ETUDE PARTICULIERE A OPTION

B 15

Directeur d'étude : M. Alain Esterle Adjoint au SCSSI

Comité d'étude :

Lieutenant Colonel Sylvie MOUZIN
Chef de Bataillon Laurent CHAPELLE
Commandant Horst HAUCK
Capitaine de Corvette Michel HOFMAN
Chef de Bataillon Olivier SERRA

Mai 2000

SOMMAIRE

INTRODUCTION GÉNÉRALE

La société de l'information, dont l'avènement est annoncé par les sociologues depuis une dizaine d'années, semble bel et bien en passe de révolutionner la société dans tous ses aspects. En ce printemps 2000, en effet, des faits de plus en plus nombreux tendent à démontrer que les bouleversements dont on ressentait les prémices depuis quelques temps sans pouvoir en évaluer l'ampleur sont les bases d'une véritable révolution.

Cette « révolution de l'information » ou « révolution numérique » devrait toucher tous les domaines. Déjà les théories économiques traditionnelles sont impuissantes à rendre compte de la situation qui règne aux Etats-Unis, où la plus longue période de croissance de l'histoire s'accompagne du plein emploi mais où l'inflation reste faible. Le comportement des marchés financiers est également inédit, avec des valorisations fondées uniquement sur le potentiel des « start-up ». Il faut invoquer la « nouvelle économie » pour expliquer la situation économique actuelle. Mais la macro et la microéconomie sont loin d'être les seuls domaines affectés. Les modes de production ont également beaucoup changé depuis quelques années. L'éclatement des grandes organisations en plusieurs centres de profits autonomes, la généralisation des organisations matricielles, pour ne citer que les mutations les plus flagrantes, rendent progressivement désuètes les organisations à la hiérarchie pyramidale qui subsistent. A n'en pas douter, les modes d'enseignement et même les rapports entre individus seront à leur tour touchés.

Cette appréciation de situation trouve sa traduction officielle en France pour la première fois dans le discours du Premier ministre à l'université de la communication d'Hourtin en 1997[1]. Ce discours décline les actions à mener dans six domaines indispensables pour préparer la France au passage à la société de l'information : l'école, la culture, le commerce électronique, les entreprises du secteur des technologies de l'information, les services publics et la régulation.

L'Union européenne a elle aussi pris la mesure des changements à venir à brève échéance. Ainsi, sous le nom de e-Europe, dix domaines d'action prioritaires, notamment l'éducation, les transports, les soins de santé et les handicapés, ont été pris en compte au conseil européen de Lisbonne en mars 2000.

Il est frappant de constater, alors que tous les domaines de la société sont supposés être radicalement transformés par la lame de fond de la « révolution numérique », qu'il n'est guère question en Europe de la Défense. Aux États-Unis, en revanche, la Défense est en train d'entrer de plein pied dans la société de l'information. Il est en effet aujourd'hui indéniable que la *Revolution in Military Affairs*, qui est au cœur du débat stratégique depuis une dizaine d'années, est en train de se traduire dans les faits. Les pays européens, jusque là dubitatifs quant à l'opportunité d'entrer dans la logique américaine de la *RMA*, vont devoir prendre position plus clairement. D'une part parce que la société tout entière évoluant, la Défense sera obligatoirement touchée, d'autre part à cause des impératifs d'interopérabilité entre les alliés. La seule existence d'une *RMA* aux Etats-Unis contraint les Européens au moins à mener une réflexion approfondie dans ce domaine.

[1] Discours du Premier Ministre à Hourtin le lundi 25 août 1997 ; « *Préparer l'entrée de la France dans la société de l'information* ».

Le contexte récent, d'où semble émerger une réelle volonté politique de construction d'une Europe de la Défense, peut à cet égard représenter une véritable opportunité. Le nœud gordien de la réaction à adopter face à la *RMA* est en effet l'antagonisme entre d'une part, la faiblesse des budgets nationaux des pays d'Europe en matière de *R&D*[2], qui leur interdit d'envisager une « *RMA* nationale » et d'autre part, la volonté de conserver une certaine indépendance vis-à-vis des USA, qui en conduit certains à refuser les propositions américaines qui peuvent se résumer dans la formule « *Buy American* ».

A la lumière de l'état des lieux dressé sur la société de l'information et sur sa prise en compte par les sociétés occidentales, l'analyse des enjeux qu'elle représente pour la construction de l'Europe de la défense conduit à la recherche et la définition d'un concept de « stricte suffisance » en matière d'information, où les aspects de maîtrise et de domination de l'information s'entremêlent et où la guerre de l'information devient tour à tour défensive et offensive. Les armées nationales européennes, seules ou ensemble, devront s'adapter et donc trouver leur place dans un monde bouleversé par la révolution technologique majeure apportée par la société de l'information.

[2] R&D : Recherche et développement

1 SITUATION ACTUELLE

1.1 L'EMERGENCE DE LA SOCIETE DE L'INFORMATION

Au cours de ce siècle nous sommes progressivement sortis de l'ère industrielle pour entrer dans celle de l'information pour laquelle les valeurs immatérielles, telles que l'information, sont devenues la ressource clef.

Après que la révolution agricole d'il y a dix mille ans ait lancé une première vague de transformations dans l'histoire de l'humanité, que la révolution industrielle d'il y a trois cents ans ait déclenché une nouvelle vague de changements, nous sommes en train d'assister à l'émergence d'une nouvelle société, une société post-industrielle dans laquelle la matière première essentielle est l'information. Cette société est ainsi décrite par Alvin et Heidi Toffler[3] : « *L'humanité s'apprête à faire un bond quantique en avant. Elle est confrontée au bouleversement social et au processus de restructuration créatrice les plus brutaux de tous les temps. Sans en avoir clairement conscience, nous sommes en train d'édifier à partir de zéro une civilisation sans précédent. Telle est la signification de la troisième vague*. »

Selon cette thèse, de même que l'on a parlé de « société industrielle » on peut donc aujourd'hui parler de « société de l'information ». Trois grandes évolutions conduiraient à l'émergence de cette société :

- La généralisation de l'usage des technologies et des réseaux d'information,
- Les évolutions technologiques de plus en plus rapides, qui s'accompagnent d'un développement exponentiel des marchés,
- La mondialisation des flux d'information.

Cette société peut être caractérisée par la technologie de l'information, par le commerce de l'information et par la dépendance à l'information. Il s'agit donc, avant tout, d'une forme nouvelle d'organisation de l'économie et de la production.

Cette ère de l'information a un impact profond sur notre mode de vie, notre organisation sociale, nos habitudes culturelles : les frontières nationales perdent leur importance et les états deviennent des *global players*. Le nouveau réseau global, à cause de son potentiel de croissance et de sa capacité à créer de la prospérité, aura des répercussions sur tous les aspects de la vie quotidienne. Il y aura donc une dépendance de plus en plus forte de notre société vis-à-vis des systèmes d'information.

Du point de vue militaire, les infrastructures de commandement et de contrôle, qui dépendent essentiellement de la technologie et des réseaux civils, sont devenues de plus en plus vulnérables à des pertes, délibérées ou accidentelles, de données. Il est donc important de pouvoir évaluer les risques de perte, de manipulation, de saturation ou de collecte passive de données.

[3] Alvin et Heidi TOFFLER. *La troisième vague.* Ed. Denoël, 1980.

1.2 LES NOUVELLES VULNERABILITES INDUITES PAR LA SOCIETE DE L'INFORMATION

Au fur et à mesure du développement des nouvelles technologies nous sommes passés des risques technologiques aux menaces liées à la délinquance informatique ; la vulnérabilité de la société de l'information s'est accrue.

Il semble que se soit avec la création du premier ordinateur électronique en 1946, ENIAC, *Electronic Numerical Integrator and Calculator*, qu'est apparue, en germe, la « société de l'information ».

Jusqu'aux années 70, les risques étaient essentiellement techniques (bugs) et les menaces limitées aux activités de défense. Les progrès techniques de l'informatique et l'informatisation du monde de l'entreprise ont changé les données du problème.

A partir des années 70 les premiers ordinateurs individuels sont apparus : ce sont tout d'abord les APPLE de Steve Jobs puis les PC (*Personal Computers*) de la firme IBM ; d'une culture ésotérique l'informatique est devenue accessible à tous. Les Anglo-saxons inventent le concept de *userfriendless* : le PC devient l'ami.

Avec la naissance du réseau ARPAnet[4] en 1970 on assiste, de plus, à une mise en réseau mondiale des ordinateurs : d'une organisation informatique centralisée on passe à une diffusion d'informations tous azimuts et à des systèmes « ouverts ».

Ainsi, si les risques accidentels deviennent de plus en plus rares, de nouvelles menaces apparaissent liées principalement à la délinquance informatique due à la mise en réseau : du vol physique de matériels et logiciels à la production de virus et aux pénétrations des systèmes par les *hackers*.

A partir des années 90, le développement de l'Internet dû principalement à la création en 1992 du *World Wide Web* par Tim Berners-Lee a accru les menaces ; pour certains on peut parler de véritable guerre de l'information. Cette guerre virtuelle n'est plus seulement militaire : c'est une guerre invisible mais dont les dégâts sont considérables.

Les risques évoluent. S'ils portaient avant tout sur la confidentialité et la disponibilité, ils agissent également et de plus en plus sur l'intégrité des données. Sur des réseaux ouverts les messages peuvent être interceptés et manipulés, la validité des documents peut être contestée. Sur les réseaux de communication mondiaux, les frontières se sont estompées et les menaces sont principalement de deux ordres : le développement de formes nouvelles et difficilement maîtrisables de criminalité et l'hégémonie culturelle et économique de grandes entreprises mondiales.

[4] ARPAnet : réseau crée par l'agence américaine ARPA (Advanced Research Project Agency) du DoD afin de renforcer les développements scientifiques pouvant être utilisés à des fins militaires ; il a cessé d'exister en 1990 et a été « remplacé » par l'Internet.

1.3 POSITION EUROPEENNE SUR LA SOCIETE DE L'INFORMATION

1.3.1 Position des institutions européennes

A partir du début des années 90, l'Europe a orienté sa politique vers les technologies de l'information et de la communication, vers l'usage de ces technologies et leurs effets sur le bien-être collectif et la compétitivité des entreprises.

C'est sous le titre de « l'Europe et la société de l'information planétaire » qu'a été publié, le 26 mai 1994, le premier document communautaire proposant une approche politique de la société de l'information. Appelé plus couramment « rapport Bangemann »[5] (président du groupe de personnalités ayant travaillé sur ce sujet), ce dernier formulait deux recommandations importantes :

- L'accélération du processus de libéralisation du secteur des télécommunications,
- Le développement d'un cadre réglementaire commun.

On peut notamment y lire : *« cette évolution est basée sur l'information, elle-même expression du savoir humain. Le progrès technique nous permet désormais de traiter, de stocker, de trouver et de communiquer des informations sous quelque forme que ce soit (voix, texte, image), sans être limité par des contraintes d'espace, de temps, ni de volume. Cette révolution offre à l'intelligence humaine de nouvelles et considérables capacités, et modifie notre manière de vivre et de travailler ensemble ».*

Un plan d'action complet a, par la suite, été élaboré et mis en œuvre à partie de 1994[6]. Il s'appuie sur quatre piliers :

- L'adaptation du cadre législatif,
- La promotion des réseaux et du contenu,
- L'approfondissement des impacts sociétaux,
- La sensibilisation.

La commission européenne (Direction Générale XIII) a, quant à elle, publié en 1997 un document intitulé : « Assurer la sécurité et la confiance dans la communication électronique : vers un cadre européen pour les signatures électroniques et le chiffrement ». Cette communication prévoyait un plan de mise en œuvre avec :

- Pour le 2ème trimestre 1998, une directive sur les signatures numériques,
- D'ici 2000, la mise en place à travers l'Union européenne (UE) d'un cadre commun pour la cryptographie.

Si la directive sur les signatures numériques a bien été adoptée à la fin de 1999 (Directive européenne 9993 CE du 13/12/99), la politique sur la cryptographie n'a toujours

[5] « Europe and the Global information Society – Recommendations to the European Council » . Rapport Bangemann, mai 1994.

[6] « L'Europe vers la société de l'information : un plan d'action ». Communication de la Commission, COM(94) 347, juillet 1994.

pas été entièrement explicitée.

La cryptographie est un moyen technologique d'assurer la sécurité de l'information du point de vue de sa confidentialité, de son intégrité, de son authenticité et de sa disponibilité. Cette technologie est essentielle au développement et à l'utilisation des réseaux d'information et de communications nationaux et mondiaux, et au développement du commerce électronique. L'utilisation généralisée de la cryptographie a des implications pour la protection de la vie privée, la protection des informations d'affaires et financières, ainsi que pour la sécurité publique et la sécurité nationale.

Ces dernières années, la plupart des pays ont œuvré pour essayer d'harmoniser leurs politiques à l'égard de la cryptographie, la tendance étant de réduire toute législation nationale qui serait de nature à freiner le développement des réseaux d'information, notamment en ce qui concerne le commerce électronique.

Cependant, pour ce qui concerne l'exportation des produits de chiffrement, la presque totalité des pays pratique une politique de contrôle rigoureuse pour interdire l'accès d'opposants étrangers aux techniques de chiffrement, et prévenir ainsi la prolifération au niveau international de ces technologies. C'est ainsi que les produits de chiffrement, qui étaient inclus dans la liste du COCOM[7], font désormais partie intégrante de l'arrangement dit de Wassenaar élargi à 28 états (dont, entre autre l'Allemagne, la Belgique, l'Espagne, la France, les Etats-Unis). Cet accord concerne principalement l'exportation des technologies clefs et celle des marchandises à usage dual (*dual-use goods*).

D'après cet arrangement, l'exportation des systèmes de cryptographie était strictement contrôlée. Avec le renouvellement de l'arrangement en 1998, le but européen, la suppression des restrictions d'exportation des produits cryptographiques pour renforcer le commerce électronique, ne pouvait pas être atteint. Un accord a été trouvé pour traiter le *Hardware* et le *Software* de la même manière et pour ne réglementer les exportations qu'à partir de 56 bits (avec quelques exceptions pour le «*public domain software* » dont l'exportation va jusqu'à 64 bits).

D'après l'arrangement de 1998, l'exportation de logiciels cryptologiques est possible sans *key-recovery*, c'est-à-dire, sans dépôt de la clé de décryptage à une organisation officielle. Mais les clefs à 64 bits ne sont plus considérées comme sûres. C'est pourquoi les pays européens tendent à supprimer ces réglementations pour assurer la confidentialité sur Internet et pour renforcer le commerce électronique sans être obligé de recourir au procédé de *key-recovery*. L'arrangement est à renouveler en l'an 2000.

C'est dans cet esprit de contrôle que les pays membres de l'O.C.D.E.[8] ont aussi établi huit principes directeurs concernant la politique de cryptographie. Ils ont lancé un projet sur la politique de cryptographie en constituant un groupe ad hoc d'experts. Celui–ci a rendu son rapport à la fin de 1996, dont les lignes directrices ont été adoptées en tant que Recommandation du Conseil de l'OCDE du 27 mars 1997 et publiées dans le rapport « La politique de cryptographie : les lignes directrices et les questions actuelles (OCDE/GD(97)204) ».

De même, la commission au Parlement européen a souligné le besoin « d'assurer la sécurité et la confiance dans la communication électronique ». Ces directives visent essentiellement à libéraliser l'usage des matériels de cryptographie. Néanmoins, la mise en

[7] COCOM : Coordination Committee for Multinational Export Controls

[8] O.C.D.E. : Organisation pour la coopération et le développement économique

œuvre de contrôles nationaux plus stricts demeure possible.

Enfin, dans la perspective d'une standardisation de la cryptographie en Europe, des centres de recherche scientifique ont formé un projet appelé NESSIE (*New European Schemes for Signatures, Integrity, and Encryption*) financé par la commission dans le cadre du 5° PCRD[9]. Celui-ci, officiellement en activité depuis le 1er janvier 2000, a pour but d'harmoniser les différents outils de cryptographie et de proposer aux instances européennes des produits de chiffrement standards dans les domaines de la signature électronique, de l'identification numérique ou de la cryptographie asymétrique.

La commission européenne a, quant à elle, lancée l'initiative « eEurope – Une société de l'information pour tous », axée sur dix domaines d'actions prioritaires[10] et visant à permettre à tous les citoyens européens de profiter de la société de l'information.

Pour ce qui est de l'UEO[11], un règlement sur la sécurité des communications a été publié en 1996 : il s'agit du RS 1000 de l'UEO équivalent du CM(55) 15 qui est la bible de sécurité de l'OTAN[12].

1.3.2 Position de la France vis à vis de la société de l'information

La France, qui n'a pas voulu reconnaître la révolution d'Internet a tardé à réagir et a pris un certain retard. Bien qu'elle ait pris certaines mesures dans les années 70 (le SGDN[13] a publié dès le 6 décembre 1976 l'instruction interministérielle N° 1900/SGDN/SSD[14] sur la protection du secret de défense en informatique, la loi « informatique et libertés » a été adoptée en 1978) l'entrée dans la société de l'information ne s'est accélérée qu'à partir de l'année 1998 car accompagnée d'une volonté politique très forte. Elle fut marquée tout d'abord par le discours du Premier Ministre à Hourtin en août 1997, puis par la rédaction du Programme d'action gouvernemental pour la société de l'information (PAGSI). Le Premier Ministre suivait ainsi les traces de Bill Clinton et d'Al Gore, qui avaient lancé le projet de construction des autoroutes de l'information (*information superhighways*) aux États-Unis en 1992.

Le PAGSI établit six domaines prioritaires pour réaliser l'entrée dans la société de l'information :

- L'éducation : il faut développer l'utilisation des technologies de l'information en milieu scolaire. Pour cela il faut des moyens, il faut former les enseignants et développer les contenus pédagogiques,

[9] PCRD : Programme Cadre de Recherche et Développement

[10] La jeunesse européenne à l'ère numérique, l'accès moins cher à Internet, l'accélération du commerce électronique, l'accès rapide à l'Internet pour les chercheurs et les étudiants, les cartes à puce pour l'accès électronique, le capital risque pour les PME de haute technologie, « eParticipation » pour les handicapés, les soins de santé en ligne, le transport intelligent, les administrations en ligne.

[11] UEO : Union de l'Europe occidentale

[12] OTAN : Organisation du Traité de l'Atlantique Nord

[13] SGDN : Secrétariat Général de la Défense Nationale

[14] Elle sera remplacée le 20 juillet 1993 par l'instruction générale interministérielle 900 sur « *la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.* »

- La culture : il faut numériser notre patrimoine culturel,
- Le commerce électronique : il doit être développé grâce à l'initiative privée,
- Les entreprises du secteur des technologies de l'information et de la communication,
- La réforme des services publics, en particulier par leur mise en réseau,
- La régulation : aménagement d'un cadre législatif et réglementaire protecteur.

Dans ce cadre, l'État doit jouer un rôle d'entraînement en utilisant les nouvelles technologies de l'information et de la communication (NTIC) pour moderniser son fonctionnement interne et faciliter les relations entre l'administration et les citoyens.

La circulaire du Premier Ministre en date du 3 juin 1998 demande aux ministères de rédiger un Plan Pluriannuel de Modernisation (PPM), dans lequel s'inscrit le Programme d'Action Ministériel pour la Société de l'Information (PAMSI) qui est la déclinaison ministérielle du PAGSI. Elle met en évidence l'importance des nouvelles technologies de l'information et de la communication dans la mise en œuvre de la politique de modernisation de l'État.

Le « PAMSI défense » liste l'ensemble des projets et réalisations du ministère de la défense mettant en œuvre les NTIC. Ces projets contribuent à l'accomplissement des missions fondamentales du ministère et prolongent de façon concrète les décisions prises en matière de modernisation.

Les moyens mis en œuvre pour atteindre les objectifs énoncés sont nombreux : création d'un Comité Interministériel pour la Société de l'Information (CISI), restructuration des instances de coordination de niveau interministériel avec la création de la délégation interministérielle à la réforme de l'état (DIRE) et de la mission de soutien technique pour le développement des nouvelles technologies de l'information et de la communication dans l'administration, rédaction et diffusion de textes (décrets, circulaires…), constitution de groupes de travail interministériels, réalisation de guides …

Il semble que le PAGSI ait été appliqué de manière inégale dans les administrations et notamment au ministère de la défense, où la mise en œuvre du PAMSI s'est heurtée à de nombreuses réticences.

Avec le développement des infrastructures mondiales de l'information ; les utilisateurs des nouvelles technologies ont voulu avoir une plus grande confiance dans la sécurité des réseaux et des systèmes d'information et de communication qu'ils étaient amenés à utiliser. Ainsi, dans le domaine économique, les Français utilisent de plus en plus l'Internet qui de par sa conception, n'est pas sécurisé ; ils souhaitent donc pouvoir sécuriser leurs échanges et avoir une entière confiance dans les transactions qu'ils effectuent. En effet, les données qui circulent sur ces infrastructures sont de plus en plus vulnérables à des menaces sur leur sécurité mettant en jeu des moyens perfectionnés (comme, par exemple, le réseau Echelon).

Afin de garantir cette sécurité et d'assurer l'essor du commerce électronique le gouvernement français a récemment légiféré pour assurer une plus grande libéralisation de l'usage de la cryptologie ; en effet, la cryptologie est un outil efficace pour un usage sûr des technologies de l'information car elle garantit la confidentialité, l'intégrité et la disponibilité des données et fournit des mécanismes pour l'authentification et la non-répudiation de ces données. Ainsi que l'a déclaré le Premier ministre le 19 janvier 1999 : « *la cryptologie*

apparaît comme un moyen essentiel pour protéger la confidentialité des échanges et la protection de la vie privée »[15].

Le chiffrement des données a longtemps été considéré comme une arme de guerre : les moyens cryptographiques ont été, tout d'abord, rattachés à la notion de *matériel de guerre de 2ème catégorie* par le décret du 18 avril 1939 (il était interdit, en principe, de détenir des matériels cryptographiques et toute autorisation éventuelle de détention était discrétionnaire).

Jusqu'en 1990, la majorité des moyens de cryptologie, qu'ils assurent des fonctions d'intégrité, de confidentialité ou d'authentification, a donc été soumise à contrôle en ce qui concerne son importation, son exportation, sa fourniture ou son usage. Ce n'est qu'en 1990, soit 50 ans après la classification en matériel de guerre, qu'a réellement débuté le processus de « libéralisation » de l'utilisation de la cryptologie : de par la loi du 29 décembre (90 1170) la cryptologie n'est plus considérée comme un « matériel de guerre » : c'est un ensemble de « *prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse grâce à des moyens, matériels ou logiciels conçus à cet effet* »(article 28).

Le développement de l'Internet et les besoins du commerce électronique (signature, télépaiement…) ont accéléré ce processus de « libéralisation » ; la France, afin d'assouplir sa réglementation tout en conservant un contrôle étatique strict, a tout d'abord adopté un système intermédiaire entre l'interdiction totale du chiffrement et la liberté absolue (loi 96-659 du 26 juillet 1996) : elle a mis en place une structure originale de « *Tiers de confiance* » (organisme agréé que l'on pourrait assimiler à un notaire électronique) qui permettait l'utilisation de certains systèmes de chiffrement « forts » mais avec un dépôt des clefs (de confidentialité) chez ce tiers agréé.

Cette loi libéralisait l'utilisation des moyens de cryptologie assurant l'authentification, l'intégrité et la non répudiation des messages et mettait en place un seuil technique pour la longueur de la clef de chiffrement : en dessous de 40 bits l'utilisation d'un moyen de chiffrement était libre pour faire de la confidentialité, au-dessus il était autorisé si l'on déposait sa clef auprès d'un organisme agréé ; cela permettait notamment à l'autorité judiciaire d'obtenir auprès de cet organisme la clef secrète nécessaire au déchiffrement des documents chiffrés.

Par la suite, lors de sa conférence de presse du 19 janvier 1999 M. Lionel Jospin, Premier Ministre, avait déclaré que le Gouvernement, en accord avec le Président de la République, avait décidé de s'orienter vers une "*liberté complète dans l'utilisation de la cryptologie*" ; il a précisé que "*le Gouvernement avait décidé de relever le seuil de la cryptologie dont l'utilisation est libre, de 40 bits à 128 bits, niveau considéré par les experts comme assurant durablement une très grande sécurité*".

Suite à cette intervention et aux décrets parus le 19 mars 1999, le seuil de la cryptographie libre de toute autorisation a été relevé de 40 à 128 bits pour un usage privé ; ce n'est cependant qu'une mesure technique, la volonté gouvernementale étant de libéraliser totalement la cryptographie et de supprimer le recours obligatoire aux tiers de confiance pour le dépôt des clefs secrètes de chiffrement : la France doit d'ailleurs, en l'an 2000, se doter d'une loi sur la société de l'information qui précisera ces mesures.

Enfin, la France s'est dotée d'un schéma d'évaluation et de certification de la sécurité

[15] Discours du Premier ministre du 19 janvier 1999 disponible sous http: //www.premier-ministre.gouv.fr/PM/D190199.HTM

des technologies de l'information : la mise en œuvre de ce schéma, qui permet aux utilisateurs d'avoir une entière confiance dans les mesures de sécurité mises en œuvre dans les produits, a été confiée au SCSSI[16] : celui-ci est l'organisme de certification national unique.

1.3.3 La société de l'information : le point de vue allemand

Même si quelques pays européens sont en « pointe » dans le domaine de la société de l'information, rares sont ceux qui ont prévu, comme va le faire la France, de se doter d'une loi sur la société de l'information. En octobre 1997, le cabinet fédéral allemand a adopté le « *Progress Report of the Federal Governement-Info 2000 : Germany's Way to an information Society* ». Les principaux textes réglementaires sont centrés sur la politique d'utilisation de la cryptologie et l'application de la directive européenne sur la signature numérique.

L'Allemagne a toujours souligné la nécessité d'une coopération internationale. Cette volonté apparaît bien dans le rôle actif pris dans la « *Global Information Society Initiative* » pendant le sommet du G7 à Naples en juillet 1994, ainsi que lors des rencontres des ministres à Bruxelles en 1995. Pendant ces rencontres, onze projets différents pour la société globale de l'information ont été lancés (par exemple dans les domaines du commerce, de la culture, de l'éducation, de l'environnement, de la santé et de l'administration publique).

Les résultats de ces projets ont été publiés en juillet 1999, pendant la présidence européenne de l'Allemagne, à l'occasion du sommet du G8 à Cologne. Ces projets ont démontré, de manière claire, le potentiel de la société de l'information dans les domaines déjà mentionnés.

Non seulement dans le domaine civil, mais également dans le domaine militaire, l'Allemagne a, pendant les consultations franco-allemandes de Nuremberg du 9 décembre 1996, déclaré que le concept franco-allemand actuel en matière de défense et de sécurité constitue le cadre pour la poursuite du développement des relations bilatérales entre la France et l'Allemagne. Un des quatre éléments mentionnés est celui de la constitution de capacités militaires communes. Cela inclut des relations étroites entre les mondes militaire et industriel en matière de prévention des conflits et l'acquisition de moyens de renseignements stratégiques et de commandement. La lutte pour l'information et surtout la recherche de la supériorité de l'information (I*nformation Dominance*) sont des caractéristiques fortes des opérations à venir.

Le développement d'une politique européenne globale en matière d'armement ne doit pas être mené au détriment de la coopération transatlantique[17]. Cette volonté a été réaffirmée lors de la déclaration commune du sommet franco-allemand de Potsdam (30 novembre au 1 décembre 1998) : « A l'heure de la globalisation, nous favoriserons les projets industriels ou technologiques communs dans la perspective de pôles européens notamment dans le domaine des industries aéronautique et de défense, de l'intégration des marchés financiers et du développement de la société de l'information. » Le Conseil franco-allemand de défense et de sécurité, dans son protocole du 30 novembre 1999 à Paris, a de nouveau souligné que la France et l'Allemagne restent dépendantes d'une industrie de l'armement moderne et efficace. La base nationale de l'industrie de l'armement reste cependant le socle de la coopération souhaitée dans le domaine de l'armement en Europe et dans l'alliance.

[16] SCSSI : Service Central de la Sécurité des Systèmes d'Information

[17] Consultations franco-allemandes de Nuremberg, 9 décembre 1996

L'interopérabilité au sein d'organisations multinationales nécessite une évolution et une adaptation des moyens à long terme. L'échange des données n'est possible que sur la base de modèles standardisés. Par conséquent, pour une coopération étroite avec des partenaires, un modèle multinational est à développer. Pour cette raison, le « *Modeling & Simulation (M&S) Masterplan* » de l'OTAN est une base importante. Les Etats-Unis sont le moteur du développement du *M&S* et l'unification de toutes les applications possibles dans un cadre commun reste le but le plus important. Ce cadre commun peut être ce qu'on appelle le *High Level Architecture* (HLA). De plus, il faut préciser le *Conceptual Model of Mission Space* (CMMS). Enfin, il restera à standardiser les données et les interfaces entre les différents systèmes de commandement et les systèmes d'information (*Modular Reconfigurable C4I Interface : MRCI*). Le système d'information de la Bundeswehr permet l'échange des données entre alliés et partenaires de manière sécurisée.

L'Allemagne a libéralisé la cryptographie : elle a édité un document définissant les fondements de la politique allemande en matière de cryptographie[18], qui a clairement adopté le principe d'une liberté d'usage des outils de chiffrement, jusqu'à des clefs de 128 bits et plus.

L'action de l'Allemagne au sein de l'OCDE cherche à souligner l'importance de la protection des utilisateurs et à faire adopter une approche plus libérale de l'utilisation et de la réglementation de la cryptographie.

L'Allemagne est allée de l'avant en publiant dès 1997 une loi réglementant les signatures numériques (*Digital Signature Law : SigG*). Celle-ci, ainsi que l'initiative du gouvernement fédéral concernant le commerce électronique, ont pour objectif d'instaurer une protection maximale pour les utilisateurs. Cela s'avère nécessaire pour créer la confiance entre partenaires commerciaux et permettre ainsi le commerce électronique. Les composantes techniques intervenant dans cette mise en œuvre sont les moyens de création et de chargement des clés de signature dans le système, la capacité de signer (par exemple, au moyen d'une carte à puce), la préparation sécurisée du processus (acte de signature, vérification et visualisation sécurisée), un répertoire de clés publiques et un dispositif d'horodatage. En ce qui concerne les autorités de certification, la loi allemande donne des informations supplémentaires sur leur mise en œuvre : L'autorité supérieure (organisme d'Etat) délivre des licences à des entreprises privées, les autorisant à opérer comme autorité de certification. Elle publie les conditions des licences, fournit des guides techniques sur les produits et les procédures, certifie les clés publiques des titulaires de licence, publie les algorithmes agréés, contrôle périodiquement la sécurité des autorités de certification, etc. Une autorité de certification assure la vérification en ligne des certificats, authentifie les utilisateurs, éventuellement génère des paires de clés et les enregistre sur des cartes à puce, éventuellement assure un service d'horodatage etc. Les autorités de certification doivent se conformer à la loi allemande sur la confidentialité des données, recourir à des composants et des contrôles suffisamment sûrs évalués conformément aux degrés de l'ITSEC (Critères d'évaluation de la sécurité des technologies de l'information) et les autorités de certification ont obligation de se conformer à des procédures et des règles de sécurité très strictes.

[18] « Eckpunkte der deutschen Kryptopolitik » 2 juin 1999

1.4 LA PRISE EN COMPTE DE LA SOCIETE DE L'INFORMATION AUX ETATS-UNIS

Comme nous l'avons vu, la décennie 90 a connu, avec l'émergence de la société de l'information, un bouleversement profond et de dimension planétaire. Les États-Unis ont rapidement pris conscience de ce bouleversement et ont mis en place une politique volontariste pour accélérer l'émergence de cette nouvelle société.

Afin de stimuler le développement de cette société de l'information et d'établir l'hégémonie américaine mondiale dans la maîtrise des NTIC, le gouvernement Clinton a adopté, au début des années 1990, un programme d'action nommé «*National Information Infrastructure* » (NII). La politique du NII s'appuie sur trois instruments :

- Un effort de financement et de valorisation de la recherche,
- L'informatisation des fonctions administratives,
- L'adaptation du cadre réglementaire et législatif.

Initiative de l'exécutif américain, ce programme comprenait un ensemble complet de mesures orienté principalement vers le secteur privé. Il a été globalement un véritable succès car il a permis de fédérer la plupart des résultats des efforts de recherche. Il a connu cependant un échec majeur pour ce qui est de la protection de la vie privée. En effet, quand le gouvernement américain a cherché à contrôler la diffusion et l'usage des produits cryptologiques (notamment avec le programme *« Clipper Chips »*) il a suscité une levée de boucliers et un tollé général de tous les acteurs (citoyens et industriels). L'administration américaine a dû céder et abandonner ce projet.

Enfin, l'action menée au plan intérieur a été étendue au plan international par une politique de promotion de la société de l'information : la « *Global Information Infrastructure* » (GII). Celle-ci a pour principal but de faciliter le développement du *Business* américain.

Pour ce qui est de l'évaluation des produits commerciaux de sécurité (logiciels et matériels) elle est confiée au NCSC[19] qui est la branche de la NSA[20] responsable des programmes informatiques sûrs du Gouvernement américain. Le NCSC édite l' « Orange Book » qui définit les exigences en matière de sécurité. Quant à l'édition des standards ouverts afin de favoriser le développement économique de l'industrie informatique américaine il est confié au NIST[21] qui est une division du Département du Commerce.

1.5 LA « REVOLUTION IN MILITARY AFFAIRS »

La *RMA* est au cœur du débat stratégique américain depuis une dizaine d'années. Elle peut être interprétée comme le passage de la défense américaine d'un système de l'ère industrielle à un système de l'ère de l'information. Dans cette approche, qui ne fait cependant pas l'unanimité, les transformations devraient toucher tous les domaines : les matériels, en

[19] NCSC : National Computer Security Center

[20] NSA : National Security Agency

[21] NIST : National Institute of Standards and Technology

plaçant l'information au cœur des systèmes d'armes ; « les hautes parties de la guerre », en plaçant l'information au cœur des stratégies ; les hiérarchies, en plaçant l'information au cœur des organisations militaires[22]. Aujourd'hui, si la notion de nouvelle civilisation est encore contestée, force est de constater que le monde est en train de changer et qu'un bon nombre de grilles de lectures sont devenues inopérantes. La *RMA* semble donc aller « dans le sens de l'histoire ». Il convient de faire un point sur les transformations en cours aux États-Unis dans les trois domaines des matériels, des organisations et des stratégies militaires.

La *RMA* est donc un concept très large. Seuls, les aspects pouvant concerner l'autonomie de défense de l'Europe au regard de la maîtrise de l'information seront abordés dans la suite.

1.5.1 L'information au cœur des systèmes d'armes

L'information est au cœur des systèmes d'armes. Qu'il s'agisse de son traitement (numérisation), de sa transmission (fibres optiques, satellites), ou de son stockage, les progrès sont rapides et semblent à même de provoquer des ruptures, des sauts qualitatifs, notamment par la très grande précision qu'ils confèrent aux moyens de renseignement, ainsi qu'aux moyens de frappe.

Des tendances déjà anciennes de la guerre s'en trouvent considérablement accélérées : compression du temps, extension de l'espace et intégration des systèmes.

- *La compression du temps.* L'action militaire est de plus en plus rapide. L'acquisition et la transmission du renseignement électronique se font de manière quasi immédiate. La cadence des opérations s'accroît considérablement. On peut aujourd'hui parler d'observation en temps réel (délai 30 secondes) avec une résolution de 10 cm. Le cycle observation-décision-action est accéléré.

- *L'extension de l'espace.* Le théâtre d'opérations s'étend de manière exponentielle : Bataille d'Ulm (1805), 150*150 miles ; bataille de Chancellorsville (1863), 200*200 miles ; bataille de France (1940), 550*650 miles ; guerre du Golfe (1991), 1000*1000 miles. La densité des forces sur le terrain décroît dans les mêmes proportions : batailles de l'antiquité, 100 000 hommes/km^2 ; guerres napoléoniennes, 4 800 hommes/ km^2 ; 1914-1918, 400 hommes/ km^2 ; 1939-1945, 36 hommes/ km^2 ; guerre du golfe, 2 à 4 hommes/ km^2.

- *L'intégration des systèmes.* Les équipements militaires s'intègrent les uns aux autres pour former un « système de systèmes ». Cette intégration poussée est rendue possible par les NTIC. Elle est rendue nécessaire par l'accroissement du rythme des opérations.

Au-delà du renforcement de ces trois tendances anciennes, on assiste au développement de la précision des armements, voire de leur non-létalité. La frappe de précision, à distance, semble devoir devenir l'élément central de l'art militaire. Il en résulte une modification de l'économie des moyens militaires et un abaissement du coût en vies

[22] Cette analyse est développée (au conditionnel) par Bruno TERTRAIS dans *Faut-il croire à une révolution dans les affaires militaires ?* in Politique Etrangère 3/98 pages 611 à 629

humaines des engagements. On peut d'ailleurs se demander si, dès lors que les possibilités techniques de limiter les pertes amies comme les dégâts collatéraux existeront, les opinions publiques ne deviendront pas réticentes à l'emploi d'armes plus rustiques. La nécessaire conservation d'une liberté de manœuvre dans la décision politique d'engagement des forces armées pourrait alors forcer à l'adoption de modèles d'armées *high tech*.

1.5.2 L'information au cœur des organisations

Les trois tendances lourdes évoquées ci-dessus auraient atteint un niveau tel que l'organisation militaire serait en passe de subir des transformations radicales, imitant en cela bon nombre d'organisations du secteur privé qui, pour devenir plus réactives et tirer le meilleur parti des NTIC, ont été amenées à se transformer (organisation matricielle…). La *RMA* favoriserait les petites unités autonomes au détriment des grandes plates-formes.

Dans cette lecture de la *RMA*, nous serions en train d'assister à la fin de la plupart des modes d'organisation militaire : confusion progressive entre les niveaux tactique, opératif et stratégique avec l'apparition d'un théâtre global ; fin des distinctions entre armées, la notion d'opérations « fusionnées » étant en quelque sorte, le stade ultime de l'interarmisation.

Il va de soi que cet aspect organisationnel, plus encore que les autres aspects de la *RMA* suscite de fortes réticences et des débats passionnés. Aussi, le bouleversement organisationnel jugé inéluctable par de nombreux analystes se fera certainement attendre plus longtemps que ne le souhaitent les plus ardents partisans de la *RMA*.

1.5.3 L'information au cœur des stratégies

L'idée consistant à voir la guerre de l'information comme un espace de bataille autonome, le quatrième, qui tend à englober l'espace[23], prend peu à peu consistance et commence à se traduire dans les faits. Ainsi, le 1° octobre 1999, l'US Space Command s'est-il vu confier la mission de coordination de la défense des réseaux informatiques, et devrait se voir confier la mission d'attaque des réseaux informatiques le 1° octobre 2000[24]. Plus largement, l'idée selon laquelle l'information sera au cœur des rapports de force stratégiques de demain est de plus en plus largement admise. L'article « *America's Information Edge* », cosigné par l'amiral Owens (ancien *Vice Chairman of the Joint Chiefs of Staff*)[25] est tout à fait emblématique de cette tendance. Dans cette thèse, la maîtrise de l'information jouera un rôle identique à celui tenu jusqu'ici par les armes nucléaires. En effet, les Etats-Unis, grâce à leur avance technologique dans les domaines de l'information, seraient en passe d'acquérir la faculté de tout savoir, partout dans le monde et en temps réel. Ils se doteraient également de capacités de traitement de l'information permettant une réaction instantanée. Ces deux capacités complémentaires seraient suffisantes pour dissuader tout ennemi potentiel d'agir. Le parallèle va plus loin : les alliés des Etats-Unis n'ayant pas les moyens de rattraper leur retard

[23] En effet, si à moyen terme une militarisation de l'espace, avec la présence de satellites capable de détruire des objectifs sur terre est vraisemblable, aujourd'hui, les seuls objets militaires en orbite sont des satellites d'observation (optique, radar, écoute, alerte) et de communication. Dans tous les cas, ils sont partie intégrante de la dimension informationnelle de la guerre.

[24] Briefing du Général Myers, 5 janvier 2000.

[25] *America's Information Edge* , Joseph S. Nye and William A. Owens, Foreign Affairs, March/April 1996, pages 20 à 36

technologique, il conviendrait de les faire bénéficier d'un « parapluie informationnel » au même titre que du parapluie nucléaire. Cela permettrait de garantir la solidité de l'alliance atlantique.

Sans aller jusque là, l'arrivée d'armes «intelligentes », de moins en moins létales, voire d'armes informatiques semble devoir se poursuivre. Présentée comme une possibilité de plus ne devant pas se substituer aux capacités traditionnelles, elle n'en aura pas moins des implications stratégiques importantes, ne serait-ce qu'en estompant la limite entre la paix et la guerre. En effet, l'attaque d'un réseau est-elle un acte de guerre ? Et si oui, comment déterminer de manière certaine l'origine de l'attaque ?

On ne peut nier que la *RMA* est en partie instrumentalisée. Elle est en effet un thème porteur dans les débats budgétaires américains. Elle est aussi parfois présentée comme un moyen pour les Américains d'asseoir pour longtemps leur leadership sur l'Europe et le reste du monde. Le raisonnement est le suivant : il y a une *RMA* ; vous avez du retard ; vous devez vous mettre à niveau pour rester interopérable ; vous n'avez pas les moyens de recherche et développement suffisants ; achetez américain… Sans être totalement infondées, ces analyses semblent outrancières et simplistes. La *RMA* semble aujourd'hui être une réalité. Il n'en demeure pas moins qu'il n'existe aucune unanimité sur ce que recouvre ce concept. Dans son livre « La guerre au XXI° siècle »[26], Laurent Murawiec reproduit un tableau quelque peu ironique, dressé par l'universitaire Eliot Cohen, qui illustre bien les différentes approches qui luttent pour faire prévaloir leurs vues au sein du *Department of Defense.*

	Le « clone d'Owens »	**Le « vétéran du Golfe »**	**Le « sceptique »**	**Le « révolutionnaire sans certitude »**	**Le « Starship Trooper »**
Où en est la *RMA* ?	*Déjà là !*	*Déjà vu !*	*Quoi ?* *Quelle RMA ?*	*Peut-être que oui, ou non*	*Au-delà de l'horizon*
Qu'est-ce qui la meut ?	*La techno, la techno de l'information*	*La doctrine, la qualité humaine*	*La nature humaine*	*L'intégration des concepts et de la technologie*	*La biotechnologie*
Priorité n°1	*Diminuer les effectifs*	*Préserver les effectifs*	*Préserver l'éthos martial*	*Expérimenter et innover*	*Investir dans la R&D*
Menace n°1	*L'inertie*	*Rival de la même taille*	*Exagérer, surinvestir*	*Ripostes asymétriques*	*Conformisme intellectuel*
Mode d'innovation	*Retombées*	*Sans intérêt*	*Evolution, pas révolution*	*Remontées*	*Science*

Pour se forger une opinion tranchée quant à la profondeur et au rythme de la *RMA*, il conviendra de surveiller quels seront les hommes mis en place aux postes clefs du *Department of Defense* dans les prochains mois. A cet égard, la nomination récente du Général Myers, ancien commandant de *l'US Space Command*, au poste de *Vice Chairman of the Joint Chiefs of Staff* semble aller dans le sens d'une volonté de réforme. Ce sentiment pourrait se voir confirmé si, comme le laissait entendre la revue « *Defense News* »[27] en décembre 1999, l'amiral Owens devait être choisi pour succéder à William Cohen en temps

[26] *La guerre au XXI° siècle*, Laurent Murawiec, janvier 2000, éditions Odile Jacob, page 241

[27] *One to One*, Defense News, December 20, 1999, page 54

que *Secretary of Defense*.

Les pays d'Europe sont jusqu'à présent restés dans une prudente expectative face à la *RMA*. La plupart des auteurs qui se sont intéressés au sujet recommandent en substance « d'attendre et de voir ». Il faut reconnaître que dans le contexte actuel d'une Europe de la défense encore en devenir, il ne semble exister aucune alternative satisfaisante. Cette équation sans solution peut se résumer en trois exigences antinomiques : Interopérabilité, indépendance stratégique, budgets militaires limités.

Dans le modèle d'armée prévu par la *RMA*, l'efficacité sera, plus encore qu'aujourd'hui, le fruit de la circulation et du traitement largement automatisé de gros débits d'information, à grande vitesse, entre des acteurs nombreux et dans un environnement complexe. On comprend bien que dans un tel cadre la nécessaire interopérabilité avec nos alliés, au premier rang desquels les Etats-Unis, est rendue plus difficile que jamais. En effet, le grand nombre de systèmes, de calculateurs, de protocoles d'échanges de données, mais aussi d'algorithmes de traitement de l'information à rendre compatibles multiplie les difficultés techniques. Les Etats-Unis insistent d'ailleurs sur ces difficultés, ainsi que sur l'inanité d'espérer soutenir contre eux une quelconque compétition technologique. La disproportion des budgets militaires respectifs, en particulier en ce qui concerne la recherche[28], est beaucoup trop flagrante.

Cela les conduit à insister, en particulier en usant de leur influence dans l'OTAN, pour que les alliés acceptent de bénéficier de leur « parapluie informationnel » et pour qu'ils conservent un bon niveau d'interopérabilité en dépit de l'intégration de plus en plus importantes des technologies de l'information.

La solution « raisonnable » consistant à accepter ce « parapluie informationnel » des USA comporterait au moins deux inconvénients importants. D'une part la quasi-obligation d'effectuer l'achat d'une grande partie de nos systèmes auprès des Etats-Unis, avec les inconvénients économiques qui en résulteraient. D'autre part le risque de voir notre outil de défense réduit au rang de simple sous-système du « système de systèmes » que constitueraient les forces armées américaines. Ce sous-système, privé de toute capacité autonome, ne pourrait remplir sa fonction qu'au sein de l'ensemble. Il s'agirait bien de la perte de toute indépendance stratégique.

La solution qui semble avoir la faveur de la majorité des auteurs français consiste à refuser toute forme de mutation radicale dans le sillage de la *RMA*. Les raisons invoquées vont du refus de la perte d'indépendance stratégique évoquée ci-dessus à la négation de l'existence de la société de l'information, en passant par la conviction que la *RMA* américaine est vouée à rester au stade de projet. Ce statu quo, en revanche, comporte le risque de rendre inévitable un partage horizontal des tâches entre les alliés : le commandement à ceux qui posséderont des moyens d'acquisition du renseignement performant et la capacité de mener un processus décisionnel rapide dans un environnement complexe, l'exécution aux autres.

Jusqu'à très récemment, la possibilité d'une voie médiane ne semblait pas avoir été explorée. Pourtant, il importe de définir si l'entrée dans « l'engrenage de la *RMA* » nous conduirait inévitablement à faire de nos forces un simple sous-système inutilisable de manière

[28] Si le cumul des budgets de défense européens représente un peu plus de la moitié de celui des USA, le cumul des parts consacrées à la recherche représente moins d'un tiers de l'effort américain

autonome. Peut-être est-il en effet possible, au contraire, de mener une « *RMA* partielle » garantissant à la fois une certaine capacité autonome et une interopérabilité satisfaisante. Dans ce cadre, il semble indispensable d'identifier quelles sont les capacités industrielles qu'il convient de conserver ou de développer.

Il est très probable qu'une mise en synergie des budgets des pays européens, jusque là très peu coordonnés, consacrés à la recherche permettrait sans doute de retrouver une certaine liberté d'action. Un effort plus coordonné, en effet, permettrait le développement des savoir-faire indispensables à une certaine autonomie vis à vis des Etats-Unis. Pour conclure sur une note optimiste, il ne semble pas absurde d'espérer que plusieurs partenaires européens pourraient voir dans ce dossier une occasion de concrétisation de la construction de l'Europe de la défense en même temps que l'opportunité de rattraper une partie de leur retard sur les Etats-Unis en matières de technologies de l'information.

Cette piste, ainsi que d'autres, sera développée dans la deuxième partie.

2 LES ENJEUX POUR LA CONSTRUCTION DE LA SECURITE ET DE LA DEFENSE EUROPEENNE

2.1 INTRODUCTION

Depuis fin 1998, la construction de la défense européenne a reçu une impulsion spectaculaire. Le changement de la position du Royaume Uni vis-à-vis de la défense européenne se trouve à l'origine de cette accélération. L'initiative s'est concrétisée par la déclaration commune franco-britannique de Saint-Malo. Plus tard, la déclaration de Cologne et surtout le sommet d'Helsinki du 10 et 11 décembre 99 ont complété et concrétisé l'expression de cette volonté politique nouvelle et partagée à quinze.

Il y fut tout d'abord décidé que les Etats membres devraient être en mesure, d'ici 2003, de déployer dans un délai de 60 jours et de soutenir pendant au moins une année des forces militaires pouvant atteindre 50000 à 60000 personnes, capables d'effectuer l'ensemble des missions de Petersberg[29]. De nouveaux organes et de nouvelles structures politiques et militaires[30] seront créés au sein du Conseil afin de permettre à l'Union d'assurer l'orientation politique et la direction stratégique nécessaires à ces opérations. Des modalités visant à assurer une consultation, une coopération et une transparence entre l'UE et l'OTAN seront définies, en tenant compte des besoins de tous les Etats membres de l'UE.

Par la mise en place de ces organes, l'UE recherche la disponibilité d'une capacité d'évaluation des situations, de sources de renseignement et d'une capacité de planification stratégique soutenue par des forces militaires crédibles. En bref l'Union veut disposer d'une capacité d'action autonome. Une vraie capacité militaire ne signifie pas uniquement des moyens militaires. Il faut y *ajouter une façon commune de les utiliser et une volonté politique de s'en servir*[31]. Il faut donc au moins un commandement multinational avec ses propres moyens de communications et d'appui et un renseignement efficace ainsi que des forces adaptées.

Au niveau des capacités opérationnelles, une harmonisation des capacités existantes

---

[29] Le 12 juin 1992 à Petersberg, l'UEO se déclare prête à soutenir les activités de maintien de la paix de l'OSCE ou de l'ONU et définit les missions additionnelles à la défense territoriale collective, dites missions de Petersberg, qui pourront être assignées aux forces mises à sa disposition (FRUEO) :

- des missions humanitaires
- des missions d'évacuation de ressortissants ;
- des missions de maintien de la paix ;
- des missions de forces de combat pour la gestion des crises, y compris des opérations de rétablissement de la paix.

[30] Les nouveaux organes politiques et militaires *permanents* suivants seront créés :

un Comité politique et de sécurité (COPS) permanent, composé de représentants nationaux, traitera de tous les aspects du PESC. Dans le cas d'une opération militaire de gestion de crise, ce COPS exercera, sous l'autorité du Conseil, le contrôle politique et la direction stratégique de l'opération ;

le Comité militaire (CM), composé des Chefs d'EM des armées, donnera des avis militaires et formulera des recommandations destinées au COPS ;

l'Etat-Major mettra ses compétences au service de la PESC, notamment de la conduite des opérations militaires de gestion des crises menées par l'UE.

[31] Général Rupert Smith, Deputy SACEUR, Bruxelles 30 mars 2000

devra avoir lieu entre les nations. Ce processus qui se concentre entre autres sur le nombre de chars, d'avions ou de navires à acquérir devrait avoir lieu dans le cadre de l'initiative des capacités de défense, la «DCI[32]» lancée au sein de l'OTAN. Elle pourrait également avoir lieu au sein d'une initiative européenne dans le cadre du développement de la PESC[33].

Au-delà de cette dynamique d'harmonisation de capacités, la recherche de cette autonomie requerra la mise en place, au niveau européen, d'une structure de commandement et de contrôle adéquate ainsi qu'un réseau de renseignement et des moyens SIC afin de soutenir le processus décisionnel. Les problèmes qui résultent de cette volonté comportent différents aspects que nous proposons d'éclairer afin de pouvoir en tirer des conclusions et éventuellement des recommandations.

Les Européens doivent tout d'abord décider au niveau politique de l'autonomie qu'ils souhaitent. En effet, ce choix a des impacts directs sur les capacités à développer en particulier dans les domaines du renseignement et de l'aide à la décision, le commandement et le contrôle. Un premier besoin d'interopérabilité entre partenaires européens se fera sentir lors de cette réflexion. Il est accompagné d'un *nécessaire changement de culture pour que les pays européens partagent plus leurs renseignements*[34].

Le maintien d'un lien transatlantique ferme ressort très fortement également des dernières initiatives de construction de l'Europe de la défense. Dans ce cadre, il convient dès lors de débattre de l'interopérabilité transatlantique nécessaire à la conduite des opérations dans le cadre de l'OTAN. Les Américains ont entamé une révolution dans leurs affaires militaires, comme développé en première partie. Afin de maintenir un certain niveau d'interopérabilité, compte tenu des stratégies différentes des deux côtés de l'atlantique, l'Europe devra se positionner par rapport à la *RMA*.

Du point de vue capacitaire, les Européens devront de toute façon considérer l'existence ou l'acceptation d'un nouveau milieu stratégique : celui de l'information. Ici également des choix s'imposeront. L'Europe se limitera-t-elle à développer des capacités de *Defensive information warfare* ou bien s'investira-t-elle dans des capacités offensives ?

2.2 QUEL NIVEAU D'AUTONOMIE POUR L'EUROPE ?

L'autonomie stratégique, c'est-à-dire la capacité de décider où, comment, quand et pourquoi employer les armées est l'un des objectifs essentiels de la politique de défense. Elle conditionne la maîtrise de l'emploi de la «force». Elle recouvre entre autres l'intelligence des systèmes d'armes et leur mode de mise en œuvre.

L'autonomie stratégique concerne en premier lieu le Renseignement qui détermine l'opportunité et la justification de l'emploi des forces : il s'agit du renseignement humain et du « renseignement technologique ».

Outre la mobilité des forces, l'autonomie stratégique suppose également la maîtrise politique du commandement des forces. La maîtrise du commandement des forces reste essentielle dans le dispositif stratégique. Elle suppose une chaîne de commandement ininterrompue entre le pouvoir politique suprême jusqu'au fantassin, pilote ou marin sur le

[32] DCI : Defense capability initiative

[33] PESC : Politique étrangère et de sécurité commune

[34] Javier Solana, Bruxelles , 30 mars 2000

terrain. Le fonctionnement en toute indépendance de cette chaîne de commandement requiert la garantie de la confidentialité et la fiabilité de transfert de données à tous les échelons. La cryptologie en est la clé. En fonction des opérations celle-ci devra pouvoir s'adapter à la chaîne de commandement c'est-à-dire nationale, européenne, atlantique ou de circonstance. Une politique cohérente est requise en ce domaine.

La maîtrise des systèmes d'acquisition et de traitement de l'information est un enjeu de souveraineté nationale ou européenne. Ces systèmes sont les infrastructures qui fournissent la matière sur laquelle se fonde la prise de décision à tous les niveaux, du stratégique au tactique. Les perturbations, volontaires ou involontaires, dans le bon fonctionnement de ces systèmes peuvent par conséquent conduire à une incapacité de réaction ou, pire, à des décisions erronées mettant en déséquilibre la position européenne sur la scène internationale vivant en temps réel l'évolution des situations de crise.

Les leçons tirées des récents conflits, et en particulier au Kosovo, ont entre autres souligné l'importance du renseignement, à tous les niveaux. La complexité de la gestion des crises impose donc des moyens de renseignement adaptés et intégrés. Si les renseignements peuvent être partagés dans le cadre des alliances, leur maîtrise ne peut dépendre d'une puissance extérieure sauf à prendre le risque d'être désinformé voire manipulé. Actuellement, de nombreux pays de l'Alliance atlantique se reposent, pour le renseignement, sur les informations fournies par les Américains. Seule la France a été capable au Kosovo, grâce à sa capacité de renseignement propre, petite mais autonome, de proposer une certaine réplique au renseignement américain et de ce fait influencer le pouvoir de décision. Il est donc primordial pour les Européens de disposer d'une telle capacité.

Le maintien de la souveraineté doit prendre en compte aujourd'hui la nécessité d'une grande intégration au sein de structures supranationales. La position à l'égard de ces structures, quant au développement des infrastructures de renseignement et de communication, reste encore à déterminer. Or, les systèmes d'informations qui rendent opératoires les données manipulées dans les infrastructures sont également des outils de souveraineté, par le rôle qu'ils jouent dans le commandement des alliances.

Actuellement, de nombreux pays européens possèdent une capacité autonome en matière de SSI[35]. Néanmoins il n'existe pas au niveau européen une capacité commune en la matière. Au niveau de l'OTAN la sécurisation des outils cryptographiques est confiée à une instance américaine, dénommée SECAN. Cette agence d'évaluation et de certification des produits cryptologiques de l'OTAN est intégrée dans la NSA[36]. Elle est régie par un protocole avec échéance tous les deux ans (prochaine 2002) et la tendance actuelle est d'étendre ses prérogatives à tous les produits de sécurité où apparaît une fonction cryptologique, c'est à dire à toute la SSI.

Il existe donc une dépendance européenne très forte vis à vis de la maîtrise de l'information à travers SECAN. Alors que le mandat de cette agence doit être bientôt renouvelé il apparaît essentiel pour les instances européennes d'agir en vue de la création d'un « pendant » européen à SECAN.

[35] SSI : Sécurité des systèmes d'information

[36] NSA : National Security Agency

2.3 PROBLEMATIQUE DE L'INTEROPERABILITE :

2.3.1 L'interopérabilité dans les SIC

L'interopérabilité joue un rôle majeur dans les opérations interalliées et interarmées. Elle se situe dans différents domaines : les moyens, l'organisation, les tactiques et la doctrine.

Les différentes situations qui peuvent se produire dans le contexte géostratégique instable qui prévaut aujourd'hui imposent aux forces armées d'être capable d'agir efficacement dans le cadre d'une coalition multinationale et donc de s'adapter aux doctrines, aux matériels et aux procédures mises en œuvre. La difficulté majeure à laquelle sont confrontées nos forces armées réside dans le contexte politique, l'environnement international et le type de missions qui lui sont confiées. Les missions d'interposition ou d'intervention humanitaire limitent l'ouverture du feu, imposent de tenir des positions statiques, restreignent les capacités de mobilité, laissent l'avantage de la manœuvre à l'adversaire, qui peut, lui, choisir le lieu et le moment de son action. De plus, dans le cadre d'opérations multinationales, les circuits d'information et donc de décision sont plus complexes et se révèlent des freins à la vitesse de réaction et à la coordination des moyens.

La réactivité des forces armées est donc, encore plus aujourd'hui qu'hier, le gage de leur efficacité.

Or, en matière de systèmes d'information, l'interopérabilité réside dans la capacité de ces derniers et de leurs applications à pouvoir fonctionner « naturellement » en un système intégré. Celle-ci confère alors aux différents échelons les avantages offerts par l'intégration de l'ensemble des SIC[37] : réalisation de boucles de décision courtes et dynamiques, fusion des capteurs, perception globale du champ de bataille … Afin qu'en opérations, les forces armées puissent tirer profit à tous les échelons de l'intégration des SIC, l'interopérabilité des systèmes déployés est indispensable.

Or, parler d'interopérabilité ne sert souvent qu'à masquer les lacunes de la réflexion menée sur le sujet même. On ne peut en effet parler d'interopérabilité sans immédiatement préciser avec qui et pour quoi faire. Là sont les questions de fond. Des réponses à ces questions découlera l'architecture technique à mettre en place.

Cependant, la réalisation d'une telle interconnexion entre des SIC différents nécessite souvent la réalisation de modifications et de développements intermédiaires plus ou moins importants. Cette capacité doit donc être pensée dès l'expression du besoin, confirmée durant tout le déroulement du programme et vérifiée lors de toutes les expérimentations ou exercices. Elle impose la prise en compte de problèmes de nature différente, à des niveaux différents :

- interopérabilité technique : capacité de deux systèmes à communiquer et échanger des informations,
- interopérabilité procédurale : capacité à s'accorder sur la syntaxe des messages,
- interopérabilité opérationnelle : capacité à comprendre les messages selon un même référentiel.

[37] SIC : systèmes d'information et de communication

L'interopérabilité native (de bout en bout) reste une « une vertu rare et peu répandue » Cette interopérabilité se faisait plutôt sous le concept de téléport : les réseaux sont interconnectés à partir de quelques points concentrés ou l'on met des moyens techniques adaptés (passerelles).

2.3.2 Des contraintes fortes

Il faut aujourd'hui combattre l'idée selon laquelle l'interopérabilité entre les SIC est une chose qui va de soi et qu'il n'y a qu'à demander pour que cela soit.

L'interopérabilité pose des problèmes techniques qu'il convient de prendre en compte le plus tôt possible s'il l'on veut pouvoir les résoudre de manière élégante et non générer une « usine à gaz » par ajout de passerelles et autres éléments, ce qui risque d'aller à l'encontre de l'efficacité requise pour les forces armées.

De plus, cette capacité demande une analyse précise des besoins opérationnels, afin d'être en mesure de garantir l'interopérabilité opérationnelle. Pour se comprendre, encore faut-il parler le même langage et utiliser la même grammaire et le même vocabulaire, mais il faut aussi savoir pour quoi faire.

Or, dans ce domaine, le poids du passé se fait lourd. Ainsi, il peut être difficile de remettre en cause des choix faits par le passé, qui s'ils étaient parfaitement justifiés à l'époque, ne le sont peut-être plus aujourd'hui ou sont totalement obsolètes. Mais les investissements consentis hier et ceux qu'il conviendrait de consentir aujourd'hui font souvent revoir à deux fois la copie. De plus, ces choix résultent souvent de la perception qu'ont les utilisateurs de leur système, de ses capacités et des services qu'il doit offrir. Les habitudes de travail et les cultures d'utilisation sont autant de facteurs dont il est difficile de se détacher. Ces divergences culturelles nécessitent un traitement très en amont dans la conception des systèmes si l'on ne veut pas qu'elles se transforment en un frein voire en une source de blocage lors de la mise en service du système. De même, il convient de favoriser la réalisation d'outils de traduction ou de transformation automatique des données pour permettre de se libérer d'une recherche laborieuse de compromis pour trouver des solutions aux besoins opérationnels. L'exemple des travaux menés actuellement par l'armée de l'air sur la migration du STRIDA[38] vers le SCCOA[39] illustre les difficultés qui peuvent être rencontrées, en particulier pour les besoins d'interopérabilité avec le programme OTAN lié (ACCS[40]).

De plus, pour être en mesure de garantir l'interopérabilité procédurale, la tendance actuelle est de suivre les standards développés par le marché civil.

D'une part, la dynamique, dont fait preuve le milieu de l'information, a comme conséquence d'accroître la rapidité du cycle de vie des équipements et des composants, faisant de l'obsolescence une des difficultés majeures rencontrées sur les SIC. D'autre part, la dynamique imposée par le secteur civil rend peu viable économiquement et du point de vue technologique le développement de normes spécifiquement militaires. Il en résulte donc que la dynamique des technologies civiles échappe de plus en plus au contrôle du monde militaire.

En conséquence, le suivi et le respect des normes deviennent indispensables pour

[38] STRIDA : Système de traitement et de représentation des informations de défense arienne

[39] SCCOA : Système de commandement et de conduite des opérations aéreiennes

[40] ACCS : Air command and control system

garantir un niveau de performances identique entre les systèmes militaires et les systèmes civils, et pour être capable de maîtriser la complication significative générée sur les architectures techniques et opérationnelles mises en œuvre.

En conclusion, aujourd'hui, le constat est flagrant et ne devrait pas se démentir à l'avenir : les différentes avancées techniques dans le domaine des NTIC ont pour conséquence de donner à l'interopérabilité une dimension nouvelle et de lui conférer des enjeux d'une nature différente de ceux qui ne concernaient auparavant que les seuls domaines techniques liés à l'emploi des forces.

2.3.3 Interopérabilité et sécurité

En matière de systèmes d'information, il existe généralement un certain antagonisme entre INTEROPERABILITE et SECURITE. Cette dernière est généralement présentée comme un frein au plein emploi opérationnel des systèmes d'information. De plus, en regard du coût des systèmes d'information, la technologie des systèmes de sécurité est en retard, vu son faible intérêt économique et les surcoûts qu'elle engendre.

La recherche de l'interopérabilité risque de se faire au détriment de la sécurité. D'une part, l'emploi d'une technologie «ouverte » au domaine public, notamment par l'achat de produits sur étagère, peut donner l'avantage à l'adversaire, en rendant ces systèmes plus vulnérables que ceux basés sur une technologie plus « fermée ». D'autre part, l'emploi d'une technologie étrangère dans ce domaine peut fragiliser la sécurité du système, sur lequel elle est appliquée, alors que l'emploi d'une technologie spécifique européenne pourrait être générateur de « retard ».

De plus, en période de crise, lorsque la tension se fait plus pressante sur le technicien ou l'opérateur, la nécessité d'établir une liaison ou d'offrir un service risque de se faire au détriment du respect des règles de sécurité. Dans certains cas, relâcher les contraintes de sécurité peut apparaître dans un premier temps comme la solution pour garantir l'établissement du service recherché, mais cette « adaptation ad hoc » du cadre d'emploi offre autant de failles à la compromission du système et la mise en place de procédures parallèles, faisant peser ainsi un risque plus indirect sur la capacité à interopérer du système.

2.3.4 « Fossé technologique » entre les capacités opérationnelles des USA et de l'Union européenne

Avant de discuter de l'opportunité pour les Européens de suivre certaines orientations de la *RMA*, il convient de clarifier la question d'un éventuel « fossé technologique » qui condamnerait l'Europe à être dépendante des USA, soit industriellement, soit opérationnellement, soit les deux.

Si l'on ne peut nier l'existence d'un fossé technologique, il convient de constater tout d'abord qu'il résulte principalement d'un emploi intensif par les Américains des technologies de l'information et apparaît plus particulièrement dans le domaine des munitions PGM et des moyens de C4ISR[41]. De plus, ce fossé est principalement causé par une certaine asymétrie des perspectives stratégiques américaines et européennes. Là où les Européens préfèrent une approche des crises « politiquement symbolique », les Américains donnent leur faveur à

[41] C4ISR : Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance.

« l'efficacité militaire ». L'approche américaine est liée à son impulsion traditionnelle vers le déploiement découlant de sa position géographique. Les Européens, préoccupés par la défense de leurs frontières, tenaient un discours plus statique. Au fil des ans, ces deux stratégies ont implicitement fait diverger les choix dans leurs capacités opérationnelles respectives pour creuser un écart défini actuellement comme « fossé ».

Face à ce fossé, les Américains peuvent adopter deux attitudes différentes : l'une indifférente et «réaliste», l'autre proactive et plus idéaliste. L'attitude «indifférente» consisterait pour eux à maintenir le rythme actuel des développements sans attendre les Européens et sans se soucier des conséquences sur les équilibres ou déséquilibres capacitaires. Une attitude proactive de la part des Américains comme des Européens serait certainement plus opportune pour l'efficacité des coalitions dans les opérations multinationales à venir.

Comment pourrait se développer cette voie ? Si l'on accepte que les moyens devant être mis en œuvre pour résorber le fossé sont de la responsabilité aussi bien des USA que des Européens, une coopération inter gouvernementale est requise. Les gouvernements respectifs doivent pour ce faire tendre vers une définition commune des menaces les plus importantes à leurs intérêts communs et déterminer les capacités à développer pour y répondre. Afin de faciliter l'interopérabilité, il faudrait ensuite encourager l'ouverture des marchés des technologies de l'information. Par cette ouverture, une coopération industrielle entre les pays européens et les USA devrait être encouragée, ce qui contribuerait à améliorer l'interopérabilité des deux côtés de l'Atlantique.

Bien qu'on ait affaire à des technologies sensibles, des partenariats industriels entre Européens et Américains se développent, comme cela s'est produit récemment dans l'industrie aéronautique. Malgré le risque à court terme de ne pouvoir se procurer que des moyens américains, la création d'un marché transatlantique ouvert induirait un gain de performance des systèmes par un encouragement de la recherche et du développement, et une augmentation du niveau requis pour les systèmes, l'objectif étant de définir des besoins militaires communs, dans un contexte de stratégie commune. La définition des priorités opérationnelles qui en découlerait doit alors viser l'interopérabilité indispensable pour opérer dans des opérations multinationales, alliées ou de circonstance.

La coopération transatlantique préconisée doit donc se baser sur des «règles communes». L'harmonisation des besoins opérationnels, déjà mentionnés, la recherche d'un meilleur rapport coût / efficacité, la sécurisation de l'approvisionnement ou encore le partage de l'information et de la technologie pourraient servir de principes de base communs. La souveraineté des partenaires et un équilibre plus grand des relations entre les coopérants devraient être recherchés.

De plus, en matière de sécurité, les Européens souffrent du diktat imposé par les USA, qui privilégient avant tout le « savoir » et le renseignement au lieu de partager leurs informations.

Si l'Europe veut être capable d'assurer sa propre appréciation de la situation au rythme imposé par le tempo de l'activité réelle des opérations, il faudra combler le «déficit d'interopérabilité» et assurer la sécurisation des SIC. Il faudra donc être apte à repérer et donc à réagir face à des attaques sur les systèmes d'information. Ceci suggère que les Européens développent une capacité à mener des « opérations offensives de l'information ». Cette voie sera explicitée dans le paragraphe 3.4.

De leur côté, les Américains sont confrontés dans le développement de la *RMA* au problème du maintien de l'interopérabilité. Dans leur concept Joint Vision 2010, les USA ont, à l'origine, oublié de prendre en compte les alliés européens. Ils se trouvent maintenant

confrontés à une contradiction. Doivent-ils préserver leur avantage technologique pour éventuellement maintenir leur hégémonie ou doivent-ils assurer l'interopérabilité avec les alliés, et si oui, lesquels ?

Il faut d'urgence définir un certain nombre de choix stratégiques. Le retard par rapport aux USA n'est pas rattrapable dans tous les domaines. Il faut définir des pôles à conserver et les répartir entre Européens pour maintenir les coûts à un niveau supportable.

Pour essayer de combler le fossé technologique existant entre les USA et l'Europe, l'adhésion à certains principes pourrait être retenue : les USA et les Européens partagent les responsabilités dans la défense des intérêts communs et dans la confrontation aux défis militaires, l'objectif de la *RMA* atlantique doit s'inscrire dans la promotion de l'efficacité militaire de l'Alliance :

- les USA et les Européens doivent œuvrer ensemble et en collaboration étroite pour combler le fossé technologique qui les sépare,
- la technologie développée dans la *RMA* devra être partagée entre les alliés, la confiance en l'ouverture des marchés pouvant être l'une des clés de la solution définitive.

2.4 QUELLE REPONSE DONNER A LA *RMA* PAR LA FRANCE ET L'EUROPE ?

Aujourd'hui, les forces armées françaises, comme leurs homologues européennes, sont confrontées à de nombreux défis : réforme de l'appareil de défense dans un contexte budgétaire délicat, adaptation de l'outil de défense face à des engagements nouveaux des forces et dans un environnement politique de plus en plus présent. Elles doivent, en particulier, s'adapter aux nouveaux concepts de PC[42] de forces multinationales, que sont les PC GFIM[43].

Or, l'efficacité dans la conduite des opérations et la reconnaissance, par le principal leader dans la conduite d'opérations internationales à savoir les USA, du droit d'un pays à y participer imposent et imposeront de plus en plus l'emploi d'une base commune et unique pour des systèmes comme les SIC, qui sont à la base même de la coordination entre les participants.

De par l'avance en la matière et la puissance de développement qu'ils affichent, les USA sont en mesure d'imposer, comme systèmes communs, leurs propres SIC. Il sera désormais difficile à la France, aux différents pays européens et à l'Europe d'échapper au risque d'uniformisation « de facto » de leurs SIC.

Les enjeux pour la défense sont capitaux, mais que dire alors des enjeux industriels qui se cachent derrière cette dépendance annoncée à l'égard de moyens américains ? Que deviendrait alors le soutien technique et opérationnel indispensable à l'utilisation de tous moyens ?

Mais, une carte n'a, semble-t-il, pas encore été jouée : celle de l'Europe de la Défense ?

---

[42] PC : Poste de commandement

[43] GFIM : Groupement de forces interarmées multinationales

Le défi représenté par les NTIC est à la hauteur des ambitions affichées en matière de construction d'une Europe de la Défense. Disposer de ce qui apparaît désormais comme le « système nerveux » de la force armée pourrait se révéler dans un futur proche comme le domaine de prédilection de recherches et d'acquisition de capacité stratégique.

Or, une vision particulière semble se dessiner aux USA : les interventions majeures seraient réservées à l'intervention des forces armées américaines, les conflits de faible intensité feraient l'objet d'interventions des alliés à vocation strictement régionale.

Si cette orientation découle de la logique de supériorité technologique affichée jusqu'à présent par les USA, elle risque de leur conférer, de fait, la possibilité de suivre et contrôler à distance toute situation. En effet, les développements réalisés par les USA dans le domaine de l'acquisition, de la transmission et du traitement des informations découlent de leur volonté de domination technologique et d'hégémonie politique clairement affichée par leurs autorités. Ayant développé un modèle stratégique à prétention universelle, les USA ont désormais la possibilité de proposer la fourniture de toutes les infrastructures d'acquisition, de transmission et de traitement des informations, avec engagement de forces lors d'opérations majeures et sans engagement de troupes lors de crises régionales gérées par les alliés concernés, en particulier les Européens.

La position des USA peut donc se résumer à la réalisation d'un « bouclier informationnel »[44], à l'image du bouclier nucléaire fourni depuis 50 ans sur l'Europe par les Américains. Ce nouveau concept de dissuasion, comme son prédécesseur, va consolider le leadership des USA sur tous les différents types d'opérations et le contrôle stratégique, opératif et tactique de tous les théâtres d'opérations (cf. supra § 1.5.3).

Or, aujourd'hui, l'OTAN s'est engagée dans une réorganisation interne et externe, la DCI se développe offrant un cadre idéal pour l'harmonisation de nombreux projets européens d'équipements de défense et les NTIC se révèlent de plus en plus comme un domaine porteur pour la réalisation de capacités propres, répondant ainsi au besoin d'autonomie réelle manifesté par les pays européens. Les NTIC offrent à l'UE la possibilité de manifester sa volonté de définir son propre modèle stratégique de défense, à l'image de la volonté française de créer son propre modèle de dissuasion nucléaire autonome ou de la réponse allemande de « défense alternative » lors de la crise des Euromissiles.

Mais, dans ce contexte, un point de rupture existe concernant l'interopérabilité opérationnelle entre les pays européens et les USA.

Ainsi, si demain ne voit se concrétiser en Europe :

- aucune volonté politique forte dans la construction d'une Europe de la Défense,
- aucune prise de conscience de l'inévitable impact des NTIC sur les affaires militaires, à l'image de celle actuellement en cours aux USA mais adaptée à la spécificité européenne,
- aucun engagement volontaire dans la prise en compte du milieu informationnel dans les stratégies militaires,

alors, les carences observées actuellement entre les capacités opérationnelles européennes et américaines vont s'amplifier, se transformer en une absence totale

[44] Sommet de Washington, Avril 1999

d'interopérabilité et compromettre, voire rendre impossible toute action cohérente des alliés pour la sécurité commune.

Des analyses précédentes, découlent les conclusions suivantes :

- il sera difficile pour la France et ses voisins européens, comme pour l'Europe, de suivre les USA dans la course technologique et l'inflation politique qu'ils ont initiées avec la *RMA*,
- si la transposition systématique de la *RMA* à l'Europe semble hors de prix pour les Européens, une réponse partielle visant à leur conférer l'autonomie d'action et de décision recherchée est parfaitement envisageable,
- la qualité de cette autonomie dépendra des volontés politiques affichées en théorie et dans la pratique par les différents pays européens et de la capacité de l'Europe à développer en commun ses propres moyens, à défaut de démarche européenne, la France devra s'orienter vers l'acquisition de moyens autonomes, dont les capacités d'interopérabilité interarmées et interalliés doivent être un impératif majeur et dont les performances de sécurité devront être clairement définies, en mode nominal national et en mode secondaire interallié.

2.5 QUEL COMPROMIS RECHERCHER ?

L'information n'a de valeur que par sa circulation, son traitement et son exploitation, en temps utile et au bon niveau de responsabilité.

Dans ce cadre, de nombreuses contraintes jalonnent le chemin de l'interopérabilité : impératifs civils, existence de systèmes de conception hétérogène, divergences culturelles et nécessité de prendre en compte le facteur humain. Il en résulte que la recherche de l'interopérabilité est difficile et que la recherche d'une plus grande efficacité en la matière risque de s'effectuer au détriment de la sécurité des systèmes.

Il faut ainsi savoir se montrer honnête et reconnaître qu'il est parfois fallacieux de parler d'interopérabilité quand, pour arriver à établir une connexion entre des systèmes, on accepte sciemment de dégrader les performances de ces systèmes voire de compromettre leur sécurité. Si des choix techniques doivent garantir l'interopérabilité de base des systèmes, leurs conditions d'emploi doivent permettre le gain d'efficacité tant attendu.

Par ailleurs, l'interopérabilité dépend de la volonté des partenaires de coopérer. Or, la réticence que chacun manifeste souvent pour divulguer telle ou telle information joue à l'encontre de l'interconnexion des systèmes et du partage de l'information qu'elle permet.

Les SIC sont aujourd'hui incontournables. De nombreuses contraintes s'exercent sur eux et se révèlent comme autant de frein à leur efficacité. La maîtrise globale de leur fonctionnement, en particulier leur gestion et leur sécurité, est indispensable à chaque partenaire et est le gage impératif pour en assurer un fonctionnement optimal, alors qu'ils constituent désormais le « système nerveux » de toute force armée, interarmées ou interalliée.

Choisir une architecture pour un SIC ne peut se décorréler, complètement, des décisions politiques prises sur le rôle qu'entend jouer la France sur la scène internationale, en particulier sa position à l'égard de ses alliés ou du rôle que les pays européens entendent assurer en tant qu'entité constituée.

Au-delà des enjeux technologiques, industriels et économiques, apparaissent les défis

politiques d'une dépendance forte d'un éventuel pilier de défense européenne vis-à-vis de son allié américain.

Cependant, il convient de ne pas perdre de vue la puissance militaire et diplomatique des USA. L'UE doit donc éviter une concurrence trop « frontale » en matière de défense. Il lui appartient au contraire d'essayer de définir son action dans une perspective de complémentarité par rapport à celle des USA. Dans ce but, il convient d'orienter la coopération de défense de l'UE vers des « niches stratégiques » permettant à l'Europe de développer sa propre stratégie.

3 RECHERCHE D'UN CONCEPT DE «STRICTE SUFFISANCE » EN MATIERE D'INFORMATION

3.1 LA MAITRISE DE L'INFORMATION : UNE NECESSITE ; LA SUPERIORITE DE L'INFORMATION : UNE POSSIBILITE.

Un des principes de la stratégie militaire est qu'il faut être capable de concentrer la puissance de destruction, d'occupation de terrain ou autres, en fonction de l'effet recherché, plus rapidement que l'adversaire, tout en maintenant la cohésion de ses propres forces.

Ainsi, il est capital au niveau de théâtre d'opérations de pouvoir détecter les mouvements ennemis pour permettre la concentration des forces en mesure de s'opposer à leur action. De même, au niveau de la manœuvre tactique, il est indispensable d'assurer la coordination la plus efficace des systèmes afin de tirer profit au maximum de leur complémentarité dans l'engagement.

Aujourd'hui plus qu'hier, le fait de pouvoir soutenir un rythme décisionnel plus rapide que celui de l'adversaire est une des conditions préalables de succès.

Cependant, si la vitesse de progression des technologies de l'information offre la possibilité de disposer de capacités techniques supérieures, elle ne représente un facteur de supériorité opérationnelle que par l'emploi qui en est fait. La supériorité sur l'adversaire s'acquiert, avant tout, en mettant en œuvre un cycle décisionnel plus rapide que le sien, mais aussi en perturbant son cycle décisionnel par la destruction de ses moyens de communications ou la compromission de ses informations.

Cette idée est renforcée par celle développée par les USA, selon laquelle « le pivot de la bataille consiste désormais à éclaircir le champ de bataille au sens large pour les forces amies et à l'opacifier pour les forces adverses »[45].

Si « rendre plus impénétrable aux yeux de l'ennemi le brouillard de la guerre et de le pénétrer soi-même »[46] fait partie depuis longtemps des objectifs militaires, les forces de l'ennemi qui concourrent à la perception du champ de bataille et qui lui permettent de communiquer sont devenues le centre de gravité de l'adversaire. Obliger une force militaire à renoncer à ses SIC, pour des motifs défensifs et de protection élémentaire, revient à limiter son pouvoir de nuisance à une « petite guerre », faite de guérilla ou d'actions terroristes et à priver ses autorités politiques de moyens d'actions de vive force lui permettant de défendre ses vues.

Pour un état, ce choix est intrinsèquement inadmissible. Son réflexe premier est alors l'acquisition minimale de moyens défensifs capables de mettre en échec les moyens offensifs de l'adversaire, avant de s'orienter vers une démarche plus agressive. Cette évolution est souvent attractive car les moyens offensifs et défensifs sont généralement de nature similaire.

Cette nouvelle forme de guerre se révèle un jeu de cache-cache entre brouilleur et brouillé et une surenchère entre mesures et contre-mesures. L'enjeu est le contrôle du milieu informationnel, par une maîtrise voire une supériorité de l'information.

---

[45] « Guerre informationnelle et nouveaux médias » L. Murawiec STRATEGIE (01/98)

[46] Métaphore de Clausewitz

3.2 LE « MILIEU DE L'INFORMATION » : NOUVEAU MILIEU STRATEGIQUE ?

L'information apparaît, de plus en plus aujourd'hui, comme une dimension nouvelle et autonome de l'activité humaine, comme le furent successivement le domaine terrestre, le domaine maritime, le domaine aérien et enfin le domaine spatial à la fin du siècle dernier. Elle constitue alors un domaine à part entière, que l'on appelle le cyberespace.

Cette évolution ne peut laisser les forces armées à l'écart. Elles sont impliquées dès le temps de paix et surtout en temps de crise.

En effet, dans cette perspective, la vision proposée par les forces armées américaines (cf. paragraphe 1.4) laisse apparaître une multiplication et une accélération des interdépendances entre les architectures globales, qui supportent les différentes formes de l'action sur le théâtre (observation, ouverture du feu, protection, communication, commandement …).

De telles capacités, une fois acquises complètement, devraient donner à l'état qui en dispose un avantage déterminant sur un adversaire disposant certes de forces lourdes équivalentes, mais ne disposant pas du gain capital apporté par les NTIC dans la maîtrise de l'information.

En réalité, il est possible de voir dans le cyberespace, ce nouveau milieu stratégique de l'information, l'évolution inévitable vécue par le milieu spatial. En effet, l'utilisation de l'espace se concentre, aujourd'hui, sur les vecteurs d'information et de communication, que sont les satellites de télécommunications, d'observation ou de positionnement. On peut donc penser que le milieu de l'information a absorbé le milieu spatial, les vecteurs du second concourrant tous à la maîtrise du premier (cf. supra § 1.5.3).

Désormais, il convient de parler des quatre milieux stratégiques, que sont les milieux terrestre, maritime, aérien et informationnel.

On peut cependant s'interroger sur la poursuite de ce phénomène. Le milieu de l'information, qui a envahi aujourd'hui nos sociétés et touche toutes nos activités, submerge également les milieux stratégiques traditionnels des forces armées et modifie en profondeur leurs modes d'actions. Ainsi, la perspective de le voir tout simplement les supplanter dans l'avenir ne doit pas être ignorée.

Cependant, dans le cadre de conflits asymétriques, où l'adversaire refuse l'affrontement direct et préfère user de modes d'action plus adaptés à ses forces et à son environnement, le gain apporté par une supériorité technologique en matière de SIC peut se révéler plus limité. En effet, l'impact des NTIC se trouve alors confronté à la capacité de dissimulation mise en œuvre par ces modes d'actions (exemple, la guérilla) et à la rusticité des moyens engagés par un adversaire sous-équipé. L'exemple de l'intervention internationale en Somalie, en particulier la participation américaine, est là pour en témoigner.

L'aspect stratégique de ce quatrième élément et le gain d'efficacité apporté par la maîtrise de l'information n'apparaissent donc pas aussi distinctement dans les conflits de basse intensité. Seule, la gestion médiatique des évènements, de par l'impact potentiel qu'elle peut avoir sur les opinions publiques internationales, échappe à cette règle et peut même constituer souvent l'enjeu de certaines actions. En effet, les nouveaux concepts opérationnels mettent en évidence que la victoire militaire sur l'adversaire n'est plus forcément l'objectif à atteindre, ce qui est souvent le cas dans les missions d'interposition ou de maintien de la paix.

3.3 VERS UN CONCEPT DE « STRICTE SUFFISANCE » POUR LA MAITRISE DE L'INFORMATION

La France est une puissance de taille moyenne, qui souhaite pouvoir disposer d'une capacité de décision et d'action autonomes, tout en prenant la part de responsabilités qui lui incombe dans les alliances et accords internationaux en matière de défense.

La maîtrise des systèmes d'acquisition et de traitement de l'information est un enjeu de souveraineté nationale.

Or, la rapidité des opérations rend naturellement difficile le partage des décisions et donc des responsabilités. De plus, s'il y a partage de l'information, un partenaire qui aurait la main mise sur tous les moyens serait à même de s'en réserver certaines à son seul profit, comme ce fut le cas avec les USA lors de la guerre du Golfe ou pendant les opérations menées sur le Kosovo.

Les SIC sont, donc, le support indispensable à la prise de décision et d'action pour tous les niveaux. La maîtrise de ces outils impose de conserver le contrôle sur les fonctions les plus sensibles :

- la sécurité de bout en bout des systèmes, notamment par la cryptologie,
- la capacité à disposer d'un minimum de communications haut débit sécurisées.

Or, durant toutes les phases de la vie d'un système, depuis la conception jusqu'à l'implémentation, il convient d'évaluer d'une manière approfondie les objectifs de l'information et de la technologie de communication, à savoir :

- quel est le niveau de sécurité requis ?
- quelle est la sensibilité de l'information « manipulée » ?
- faut-il s'orienter vers un système en « stand-alone » ou un réseau de systèmes ?
- quel degré d'intégration avec des systèmes civils recherche-t-on ?
- quel degré d'interopérabilité recherche-t-on avec les USA ?

Ainsi, la maîtrise de certaines fonctions jugées vitales ne doit pas aller à l'encontre de la capacité d'interopérabilité de nos systèmes avec ceux des alliés, en particulier avec les USA, dont le rôle moteur en matière de NTIC et de SIC n'est plus à démontrer.

Ainsi, avant de choisir toute nouvelle orientation et prendre toute décision, il convient de :

- déterminer avec précision le besoin opérationnel exact et identifier parfaitement les fonctions vitales, dont la maîtrise et le contrôle doivent être garantis sur les différents systèmes mis en œuvre,
- définir les modalités de maîtrise et contrôle national de ces fonctions, dans leur cadre global d'emploi,
- préciser le degré de dégradation des performances de ces fonctions, qui reste acceptable compte tenu de la nécessaire interopérabilité entre systèmes alliés.

3.4 L'INFORMATION COMME MOYEN DE COMBAT

Les infrastructures essentielles d'un pays (télécommunications, banques, finance, secteur public, services de police, services d'urgence,…) sont devenues un objectif privilégié dans le cadre des opérations informatiques (IO[47]). La vulnérabilité des systèmes d'information est liée au caractère transnational de ce risque. De plus, de nombreux systèmes d'information sont interconnectés et le contrôle en est centralisé. Au niveau national, cela devient un problème interdépartemental avant d'être international. Certaines législations existantes en Europe ont été présentées en première partie.

A côté de cela les Européens sont en pleine phase d'harmonisation de leur outil militaire. Les solutions préconisées, à commencer par les besoins en renseignement et en commandement, contrôle et communications, soulignent non seulement l'importance du processus mais révèlent un retard certain ou du moins une sérieuse divergence de stratégie avec les Américains.

De cette évolution de notre environnement, il ressort que la «société de l'information» a une influence fondamentale sur la manière dont les opérations se dérouleront dans un avenir très proche. La « guerre informatique[48]» devient fondamentalement différente des opérations classiques et aura sans aucun doute des répercussions importantes sur les structures, les procédures, les doctrines mais également sur le volume des moyens nécessaires à mener des opérations. L'information devient une nouvelle forme de moyen de combat qui se déroule dans le « quatrième milieu stratégique », introduit supra, pour le moment en complément des moyens de combat classiques.

Les IO font partie de ce concept global. Elles englobent des opérations défensives et offensives. Les IO sont plus que la maîtrise de la technologie. Il s'agit d'une stratégie qui harmonise l'emploi d'éléments technologiques et non technologiques, létale ou non, afin d'obtenir la supériorité dans le domaine de l'information. Elles comprennent des aspects sous-jacents comme «l'Information assurance», la sécurité physique, la sécurité des opérations, la contre déception, le contre renseignement, la protection de l'information, la protection électronique, les opérations spéciales.

Le contenu de l'information durant des opérations militaires augmente sensiblement. Ceci est la conséquence de la prolifération des senseurs, du rythme des opérations, de l'augmentation de l'information, ou encore de l'automatisation des systèmes d'armes, … Cinq piliers sont définis à l'OTAN sous le dénominateur « *Command & control warfare* »(C²W). Il s'agit de l'attaque sur des objectifs physiques, la guerre électronique dans son acceptation la plus large, la déception, les opérations psychologiques et la protection des opérations propres. Les moyens à mettre en œuvre pour couvrir la totalité de ces opérations sont à rechercher dans toutes les capacités actuellement utilisées dans les forces armées. Néanmoins, les porteurs communs sont les systèmes SIC, performants, ainsi que le renseignement.

Pour les Européens, il convient dès lors de lancer une réflexion sur la nécessité de se doter d'une capacité de mener des opérations informationnelles et si oui, il importe de déterminer les formes d'opérations qu'ils veulent pouvoir mener. Actuellement la plupart des

---

[47] IO : information operations (MC422): actions taken in support of political and military objectives which influence decision makers by affecting adversary info while exploiting and protecting one's own info.

[48] Information warfare (MC 422) : information operations conducted during crisis or conflict in order to achieve or promote specific objectives over specific adversaries.

pays européens se limitent (volontairement ou non) à une série de mesures défensives. Une approche globale n'existe pas encore. Il importe néanmoins de maîtriser le Cyberspace afin de pouvoir conduire des IO dès que nécessaire : il faut donc procéder dès le temps de paix au rassemblement de l'information, à son analyse, à son interprétation,…. Il faut également revoir les doctrines et les procédures, afin d'envisager la manœuvre (tactique) au profit de l'information et afin d'en tirer profit au maximum, comme par exemple dans l'emploi de munitions précises.

Quelles sont les actions défensives possibles ?

Dans le cadre de la prise de décision, il s'agit de préserver l'intégrité de nos systèmes d'information. Ceci demande en tout temps des mesures de protection actives et passives telles l'analyse de la vulnérabilité des SIC stratégiques, la mise en place de banques de données dynamiques afin d'automatiser ce processus et d'exécuter des simulations, d'adapter la législation …

Dans le cadre de la prévention, il s'agirait de garantir la protection maximum des systèmes en temps de paix afin de minimiser tout dégât, de sensibiliser le personnel par la formation ou l'information, par l'emploi sélectif d'Internet pour la mise en réseau d'information sensibles et/ou classifiées. Les mesures de protection, de détection et contre-mesures d'information, l'interopérabilité interdépartementale et internationale ainsi que la R&D peuvent contribuer à une meilleure protection des systèmes.

Dans le cadre de la gestion des crises, il convient par exemple de protéger physiquement les infrastructures critiques.

Bon nombre d'actions sont donc possibles. Avant de pouvoir harmoniser des capacités existantes ou à développer, les Européens devront définir leurs choix en la matière.

3.4.1 A propos de la dissuasion informationnelle

Dans ce contexte, on pourrait imaginer que la maîtrise de l'information, dès le temps de paix, puisse concourir à dissuader un belligérant d'intenter une action contre toute nation devenue puissante par l'acquisition de cette maîtrise. Mais, peut-on vraiment développer une capacité de dissuasion dans le domaine de l'information, et à fortiori peut-on développer une capacité de dissuasion « classique » basée sur la maîtrise de l'information ?

Avant de parler de dissuasion informationnelle, il faut pouvoir répondre à différentes questions. Comment localiser un attaquant, l'identifier et connaître ses intentions ? Comment collectionner des preuves ? Quelle « flexibilité » peut-on avoir pour la réponse ? Dans ce domaine, il faut reconnaître que dissuader, par la maîtrise de l'information, un belligérant de mener des opérations n'est pas aisé, parce que les paramètres nécessaires à l'analyse de la situation ne sont pas disponibles dans les mêmes proportions et dans la même échelle de temps que pour la dissuasion classique. Ainsi, malgré tous les moyens de renseignement et d'analyse mis en œuvre par les grandes puissances, il n'a pas été possible de prévoir l'invasion du Kuweit par l'Irak ou encore le génocide au Rwanda. On est donc encore loin de toute forme de dissuasion informationnelle. Les derniers essais nucléaires indiens en sont un autre exemple.

On peut néanmoins parler de dissuasion informationnelle (même si elle ne remplacera pas la dissuasion nucléaire) dans le sens où l'effort à réaliser est analogue à celui qui a été déployé pour développer la dissuasion nucléaire, principalement l'effort financier et technologique.

3.4.2 La protection de l'information

Avant de développer une capacité européenne de guerre de l'information, de façon à pouvoir mener à terme des opérations offensives, les nations doivent se concentrer sur la protection de leur information. De nombreuses pistes ont déjà été développées mais n'ont probablement pas encore été exploitées de façon optimale. Les quelques recommandations reprises ci-dessous ne sont proposées qu'à titre de réflexion.

La conduite des IO passe par la protection des réseaux d'information qui demande elle-même une coordination en matière d'assurance informationnelle pour l'aspect conceptuel, un emploi optimum de la technologie d'Internet avec tous les enjeux sécuritaires ou encore la création de « *Red teams* » pour l'angle le plus offensif des opérations. Ces trois points seront développés dans ce paragraphe.

a) Assurance informationnelle (IA)[49]

Lorsque nous analysons les vulnérabilités dans le cadre de l'information, nous nous rendons compte que la négligence ou l'incompétence du personnel représente un chaînon particulièrement faible rendant l'accessibilité de l'information et des réseaux particulièrement aisée. Hormis ce manque de sensibilisation (*awareness*), le manque de sécurisation accentue la vulnérabilité. Un effort est donc indispensable dans ces domaines, si possible au niveau international.

L'informatique et les communications comme vecteurs de la communication et de l'information revêtent une grande importance dans l'épanouissement de notre société mais génèrent une dépendance totale des technologies mises en œuvre. Il faut en outre être conscient des risques associés à l'interconnexion des réseaux. Il est donc impératif de prendre un certain nombre de mesures préventives et défensives afin de garantir la sécurité des réseaux d'information et des données, basée sur les trois principes de disponibilité, d'intégrité et de confidentialité, sans oublier l'authentification nécessaire à l'identification des transmissions de données.

Comment concilier la dissémination croissante de l'information et la garantie de sa sécurisation (confidentialité, non-répudiation,…). Cette idée s'inscrit dans le cadre global de la protection des infrastructures critiques. Celle-ci passe certainement par la protection physique des infrastructures à protéger, par l'acquisition ou le déploiement de systèmes d'armes (défense anti-aérienne par exemple). Du point de vue strictement informatique cela passe également par la protection de l'information ou encore la protection des réseaux suggérée ci-dessus.

Les quelques recommandations proposées ci-dessous sont suggérées afin d'améliorer l'assurance informationnelle au niveau interdépartemental (national) ou international :

- établissement d'une capacité d'IA centralisée,
- exploitation de la connaissance en opérations des informations existantes,

[49] Information Assurance are actions taken to ptotect the State/Union, its society, its internationale allies, its economical national and international interests against the effects of attacks on, and disturbances of, information systems, info infra, info-based processes, and essential information infra and services

- création d'un pool de personnel (éventuellement de réserve), ayant une connaissance et une expérience en matière d'information opérationnelle et avec des expériences ethniques, religieuses et culturelles,
- développement d'une politique et d'une doctrine de l'information opérationnelle.

L'assurance informationnelle doit donc inclure des aspects tels la sécurité informatique, la protection des infrastructures de l'information et des opérations d'information défensives.

b) Internet – Intranet

Les futurs systèmes militaires doivent tenir compte du besoin croissant de moyens de « *data collection, information handling, smart filtering and storage capabilities* ». Ceci inclus un besoin croissant d'INTERNET et d'INTRANET, combinant des sources et moyens militaires et civils.

Il serait pertinent de développer un intranet défense offrant toutes les garanties de sécurité. Il convient à cette fin de définir les besoins opérationnels des différents organismes concernant l'organisation et le contenu de ce réseau. La connexion aux réseaux locaux représente également un problème, de même que la connexion à Internet et en particulier la gestion des adresses e-mail. Il est certain qu'une politique de sécurité globale doit être développée.

De plus, grâce à la souplesse d'utilisation offerte par les infrastructures nouvelles, les différences s'estompent désormais entre les systèmes déployés en métropole et ceux déployés sur des théâtres d'opérations. La centralisation dans le traitement des informations se fait de plus en plus importante, en limitant au maximum le stockage de données sur le théâtre au profit de la transmission de l'information.

Dans l'objectif de garantir la sécurité sur l'Internet, le Premier ministre avait déclaré à l'issue du CISI du 19 janvier 1999 :*« afin de renforcer et de coordonner la lutte contre les intrusions dans les systèmes informatiques des administrations de l'État, le Gouvernement décide la création d'une structure d'alerte et d'assistance sur l'Internet, chargée d'une mission de veille et de réponse aux attaques informatiques. »*

La France a donc crée récemment, pour l'administration, le centre de recensement et de traitement des attaques informatiques, dénommé CERT[50]/A qui est chargé d'assister les organismes de l'administration victimes d'incidents ou d'agressions informatiques. Cet organisme est placé au sein du Service central de la sécurité des systèmes d'information et participe au réseau mondial des CERT.

c) Création de «Red Teams»

Les faiblesses et les vulnérabilités d'un système informatique se situent dans les phases de spécification, d'implémentation et d'opération des systèmes et résultent de différents facteurs, volontaires ou non. Au niveau implémentation, par exemple, certains systèmes prévoient la possibilité un programmeur d'exploiter une fonction cachée.

Afin d'exploiter au mieux toutes ces vulnérabilités, la création de «*Red teams*» doit

[50] CERT : Computer Emergency Response Team

contribuer à la conduite des opérations informatiques, aussi bien en soutien des opérations défensives qu'offensives.

En quoi cela consiste-t-il ? Il s'agit en fait de collecter des informations sur les réseaux, leur structure, leur contenu, afin de pouvoir, du côté ami, contribuer à une meilleure protection des propres systèmes, et, du côté adverse, exploiter les faiblesses de façon à mener des opérations contre l'adversaire, qu'elles soient informatiques ou classiques. Notons néanmoins que la notion ami et adversaire reste résolument floue dans ce cadre, les divulgations sur le réseau « Echelon » sont là pour le confirmer. L'on pourrait définir les «*Red teams* » de « *Hackers* » à des fins constructives lorsqu'ils s'attaquent aux réseaux propres, à des destructives contre l'adversaire. Les « *Red teams* » ont donc différents domaines d'action.

Du point de vue technique tout d'abord, ils peuvent collecter des informations à propos de la structure des réseaux, des systèmes et des informations afin de détecter les faiblesses. Ils peuvent aussi exploiter une relation de confiance entre deux personnes. Une application « tactique » de ce principe s'appelle « *Spoofing* ». L'une des deux personnes ayant des intentions hostiles, il s'agit d'exploiter cette relation pour obtenir des informations. D'autres méthodes consistent à conduire des attaques « *Backdoor* », par l'exploitation de «chevaux de Troie» par exemple, ou encore à conduire des attaques passives, c'est-à-dire que l'utilisateur ne se rend pas compte de la connexion d'un « *Red team* » sur son réseau.

Du point de vue social, les «*Red teams*» ont également une tâche à remplir. Ils peuvent en effet observer physiquement le comportement des utilisateurs de manière à rentrer dans leur système. De nombreuses informations peuvent en effet être collectées par l'acquisition des mots de passe en exploitant les comportements humains.

L'avantage de la création des «Red teams» se situe dans les réformes structurelles qu'elle peut amener dans les modèles d'armée comme suggéré auparavant. Il conviendra éventuellement de revoir les priorités. Le processus d'harmonisation des capacités actuellement en cours est propice à cette révision et représente une excellente opportunité.

CONCLUSION GÉNÉRALE

L'univers est un lieu d'échanges. Il n'y a pas de vie sans communication et sans échanges d'informations entre les personnes ou entre les entités qui les représentent. Une entité n'existe que par les échanges qu'elle a avec son environnement et par les relations qu'elle établit avec d'autres. Ces échanges et ces relations sont d'ailleurs, particulièrement accélérés en période de crise. Aucune activité de la société humaine n'échappe à ce phénomène. Les forces armées, au même titre que les entreprises ou les milieux politiques, ne peuvent s'y soustraire. L'art de la guerre a, en effet, toujours été tributaire de la capacité des armées à communiquer. Les forces armées ne pourront donc pas, non plus, échapper à la révolution amenée dans le milieu de l'information par les NTIC.

Dans cette perspective, les USA ont développé le concept de *RMA*, qui illustre leur nouvelle vision de l'art de la guerre : gagner, vite et fort, sans faire couler le sang de leurs soldats, c'est-à-dire exploiter au maximum la supériorité technologique jusqu'à dissuader l'adversaire de s'engager dans des opérations militaires rendues hasardeuses. L'engagement de forces, acte ultime dans la manifestation de la volonté politique, se fait alors avec une puissance de feu maximale et un support logistique optimal, pour défaire l'adversaire rapidement et avec le souci constant du « zéro mort ». Dans ce contexte, la guerre de l'information devient un des domaines privilégiés de la guerre. Mais, comme l'a démontré il y a plusieurs siècles Sun Tsu, il s'agit avant tout d'utiliser l'information pour assurer une supériorité sur l'adversaire, afin qu'il soit défait avant même que ses premières forces aient pu être déployées ou un premier tir effectué.

Comme la Guerre du Golfe l'a démontré, plus que de la maîtrise de l'information et des tirs de précision, la révolution viendra de la capacité à exploiter les erreurs adverses par une supériorité technologique. L'information n'est donc pas seulement un médium qu'il convient de maîtriser mais elle représente le point d'entrée qui initialise tout processus de décisions et d'actions, qu'une force armée se doit de maîtriser. Il s'agit donc bien de ne pas confondre « données », qui est l'information à son plus bas niveau, avec la « connaissance » de l'information, ou plus important, avec la « compréhension » de l'information. Posséder une masse de données ne signifie pas que le décideur soit en mesure de comprendre leur signification ou de savoir quelles actions entreprendre.

Dans ce domaine, les NTIC offrent aujourd'hui un fantastique potentiel pour réaliser une véritable révolution dans les affaires militaires. Les innovations technologiques actuelles sont de nature à changer radicalement certains aspects de ces affaires militaires pour certains types de conflits. Cependant, la *RMA* n'est certainement pas la panacée pour tous les problèmes. Elle est basée sur une approche très américaine de l'art de la guerre et pourrait voir son application limitée à des situations bien définies.

De plus, une révolution ne prend pas sa place, uniquement, dans des laboratoires ou des champs de bataille, mais avant tout dans l'esprit des hommes, dans les concepts développés sur l'utilisation de la puissance militaire et dans les organisations mises en place pour son emploi opérationnel. Les NTIC ne consistent donc pas à elles seules une *RMA*. Elles doivent s'inscrire dans un processus complet d'élaboration d'une doctrine et d'une organisation nouvelles.

Mais, quelque soit le point de vue ou le niveau auquel l'on se place, le « milieu de l'information » est désormais un milieu stratégique à part entière. La fluidité des échanges, l'ubiquité des utilisateurs, l'abolition des frontières et la vitesse de circulation des idées qu'il

engendre bouleversent les usages traditionnels et s'accordent mal d'une politique refermée sur son territoire et se concentrant sur le court terme. Or, militaires, hommes politiques et législateurs ont encore besoin de poursuivre leurs réflexions sur l'art de planifier, d'organiser et de gérer les futures guerres « high-tech » et sur leurs implications dans la constitution et l'emploi des forces.

Mais, les pays européens doivent éviter de prolonger, longtemps encore, l'attentisme préjudiciable dans lequel ils semblent se trouver. Une entrée tardive dans la société de l'information représentait, il y a encore quelques années encore, un risque fort de perte de compétitivité pour les industries et les pays qui n'avaient pas su s'adapter. De manière similaire, elle représente, aujourd'hui, pour les systèmes de défense nationaux et le système de défense européen un risque majeur de perte de capacités. Les Européens ont donc, dans ce domaine, un challenge de taille à relever pour, d'une part récolter les bénéfices potentiels apportés par les NTIC, et d'autre part trouver leur propre place dans le contexte mondial et apporter leurs propres réponses aux menaces actuelles.

Ainsi, alors que l'Europe dispose de plus d'hommes en armes que les USA, il convient désormais qu'elle soit en mesure de disposer des outils de commandement et de conduite des opérations, qui lui ont fait défaut jusqu'à présent. Elle doit donc définir un **niveau de stricte suffisance en matière de maîtrise de l'information** et déterminer les fonctions jugées vitales en la matière et dont elle entend conserver le contrôle total. Tout en veillant à répondre au besoin d'interopérabilité de ses systèmes avec ceux de ses alliés, elle doit également prendre soin de déterminer avec précision le besoin opérationnel pour être en mesure de définir les orientations en matière d'équipements et d'emploi des forces. Cependant, elle doit s'astreindre à définir les modalités de maîtrise et de contrôle des fonctions vitales et préciser le degré de dégradation acceptable pour les performances de ces fonctions, afin d'assurer l'interopérabilité avec les systèmes alliés.

Dans cette perspective, trois domaines en particulier devront faire l'objet de réflexions plus approfondies :

- L'assurance informationnelle, pour fixer l'aspect conceptuel des activités civiles et militaires,
- Les réseaux Internet et Intranet, pour répondre aux enjeux majeurs de sécurité de ces réseaux de communications,
- Les « *Red Teams* », pour maîtriser les aspects offensifs liés à la guerre informationnelle.

Aujourd'hui, des éléments de réponse existent à court terme dans le programme de construction de l'Europe de la défense : la mise en place des premiers instruments de commandement pour 2001 et le développement de capacités de projection de forces pour l'horizon 2003. A plus long terme, il est impératif pour l'UE de se doter de moyens propres en matière de maîtrise de l'information, afin d'atteindre le niveau de stricte suffisance présenté supra, d'être en mesure d'affronter les nouvelles menaces et de pouvoir conduire les nouvelles formes de guerre. La maîtrise de l'information représente un défi identique à celui que relèvent actuellement les Européens pour se doter de moyens spatiaux et de renseignement communs.

Le véritable enjeu de la construction de l'Europe de la défense est là : doter le système de défense européen d'un véritable système nerveux, de vastes mémoires permettant de stocker les informations les plus diverses et d'y accéder selon les besoins, bref lui donner la capacité de voir, d'écouter, de communiquer, de décider et d'agir, en toute liberté.

ANNEXE 1 : GLOSSAIRE

CERT :	Computer Emergency Response Team
CM :	Comité militaire
COCOM :	Coordination Committee for Multilateral Export Controls
COPS :	Comité politique et de sécurité
CISI :	Comité interministériel pour la société de l'information
C2W :	Command and Control Warfare
C4ISR :	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
DCI :	Defense Capability Initiative
DIRE :	Délégation interministérielle à la réforme de l'état
GFIM :	Groupement de forces interarmées multinationales
GII :	Global Information Infrastructure
IA :	Information Assurance
IO :	Information Operations
ITSEC :	Information Technology Security Evalauation Criteria
IW :	Information Warfare
M&S :	Modélisation et simulation
NII :	National Information Infrastructure
NCSC :	National Computer Security Center
NIST :	National Institute of Standards and Technology
NSA :	National Security Agency
NTIC :	Nouvelles technologies de l'information et de la communication
OCDE :	Organisation pour la coopération et le développement économique
OTAN :	Organisation pour le traité de l'Atlantique Nord
PAMSI :	Programme d'Action Ministériel pour la Société de l'Information
PAGSI :	Programme d'Action Gouvernemental pour la Société de l'Information)
PC :	Personal Computer ou Poste de commandement
PCRD :	Programme Cadre de Recherche et Développement
PESC :	Politique étrangère et de sécurité commune
PFI :	Private Finding Initiative
PGM :	Precise Guided Munition
PPM :	Plan pluriannuel de modernisation

RMA :	Revolution in Military Affairs
R&D :	Recherche et développement
SCSSI :	Service central de la sécurité des systèmes d'information
SIC :	Système d'Information et de Communication
SSI :	Sécurité des Systèmes d'Information
UE :	Union européenne
UEO :	Union de l'Europe occidentale

ANNEXE 2 : SOURCES

- IP/99/953 : Romanio Prodi lance l'initiative eEurope (8 décembre 1999)
- Conseil Scientifique de la défense : rapport du groupe de travail présidé par M. Jacques Stern sur le thème *« maîtrise et guerre de l'information »*
- *« Penser la société de l'information »* article de Jacques Lesourne
- Compte rendu du groupe de travail (EMA/DAS/DRM/SGDN) sur la RMA du 8 février 1999 (N° 990303 /DEF/EMA/ESMG).
- *« Faut-il croire à la révolution dans les affaires militaires ?»* article de Bruno TERTRAIS dans la revue Politique Étrangère 3/98
- *« La société de l'information au XXI° siècle. Enjeux, promesses et défis »* Joël de Rosnay
- *« La politique de cryptographie : les lignes directrices et les questions actuelles »* Organisation de coopération et de développement économique (OCDE/GD(97)204
- *« Une société de l'information pour tous »* Résolution du parlement européen-Lisbonne 23 et 24 mars 2000
- *"Révolution dans les Affaires Militaires"* Rapport final du Centre de Recherches et d'Etudes Sur les Stratégies et les Technologies (N°852/CREST/LRMA du 18 décembre 1998).
- *"CORI : Conséquences Opérationnelles de la Révolution de l'Information"* Recherches & Documents du CREST - N°4 – Mai 1998
- Conseil Européen de Lisbonne : 23 et 24 mars 2000 : société de l'information : initiative eEurope
- « *La guerre au XXI° siècle »* , Laurent Murawieck, janvier 2000, éditions Odile Jacob, Paris
- *« Préparer l'entrée de la France dans la société de l'information »* discours du Premier ministre à Hourtin, le 25 août 1997
- Discours du Premier ministre à l'Université d'été de la communication à Hourtin, le 26 août 1999.
- Conférence de presse de Monsieur Lionel Jospin, Premier ministre, à l'issue du Comité interministériel pour la société de l'information le 19 janvier 1999.
- *« La guerre de l'information : quelle stratégie pour survivre au XXI° siècle »,* sous la direction du COL KUTTLEIN, EPO CID 1996.
- *« Horizon 2030, L'armement », (revue de la DGA), ,* mars 2000.
- *« The Revolution in Military Affairs : Allied Perspectives »,* Robbin F. Laird and Holger H. Mey, Mc Nair Paper 60, avril 1999.
- *« Stratégie, information, communication »,* stratégique N° 69, 1998.

- *« La société de l'information au XXI° siècle, enjeux, promesses et défis »*, Joël de Rosnay, RAMSES 2000.
- *« Joint Vision 2010 »*, site Internet du Chairman of the Joint Chiefs of Staffs
- *« Concept for Future Joint Operations (expanding Joint Vision 2010) »*, mai 1997, site Internet du Chairman of the Joint Chiefs of Staffs.
- *« America's Information Edge »*, Joseph S. Nye and William A. Owens, Foreign Affairs, mars/avril 1996.
- *« Guerre et contre guerre »*, Alvin et Heidi Toffler, édition française : Fayard, 1994
- *« Penser la société de l'information »*, Jacques Lesourne, COMMENTAIRE N°77 (1997)
- *« The RMA – Panacea or myth », Wing Commander David Caddick, AIR POWER REVIEW.*
- *« Netherlands annual review of military studies 1999- Information operations », J.M.J. Bosch, H.A.M. Luiijf, A.R. Mollema, Koninklijke Militaire Akademie.*
- *« Mind the gap », David C. Gompert, Richard L . Kugler, Martin C. libicki, National Defense University Press 1999.*
- *« Une révolution dans les affaires militaires ? », sous la direction d' Yves Boyer, Les cahiers de la fondation pour les études de défense, Cahier n° 13.*
- *« Defense Information Superiority and information assurance- Entering the XXI century. », Discours du Lieutenant General John L. Woodward, USAf director for C4 systems, devant le « House committe on Armed Forces », Février 1999.*
- *« Defense Information Superiority and information assurance- Entering the XXI century. », Discours du Vice Amiral Robert J. Natter, Director space, Information warfare, C2 CNO, devant le « House committe on Armed Forces », Février 1999.*
- *« Defense Information Superiority and information assurance- Entering the XXI century. », Discours de Arthur L. Money, senior civilian official of the assistant secretary of defense for C3I, devant le «House committe on Armed Forces », Février 1999.*
- « L'avenir de la défense européenne », Paul'Ivan de Saint germain, Le Figaro, 9 décembre 99.

ANNEXE 3 : ENTRETIENS

NOMS	FONCTION	Date de l'entretien
Général **ASCENCIO**	Secrétariat permanent du directoire des SIC	Mercredi 05 janvier 2000
Contre-amiral **D'ARBONNEAU**	EMA / ESMG	Mardi 21 décembre 1999
CV **ROLLIN**	EMA/OCO/C3R/COM	Vendredi 14 janvier 2000
Général **CHAMINADAS**	EMA / TSIC	Mardi 11 janvier.2000
IGA **NAVILLE**	DGA / SYST.FORCES	Mardi 04 janvier.2000
M. **PASCO**	FRS / Chargé de recherche	Lundi 17 janvier 2000
M. **LEVIEUX**	THOMSON CSF	Jeudi 16 mars 2000
Général **PETKOVSEK**	SGI (SILICON GRAPHICS)	Jeudi 16 mars 2000