé sur une carte spécifiquement militaire, que le véhicule militaire ne se distinguant de la version civile que par sa couleur.

La dualité peut aussi être définie par l'absurde, c'est à dire par ce qu'elle n'est pas. Ce type d'approche est relevé dans un rapport de la 34^{ème} Session du CHEAR¹ qui définit tout ce qui ne peut être pris en compte par des technologies duales :

*« - tout ce qui n'a pas d'équivalent civil dans sa fonction,
- tout ce qui semble avoir une fonction civile équivalente mais qui est soumis à des contraintes d'environnement très particulières requérant de fait des technologies ou des développements militaires »*

Cette seconde approche est plus précise, notamment dans sa deuxième partie. En effet, la militarisation d'un produit civil qui peut être vue comme une application judicieuse du principe de la dualité peut se révéler désastreuse en terme de coût et de délais tout simplement parce que le produit qui semblait avoir une fonction civile équivalente était soumis à des contraintes militaires trop fortes. Ce point doit toujours rester à l'esprit des responsables chargés de la définition de nouveaux produits.

Il nous appartient à présent de définir ce qui dans notre étude sera considéré comme technologie duale. La première précaution sera de ne pas se limiter au terme de « technologie ». Dans le cadre des activités de défense il est important de préciser, dès à présent, que le service dual sera aussi pris en compte. Entendons par ce terme un service qui pourra être sous traité ou externalisé à un organisme civil. Abonnement téléphonique, maintenance d'un équipement, location de canaux de diffusion sur un satellite de télécommunication civil sont donc des activités duales au sens de notre étude.

Sur le plan de la réalisation de système nous nous attacherons à ne pas confondre le soutien financier de l'industrie civile avec la réelle dualité. En d'autres termes, la dualité civilo-militaire n'est dans notre esprit envisageable que si elle apporte effectivement soit un gain de temps de mise au point, soit un gain financier, soit un gain opérationnel. Elle doit permettre à la défense de maintenir sa capacité opérationnelle à un niveau acceptable qu'il faudra définir pour chaque application envisagée, malgré la diminution des budgets militaires. La dualité ne doit pas se limiter au strict soutien financier d'une industrie de défense en pleine restructuration.

Ces remarques préliminaires nous amènent naturellement à souligner un premier paramètre à prendre en compte si on veut aborder le problème de la dualité de façon pragmatique : la réalité des marchés publics. En effet rien ne sert de définir des projets financièrement et techniquement séduisants, s'ils ne respectent pas le code des marchés publics.

2.2 Les spécificités militaires

Plutôt que de nous lancer dans une étude qui ne saurait être exhaustive des spécificités des besoins militaires, citons les conclusions d'un groupe de l'OTAN² chargé de la normalisation des

¹ Rapport du comité du groupe 2 de la 34^{ème} session du CHEAR page 17.

² Groupe de normalisation des télécommunications de l'OTAN. Référencé dans l'article d'Emmanuel Sprariel ingénieur de

télécommunications. Huit caractéristiques spécifiquement militaires sont identifiées, nous les retrouverons au cours de notre étude :

- la **sécurité**, qui garantit que l'information ne peut être connue que par son destinataire et que celui-ci à l'assurance de son origine et de son authenticité.
- la **robustesse**, l'architecture des réseaux militaires doit leur permettre de résister à de nombreuses agressions, brouillage, impulsion électromagnétique. Ce facteur prend aussi en compte les agressions physiques, la disponibilité, la survivabilité en ambiance dégradée.
- la **gestion des réseaux**, qui doit permettre d'éviter les saturations et de multiplier les possibilités d'accès à un même point afin de garantir le transfert rapide et permanent de l'information.
- l'**interopérabilité**, pour pouvoir communiquer d'un réseau à un autre, avec les autres armées, avec les alliés.
- la **priorité**, possibilité d'interrompre les communications pour pouvoir passer une information prioritaire.
- les **connexions multipoints**,
- les **abonnés mobiles**,
- les **communications tactiques**, qui nécessitent une mobilité de l'ensemble du réseau.

Cette classification se rapporte aux réseaux, mais elle permet cependant de distinguer certaines spécificités propres à l'utilisation de tout système d'armes. Ce sont essentiellement :

- la sécurité et la nécessité de crypter, d'identifier,
- la robustesse,
- les fonctions propres au domaine militaire, nécessitant une interface spécifique.

2.3 Le rôle prépondérant du code des marchés publics

Au cours des différentes interviews réalisées, chaque intervenant s'est attaché à souligner le rôle prépondérant du code des marchés publics dans le processus décisionnel. Nous ne décrirons pas le déroulement d'un programme d'armement, ce qui sortirait de notre sujet, en revanche nous relèverons deux paramètres importants à nos yeux dès qu'il est question de dualité :

- La difficulté de passer de l'expression de besoin aux caractéristiques techniques,
- La lourdeur de la gestion des programmes.

2.3.1 L'expression du besoin

La fiche de caractéristique militaire (fcm), est le point de départ de tout programme d'armement. Dans celle-ci les états majors vont décrire le besoin en terme de capacités à remplir par le système, limites de fonctionnement, performances. Dès lors que certains paramètres seront fixés à cette phase, le recours à la technologie civile sera envisagé ou définitivement exclu. Prenons un exemple simple, la plage de fonctionnement en terme de température des systèmes informatiques. Si dans la fcm la contrainte est plus forte que la norme civile en vigueur, le système ne pourra pas être réalisé à partir de matériels civils. Il faudra développer un équipement spécifique. La dualité sera abandonnée, au moins pour l'aspect matériel informatique, dès la phase de définition du besoin.

2.3.2 La gestion des programmes

Les programmes militaires pouvant s'étirer sur une durée très longue, le problème se pose en terme de capacité à suivre l'évolution des matériels. Le temps moyen de développement d'un programme d'armement est estimé à six ans. Il peut être plus important pour les programmes majeurs (Rafale, Leclerc) ou plus faible pour des programmes de moindre importance (système d'information). Quelque soit cette durée elle est souvent incompatible avec le cycle de renouvellement des matériels civils, poussés par le marché privé et la concurrence. Citons à titre d'exemple la micro informatique, très présente dans de nombreux systèmes militaires, son cycle de vie est estimé aujourd'hui à deux

ans. Face au relatif immobilisme de la demande militaire, le recours aux technologies duales peut se traduire par la mise en service après trois années de développement d'un système d'arme qui fonctionne à partir d'une technologie informatique obsolète depuis plus d'un an. Ce qui évidemment pose des problèmes en terme de formation des personnels, gestion des pièces de rechange.

2.3.3 Les évolutions nécessaires

La mise en place des premiers contrats d'armement faisant appel à des techniques duales, montre qu'une évolution du code des marchés publics est nécessaire afin de prendre en compte les spécificités du monde civil. Cependant, en marge d'une refonte de la réglementation qui ne pourra être que longue et progressive, une action a déjà été menée au niveau de la rédaction des contrats. L'effort doit être poursuivi et porter sur l'évolutivité du système.

Il faut notamment prendre en compte, dès la rédaction du contrat, le rythme d'évolution des éléments civils intégrés. A titre d'exemple, pour un système informatique basé sur une carte mère susceptible d'évoluer régulièrement ; il faut prévoir, dans le contrat, en relation avec l'industriel maître d'oeuvre :

- l'évolution du matériel en termes d'achat de carte mère de nouvelle génération,
- l'évolution nécessaire du logiciel,
- l'organisation de la noria pour garantir la pérennité du service rendu.

Le coût devra être évalué et le financement prévu sur une ligne budgétaire. En procédant de la sorte, les utilisateurs se mettent à l'abri de nouvelles négociations commerciales qui induisent des délais administratifs incompatibles avec le calendrier d'évolution d'un matériel civil standard.

2.3.4 Conclusion

Le code des marchés joue donc un rôle important, d'autant plus qu'il contient en filigrane un rôle attribué à la DGA qui est le soutien à l'industrie de défense nationale. Aussi, le risque de nommer dualité ce qui n'est qu'un soutien plus ou moins déguisé à une industrie civile en difficulté n'est pas inexistant.

Dans un contexte de regroupement des entreprises européennes, les appels d'offre sont aujourd'hui passés au niveau international. En conséquence, les risques de blocage d'un programme pour des problèmes de non respect du code des marchés publics est multiplié. La dimension administrative et pénale des contrats d'armement est un paramètre essentiel. Le respect des règles et des procédures doit être pour les responsables de programmes un souci constant.

2.4 Dualité et notion de système

Dès que l'on aborde le problème de la dualité, la notion de système technique devient prépondérante. En effet, nous pouvons grâce à ce concept dresser un rapide bilan qualitatif de l'état de la dualité aujourd'hui. Pour cela plaçons nous successivement à trois niveaux technologiques différents ; le système, le sous système, le composant.

le système complet :

A ce niveau parler de dualité signifie qu'un système civil peut répondre à un besoin militaire sans modification du produit, on est donc dans le cas de l'achat sur étagère. Remarquons en premier lieu que la défense est une activité humaine au même titre que la finance ou la médecine. Personne aujourd'hui ne conteste à ces domaines le droit à des applications spécifiques qui sont par ailleurs développées et commercialisées par des industriels spécialisés. Pour les militaires, la problématique est la même, la dualité au niveau système reste donc a priori très marginale. Elle ne s'applique qu'à des activités génériques telle que la bureautique, la gestion.

Le sous système ou équipement :

Le champ d'application est plus large et en pleine évolution. Aujourd'hui, la Défense ne fait plus développer des calculateurs spécifiques, ou des écrans de visualisation adaptés aux contraintes militaires. Pour des raisons d'économie, mais aussi pour améliorer les performances, le système d'arme est réalisé de plus en plus fréquemment à partir de sous systèmes complètement duaux. Citons les stations de travail de la marque SUN qui se sont imposées dans les systèmes informatiques de commandement.

Deux facteurs ont permis ce rapprochement, l'amélioration de la robustesse des systèmes civils, et l'adaptation voire l'abandon progressif de certaines normes militaires. Il y a eu convergence des spécifications civiles et militaires. Bien sûr, une adaptation reste parfois nécessaire, les sous systèmes civils sont protégés par des containers adaptés, les cartes durcies par des procédés extérieurs. Le surcoût n'est pas négligeable, mais les gains vis à vis d'un développement spécifiques sont importants.

En fait la dualité des sous systèmes est effective et quasiment systématique, sauf lorsque la contrainte reste propre au domaine militaire. Ainsi, un ordinateur embarqué sur un avion d'arme est encore équipé de mémoires spécifiquement développées pour lui. Les niveaux de fiabilité et de résistance aux accélérations qui sont demandées par l'utilisateur n'étant pas compatibles avec ceux des matériels embarqués civils et à fortiori des matériels sols.

Le composant :

A ce niveau la dualité atteint même les applications typiquement militaire. Reprenons l'exemple du calculateur. Si la carte mère a été développée de façon spécifique afin de permettre, par une architecture adaptée, de prendre moins de place et de mieux résister aux accélérations, ses composants sont issus des chaînes de fabrication civiles. Le composant militarisé n'est en fait qu'un composant trié par l'industriel qui ne fait que s'assurer individuellement de sa qualité. On peut sans doute encore trouver pour des applications très spécifiques comme l'autodirecteur d'un missile des composants produits pour les armées, mais ils sont peu nombreux. Dans le domaine du composant du système, la dualité est quasiment totale.

En fait, il apparaît que le terme dualité civilo-militaire peut s'appliquer à un ensemble de processus de fabrication d'un système d'arme, qui va de l'achat simple sur étagère d'un produit qui sera utilisé sans modification par la défense (logiciel WORD pour le traitement de texte), à l'adaptation ou l'assemblage, parfois complexe et coûteux, de sous ensembles ou de composants.

Cependant, si la dualité s'est bien généralisée au niveau des composants et des sous systèmes, il reste de nombreux problèmes à gérer pour les militaires. En terme de maintenance en premier lieu ; la durée de vie d'un système d'armes est en général bien supérieure à celle d'un composant civil ; il faudra donc pouvoir s'approvisionner ou évoluer de façon à toujours pouvoir être en mesure de réparer le système. Ce qui a pour conséquence l'achat d'un stock important de rechanges.

En terme de sécurité, le problème des sous systèmes « boîtes noires » se pose aussi. Comment s'assurer que telle ou telle carte programmée pour une fonction principale adaptée au besoin n'est pas capable par ailleurs de déclencher un « virus informatique », un « vers » ou « une bombe logique »³ à un moment donné.

2.5 L'achat sur étagère

Le procédé paraît séduisant, mais recèle un certain nombre d'écueils sur lesquels il est facile de s'échouer. Les besoins de la défense sont souvent proches de certaines applications civiles, cependant certaines des contraintes précédemment citées ne sont pas prises en compte par les technologies civiles. Citons la sécurité, l'interopérabilité, la robustesse. Dans le cas de l'achat sur étagère quatre contraintes supplémentaires s'ajoutent :

- la pérennité de l'équipement en terme approvisionnement et de maintenance,
- l'interopérabilité avec les équipements déjà en service,
- la robustesse nécessaire à tout matériel opérationnel,
- l'intégration à un porteur pour le cas où l'équipement sera embarqué.

³ Le virus s'attaque aux données résidentes, le vers s'attaque aux réseaux saturants, la bombe logique se déclenche sous l'effet de l'envoi d'une commande inconnue de l'utilisateur, ou à une date donnée.

2.5.1 Nécessité d'être pérenne

Le monde civil est porteur de nouvelles technologies, la loi de l'offre et de la demande fait que parfois tel ou tel standard, prometteur au demeurant, disparaît après quelques mois de commercialisation victime de son concurrent direct. Citons dans le domaine de l'enregistrement vidéo le système VHS qui a détrôné le standard BETACAM. Plus proche de nous, la cassette audio numérique de PHILIPS, la DCC, détrônée et retirée du commerce, pour ce qui est des enregistreurs et des lecteurs, par le succès des mini disques de SONY.

Chaque domaine technologique nouveau voit s'affronter les grands constructeurs dans une lutte acharnée. Tant que les formats ne sont pas figés, il est hasardeux de faire un choix pour un système d'arme dont la durée de vie est estimée en moyenne à une vingtaine d'années. Si nous pensons être interopérables grâce à une technologie civile émergente, nous commettons une erreur. La normalisation des systèmes civils n'intervient qu'après la disparition des différents concurrents. Pour imposer la norme, la loi du marché fait foi. Aucune excellence technologique ne met un procédé nouveau à l'abri d'un échec commercial, donc d'une disparition certaine à court terme.

2.5.2 Nécessité d'être interopérable

Même si le système civil choisi s'impose et élimine ses concurrents, cela ne garantit pas l'interopérabilité. Les normes civiles existent mais elles ne s'appliquent pas à tous les domaines d'activité. Choisir un produit sur étagère garantira en général une facilité d'utilisation sur le territoire national, mais dès que l'on opère en dehors de la France ou de l'Europe, les problèmes se multiplient. Citons les différents standards de télévision, SECAM, Pal et NTSC, ou plus trivial encore la fréquence et l'intensité du courant électrique distribué en France et aux Etats Unis. Par ailleurs, normes civiles et militaires ne sont pas toujours compatibles. Même si l'OTAN fait actuellement de nombreux efforts pour transformer certains de ses accords de standardisation (STANAG), des domaines restent spécifiquement militaires et soumis aux décisions de l'OTAN.

Dans un contexte interallié, où la normalisation OTAN est la référence, le recours à un système civil non normalisé reste donc hasardeux. Quant à l'achat sur étagère de produits respectant les normes OTAN, il est souvent au profit d'industriels américains pour qui l'OTAN et ses STANAG restent une valeur sûre.

2.5.3 Nécessité d'être robuste

Pour le durcissement au brouillage et à l'impulsion électromagnétique, le problème est essentiellement financier. Le monde civil produit avec le souci de réduire les coûts afin d'obtenir un produit compétitif. Il met en oeuvre des techniques d'analyse fonctionnelle et d'analyse de la valeur qui permettent d'identifier chaque fonction du système et d'en évaluer son prix relatif. Il est donc possible de chiffrer en terme de coût de développement l'ajout ou le retrait d'une fonctionnalité.

Il est clair que pour un système de téléphonie civil dont la fonction principale est la communication en temps de paix dans un environnement sécurisé, les contraintes de robustesse ne seront pas prises en compte par le cahier des charges. Même si les modifications nécessaires sont mineures en terme de coût si elles sont prévues dès la conception, elle ne seront réalisées que si le marché militaire est ciblé dès la conception du produit. Ce qui n'est envisageable que si la défense participe au coût de développement, ce n'est plus alors réellement un achat sur étagère.

Pour la résistance aux contraintes physiques extérieures, intempéries, aérotransport, montage et démontage, une adaptation des matériels civils est très souvent indispensable. Les systèmes informatiques de commandement sont une bonne illustration de cette contrainte de durcissement. Réalisés à partir de stations de travail achetées sur étagère, ils imposent de part la nécessité de les transporter et de les déployer fréquemment la mise en container spécifique ou la mise en shelter.

2.5.4 Nécessité d'être intégré à un porteur

Ce dernier besoin est à la frontière de deux contraintes précédemment évoquées, le respect du développement des programmes, et les contraintes d'interopérabilité. En effet, l'intégration à un porteur est très contraignante en terme de sécurité d'emploi, de sécurité des vols notamment pour les aéronefs, mais aussi en terme d'espace disponible. Pour illustrer notre propos prenons deux exemples, l'un terrestre et l'autre aérien.

Pour le terrestre, intégrer un système de communication dans un véhicule se fera de façon à optimiser l'emploi et l'espace occupé, car celui-ci est par définition restreint. En conséquence, il sera souhaitable que le poste radio mis en place puisse servir aux communications de service courant, et aussi aux transmissions plus confidentielles. En d'autres termes, si un système civil performant donne satisfaction pour transmettre des données non confidentielles, et qu'un autre système durci et militarisé est nécessaire pour les liaisons protégées il faudra doubler la place, doubler les opérations de transmission, la formation des équipages, les pièces de rechanges, la maintenance. L'opération ne sera peut être pas techniquement possible ni opérationnellement acceptable.

Cependant, certains systèmes complètement civils ont été intégrés avec succès à des porteurs militaires. Citons l'exemple de caméras vidéos bâtons de surveillance connectées au magnétoscope de bord d'un mirage F1. Cette réalisation a nécessité des études et des essais importants de la part d'organismes spécialisés tels que le CEAM⁴ de Mont de Marsan. Etudes menées en relation avec l'industriel responsable de la conception du porteur, toute modification de la cellule ou de la cabine d'un avion étant soumises à des règles précises. La modification réalisée et validée sur un avion équipé d'un prototype, l'achat du matériel nécessaire à la modification de l'ensemble de la flotte fait l'objet d'un appel d'offre. Si celui ci est remporté par une société proposant une caméra équivalente mais différente de celle utilisée pour la réalisation du montage prototype, de nouveaux essais seront nécessaires. On le voit, cet exemple réel est bien loin de la souplesse qui vient à l'esprit dès que l'on évoque l'achat sur étagère.

La dernière contrainte à citer dans le cadre de l'intégration au porteur est la compatibilité électromagnétique. Ce point est technologiquement complexe et doit faire appel à des équipements sophistiqués tels que des chambres sourdes qui ne sont disponibles, pour les matériels importants, que chez quelques industriels. Le but est de garantir que l'équipement intégré ne perturbera pas le fonctionnement des autres systèmes du véhicule par son propre rayonnement. C'est pour cette raison notamment que l'utilisation des portables est interdite à bord d'un avion car le rayonnement produit peut affecter les commandes de vol électriques de l'appareil. Sur un porteur doté de systèmes de guerre électronique, tels que des détecteurs de départs missiles ou d'émission radar, ce point est particulièrement délicat à traiter.

2.6 L'assemblage de sous système

Ce procédé possède de nombreux avantages. Prenons l'exemple d'un matériel informatique. Un développement spécifique d'un ordinateur nécessite de longs mois d'étude, génère des coûts de développement importants. Le système mis en service, aucune évolution ne sera envisageable sans de nouveaux développements. En conséquence, le monde informatique étant en constante évolution, après deux années de service le système sera largement dépassé.

A l'inverse intégrer à un système militaire une carte mère civile peut permettre de faire évoluer celui-ci régulièrement en fonction des progrès de la technologie.

Bien appliqué, ce principe est parfaitement adapté au développement de systèmes militaires spécifiques répondant au besoin opérationnel. Cependant certaines précautions doivent être prises :

- Au niveau du contrat passé avec l'industriel en premier lieu. L'évolution des matériels militaires est lourde car elle est issue de l'époque où chaque système d'armes était construit spécifiquement. Dans un tel contexte faire évoluer un système au bout de quelques mois n'avait pas de sens. Aujourd'hui, les constructeurs de matériels informatiques font évoluer leurs

⁴ Centre d'expériences Aérienne Militaire chargé notamment de l'évaluation opérationnelle des nouveaux systèmes d'armes de l'Armée de l'air

machines tous les six mois, un ordinateur a une durée de vie estimée à deux ans. Ce fait doit être inclus dans le contrat, afin de ne pas perdre, pour des raisons administratives, le temps gagné par le recours à la dualité.

- Dans le domaine du logiciel, l'applicatif militaire repose souvent sur un système d'exploitation civil, il faut que les évolutions de celui-ci ne rendent pas l'applicatif spécifique inopérant après quelques années. A titre d'exemple, aujourd'hui, WINDOWS 3.1 n'est plus maintenu. Si une incompatibilité était détectée entre ce système d'exploitation et un applicatif militaire elle ne pourrait pas être techniquement résolue. En effet, Microsoft ne serait pas tenu d'apporter les corrections nécessaires de plus, l'industriel ayant développé l'applicatif n'a pas accès aux sources du logiciel WINDOWS. On aboutirait à une situation de blocage. Il faut donc faire évoluer l'applicatif avec chaque version du système d'exploitation.

- Dans le domaine de la sécurité, la remarque faite précédemment relative à l'effet « bombe logique » s'applique particulièrement. N'ayant aucun accès aux sources de certains logiciels d'exploitation ou de gestion de microprocesseurs, nous sommes très exposés à toute action d'espionnage dans le cas de systèmes reliés à des réseaux, ou de sabotage sous la forme de logiciels cachés programmés pour agir de façon spécifique dans des situations données (date, action précise).

Nous concluons cette partie par une remarque plus générale sur l'intégration de sous systèmes ou logiciels civils. La condition nécessaire à la rentabilité de l'utilisation d'une technologie duale est que celle-ci soit déjà mature et rentable pour l'industrie civile. En d'autres termes, il ne faut pas que cette technologie soit à la recherche de financement pour se perfectionner ou pour évoluer, et que son utilisation militaire ne soit qu'un soutien déguisé à une industrie en déficit.

Ce cas de figure peut être envisagé mais il sort de notre sujet, ce n'est plus de la dualité, mais de la recherche et du développement.

2.7 Service dual ou externalisation

Tout ou partie de ce qui vient d'être développé s'applique à la notion de service dual dans la mesure où les contraintes ou avantages évoqués ont un sens lorsqu'ils s'appliquent à un service et non à un système. A titre d'exemple, l'effet « boîte noire » qui peut contenir un « cheval de Troie informatique » s'applique aux télécommunications spatiales. La location de capacité de communication dans le cas de transmissions classifiées ne peut être envisagée que si on est certain que le satellite civil ne sera pas apte à écouter nos messages.

La dualité des services se heurte cependant à une contrainte majeure de la fonction militaire. Certaines de ses activités ne peuvent pas être programmées en terme de date, de localisation et de capacité nécessaire à un moment donné. Or, toute externalisation d'un service nécessite la rédaction d'un contrat décrivant le service proposé et garanti par l'industriel. Une entreprise civile ne peut pas se permettre de fixer un prix compétitif pour un service qui n'est pas précisément quantifiable. La rédaction de contrats d'externalisation est donc ardue et ne semble pouvoir s'appliquer qu'aux fonctions d'entraînement, ou non essentielles à la conduite de la manoeuvre.

De plus, l'externalisation n'est envisageable que pour des activités qui ne sont pas spécifiquement militaires. En effet, si la société civile ne travaille que pour la défense, il n'y a aucune raison que des employés civils soient plus productifs que des militaires. On retrouve une contrainte citée pour les systèmes : la condition nécessaire à la rentabilité de l'utilisation d'un service dual est que celui-ci soit déjà mature et rentable pour le monde civil.

2.8 Conclusion

Cette première partie nous a permis d'identifier certains avantages mais aussi des contraintes de la dualité.

Les avantages peuvent se résumer à :

- gain de coût de développement et de fabrication,
- fiabilité mieux maîtrisée sur les grandes séries,
- performance accrue et évolutive des systèmes d'armes.

Les inconvénients sont :

- vulnérabilité des systèmes civils qui nécessitent une adaptation
- effets « boîtes noires » dont on ne maîtrise pas le contenu,
- inadaptation du code des marchés publics,
- difficulté de contractualiser le besoin militaire,
- spécificité de certains besoins militaires,

Nous allons à présent étudier dans trois domaines précis comment, en tenant compte des éléments listés dans cette première partie, est prise en compte la dualité dans les programmes militaires.

3. Les systèmes d'information et de communication (SIC)

3.1 Les Systèmes de Communication (SC)⁵

Le besoin actuel des armées est de déployer des forces modulables sur des théâtres d'opérations multiples, et de fournir à ces éléments, depuis le territoire national le soutien opérationnel, dont elles ont besoin, notamment en matière de renseignement. Cette demande nécessaire à la maîtrise d'un environnement de plus en plus complexe a conduit à un accroissement très important des besoins en capacité de transmission.

Les progrès techniques constants doivent permettre de faire face à cette demande en augmentation, cependant dans le contexte budgétaire actuel et face à une technologie en perpétuelle mutation le recours à la dualité s'impose.

Il apparaît aujourd'hui souhaitable de préférer à une politique de programmes militaires spécifiques, souvent longue à mettre en oeuvre, une logique d'acquisitions de produits de consommation courante immédiatement disponibles.

3.1.1 Les systèmes de communication militaires

Le champ de bataille du futur verra surgir, jusqu'aux plus bas échelons, une abondance de systèmes informatisés dont les grandes capacités ne seront pleinement utilisées que s'ils sont reliés par un système global de communication qui permette le transfert d'informations en quantité et en temps réel à tous les utilisateurs potentiels, qu'ils soient sur le théâtre d'opérations ou en métropole. Les systèmes d'information et de communication militaires (SIC), comprenant les systèmes d'information (SI) et les systèmes de communication (SC) seront parties intégrantes de ce système global qui utilise également, selon le besoin, des moyens civils complémentaires assurés par des opérateurs publics ou privés.

Les SIC fixes sont armés par la chaîne TEI⁶ autour du réseau interarmées SOCRATE⁷, prolongé par des réseaux de desserte, MTGT⁸ pour l'Armée de Terre. La chaîne TEI est interconnectée aux différents réseaux nationaux militaires et civils, aux réseaux alliés et prolongée par des liaisons filaires, satellitaires et radioélectriques vers les forces projetées en action extérieure, les forces stationnées outre-mer et les ambassades à l'étranger.

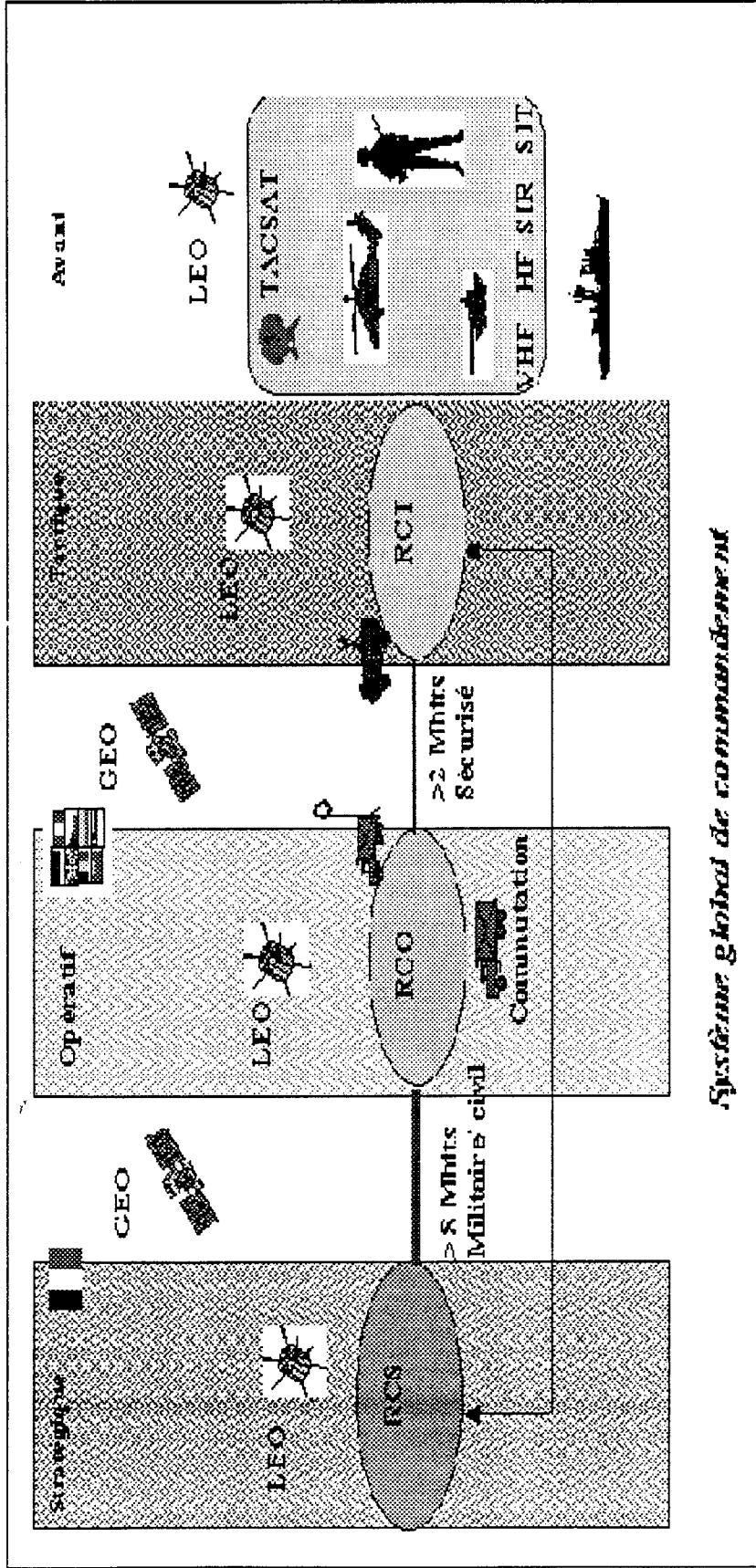
Les SIC projetables seront articulés autour du réseau commuté RITA 2000 qui doit s'imposer comme système fédérateur du niveau opératif.

⁵ D'après une « étude prospective des besoins en SIC » par le CETE de Rennes

⁶ Télécommunications et Informatique

⁷ Système Opérationnel Constitué des Réseaux des Armées pour les Télécommunications

⁸ Moyens de Transmissions des Garnisons Terre



Système global de communication

3.1.2 Les services attendus

Qu'ils soient militaires ou civils, nationaux ou alliés, les supports doivent assurer, depuis la métropole jusqu'au théâtre les services suivants, sans rupture pour l'exploitant et en toute transparence pour l'utilisateur avec les niveaux de sécurité convenables :

- La téléphonie et la télécopie militaires de niveau CD, voire SD,
- La téléphonie et la télécopie publiques de niveau inférieur au CD,
- Une messagerie incluant la messagerie d'autorité de niveau CD,
- La transmission de données (dont de très gros fichiers en temps réel) et la consultation de fichiers à distance de niveau CD,
- La transmission d'images (renseignement),
- La vidéo-conférence, jusqu'au niveau CD,
- La phonie tactique de niveau CD,
- Les multimédias.

3.1.3 La dualité dans un nouveau contexte technologique et budgétaire

La dualité, particulièrement applicable dans le domaine des télécommunications, doit permettre de diminuer les délais d'acquisition, de disposer sur de courtes périodes (4 à 6 ans) de matériels performants à un coût devenu raisonnable, aisément évolutifs ou remplaçables, et de limiter les études spécifiques aux stricts besoins du « noyau dur télécommunications ».

Le recours aux technologies civiles doit en particulier permettre aux armées de progresser rapidement et à moindre coût dans les domaines suivants :

- Utilisation des réseaux radiomobiles (sol ou satellite) en temps de paix, mais aussi en opérations.
- Développement de systèmes supports fiables et peu coûteux.
- Réseaux d'information, composés d'un système de transport et d'un système de traitement distribué, transparents pour les utilisateurs (maîtrise des interfaces et des plans de numérotation, transparence des interfaces techniques).
- Capacité de commutation du niveau théâtre d'opération.
- Généralisation et développement à tous niveaux des systèmes informatiques.
- Consultation des bases de données à distance.

Cependant le recours à la dualité impose à l'Armée de Terre de prendre en compte deux concepts nouveaux :

- L'Armée de Terre doit devenir un « **opérateur télécom militaire** » au même titre que tout autre opérateur civil, afin d'être reconnu par les organismes ou industriels civils et d'être partie prenante dans des systèmes satellitaires (Les USA ont par exemple investi 9 G\$ dans le projet Télédésic).
- L'Armée de Terre, devra disposer d'un **service de suivi et de contrôle**, en liaison avec l'EMA et la DGA, qui tiendra à jour un catalogue des ressources offertes par l'industrie civile nationale ou étrangère, dans les différents domaines que sont les supports, la desserte des abonnés, l'administration des systèmes, l'informatique générale, la sécurité des systèmes d'informations. Les ressources devront être validées et régulièrement évaluées en terme de fonctionnalité et de sécurité. De cette façon, lors du passage d'un nouveau marché, le produit répondant le mieux au besoin sera proposé immédiatement, sans nouvelle consultation des organismes proposant, de façon à limiter les délais d'acquisition des nouveaux produits.

3.1.4 Ensembles fondamentaux

Tout système global de communication repose aujourd'hui sur une complémentarité de différents systèmes : réseaux d'infrastructure, réseaux tactiques et systèmes satellitaires. A titre d'exemple, pour l'Armée de terre la continuité SIC du niveau stratégique jusqu'au niveau tactique reposera sur 5 ensembles fondamentaux :

- Un réseau commuté stratégique national dont le nœud central sera SOCRATE.
- Un réseau commuté de transit de théâtre (opératif), interopérable avec les réseaux stratégiques et tactiques, nationaux ou alliés, civils ou militaires, assurant la totalité des services de communications.
- Une composante satellitaire type multicanal travaillant dans des gammes de fréquences compatibles avec les systèmes alliés, principalement SHF (8 Ghz uplink, 7 Ghz downlink) et EHF (44 Ghz uplink, 20 Ghz downlink), disposant d'une commutation à débit variable adaptée aux services et possédant une forte résistance au brouillage pour une partie des communications. Cette composante doit être capable d'intégrer, de manière transparente, un ou plusieurs vecteurs spatiaux civils ou militaires alliés. De plus, elle doit présenter une interopérabilité totale avec les autres systèmes satellitaires.
- Un réseau commuté tactique des forces terrestres, interopérable avec les réseaux commutés opératifs, les réseaux tactiques alliés de même nature et les réseaux tactiques de l'avant, nationaux ou alliés, civils ou militaires, assurant également la totalité des services de communications.
- Des réseaux radio multibandes et multimodes de l'avant, d'encombrement très réduit et capables d'acheminer jusqu'aux plus bas échelons (sections et en dessous) des données et de l'imagerie. Ces moyens doivent être compatibles avec les réseaux commutés de théâtre et la composante satellite monocanal.

3.1.5 Les réseaux support

3.1.5.1 Niveau stratégique

A l'intérieur du territoire métropolitain, les liaisons stratégiques seront assurées par un réseau de télécommunications de transit interarmées multiservices réunissant dans un maillage commun les réalisations existantes ou en cours. Ce réseau doit faire partie du **noyau dur**.

Les commandants supérieurs dans les départements et territoires Outre-mer (COMSUP), les commandants des forces françaises à l'étranger (COMFOR), les forces prépositionnées ou projetées doivent bénéficier **des mêmes services** que les Etats-majors de métropole afin de pouvoir servir en cas de besoin de " Q.G. parent " aux PC de théâtre projetés. Cela nécessite que leur raccordement soit assuré par des réseaux militaires et civils satellitaires interopérables avec les réseaux américains, alliés, ONU et OTAN. L'interopérabilité avec les supports de transmissions civils et le réseau de transit d'infrastructure à couverture mondiale devra aussi être effective.

Le réseau support stratégique doit pouvoir intégrer des **systèmes SIC civils** (exemple des réseaux radiomobiles) afin de compléter les services offerts dans des domaines non réalisés par des moyens militaires. Il doit être capable de raccorder de manière transparente le réseau commuté opératif.

3.1.5.2 Niveau opératif

Les besoins de communications du niveau opératif seront satisfaits par des **moyens longue portée** (satellites militaires ou civils), à **haut débit et sécurisés**, par des **moyens de transmissions civils** assurant l'écoulement du trafic non protégé, et des systèmes hertziens de nouvelle génération. L'ensemble de ces supports doit permettre l'intégration de tous les nouveaux services.

Les réseaux supports des commandements opératifs doivent s'appuyer sur une composante stratégique nationale, mettre en œuvre un **système commuté unique** (système fédérateur de théâtre), assurer des débits de l'ordre de 8 Mbits aussi bien vers le haut que vers les subordonnés, être entièrement interopérables avec les réseaux d'armées opératifs alliés et les réseaux d'infrastructure de la nation hôte, et être totalement transparent pour les utilisateurs. Il doit être capable de raccorder de manière transparente le réseau commuté tactique.

3.1.5.3 Niveau tactique

Les besoins de communications du niveau tactique seront satisfaits par des **moyens moyenne portée** militaires sécurisés (satellites, FH NG), à **moyen débit**, et par des **moyens de transmissions civils** assurant l'écoulement du trafic non protégé. L'ensemble de ces supports doit permettre l'intégration de tous les nouveaux services.

Les réseaux support des commandements tactiques doivent s'appuyer sur une composante opérative de même technologie, mettre en œuvre un **système commuté unique**, assurer des débits de l'ordre de 2 Mbits aussi bien vers le haut que vers les subordonnés, être entièrement interopérables avec les réseaux d'armées nationales ou alliées de même niveau, et être totalement transparent pour les utilisateurs.

Il doit être capable de raccorder de manière transparente les réseaux tactiques de l'avant.

3.1.5.4 Les réseaux support de combat de l'avant

Les moyens de communication de l'avant devront couvrir les besoins en liaisons sol-sol, sol-air et air-air (ALAT) du théâtre (commutation, transit inter zones). Ils devront permettre le raccordement d'abonnés fixes ou itinérants, isolés ou groupés, parfois très éloignés, avec des services identiques à ceux offerts en métropole.

Les abonnés, appartenant à un même réseau, doivent pouvoir converser par des moyens de natures différentes (non homogènes). Ceci exige en particulier la constitution de réseaux pour le commandement d'unités subordonnées agissant sur un théâtre lacunaire, à des distances hétérogènes, que ne **couvrent pas les moyens classiques**. De ce fait, les réseaux de l'avant doivent pouvoir être réalisés par radio, par **satellite (TACSAT)** ou par systèmes mixtes.

L'ensemble des moyens SIC militaires mis à la disposition des forces devra être complété par l'emploi de systèmes de communications civils (satellites, radio, réseaux supports) de service courant, soit acquis, soit mis en œuvre par protocoles.

3.1.5.5 Les réseaux locaux (SI)

Le rapprochement permanent entre les fonctions assurées par les réseaux locaux de type informatique et les systèmes téléphoniques accroît le besoin d'ouverture des premiers vers le monde extérieur, notamment vers les systèmes d'information des alliés, en tenant compte des précautions particulières et délicates de sécurité en la matière. L'interconnexion entre les réseaux est réalisée au cas par cas en fonction du besoin.

3.1.6 Le « Noyau dur » de télécommunications militaires

Le recours aux moyens de transmissions civils ne dispensera pas l'Armée de Terre de disposer d'un « noyau dur » de télécommunications militaires, notamment pour les liaisons de commandement du CEMA et les communications de théâtre. Il faut donc disposer d'un réseau commuté stratégique national, de satellites de communication et de réseaux commuté de théâtre.

Cette notion de « noyau dur » peut par contre se révéler dangereuse, car l'ambiance des contraintes budgétaires sévères entraînera le décideur à sacrifier tout ce qui n'est pas noyau dur. La cohérence du système global de communications sera-t-elle alors toujours garantie, et disposera-t-on

toujours de moyens civils adaptés en quantité et en qualité à chaque fois que les Armées en auront besoin ?

Par ailleurs, le recours aux moyens de transmissions civils rend obligatoire de se prémunir davantage contre les actions de malveillance et d'espionnage. Un effort plus important doit donc être fait dans le domaine de la sécurité des systèmes d'information (SSI). La recherche spécifique doit être conservée, avec un temps d'avance sur la technologie civile. Par ailleurs, l'interopérabilité nécessaire doit notamment conduire à une uniformisation nationale des clés et à la mise en place d'une cellule SSI interarmées.

3.2 La composante satellitaire⁹

Le concept nouveau de projection fait qu'il faut aussi des systèmes de communication projetables, facilement redéployables sur le théâtre et servis par un nombre limité de personnels. Les unités SIC de l'échelon initial, des PC de l'avant ou les éléments isolés doivent également bénéficier du système global de communication. La solution technique passe par l'usage des satellites qui permettent de relier tout le monde, en évitant les coupures géographiques, les aléas de la propagation HF, et ceci à des conditions économiques qui seront acceptables.

3.2.1 Besoin satellitaire militaire à l'usage des forces projetées

Les services satellitaires militaires nécessaires aux forces projetées sont organisés en 3 catégories :

- La desserte bidirectionnelle d'usagers individuels à bas débit < 64 kbit/s (téléphonie, télécopie, messagerie) pour des missions de renseignement, les contrôleurs avancés, la recherche humaine, les détachements de liaison (DL).
- Les artères de communications bidirectionnelles à moyen débit 2 Mbit/s entre les postes de commandement.
- Les services unidirectionnels de diffusion haut débit à partir de la métropole (images, rens, météo, cartographie...)

3.2.2 Le « noyau dur » satellitaire

Syracuse I, lancé à partir de Télécom 1A (1984) et 1B (1985) pour un coût de 2 milliards de FF s'était caractérisé par de très grosses stations à bas débit, résistantes aux agressions de brouillage et aux effets nucléaires. Le succès de son utilisation dans les armées a conduit au lancement de Syracuse II à partir de Télécom 2 (1991) pour un prix équivalent à Syracuse I. Les entreprises engagées étaient Matra, Aérospatiale et Thomson-CSF. Le principe de mise en place de répéteurs militaires sur un même satellite civil se révéla moins onéreux pour les militaires qu'un système militaire indépendant avec des satellites autonomes.

Dans le cadre du projet TRIMILSATCOM (France, Grande-Bretagne, Allemagne), Syracuse III représentera le noyau dur futur des télécommunications par satellite en constituant l'ossature des liaisons protégées et de grande élongation, indispensable à la chaîne de commandement de CEMA. Il assurera les liaisons avec les centres de commandement déployés sur les théâtres d'opérations extérieurs, les forces prépositionnées, ainsi que les liaisons permanentes de commandement des forces navales. Sur le lieu de l'action, il supportera de surcroît les liaisons nécessaires à l'engagement en toutes circonstances des forces, quand l'utilisation d'autres moyens ne peut être envisagée. Il assurera ainsi notamment l'interconnexion des bulles RITA dans un dispositif lacunaire.

Ce noyau dur doit permettre de garantir la souveraineté et la maîtrise du système, la disponibilité des liaisons (protection contre le brouillage et la saturation), la protection contre la localisation (discrétion de la station émettrice), la sécurité de certaines liaisons (liaisons du CEMA, liaisons 2 Mbit/s du PCIAT), l'interopérabilité avec les autres systèmes nationaux et alliés. Il doit

⁹ d'après « Parti à tirer des systèmes civils » de la DGA et « Syracuse III » de l'EMA/TSIC

permettre également d'éviter la multiplication des équipements nécessités par le recours à plusieurs systèmes civils complémentaires. Les bandes utilisées seront SHF et EHF. Son dimensionnement a été évalué à 110 Mbit/s dont 33 Mbit/s pour l'Armée de terre avec 226 stations terminales de type haut et moyen débits (exemple de la station tactique TANIT à 512 kbit/s).

Mais la Grande-Bretagne s'est retirée du projet, sans doute au profit d'une solution nationale dérivée de leur système civil Skynet. La France doit alors s'orienter vers une solution de transition ou « gap filler » : Disposant d'une capacité supérieure, le satellite de transition à Syracuse II pourra dans un premier temps fonctionner sans aucune évolution du segment sol. Une modification suivie d'une rénovation de ce segment sol sera ensuite nécessaire pour assurer la cohérence d'ensemble.

Cependant, le système Syracuse ne reste qu'une « boîte noire » à bord de satellites civils. Il ne faut donc pas tout « miser » sur le satellite et disposer de moyens terrestres longue portée telle que la HF.

3.2.3 L'offre commerciale

L'offre commerciale, jusqu'à présent, se sépare en deux classes :

- Les services fixes à débit élevés (Intelsat, Eutelsat), accessibles à des stations moyennes ou légères (VSAT).
- Les services à débit plus faible (Inmarsat), accessibles à des stations très légères et mobiles.

Devant être compétitifs par rapport aux systèmes sol, les systèmes satellitaires devront cibler la part de marché visée et optimiser leur conception pour les services assurés. L'offre future verra alors trois types de systèmes spécialisés :

- La dernière génération des services fixes ou dédiés à la diffusion (TV essentiellement).
- La téléphonie radiomobile par satellite.
- Les systèmes fixes multimédias, offrant un multiplex de services différents (phonie, données, vidéo ...) avec un débit élevé.

Services	Principaux systèmes défilants	Principaux systèmes géostationnaires
téléphonie radiomobile	Iridium, Globalstar, ICO	East
multimédia	Skybridge, Télédesic	West
Diffusion TV		Eutelsat

3.2.4 Utilisation de l'offre commerciale

Les systèmes existants sont géostationnaires. Les armées utilisent principalement le système Inmarsat en complément de Syracuse II (250 terminaux pour un coût de fonctionnement de 30 à 50 MF/an). Le retour d'expérience montre qu'en situation de crise, ce type de moyen ne permet pas l'accès immédiat aux communications pour cause de saturation ni l'établissement à la demande de jonction à haut débit. Seule une connexion permanente permettrait de s'affranchir de cette difficulté mais serait particulièrement onéreuse. Outre Syracuse III, il sera donc nécessaire de compléter avec des systèmes défilants qui pourraient ne pas être adaptés à des utilisations militaires car ils nécessitent la localisation des abonnés pour des raisons de facturation, et présentent donc une vulnérabilité importante.

Les systèmes commerciaux peuvent offrir 2 types de services : une desserte bas débit non protégée jusqu'à 64 kbit/s (abonnées mobiles hors de la couverture des réseaux tactiques) et une desserte haut débit non protégée (gros fichiers de cartographie ou de météorologie) entre la métropole et les forces projetées. Les liaisons ainsi assurées ne sont pas jugées primordiales à la conduite de l'action, leur établissement et leur exploitation peuvent être différées dans le temps en cas d'interruption de service. Elles recouvrent en particulier :

- les communications pour le soutien psychologique du personnel (téléphonie, télévision et radio),

- les communications de certains personnels dont la sécurité n'est pas menacée (observateurs ONU...),
- les communications liées aux affaires civilo-militaires,
- les communications administratives, de documentation, de reportage (SIRPA).

Les abonnés mobiles devront pouvoir utiliser de manière transparente soit d'un réseau satellitaire, soit d'un réseau radiomobile (terminaux bimodes).

Un panorama sur l'usage possible des systèmes civils par la Défense est joint en annexe.

Aux USA, le Pentagone s'appuie également sur des services commerciaux pour ses besoins en communication avec les théâtres extérieurs (prévision d'un besoin de 4 Gbit/s d'ici 10 ans). Par ailleurs, l'US Army louait déjà en 1997, 300 Mbit/s de capacité sur des satellites commerciaux pour un coût annuel de 135 M\$.

Les critères d'analyse de l'adéquation du besoin des Armées et de l'offre commerciale sont principalement

- Les conditions d'emploi par l'utilisateur (niveau de risque que les opérationnels sont prêts à prendre sur le brouillage, l'écoute, l'interception des communications) en cherchant à desservir par des systèmes commerciaux les services ne nécessitant pas de conditions d'emploi militarisées
- L'intégration physique et électromagnétique sur les porteurs

3.2.5 Limites de l'offre commerciale

Le service

- Les systèmes civils seront spécialisés en visant une ou deux catégories de service, d'où un morcellement de l'offre entraînant une multiplication des opérateurs et des équipements adéquats.
- Très peu d'opérateurs offrent véritablement une desserte de toutes les zones du globe. Les satellites géostationnaires n'assurent qu'une couverture régionale et ne peuvent couvrir les zones extrêmes (pôles). Les satellites moyenne et basse altitude ont une vocation mondiale, mais souvent se restreignent pour des impératifs techniques ou économiques (rentabilité). Des passerelles avec le sol ne sont pas déployées sur les océans, et certains satellites se mettent en veille sur les zones non rentables. Seuls ICO, Iridium et Télédésic ont la capacité technique à desservir le globe tout entier.
- Les services mobiles sont offerts uniquement pour le bas débit.
- Il n'y a pas d'interopérabilité avec les systèmes militaires normalisés selon les stanags OTAN.
- La disponibilité des systèmes civils est élevée, mais ne garantit pas 100% car les normes « grand public » permettent un compromis coût / garantie de service très en faveur des coûts.
- La pérennité d'un système civil n'est pas garantie. Autant les Armées peuvent en être un client, autant elles ne pourraient à elles seules en assurer la survie.
- Par ailleurs, que faire en cas de contrat non respecté, synonyme de service non assuré ? Il faut s'assurer d'un service minimum ou de substitution auprès de la société prestataire (protocole d'accord), ou d'une société concurrente, ou par des moyens militaires (par exemple HF).
- La fidélisation à un opérateur (par exemple Inmarsat) ne sera plus garantie puisqu'il faudra repasser les marchés, au niveau européen, tous les 2 ans.

Le brouillage

- La recherche de minimisation du coût des terminaux, donc de leur taille et de leur puissance, oblige les satellites à avoir une sensibilité accrue, y compris intrinsèquement au brouillage.
- Le nombre croissant de satellites en service et en projet aboutit à un encombrement

croissant des positions orbitales et des bandes de fréquence et par là-même à une augmentation des problèmes de brouillage. Il suffit de notifier son intention de réaliser un système satellitaire pour obtenir et bloquer des ressources.

- Brouiller les liaisons civiles est plus facile et moins coûteux que s'attaquer aux liaisons militaires Syracuse 3.

Le coût

- Le support satellitaire civil utilisé par la France est INMARSAT. Il couvre notamment le Pacifique non couvert par Syracuse. Le coût est de plus de 5\$ / minute. Le coût prévisible des nouveaux opérateurs varierait entre 1 et 2,5 \$ /minute pour les LEO et entre 0.5 et 1\$ / minute pour les systèmes géostationnaires.
- Les coûts des terminaux civils sont également tirés vers le bas de manière très importante, grâce à des investissements technologiques très poussés et des séries très longues. Les terminaux multimédias à vocation « stable » ne sont pas conçus pour supporter les démontages, les transports, les chocs, encore moins des aéronefs. Par contre les terminaux portatifs à vocation « mobile » sont plus robuste mais coûtent plus chers malgré leur taille plus petite et leur plus faible débit.

La sécurité

- Les opérateurs français et européens préconisent une desserte locale (Skybridge, East), c'est-à-dire la nécessité d'un ancrage d'une grosse station par région puis l'utilisation d'opérateurs terrestres nationaux qui peuvent être un jour ceux d'un pays belligérant. A l'opposé, les systèmes US proposent des liaisons intersatellites (Iridium, Teledesic), mais ils ont par conception la possibilité de rapatrier toute l'information aux USA.
- La réglementation sur la taxation des télécommunications impose aux opérateurs de localiser les émetteurs mobiles, ce qui s'avère incompatible de la vocation discrète de certaines stations militaires. Il faut donc un chiffrement des communications que la législation actuelle en France et aux USA impose d'être aisément contournable par des moyens gouvernementaux.

3.2.6 Une étude de coût intéressante

Nous avons vu dans une partie précédente, que la Grande-Bretagne s'est retirée du projet Trimilsatcom, laissant dans l'embarras et en recherche d'une solution palliative ses partenaires à savoir l'Allemagne et la France. Cette décision a eu pour conséquence le lancement par la DGA de différentes études relatives aux nouvelles possibilités de coopération entre la France et l'Allemagne pour le remplacement de Syracuse II.

L'étude d'un document de travail confié par le SPOT¹⁰ nous permet d'obtenir des éléments de prix comparatifs entre une solution s'appuyant sur une sous traitance totale des services de communication à des sociétés telles que INTELSAT et EUTELSAT, et des solutions purement militaires basées sur le lancement d'une constellation spécifique de trois satellites géostationnaires.

Trois options ont été chiffrées.

option 1 : appel aux services de INTELSAT et EUTELSAT.

option 2 : l'Allemagne s'engage à payer à la France une redevance pour l'utilisation du premier satellite de la constellation qui devrait être lancé en 2003. Cette hypothèse se décompose en deux scénarios :

option 2a l'Allemagne s'engage tôt et pour une période importante.

option 2b l'Allemagne s'engage tard et pour une faible période.

option 3 : L'Allemagne participe à la mise en oeuvre du satellite qui doit être lancé en 2003. En échange de cette prise de risque initiale liée à la participation au développement du programme, elle bénéficie de prix plus attractifs en terme d'exploitation. On distingue la aussi deux sous options liées à l'étalement des paiements par l'Allemagne.

Les prix indiqués sont en millions de francs par Méga Hertz et par an.

¹⁰ Joint Programme Office report on Franco-German Mid-Term Solutions 06.11.98

Option	évaluation haute	évaluation basse
location service civil	0.91 MF	0.61 MF
option 2	0.60 MF (option 2a)	0.41 MF (option 2b)
option 3	0.31 MF (option 3a)	0.24 MF (option 3b)

Ce tableau amène deux remarques.

La première est qu'à priori, le financement d'un projet spatial militaire ne semble pas plus coûteux que l'appel à la sous traitance du service par une société civile. En effet, même avec une participation réduite de l'Allemagne sous forme d'une location de capacité de transmission à la France le projet de développement spécifique reste dans une fourchette de coût voisine de celle de la sous traitance.

La seconde est que la comparaison se fait en terme de capacité de transmission offerte par an. Il est donc essentiel de bien déterminer les besoins des armées avant de déclarer telle ou telle solution rentable. L'appel aux solutions civiles tout comme le développement de solutions spécifiques peuvent s'avérer catastrophiques, en terme financiers, en cas d'erreur d'appréciation. Dans le premier cas le risque est de payer le prix fort parce que l'on a dépassé les capacités de transmission allouées par le contrat d'abonnement ; dans le second cas le risque est de développer des capacités spécifiques sur dimensionnées et dont l'équivalent en terme d'abonnement aurait coûté moins cher.

Cependant compte tenu de la nécessité pour les forces armées de disposer d'un noyau dur des communications dont la composante spatiale est incontournable, cette étude apporte un argument intéressant et montre que sous certaines hypothèses d'utilisation et de coopération, l'acquisition d'une constellation de satellites de communication militaires reste envisageable.

3.3 La composante terrestre

3.3.1 Le besoin opérationnel

Les besoins futurs dans le domaine des communications non satellitaires proviennent essentiellement de l'augmentation très forte du débit nécessaire, et de l'aspect lacunaire du champ de bataille qui nécessite des liaisons longue distance entre deux zones de présence sur le théâtre. Les besoins à court et moyen termes sont les suivants : augmentation du débit du PR4G pour satisfaire les besoins en transmission de données du champ de bataille, faisceau hertzien de nouvelle génération pour RITA NG autorisant un débit supérieur à 8 Mbits/s, faisceau hertzien troposphérique, poste radio multimode (HF et VHF), commutateur de grande capacité. Ces différents composants relèvent aisément d'une dualité du niveau composant ou équipement.

3.3.2 Intérêt et limites de la dualité

Les communications du champ de bataille, depuis le niveau stratégique jusqu'au niveau du combat de l'avant, font désormais appel à la notion de **système global de communication**, avec des contraintes très fortes d'intégration entre les différents sous-systèmes, et d'interopérabilité avec les systèmes alliés. Pour cette raison, le domaine militaire doit forcément garder le contrôle des principaux sous-systèmes (réseau RITA fédérateur au niveau opératif et tactique par exemple) et la dualité peut apparaître seulement :

- **au niveau des équipements**, si les systèmes civils existants permettent de satisfaire les spécifications militaires;
- **au niveau des composants** pour les systèmes de transmissions les plus lourds (faisceaux hertziens par exemple) qui dans le secteur civil ne sont pas conçus pour une utilisation en environnement hostile et manquent de robustesse. Dans ce cas, il convient de poursuivre et de développer l'effort réalisé par exemple lors du développement du PR4G, dans l'amélioration du dynamisme de la conduite des programmes;

- **au niveau des services** mais dans des domaines limités, qu'il convient de définir très finement au cas par cas pour chaque situation, en fonction du risque pour la maîtrise de l'information et du risque consenti par l'opérateur civil pour la sécurité de ses personnels et de ses installations.

L'achat sur étagère de petit matériel portable est envisageable ponctuellement chaque fois que le système global ne répond pas aux besoins d'une situation particulière, mais les contraintes d'intégration à ce dernier devront être soigneusement étudiées auparavant (gestion globale de la sécurité, environnement électromagnétique...).

3.3.3 L'exemple du programme PR4G

Concernant le programme radio PR4G, il s'agit d'une dualité au niveau des composants civils introduits dans un système militaire pour remplir des fonctionnalités spécifiquement militaires telles que l'évasion de fréquence, la discrétion et le chiffrement.

Dès son lancement en 1986, le programme PR4G a été dominé par une très forte pression sur les coûts, ce qui a conduit à de gros efforts pour en optimiser l'organisation. L'une des grandes options a été l'utilisation de composants montés en surface (CMS) à encapsulation plastique, une première mondiale sur ce type d'équipement. Cette technologie, outre le fait qu'elle entraîne une réduction significative des coûts de production et de possession par rapport aux composants en boîtier céramique, confère aussi une assurance élevée de disponibilité du fait de sa très grande diffusion dans les applications civiles. Une autre option importante fut de **reconcevoir le produit en cours de fabrication**, opération dite de convergence technologique. Cela a permis de bénéficier des dernières avancées dans le domaine des composants dont la miniaturisation croissante et le gain de productivité dans le secteur, conduisent à des gains de performance accrus pour des prix moindres. De plus, les risques liés à l'obsolescence des composants critiques ont été réduits, et il a même été possible de rajouter des fonctionnalités, compte tenu du gain de place sur les cartes.

Ainsi dans ce cas précis, la dualité du niveau composant a permis des gains très importants, mais cela a surtout été possible grâce à une organisation dynamique et originale de la conduite du programme. Les points clé furent:

- la limitation de certaines spécifications initiales qui a permis d'atteindre un niveau de technologie plus intéressant,
- l'utilisation de l'évolution technologique pour la reconception au cours de la phase de production,
- l'optimisation du concept d'emploi à l'issue des premières expérimentations, toujours pendant la phase de production, avec pour conséquence une adaptation des contrats avec l'industrie, par exemple afin d'adapter le volume de commande des équipements périphériques.

3.3.4 Les réseaux radio-mobiles civils

Ces systèmes peuvent être utilisés en complément du noyau dur constitué par le système commuté de théâtre, pour acheminer un trafic non protégé soit au sein du théâtre, soit vers la métropole. La tentation est grande aujourd'hui d'utiliser ces systèmes au profit des opérationnels en complément du réseau protégé PR4G. Les deux raisons principales sont la couverture en principe assurée des zones lacunaires, et la facilité de liaison en zone urbanisée que ne permettent pas les postes de la gamme VHF. Même si cette permanence de la liaison donne une capacité de réaction immédiate, en particulier en matière de sécurité des personnels, les radiotéléphones mobiles ne doivent être utilisés qu'en complément tant que l'on ne dispose pas de moyens de chiffrement d'extrémité.

Un autre type d'utilisation crée un risque pour la maîtrise de l'information sur un théâtre d'opération : il s'agit de l'utilisation par les soldats de tous grades pour communiquer avec leur famille. De nombreuses informations normalement protégées telles que la localisation, l'état ou les intentions

de certaines unités, peuvent ainsi être interceptées, utilisées ou médiatisées. Cela suffit à compromettre gravement la sécurité d'un dispositif ou la réussite d'une mission.

Enfin la prolifération de ce type d'équipement constitue un autre risque. Car il faudra bien payer les abonnements et les communications et il existe forcément une limite à ne pas dépasser pour que l'utilisation de ce service soit « rentable ». Celle-ci doit faire l'objet d'un calcul suffisamment fin.

3.3.5 Internet

Internet comme tous les réseaux non protégés offre aujourd'hui des possibilités limitées au trafic non classifié. Il présente cependant certaines spécificités :

- c'est un réseau universel de couverture mondiale, avec lequel il convient de se familiariser pour pouvoir le moment venu, en tirer le meilleur profit. De plus, il permettra, à terme, de transmettre des messages chiffrés ;
- il est encore en pleine évolution, que ce soit dans ses normes technologiques, son concept d'emploi (même dans le domaine civil), et ses modalités de gestion.
- l'interconnexion des réseaux dont il offre la possibilité est un facteur de vulnérabilité extrêmement important dont il convient de se prémunir, soit en refusant toujours de connecter un réseau militaire à Internet (ce qui constitue la solution actuelle), soit en développant les moyens de protection informatique type pare-feu, domaine dans lequel le secteur civil effectue des recherches très importantes.

3.3.6 Externalisation des télécommunications d'infrastructure :

Sous le poids des contraintes déjà évoquées, la notion d'externalisation bien connue des entreprises civiles depuis une dizaine d'années, tend naturellement à s'imposer dans le domaine des télécommunications militaires d'infrastructure, libre à première vue de toute contrainte opérationnelle. En première approche, cette évolution permettrait d'effectuer des gains financiers et en personnels qui pourraient être utilisés à des tâches plus spécifiquement militaires (c'est la notion de recentrage sur le métier). Dans cet objectif, un groupe de travail piloté par l'EMA a déjà réfléchi aux différentes solutions possibles. Cette étude, qui n'est pas encore terminée, a pour l'instant dégagé quelques grandes lignes de ce domaine totalement inconnu des militaires.

La définition suivante a été proposée¹¹ pour l'externalisation: « *démarche par laquelle un organisme ou une entreprise décide de confier une partie ou la totalité des ses systèmes de télécommunication à un tiers, met en œuvre cette décision et en assure le suivi, les résultats et les conséquences au cours du contrat* ».

Elle met en avant la volonté de contrôle de la prestation fournie par l'opérateur civil, et l'importance du contrat passé avec ce dernier. En effet l'un des principaux soucis mis en avant est bien la **défaillance du prestataire** consécutive par exemple à des troubles sociaux, des difficultés de trésorerie, des changements de stratégie trouvant leurs origines dans des restructurations du secteur ou des aléas des circuits financiers internationaux. Cependant il en existe d'autres tout aussi importants tels que:

- l'irréversibilité presque certaine du processus due à la perte de compétence dans le domaine externalisé, qui se traduit par une **dépendance excessive** vis à vis de l'opérateur,
- les **risques contractuels** conséquences d'un contrat mal négocié qui peuvent conduire à une rupture délicate, aussi bien de la part de l'opérateur constatant qu'il ne trouve pas le retour sur investissement escompté, que des armées non satisfaites de la qualité des services offerts (l'expérience de l'externalisation dans le civil a clairement mis en évidence toute la difficulté qu'il y a, à prévoir totalement dans un contrat toute la qualité du service désiré, ce qui a souvent poussé les entreprises à faire marche arrière en matière d'infogérance, au bout de quelques années),
- l'insuffisance des **garanties en matière de sécurité**, liée à la méconnaissance de la culture militaire par l'opérateur.

¹¹ Rapport d'étape n°2 transmis au Cabinet du ministre par note de l'EMA n° 10300/DEF/EMA/TEI/6 DU 13 novembre 1998

En revanche, des avantages certains sont escomptés. D'une part les domaines techniques externalisés seront maintenus à la pointe de la technologie, tout en transférant l'effort correspondant chez le prestataire, et en favorisant l'interopérabilité. D'autre part, des gains financiers sont attendus bien qu'ils n'aient encore pu être exprimés avec précision.

Parmi les différents scénarios envisagés, l'un prévoit dans une première étape l'externalisation du réseau interarmées SOCRATE. Celle-ci pourrait aller de la cession onéreuse totale ou partielle du réseau, à une location assortie de conditions précises en matière de qualité de service. Une deuxième phase verrait ensuite l'externalisation des moyens de transmission des différentes armées (MTGT, MTBA, RVDM).

Dans tous les cas, la notion de « noyau dur » est présente, même s'il ne s'agit pas forcément d'une sous-partie de réseau qui resterait militaire de bout en bout. On peut envisager par exemple des grandes fonctions à conserver dans la main des militaires, telles que le commandement du réseau, réalisé par intégration d'officiers au sein de l'entreprise civile, ou la sécurité des systèmes d'information.

L'expérience britannique en la matière a été étudiée et a montré la lenteur du processus (il s'est écoulé 17 ans entre les premières études et la signature d'un contrat), et les difficultés pour rédiger un contrat.

3.4 Les Systèmes d'information :

Les systèmes d'informations (SI) sont particulièrement aptes à profiter des progrès technologiques issus du monde civil. Architecturés autour d'un système informatique, ils sont aujourd'hui réalisés à partir d'ordinateurs civils. Citons, à titre d'exemple, le système de préparation de missions (CINNA 3) de L'Armée de l'air utilisant des stations de travail SUN. Développé depuis le début des années 80, il offre un retour d'expérience intéressant pour ce qui est de l'emploi de technologies duales par les armées dans le domaine des SI.

3.4.1 Le besoin militaire

Les systèmes d'informations sont constitués de réseaux informatiques locaux capables d'être interconnectés. Ils mettent en oeuvre une famille de logiciels utilisant une base de données commune. Ces différents réseaux sont déployés en des lieux géographiques différents et communiquent par des interfaces de type modem. On le voit cette description sommaire peut s'appliquer à de nombreuses applications civiles. Cependant, l'utilisation militaire du système engendre des contraintes spécifiques.

En premier lieu, la sécurité de la transmission des données doit être garantie. Le SI est en effet le lieu de stockage et de transit de nombreuses informations possédant un caractère confidentiel. Coordonnées d'objectifs, situation tactique du champ de bataille, ordre d'opération, images de reconnaissance. Il y a donc nécessité de protéger l'accès à l'information, mais aussi d'identifier l'émetteur et le destinataire de chaque message. Par ailleurs, toute information confidentielle émise doit être cryptée. Employés dans des environnements très divers, le principe de confidentialité ne peut pas reposer uniquement sur un durcissement des réseaux de transmission.

Les contraintes de robustesse sont aussi importantes. De tels systèmes sont employés par les états majors et les unités combattantes, entités susceptibles d'être déployées avec un faible préavis sur un théâtre d'opérations où les conditions d'accueil sont parfois sommaires. Le système devra donc être aérotransportable, protégé contre les chocs et les conditions climatiques difficiles, facilement démontable et modulable. Il devra notamment être à géométrie variable, c'est à dire être facilement adapté au volume d'une force déployée en terme de nombre de postes de travail, et de type de missions à accomplir.

Par ailleurs, sur un théâtre d'opérations, à la différence du monde civil, un service informatique n'est pas facilement disponible en cas de défaillance. De plus, une assistance technique de la part du maître d'oeuvre ou d'un contractant n'est pas toujours envisageable sur site. En conséquence, des

procédures de remise en état rapides et réalisables sur place par des personnels militaires non experts doivent être prévues.

Enfin, l'applicatif qui sera implanté sur le système sera spécifique. Qu'il soit destiné à la gestion des forces, l'exploitation du renseignement ou la préparation de missions, le SI met en oeuvre des logiciels militaires. Même si ceux ci sont élaborés à partir de briques logicielles duales comme des gestionnaires de base de données, des messageries, ou des logiciels de traitement d'images, il sera toujours nécessaire d'adapter l'interface et les fonctions des applicatifs au monde militaire. Cette exigence est issue d'une volonté de standardiser les interfaces homme machine des systèmes militaires afin de faciliter la formation des hommes.

Témoin de cette volonté, les recommandations de la charte NEWTON établie par la DGA au profit de L'Armée de l'air. Cette charte impose au SIC gravitant autour du système d'armes RAFALE d'offrir des interfaces communes. A titre d'exemple, le déplacement d'une carte géographique à l'écran se fera toujours par une même action à la souris. En conséquence, un système civil proposant un dispositif de type « track¹² ball » ne pourra être adopté sans modification.

3.4.2 Les difficultés engendrées par la dualité

La mise en oeuvre des premiers systèmes duaux ne s'est pas faite sans heurt, essentiellement par méconnaissance des exigences liées à l'emploi de sous ensembles civils, et aussi parce que les règles de maintenance et de gestion de configuration des matériels appliqués depuis toujours aux systèmes développés au seul profit des armées ont été reconduites sans discernement aux systèmes duaux.

La gestion des configurations logicielles est un premier écueil. Sur un système développé au seul profit des armées, le calculateur, le logiciel d'exploitation, l'applicatif et les périphériques sont gérés par un seul maître d'oeuvre. Toute anomalie est donc traitée et corrigée par un seul intervenant. Il n'y a donc jamais de conflits de compatibilités à régler entre deux produits informatiques de fournisseurs différents.

De plus, en plongeant dans le monde dual, la défense rencontre les problèmes de tous les utilisateurs de WINDOWS ou d'UNIX. Elle devient un client parmi des milliers d'autres. Son problème n'est pas plus urgent à résoudre que celui de telle ou telle entreprise ayant acheté parfois plus de machines et de licences. Le statut de client unique et privilégié est perdu.

La pérennité du produit est le second point délicat. Livré aux Forces en 1990 le système de préparation de mission CINNA 3 a été maintenu en service avec les mêmes station de travail SUN jusqu'en 1998. Soit huit années de fonctionnement sans augmentation des capacités de calcul et de mémoire. Les spécifications techniques encore plus anciennes, ont figé dès la signature du contrat le type de machines et de périphériques employés, l'obsolescence matérielle n'en a été que plus flagrante. A titre d'exemple, les fonds cartographiques étaient chargés à partir de bandes magnétiques alors que depuis plusieurs années, le moindre PC était équipé d'un lecteur de CDROM.

Aucune entreprise civile n'utilise aussi longtemps un matériel informatique. Il y a donc rapidement des difficultés d'approvisionnement et de maintenance logicielle du système. Le point critique est atteint lorsque la société chargée de la fourniture des machines ne garantit plus la maintenance des stations devenues trop anciennes, ni la résolution des anomalies du système d'exploitation dans ses versions anciennes. Il faut alors envisager un changement de machine qui nécessite une modification de l'applicatif.

La difficulté est essentiellement liée au fait que l'applicatif n'est pas standard au même titre que WORD alors que le logiciel d'exploitation est tout à fait normalisé. En effet, si le système d'exploitation rencontre une difficulté pour utiliser un logiciel vendu à plusieurs millions d'exemplaires, la modification de MICROSOFT ou d'UNIX sera rapidement réalisée et distribuée. En revanche, si l'applicatif considéré n'est mis en oeuvre que sur quelques dizaines de machines, il restera marginal et pourra même n'être jamais résolu. S'en reporter alors au maître d'oeuvre de l'applicatif est hasardeux puisque celui ci ne possède pas nécessairement tous les éléments lui permettant d'intervenir sur une couche logicielle proche du système d'exploitation. En final, le coût de modification risque d'être partagé entre le maître d'oeuvre et le contractant. De plus une telle procédure de modification de système si elle n'a fait l'objet d'aucune prévision dans les contrats initiaux sera longue.

¹² Système de pointage à l'écran basé sur l'utilisation du déplacement d'une boule en lieu et place de la souris traditionnelle.

3.4.3 Les avantages de la dualité

Si les inconvénients précédemment étudiés sont réels et pénalisants, il faut reconnaître que ceux ci proviennent essentiellement du fait que l'on met en parallèle une utilisation civile et militaire d'un même système. En revanche, comparer un SI dual à un SI produit spécifiquement pour la Défense permet de mettre en avant les gains engendrés par le recours aux technologies duales.

Les gains de coût de développement sont très importants. En effet, aucune entreprise aujourd'hui ne s'aventurerait dans la construction d'un ordinateur spécifique pour une utilisation parfaitement standard. Même si les coûts engendrés par la nécessité de protéger les cartes et les périphériques n'est pas neutre ils sont sans commune mesure avec les moyens financiers nécessaires à la mise au point d'une nouvelle génération de micro processeurs. Comment en effet lutter en terme de financement de la recherche avec des sociétés comme INTEL dont chaque avancée technologique est immédiatement rentabilisée par un marché potentiel de plusieurs millions de clients alors qu'un système militaire ne pourra compter au plus que quelques dizaines d'utilisateurs. Dans une période où la diminution des crédits de Défense doit inciter à une utilisation ciblée des moyens il est essentiel de restreindre la recherche et le développement à ce qui est indispensable au maintien des capacités militaires, l'informatique standard n'est pas un domaine prioritaire. Justifions notre propos par des chiffres. En téléphonie mobile, le système GSM a fait l'objet d'un milliard de francs d'investissement en terme de recherche et développement pour une année. En 1997, les crédits de recherche et développement consacré à la défense sont estimés à 3,7 milliards de francs. On le voit sur une seule application relativement marginale, plus d'un quart du budget serait nécessaire pour se maintenir au niveau du monde civil.

De plus, la fiabilité, et l'évolutivité des systèmes reposant sur des technologies duales sont améliorées par rapport à des systèmes développés spécifiquement qui restent plus proche du prototype que de la série. On imagine mal un microprocesseur vendu à plusieurs millions d'exemplaires présentant un défaut de fiabilité important. Par ailleurs, chaque évolution, passage du PENTIUM II au PENTIUM III par exemple, peut être immédiatement répercutée sur l'ensemble des systèmes reposant sur une architecture WINDOWS à un coût très faible pour peu que cette éventualité ait été prévue par le contrat.

3.4.4 Un exemple de dualité dans le domaine des SI

Afin d'illustrer nos précédents propos, intéressons nous au système FINDeRS¹³ du char Leclerc.

Ce SIC est un Système de Coordination du Combat de niveau Escadron et Compagnie pour les armes de mêlée. Développé par GIAT industries au profit de l'export, deux objectifs fonctionnels étaient visés :

- Aider le chef d'engin à exploiter au mieux les capacités de son système d'arme et valoriser les fonctions majeures.
- Aider le chef d'unité (commandant de compagnie ou chef de section) à commander et coordonner l'action des moyens de son unité.

Une contrainte majeure est imposée, FINDeRS doit s'adapter aux performances des moyens radio existants.

A partir de ce cahier des charges, et après avoir étudié des solutions techniques spécifiquement militaires, GIAT s'est orienté vers l'emploi de calculateurs standards civils sous UNIX durcis de façon à s'intégrer dans un environnement militaire. Ce choix a permis de respecter le calendrier suivant : en avril 1993, lancement du développement en interne par GIAT industries ; décembre 1995 acceptation du premier char Leclerc de série équipé. A l'été 1998, 120 Leclerc de série équipés ont été livrés à l'Arabie Saoudite.

Grâce à cette approche duale, les délais de développement et de production ont été minimisés. Les avantages qui en ont été tirés en terme de performance et de capacité d'évolution conduisent le GIAT à poursuivre son effort de communauté de technologie avec le monde civil. En effet, dans le cadre d'une proposition faite à l'Armée de Terre, il est envisagé les évolutions suivantes :

- Exploiter les nouvelles possibilités offertes par la technologie civile disponible en 1998,

¹³ Fast Information Navigation Decision and Reporting System .

- Nouvelle architecture matériel, basée sur Windows NT et une carte processeur INTEL
- Réduction des coûts et simplicité de rétrofit.

Pourtant les problèmes d'intégration au système Leclerc ont été réels, notamment en terme de compatibilité électromagnétique des postes PR4G utilisés par FINDeRS. Donc, même pour un programme complexe et exigeant en terme de durcissement, l'environnement d'un char de combat étant représentatif de conditions extrêmes d'utilisation, la technologie duale reste une solution viable et performante.

3.4.5 Les différent niveaux de dualité dans les SI

Dans le domaine des SI, la dualité semble aujourd'hui bien implantée et en développement. Cependant, celle ci peut revêtir différents aspects qui vont de l'achat sur étagère à l'intégration lourde de type FINDeRS. En fait, une analyse rapide de la situation basée sur quelques produits opérationnels permet de cibler trois familles de SI qui se distinguent essentiellement par le budget qui leur est alloué :

- Les programmes importants, d'un montant de quelques dizaines de millions de francs. Ce sont en fait les intégrations de briques civiles dans un environnement militaire, par exemple, le système FINDeRS, les systèmes de préparation de missions de L'Armée de l'air.
- Les programmes moyens, inférieurs à cinq millions de francs. A partir d'un progiciel civil, une société propose un habillage militaire de l'interface. Ce type d'application est parfaitement adapté aux SI devant être employés dans un environnement non hostile, états majors ou unités fixés en métropole. Citons l'exemple du catalogue des données géographiques de la défense « GEODEFENSE ». Ce produit a été réalisé à partir du logiciel GEOMEDIA de la société INTERGRAPH, et de la base de données ORACLE. Le coût des licences et du matériel est de un million de francs, celui de l'adaptation au besoin militaire est identique. le produit final est donc obtenu pour deux millions de francs, il profitera de tous les progrès réalisés par les logiciels GEOMEDIA et ORACLE.
- L'achat sur étagère, la Défense achète le produit du marché, finance si nécessaire des fonctions supplémentaires mais celles ci sont intégrées au produit standard. Le coût de la licence reste faible, les coûts de développement des fonctions spécifiques sont évalués précisément et demandés par les utilisateurs, selon le même processus que pour un client civil.

Lors de toute expression de besoin dans le domaine des SI, chacune de ces approches peut être envisagée. La solution moyenne semble adaptée à de nombreuses applications sous réserve que les contraintes extérieures d'intégration et de robustesse ne soient pas trop fortes. Elle devrait être systématiquement explorée pour chaque nouveau programme, elle représente un compromis coût, performances opérationnelles intéressant. Elle doit limiter le nombre d'applications spécifiques non justifiées.

4. La sécurité des systèmes d'information

4.1 Un dispositif juridique grâce au Code pénal de 1992

Le domaine de la sécurité est en pleine expansion technique mais aussi juridique. Il intéresse évidemment les entreprises soucieuses de mieux sauvegarder la confidentialité et l'intégrité de leur système de traitement de l'information. En France la profession de l'assurance a été l'un des pionniers de cette mobilisation en faveur de la sécurité informatique, créant le CLUSIF (Club de la Sécurité informatique français) et faisant la promotion de la méthode d'analyse de risques MARION. Le législateur est intervenu à son tour pour adapter le code pénal à la répression de certaines infractions informatiques par la loi du 5 janvier 1988, aujourd'hui reprise pour l'essentiel dans le **nouveau Code pénal de 1992**.

Les responsables militaires et gouvernementaux, dont les systèmes informatiques ont besoin de disposer d'une sécurité maximale, ne sont pas restés inactifs devant cette évolution. Les efforts du Pentagone et de la "National Security Agency" pour coordonner la recherche et les normes en matière de sécurité informatique sont déjà bien connus, mais la France a, elle aussi, renforcé ses moyens en réorganisant les services du chiffre au sein d'un "service central de la sécurité des systèmes d'information" (SCSSI) placé sous la tutelle d'une délégation interministérielle (DISSI) dépendante du SGDN. Et la DGA a, de son côté, mis au point une méthode originale d'analyse des risques informatiques, la méthode MELISA. Quant au nouveau Code pénal, il va, pour la première fois, sanctionner spécifiquement les atteintes au système de traitement informatisé d'informations susceptibles de porter atteinte aux "intérêts fondamentaux de la nation"(article 411.9)

4.2 Des menaces en cas de coopération

On doit noter, en outre que, sur le plan de la propriété industrielle, l'informatique, en particulier avec les logiciels, a provoqué l'apparition de situations nouvelles et de risques nouveaux consécutifs au vide juridique existant dans la plupart des pays pour cette spécialité. Le problème réside alors dans les moyens de diffusion des résultats de recherches dans les transferts de technologies. Ceci est particulièrement vrai des réseaux informatiques qui constituent un facteur de risque non négligeable quand leur sécurité n'est pas prise en compte, heureusement il semble qu'elle le soit de plus en plus.

4.3 Le recours à l'externalisation dans ce cadre juridique

En ce qui concerne l'externalisation, l'instruction interministérielle 1300 du 12 mars 1982 - qui constitue le texte d'application du décret de 1981 - prescrit notamment que :

*"Lorsqu'il est nécessaire de recourir aux services d'organismes ou d'entreprises extérieures pour la réalisation d'études, de travaux ou de fabrication intéressant la Défense nationale et la sûreté de l'État, il est recommandé de faire exécuter de telles prestations ; notamment dans le domaine informatique et celui des installations de dispositifs de protection des zones sensibles, dans le cadre de **marchés classés de défense** en raison des garanties particulières résultant des clauses contractuelles de sécurité qui sont insérées" (article 48.1).*

Le problème réside surtout dans le fait que les technologies ou les produits à « double vocation » (ou dual), relève de réglementations de contrôle de la destination finale spécifiques, soit au titre du COCOM¹⁴, soit au titre des différents régimes de non-prolifération. Mais les informations techniques ou commerciales relatives à ces produits ou technologies dont l'exportation peut être limitée, ne sont pas considérées comme des secrets de défense et ne font pas l'objet en elles-mêmes d'une protection particulière.

¹⁴ Coordinating Committee on Multilateral Export Controls.

En effet, en dehors de l'implication directe ou indirecte d'un agent de renseignement, les informations relatives à des produits ou des technologies duales relèvent bien du seul droit commun alors même qu'elles peuvent toucher à des domaines stratégiquement sensibles. L'analyse de notre outil militaire, qui emploie de plus en plus des systèmes informatiques ouverts, issus du monde civil, et donc certainement plus vulnérables que ceux qui étaient développés autrefois spécifiquement pour les besoins de notre défense, nous impose de constater la dépendance réelle de la France vis à vis des technologies issues pour la plupart des Etats-Unis.

4.4 La vulnérabilité des entreprises civiles.

Si le choix a été pris de confier la mise au point de tel ou tel programme informatique ou logiciel à une entreprise, ce qui est tout à fait possible, compte tenu du paragraphe précédent, quelle sera l'attitude de celle-ci en cas de guerre de l'information ? En effet, le monde de l'Internet et des logiciels civils nous fournit déjà des exemples d'agression – écoute du réseau, constitution de dossiers d'utilisateurs, exploration du contenu d'ordinateurs de travail lors de l'installation d'un système d'exploitation, etc.

Poussé par des contraintes économiques sévères, les responsables des systèmes informatiques ont progressivement fait évoluer leurs installations de systèmes propriétaires, et donc robustes aux violations, vers des architectures standards et ouvertes, et par conséquent vulnérables. Cette évolution n'est pas sans rappeler la problématique développée à propos de notre outil militaire. Cependant, cette situation ne saurait masquer le manque de dialogue et de coordination au niveau national, alors que l'État a le devoir de définir auprès des industriels et des organismes civils les menaces à prendre en compte de façon privilégiée, les services stratégiques pour le fonctionnement du pays et le niveau de robustesse aux agressions des installations informatiques. De même, le rôle de l'état doit permettre de mener des évaluations du niveau de protection des systèmes d'informations utilisés, apporter un savoir-faire et des compétences dans des domaines technologiques en perpétuelle évolution, et proposer enfin des architectures informatiques qui répondraient au niveau de sécurité exigé.

4.5 La sécurité des systèmes d'information vue par THOMSON-CSF

Sécuriser les réseaux informatiques et de télécommunication, analyser et gérer les risques liés aux systèmes d'information, protéger l'information sur les nouveaux médias de communication : la sécurité des systèmes d'information revêt de multiples aspects pour lesquels la maîtrise de plusieurs technologies est indispensable. Thomson-CSF communications a lancé en 1997 des nouveaux produits sur ce marché en croissance. Pour la sécurisation des réseaux de communications militaires, la société propose désormais un nouvel équipement de chiffrement des réseaux X25 ainsi que son filtre de confiance (firewall) gouvernemental qui a reçu le premier certificat français au niveau E4 (très haut niveau de confiance).

De plus la société a ouvert une antenne commerciale dans la région de Rennes pour se rapprocher de l'un de ses principaux clients, le CASSI¹⁵, hébergé dans l'enceinte du CELAR¹⁶. Parfaitement compétente, cette entreprise bénéficie d'une expertise exceptionnelle dans le domaine de la protection informatique et du chiffrement, elle est particulièrement bien intégrée dans les marchés militaires et travaille au sein de sites très sécurisés. Enfin, on ne compte plus les applications dans tous les domaines qui font que Thomson-CSF devient le premier industriel européen capable d'œuvrer sans faire appel à des technologies américaines.

¹⁵ Centre de l'Administration pour la Sécurité des Systèmes d'Information

¹⁶ Centre de l'Electronique de L'ARmement.

4.6 Le problème de la cryptographie.

Les codes et chiffres militaires et diplomatiques sont la cible des services de renseignement ennemis. Leur décryptage peut avoir des conséquences graves, même en temps de paix. L'ancien chef adjoint pour la sécurité des communications à la National Security Agency (NSA) a déclaré devant un tribunal américain le 25 mars 1986 :

"Donnez-moi accès à vos codes, à vos chiffres et je n'ai plus besoin de vos secrets. La cryptographie n'a pas de prix."

Au cours des quinze dernières années, la cryptographie est sortie de l'ombre des sphères militaires et du renseignement pour faire l'objet d'une recherche - développement intense non couverte par le secret. La plupart des algorithmes cryptographiques militaires restent secrets, mais le monde ouvert des systèmes civils permet de recueillir des indications sur les techniques cryptographiques militaires actuelles et leur vulnérabilité éventuelle.

En définitive, les concepteurs et décrypteurs de code du monde secret sont probablement très en avance sur leurs homologues travaillant sur des systèmes non secrets et la rapidité croissante de l'électronique numérique fait qu'un cryptage solide hier, peut être faible aujourd'hui et violé demain. Il est donc nécessaire de porter toute notre attention sur ces procédés de chiffrement, car aujourd'hui tous les algorithmes de chiffrement sont ou seront bientôt connus, même le code Vernam¹⁷ réputé théoriquement inviolable, est en fait vulnérable s'il est mal mis en œuvre et négligemment utilisé. La législation française jusqu'alors très restrictive vient d'autoriser l'utilisation de clés civiles de 128 bits, elle étaient limitées jusqu'alors à 40 bits. Il est donc essentiel que le monde militaire conserve son avance dans ce domaine.

¹⁷ Le seul chiffre en principe inviolable est le Vernam, vieux de 80 ans.

5. Les limites de la dualité

5.1 Les risques de perte de l'indépendance nationale :

Le soutien à l'industrie d'armement se justifie par la nécessité de conserver une certaine indépendance nationale dans les domaines technologiques relatifs à la défense. Le programme nucléaire français est un bon exemple de cette volonté d'accéder à une technologie de pointe en toute indépendance.

Cette démarche a conduit à l'émergence de sociétés d'armement nationalisées, cependant les lois de la compétitivité ont modifié cette situation qui semblait figée quand l'état était à la fois le propriétaire et le client, ce qui n'était pas la meilleure des méthodes pour être compétitif.

En fait, si la dualité permet de réduire les coûts, le réel accès (plus risqué) des entreprises de Défense à la liberté du marché (privatisations) est aussi un facteur déterminant en terme d'économie. Une politique économique libérale régule naturellement le marché aux coûts correspondant à l'offre et la demande.

Devenus nécessaires pour réduire les dépenses de l'état, ces changements ne sont pas sans inconvénient : rupture d'approvisionnement, choix d'un industriel solide (santé économique, dynamisme), obsolescence des composants qui suivent des logiques de marché différentes de celles des militaires (durée de vie). L'exemple de l'ATF¹⁸ est à ce titre parlant. Typiquement dual dans sa logique d'acquisition, c'est aux industriels de mettre en oeuvre une politique duale pour remporter le marché en proposant un avion dans les spécifications demandées et au moindre coût. C'est à l'état major et à la DGA de vérifier les points de rupture possibles et d'y prendre garde.

La dualité n'est pas le point de départ d'une politique de réduction de coûts, mais une de ses conséquences, elle est englobée dans une politique à plus large échelle de restructuration des entreprises de défense. Ainsi la marge de manoeuvre se réduit sensiblement pour les états majors qui se verront contraints aux inconvénients d'un matériel dual. L'inconvénient majeur semble être la perte de l'indépendance. Il s'agit néanmoins d'être mesuré.

La première remarque concerne directement l'actionnariat des entreprises « sensibles » (matériels spécifiques). Complètement privatisées celles-ci subiraient les lois du marché, leur acquisition par une société « étrangère » est toujours possible. Cela explique en grande partie les fusions américaines et la tentative encore mal achevée européenne d'y faire face pour atteindre des tailles critiques suffisantes afin d'être compétitif (donc indépendant à l'échelle européenne).

La deuxième remarque porte sur l'approvisionnement en matériel dual. Le risque est d'autant moins important que le marché est étendu. Il est, en effet, peu probable que le gouvernement américain puisse empêcher l'accès d'un pays à un logiciel comme WINDOWS par exemple, aux puces électroniques ou à la fibre optique. Leur diffusion dans une économie mondialisée est certainement beaucoup trop large. En ce sens on pourrait dire que plus un produit est susceptible d'être dual, c'est à dire que plus son marché civil est grand, moins le risque est important de perdre l'indépendance en ravitaillement. Plus la spécificité est élevée, plus l'indépendance en maintenant un tissu industriel et technologique doit être recherché.

Les choses deviennent particulièrement complexes quand la sophistication des matériels induit une maîtrise de technologies avalées avec une perte de technologies amonts qui en dépendent, typiquement le cas des sous systèmes. Le cas du GPS est exemplaire à ce titre. La volonté de mettre en oeuvre un système européen de ce type illustre bien le risque majeur de voir les américains sélectionner ou contrôler à leur guise l'accès aux précisions dites militaires. Dans ce cas les satellites sont duaux, les récepteurs sont duaux, mais le code est spécifique.

¹⁸ Avion de Transport Futur

5.2 Les limites politiques

La coopération en matière d'équipements militaires reste bien souvent une décision politique plus qu'économique, toutefois dans le domaine des télécommunications on constate un développement des programmes spatiaux européens. Par ailleurs, la coopération semble plus facile dans le domaine de la recherche fondamentale ; le seul obstacle est d'ordre historique et psychologique : du fait qu'au lendemain de la guerre, la recherche en Europe était au point "zéro", des contacts privilégiés se sont créés entre les laboratoires européens et les Etats-Unis, ce pays disposait alors d'une recherche active. Ces contacts se sont maintenus de sorte qu'aujourd'hui les chercheurs des divers pays d'Europe ont plus de liens avec les américains qu'entre eux. Mais les choses sont en train d'évoluer rapidement dans ce domaine.

Quelques programmes civils qui peuvent servir de support à des réalisations militaires ont été réalisés pourtant à partir des années 1961. Le plus important de ces programmes est celui de la Communauté Européenne baptisé "ESPRIT", qui couvre les technologies de l'information et des composants associés. Le second par ordre d'importance, "RACE" porte sur la transmission de données à très haut débits, domaine qui n'est pas sans intérêt du point de vue de militaire.

Mais il existe de nombreux obstacles communs à toute coopération internationale :

- Les problèmes économiques de coûts supplémentaires (partage de l'industrialisation, déplacements, délais)
- Difficultés structurelles (liées aux différences de taille et de compétence des participants)
- Les problèmes d'harmonisation des législations et des pratiques d'achats publics,
- Les distorsions existant au niveau des financements de R&D
- Les problèmes de langue.

Enfin une difficulté majeure réside dans la nécessité de l'**expression claire** des besoins communs, **au même moment** et avec des **budgets cohérents**.

En définitive même si les Etats sont protégés par l'article 223 du Traité de Rome¹⁹, ils sont conscients de l'absence de frontière entre la technologie civile et militaire. Il y a donc risque pour les technologies duales car les applications civiles et militaires ne sont pas protégées de la même façon. Sur quels critères décidera-t-on d'autoriser ou non tel pays à les acquérir ?

Enfin, un organisme semble s'inscrire en précurseur d'une future agence européenne de l'armement : l'OCCAR²⁰ (Organisme Conjoint de Coopération en matière d'Armement). Sans pour autant éliminer toute étude nationale, en fonction de la volonté de maintenir des domaines de souveraineté, le rôle de cet organisme pourrait être accru, éventuellement réorienté, afin de mieux coordonner les recherches européennes en matière de SIC, terrestres ou spatiaux. Ainsi consolidées au travers de « comités techniques » constitués des responsables techniques des Etats, nos études en matière de communication seraient totalement inscrites dans une interopérabilité constante avec nos alliés et en toute confiance. Pour l'instant il semble préférable de privilégier des solutions type « traité », car toutes les nations de l'UEO ne sont pas intégrées à l'OCCAR. De plus, dans le domaine spatial la vision d'une politique européenne ne semble pas partagée par tous nos alliés, aucun d'entre eux, par exemple n'envisage une autonomie totale vis-à-vis des Etats-Unis.

En conséquence, dans le domaine de la communication et des systèmes d'information par satellites il est possible de définir plusieurs options possibles correspondant à des niveaux d'indépendance nationale différents²¹.

¹⁹ Cet article reconnaît à chaque pays « le droit de prendre les mesures qu'il estime nécessaires à la protection des intérêts essentiels de sa sécurité et qui se rapportent à la production ou au commerce d'armes, de munitions et de matériels de guerre ».

²⁰ Le 12 novembre 1996, la France et l'Allemagne ont décidé de créer ensemble cet organisme regroupant les multiples bureaux de programmes bilatéraux.

²¹ Estimations issues d'une étude du CHEAR de 1998.

- Si la France ne réussit pas à entraîner ses partenaires, l'ambition de notre pays sera de maintenir les lignes applicatives déjà développées : télécommunications de type SYRACUSE, observation optique. (budget estimé environ 2,8 GF/an).
- Dans une hypothèse plus optimiste où un consensus pourrait être obtenu entre les pays de l'OCCAR, les axes de développement pourraient s'orienter vers un système TRIMILSATCOM (budget environ 5,9 GF/an).
- Si politique spatiale européenne, les budgets seraient alors augmentés et l'Europe pourrait bénéficier d'une véritable autonomie dans ce domaine.(coût environ 8 GF/an)

6. Conclusion

Ce rapide tour d'horizon de la dualité, bien que non exhaustif, nous permet à l'issue de notre étude de dégager quelques axes de réflexion.

La dualité est nécessaire, dans le contexte géopolitique et économique actuel, car les contacts entre les mondes civil et militaire sont multiples et permanents. Sur le plan technique les derniers développements issus de l'industrie civile sont incontournables. Sur le plan opérationnel, les armées doivent aujourd'hui opérer dans le cadre de crises ponctuelles pour lesquelles la stratégie de conduite des opérations est, elle aussi, qualifiée de civilo-militaire.

Le recours à la dualité civilo-militaire s'impose donc. Cependant, il est important de maîtriser le processus. Il faut profiter de la dynamique du monde civil afin de s'interfacer facilement avec lui, tout en gardant la capacité de se protéger des inconvénients liés au recours à la dualité soit :

- l'irréversibilité de la démarche,
- la perte de l'indépendance nationale,
- l'espionnage ou la guerre de l'information,
- la non permanence du service rendu,
- l'interopérabilité entre armées et alliées.

Les télécommunications et l'informatique, choisies comme fil conducteur de notre travail donnent une bonne image de ce que peut être une politique en matière de dualité civilo-militaire. En effet, dans ces deux domaines un savoir faire minimal ou noyaux dur doit être préservé. Cette capacité technologique doit nous permettre de conserver une certaine indépendance en terme d'échange et de traitement de données classifiées. Deux pôles de connaissance sont apparus particulièrement sensibles à ce titre :

- la maîtrise des techniques du chiffre,
- les composants et logiciels produits par le monde civil et utilisés par la défense.

Dans ce cadre, l'émergence du système d'exploitation LINUX²² et des technologies d'ingénierie inverse²³ semblent être des pistes qui peuvent faire l'objet d'investissement prioritaires dans les recherches et développement militaires. Cette démarche doit s'inscrire dans le cadre d'une politique interministerielle volontaire de préparation à une guerre de l'information qui reste à mettre en place.

Enfin, dans le domaine spatial, la politique volontariste visant à mettre en orbite un système de communication militaire indépendant des prestataires de services privés doit être poursuivie. En effet, se soumettre à la sous-traitance engendre des contraintes qui ne semblent pas acceptables pour des armées en opérations en terme de sécurité et de disponibilité des moyens.

Le marché des télécommunications spatiales soumis à des contraintes de rentabilité peut rapidement se trouver dans l'impossibilité de satisfaire nos besoins sur des zones non économiquement rentables ou déjà saturées par les demandes des médias privés. De plus ce marché est dominé par l'industrie de l'Amérique du nord, notre indépendance nationale est donc menacée, les technologies actuelles permettant, sans trop de difficultés, d'intercepter et d'analyser toutes nos communications opérationnelles.

²² système d'exploitation concurrent de WINDOW qui propose aux utilisateur un libre accès aux sources du logiciel.

²³ technique informatique qui permet de connaître le contenu exact d'un logiciel ou d'un composant afin de mettre en évidence les éventuelles fonctions cachées.

ANNEXE 1 : Panorama sur l'usage des systèmes civils pour la Défense

Pays	Système	Industriel leader	Type de système	services et couverture	Principaux problèmes posés	Commentaires
France	Globalstar	Loral + Alcatel Espace	LEO	Phonie mobile Zones mondiales d'intérêt économiques	très bas débit uniquement / couverture maritime limitée / pas de connexion directe avec métropole / nécessité de passerelle tous les 1500 km et de relais par réseaux sol ou géostationnaires	Stations d'ancrage au sol dépendantes d'opérateurs pas nécessairement coopérants
	Skybridge	Alcatel Espace	LEO	Multimédia Zones mondiales d'intérêt économiques	usage fixe uniquement / couverture maritime très limitée / pas de connexion directe avec métropole / nécessité de passerelle tous les 600 km (vulnérabilité physique) et relais par réseaux infra / localisation des émetteurs / brouillage sélectif aisé	Stations d'ancrage au sol dépendantes d'opérateurs et très vulnérables
Europe	East	Matra Marconi Space	GEO	Phonie mobile Couverture lacunaire Europe, Afrique, Moyen-Orient	bas débit uniquement / couverture limitée aux zones dignes d'intérêt commercial / localisation des émetteurs par le gestionnaire du réseau / brouillage et détection aisés	Difficulté européenne (tour de table) à définir le système -> risque d'abandon en raison de la concurrence US
	West	Matra Marconi Space	GEO + MEO	Multimédia Couverture régionale puis mondiale selon rentabilité	couverture limitée aux zones dignes d'intérêt commercial / service fixe uniquement / localisation des émetteurs par le gestionnaire du réseau / brouillage et détection des émetteurs aisés	Système ambileux, sur papier avec des subventions ESA, et concurrent de Celestri
International	Eutelsat		GEO	Diffusion TV Multimédia possible Couverture régionale Europe	service fixe / couverture limitée à une région / spots mobiles non disponibles pour la Défense / Coût de location prohibitif en regard du coût d'acquisition / très aisé à brouiller / ressource à partager avec les médias	Système typique de diffusion régionale TV
	Inmarsat / ICO	Hugues	MEO	Phonie mobile Couverture mondiale	très bas débit uniquement / localisation des émetteurs par le gestionnaire du réseau / brouillage et détection des émetteurs aisés / contrôle total par firme commerciale	Système intéressant pour les communications mobiles bas débit non protégées
Etats-Unis	Celestri	Motorola	LEO	Multimédia Couverture quasi-mondiale	capacité allouée en priorité aux services commerciaux, reste forte capacité pour les militaires sur les zones polaires océaniques désertiques / contrôle total par firme commerciale US / aucune garantie ni souveraineté / brouillage aisé	Crédibilité technique contestable
	Teledesic	Boeing	LEO	Multimédia Couverture quasi-mondiale	secret très fort sur le projet / contrôle fort par gouvernement US / aucune garantie ni souveraineté / brouillage aisé / recopie des informations aux USA	Arme de suprématie par l'information largement soutenue par le DoD / crédibilité technique contestable
	Iridium	Motorola	LEO	Phonie mobile Couverture quasi-mondiale	très bas débit uniquement / accords « secrets » avec DoD US / pas de souveraineté / partage de la couverture mondiale avec ICO / couverture maritime limitée / localisation brouillage et détection extrêmement aisés / recopie des informations aux USA	Projet dont la complexité n'est pas justifiée commercialement mais est soutenue financièrement par le DoD

document F.M.A. T.S.C. 'janv 98

Annexe 2 : Liste des contacts pris au cours de l'étude

Col BREBAN	EMAA/BSA
Col CIAVEAU	DGA/SPAE
ICA ARMANDO	DGA/DCAE
Mme GAUTROT	DGA/SPOTI
IPA LEBOULC'H	DGA/SPOTI
Mr HUGUET	DGA/CEGN
Col TURBE	STAT/SCI
Lcl DE RECOURT	STAT/SCB
Lcl MANDONNET	STAT/SCI
Mr WEISBUCH	FED anciennement CREST
Mr MARGUIN	FED anciennement CREST
Lcl LE QUILLOU	CETE Rennes
Lcl MAURICE	CETE Rennes
Col BAGARIA	EMA/TEI
Mr LEPAPE	CELAR Rennes