FICHE DE PRESENTATION

1- " **Information et Défense**"

2- Chef de Bataillon (Armée de Terre) HENRY Hervé (france)

3- 5 mars 1999.

4- Division D

5- Mémoire de stratégie.

6- Résumé :

L'aube du XXI^{ème} siècle est marquée par la combinaison des bouleversements survenus dans notre environnement géostratégique et des avancées technologiques qui pourraient bien changer une fois encore l'aspect même de la guerre.

L'évolution de l'information est considérée comme le fait majeur de cette fin de siècle et la suprématie du XXI^{ième} siècle sera détenue par ceux qui maîtriseront l'information et les médias.

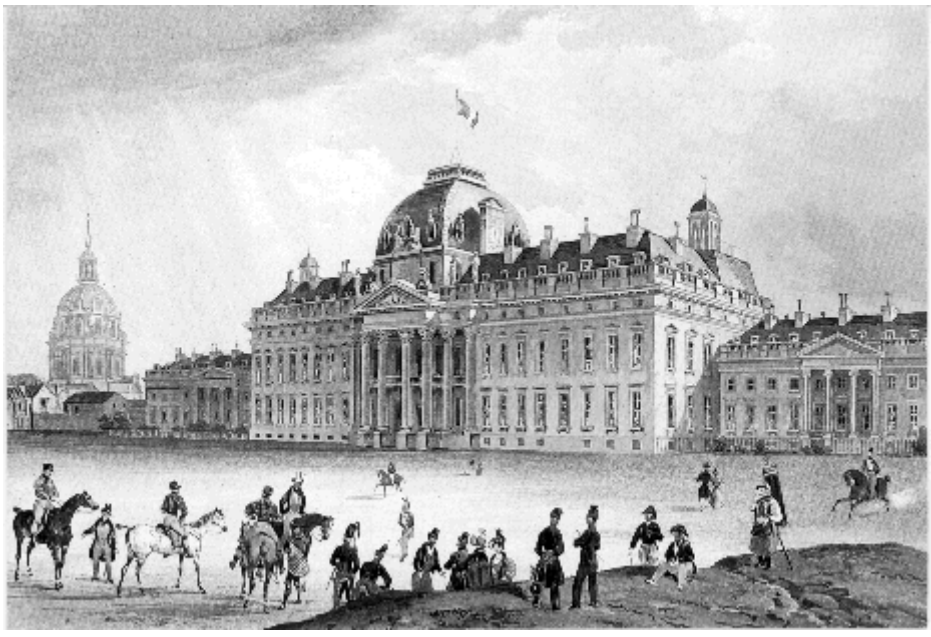
Prélude à de nouvelles formes de guerre où l'objectif stratégique est désormais la paralysie ou la destruction des systèmes adverses de contrôle et de commandement, l'apparition des nouvelles technologies,

et plus particulièrement d'un langage commun : le numérique, nous conduit vers une refonte totale du mode de pensée stratégique.

7- Mots clés : Nouvelles technologies d'information et de communications, guerre de l'information, piratage informatique, intelligence des situations, cryptologie

MEMOIRE DE STRATEGIE

Information et Défense



Chef de Bataillon H. HENRY

"Le savoir est désormais la ressource centrale de la destructivité, de même qu'il est la ressource centrale de la productivité".

Alvin et Heidi Toffler, Guerre et contre-guerre

2.2. Menaces pour l'entreprise

2.2.1. L'espionnage économique

2.2.2. La sécurité des échanges électroniques n'est pas parfaitement assurée

2.2.3. Interception d'informations sensibles et faiblesse de la cryptologie

2.2.4. Les actions criminelles

2.3. Menaces pour l'État

2.3.1. Uniformisation des valeurs diffusées par les médias et appauvrissement des diversités culturelles

2.3.2. Menées mafieuses ou déviantes

2.3.3. Interception des rayonnements électromagnétiques

2.3.4. Agression par un État étranger ou par un groupe de pression

3. guerre de l'information

3.1. Définition.

3.2. La guerre de l'information : un concept stratégique ancien

3.3. intérêt stratégique de la guerre de l'information

3.4. Les formes de guerre de l'information

3.4.1. La guerre pour l'information.

3.4.2. La guerre contre l'information

3.4.3. La guerre par l'information.

4. Conséquences stratégiques

4.1. La double incidence des bouleversements géostratégiques et des sauts technologiques:

4.1.1. Les conséquences de l'effondrement du bloc soviétique : les impératifs de réactivité et de maîtrise de l'information;

4.1.2. De la sphère commercial au monde militaire, les conséquences de l'application massive des nouvelles technologies d'information et de communication :

4.2. Les conséquences logiques de l'intégration des systèmes

4.2.1. De l'intelligence des systèmes à l'intelligence des situations :

4.2.2. La fusion des niveaux stratégiques, tactiques et opérationnels

4.3. Ajustements fondamentaux en matière d'organisation militaire et de doctrine: Les mutations organisationnelles

Introduction

En 1991, Bill Gates alerte les ministères français sur le raz de marée technologique que personne ne pourra endiguer et auquel il faut s'intéresser au plus vite. Il parle de l'enjeu déjà presque atteint du prochain millénaire : " *une planète où chacun aura accès à l'information en temps réel, ou tous les habitants pourront s'interpeller au travers du son, de l'image, du laser, des données sensitives...* ".

En 1995, le réseau gigantesque d'Internet étend sa toile d'araignée sur le monde à la vitesse d'un nouvel utilisateur toutes les deux secondes. Il relie déjà plus de 100 pays, avec le plus formidable taux de croissance jamais observé qui relie 32 millions d'individus pouvant s'échanger des milliers d'informations en un temps record. En France, la vente d'ordinateurs de type P.C. est supérieure en nombre à celle des véhicules automobiles.

En 1997 on constate que la puissance des ordinateurs double en moins d'un an. Les lasers infrarouges, les " puces " toujours plus performantes, rendent miraculeuse la précision du son et de l'image grâce à la supériorité de la technologie numérique.

En 1999, deux sociétés américaines s'apprêtent à lancer une flotte de 910 micro - satellites qui balaieront 95% du globe selon des dizaines de routes orbitales passant par les pôles. Elles ont pour objectif la transmission des millions de données de tous les habitants de la planète au moyen de petits récepteurs portables personnels du type téléphones cellulaires.

En 2000, on estime que le nombre d'utilisateurs du réseau Internet dépassera les 200 millions et que près de 200 000 réseaux seront déployés à travers le monde dont 50% aux USA, 25% pour la CEE et 2% en France.

Ainsi depuis 1991, l'homme crée pour l'homme un nouveau monde qui dilue les cultures et abolit les frontières entre les différents types de données, les différents types de domaines scientifiques et techniques. Des milliers de services sont disponibles par un simple " clic de souris ". Le monde bougera plus dans les dix ans à venir que ce qu'il l'a fait pendant les cent cinquante dernières années. Tout est désormais inéluctablement lié à tout.

Emportée par le flot de cette nouvelle révolution technologique, la nature de l'information évolue vers celle d'un produit de consommation. Elle devient un vecteur de richesse susceptible d'apporter une valeur ajoutée aux entreprises médiatiques qui la produisent et l'exploitent comme une marchandise.

Mais simultanément à ce bouleversement brutal, on remarque que la maîtrise des conséquences induites n'est pas assurée. Il s'agit en premier lieu des actions que pourrait entreprendre un ennemi ou un groupe animé d'intentions belliqueuses en vue d'annihiler nos capacités dans ce domaine ; mais aussi de celles propices à l'émergence d'effets négatifs comme les usages frauduleux.

L'information ne paraît pouvoir s'épanouir ni dans un carcan contraignant ni dans un système totalement ouvert sans règle de conduite. Quelle soit bonne ou mauvaise, elle est accessible par tous sans que nul ne puisse intervenir dès l'instant où elle est diffusée.

Parallèlement à cette évolution, l'aube du XXI^{ème} siècle est marquée par la combinaison des bouleversements survenus dans notre environnement géostratégique et des avancées technologiques qui pourraient bien changer une fois encore l'aspect même de la guerre.

A l'opposition symétrique opposant forces de l'Axe et forces alliées, puis l'OTAN et le Pacte de Varsovie durant la guerre froide, se substitue une opposition asymétrique entre un quasi-monopole militaire à l'échelle planétaire et une multitudes de menaces et de crises régionales susceptibles de dériver en guerre mondiale non programmée.

La première catégorie de dangers asymétriques regroupe l'ensemble des nations idéologiquement opposées à l'Occident susceptibles de recourir à des armes nucléaires, chimiques ou biologiques. Elle inclut également les zones de crises régionales susceptibles d'affecter les intérêts stratégiques du bloc occidental, comme le Proche Orient et le bassin méditerranéen.

La seconde catégorie est relative aux perspectives émergentes d'une nouvelle race de terroristes susceptibles d'affaiblir ou de détruire les réseaux de communication soudant l'infrastructure civile et militaire, ainsi que la logistique et les systèmes de contrôle et de commandement militaires.

Elles sont le prélude à de nouvelles formes de guerre où l'objectif stratégique est désormais la paralysie ou la destruction des systèmes adverses de contrôle et de commandement.

Aujourd'hui la Défense est globale et la stratégie a largement débordé le cadre du strict emploi des forces armées. La maîtrise de l'information est appelée à jouer un rôle stratégique de plus en plus important. Elle est devenue impérative pour la survie des nations comme elle l'était déjà pour celle des entreprises. Il faut aujourd'hui, selon l'aphorisme d'Auguste Comte, " *savoir pour prévoir afin d'agir* ".

A partir du constat sur la situation globale des médias et des systèmes de télécommunications actuels, de leur particularités techniques et de l'évolution attendue, nous étudieront les menaces qui résultent de cette révolution des Nouvelles Technologies d'Information et de Communication (NTIC). Enfin, après avoir souligné la nécessité d'une réflexion stratégique pour la guerre de l'information, nous en déduirons les principales conséquences.

1. Les nouvelles technologies et la circulation de l'information

Les *mass media* (affiches, presse, cinéma, radio, télévision...), qui sont les instruments de ce que l'on nomme " la communication de masse ", sont devenus partie intégrante de la vie quotidienne. Ils sont même la troisième occupation de l'individu après le travail et le sommeil. La " massification ", réalisée par ces médias, est l'agrégation artificielle d'individus de diverses origines sociales, de divers sexes et âges, de divers genres et niveaux de vie, de diverses professions, de divers lieux d'habitation, de diverses cultures..., qui sont exposés à la même communication (sociale, politique, publicitaire ou autre,...).

La communication de masse est publique, faite pour être consommée en un temps relativement court. Elle est axée sur l'actualité immédiate et vise la rapidité de la transmission. L'opinion publique est devenue l'enjeu de la médiatisation, c'est la course à l'audimat !

L'information véhiculée par les différents médias est caractérisée par son instantanéité et surtout par sa couverture mondiale.

Face à cette évolution qui paraît irréversible, on constate cependant deux phénomènes qui pourraient remettre en cause certaines situations établies :

D'une part, la montée en puissance de l'individu consommateur qui imposera de plus en plus son choix devant l'abondance offerte par le système.

D'autre part, une profonde remise en cause de la place et du rôle respectif des différents acteurs de la communication :

- Fin des monopoles d'exploitation d'État ;
- Ouverture des services de télécommunication à la concurrence ;
- Convergence entre les secteurs initialement séparés de la téléphonie, de l'audiovisuel et de l'informatique.

1.1 L'évolution des technologies de communication

1.1.1. La révolution technologique

Les quatre dernières décennies ont été marquées par une accélération technique jamais constatée jusque là.

Les progrès de la micro-électronique ont multiplié par 1000, tous les quinze ans, les performances de calcul ou de vitesse des microprocesseurs. Si les premiers circuits intégrés comprenaient moins de 300 transistors, le Pentium II d'Intel en possède 5 500 000.

La généralisation progressive des techniques de codage numérique sur l'ensemble de la chaîne de communication, du studio de production jusqu'au réseau de transmission améliore la performance des systèmes. En autorisant la compression des données, elle permet la réduction d'un facteur de dix à cent des quantités d'informations à transmettre tout en augmentant d'autant le débit.

L'explosion des performances des micro-ordinateurs est exponentielle comme le montre le tableau suivant pour les matériels de type P.C. :

Année	Processeur	Type	Cadence	Mémoire vive	Ecran	Mémoire de masse
1981	Intel 8088	8 bits	4,77 MHz	16 Koctets	Monochrome	Disquette 5 pouces de 160 Koctets
1984	Intel 80286	16 bits	10 MHz	512 Koctets	16 couleurs	Disque dur de 100 Moctets Disquette de 1,44 Moctets
1997	Intel Pentium II et MMX	32bits interne 64bits externe	300 MHz	64 Moctets	16 millions de couleurs	Disque dur de 6 Goctets CD Rom de 600 Moctets Disquette de 3,5 pouces de 1 à 100 Moctets
2000	Intel Merced	64bits	600Mhz	128 Moctets	16 millions de couleurs	

L'apparition des fibres optiques autorise des vitesses de transmission de l'ordre de plusieurs millions de bits par seconde. Elles permettent de transporter des signaux numériques convertis en train d'impulsions lumineuses émises par un rayon laser réduisant de ce fait les affaiblissements et les perturbations extérieures.

1.1.2. Les réseaux de communication

Dans le domaine des communications et de l'informatique, le terme de réseau recouvre des notions très différentes selon qu'on parle de supports, de structures ou de services.

-

- On distingue plusieurs types de réseaux supports :

Les réseaux hertziens terrestres. Des relais implantés sur des points élevés du terrain réémettent dans une zone déterminée les programmes de radio et de télévision qui leur sont transmis depuis les sites de production. Il n'y a pas de liaison physique entre l'émetteur et les récepteurs.

Les réseaux filaires. Ils nécessitent une liaison physique entre deux correspondants. Ils peuvent être constitués selon les cas : de câble coaxial, de fibre optique ou d'une simple paire de fils de cuivre.

Les deux types de réseaux satellitaires.

Tout d'abord, les réseaux à base de satellites géostationnaires (36000 km d'altitude). L'avantage principal de ce type de satellite réside dans leur apparente immobilité par rapport à la Terre. Ils assurent ainsi une couverture permanente sur une très large zone (un tiers de la surface du globe). Les inconvénients majeurs inhérents à ce positionnement à très haute altitude sont en premier lieu les coûts de lancement, la nécessité compte tenu des affaiblissements en espace libre d'utiliser des antennes à grand gain (le gain d'une antenne est directement proportionnel à sa surface) et d'émettre avec des puissances importantes. Enfin, le dernier inconvénient notable concerne la durée du temps de transit (environ 250 milisecondes pour le transit Terre - satellite - Terre).

Le deuxième type de réseau satellitaire met en oeuvre des systèmes plus légers sur des orbites basses (LEO) entre 700 et 2400 km d'altitude ou des orbites moyennes (MEO) entre 10 000 et 21 000 km d'altitude. L'intérêt des orbites moyennes réside dans un temps de réponse rapide (de 60 à 140 milisecondes) et dans le nombre relativement restreint de satellites nécessaires pour couvrir la planète. Les orbites basses permettent bien sur des temps de réponse encore plus faibles (de 5 à 16 milisecondes) et ne demandent qu'une puissance d'émission faible. Elles présentent toutefois le désavantage majeur de nécessiter beaucoup plus de satellites pour quadriller la Terre.

Le développement des télécommunications spatiales, par des capitaux privés est un phénomène nouveau qui vient bouleverser un ordre établi dans lequel seules les grosses organisations internationales comme INTELSAT (la plus ancienne), INMARSAT ou EUTELSAT avaient le monopole de l'exploitation de l'espace.

Aujourd'hui, le développement des services offerts par les télécommunications spatiales (bouquet numérique pour la télévision, téléphonie mobile,...) attire de nombreux nouveaux acteurs européens et américains parmi lesquels on peut citer :

	CELESTRI	GLOBALSTAR	ICO	IRIDIUM	SKYBRIDGE	TELEDESIC
OPERATEURS	Motorola	Loral, Qualcom Alcatel, etc	Immarsat, Hughes Space Telecom	Motorola Raytheon	Alcatel, Loral	Bill Gates, Craig MC Caw Boeing
APPLICATIONS	Voix, données numériques vidéoconférence	Voix, données numériques, fax	Voix, messagerie	Voix,données Messagerie numériques, fax	Voix, données numériques, vidéo conférence	Voix, données numériques, vidéo conférence
NOMBRE DE SATELLITES	63 en orbite basse + 9 en géostationnaire	56 en orbite basse	12 en orbite moyenne	66 en orbite basse	64 en orbite basse	288 en orbite basse
ORBITE	1407 et 36000 km	1422 km	10392 km	777 km	1466 km	700km
COUT en milliards de francs	78	12	15,6	22,2	21	54

Ces futurs systèmes de communication permettront prochainement des transformations considérables en assurant la couverture de la planète pour un coût d'accès indépendant des densités de peuplement.

Six projets majeurs sont aujourd'hui concernés, il s'agit de :

- Télémédecine
- Enseignement à distance
- Vidéoconférence
- Télétravail
- Téléphone portable
- Messagerie

<u>- En terme de structures de réseau, on peut trouver :</u>

Les réseaux locaux d'entreprise comme le LAN (Local Area Network). Ils permettent au sein d'un bâtiment ou d'un petite collectivité l'échange d'informations à des vitesses allant jusqu'à 100 Mbits/sec avec un très faible taux d'erreurs mais uniquement sur de faibles distances.

Les réseaux à grande distance du type WAN (Wide Area Network) qui couvrent un pays ou un groupe de pays. D'un débit faible (2 Mbits/s) jusqu'à ces dernières

années, les WAN ont fait l'objet d'investissements majeurs de la part des opérateurs et fonctionnent actuellement à de très hauts débits (technologie ATM sur support fibre optique de 155 à 622 Mbits/s)

- Au niveau des services on peut citer par exemple :

Le réseau téléphonique commuté (RTC) ;

Les réseaux mobiles (normes GSM ou DCS 1800) ;

Les réseaux à commutation de paquet (Transpac) ;

Les réseaux numériques à intégration de service (RNIS) ;

Les réseaux militaires tactiques de zone (type RITA français , Autoko allemand, ...) ;

Les réseaux de satellites (Inmarsat, GPS, ...) ;

Les réseaux informatiques spécialisés (Télétel, Réseau des universités, réseaux militaires,...).

Pour que ces différents réseaux puissent communiquer entre eux, il a donc fallu passer des accords bilatéraux entre les responsables de chacun d'entre eux (entreprises, universités, États), établir des passerelles physiques (commutateurs, routeurs, noeuds de communication) et définir des protocoles techniques (modèle d'interconnexion de systèmes OSI, X25 pour la commutation de paquets, X400 pour la messagerie, TCP/IP pour l'informatique...).

1.2. Situation actuelle des moyens d'information : conséquences sur les comportements

La révolution numérique est en train de donner naissance à de nombreux types d'équipements qui associent la qualité des images de la télévision, la force communicative du téléphone, la sélectivité et la maniabilité des journaux. Ces qualités sont déployées dans les formes et les lieux les plus divers : des téléphones cellulaires avec courrier électronique au terminal de réseau, du vidéotext au papier électronique en passant par le porte-monnaie électronique, de la reconnaissance vocale à l'audiotext. En fait, une informatique omniprésente qui nous bouscule sans cesse.

1.2.1. La presse écrite

Les années 80 marquent l'explosion de la presse dans nos sociétés occidentales. C'est le triomphe du marketing et l'explosion des journaux et revues " ciblées " (2917 titres en 1994).

Les progrès de l'informatique, la diffusion des terminaux télématiques dans le grand public (Minitel, télécopie) et le développement des réseaux de télécommunications ouvrent la voie de la presse électronique ; " Les ailettes de Mercure sont aujourd'hui dotées de turbos " Albert Du Roy.

La presse écrite est en mutation. Elle se réorganise par concentration des titres.

Ainsi si la presse d'opinion est en baisse, la presse d'information est dynamisée, confirmant le peu d'intérêt porté par les français aux problèmes de fond.

Certains titres de la presse parisienne, de la presse quotidienne régionale et hebdomadaire généraliste connaissent des difficultés économiques, en raison de l'ancienneté de leurs structures de fabrication, du traditionalisme de leur conception, du poids trop lourd de leur système de distribution et de la diminution des recettes publicitaires récupérées par la télévision.

Une nécessaire modernisation s'impose donc à ce secteur qui reste le principal producteur d'information.

1.2.2. La téléphonie mobile

Durant des années, le radiotéléphone n'a été un gadget de luxe. Si l'appareil était mobile, voire portable, il était exclu de le glisser dans sa poche. Utilisant des techniques analogiques et n'assurant seulement que la couverture des grandes métropoles, sa diffusion n'a concerné que quelques dizaines de milliers d'abonnés en France.

La réduction des coûts (divisés par dix en cinq ans à peine), l'utilisation de la norme GSM (Global System for Mobile Communication); la suppression des monopoles et l'apparition d'une concurrence européenne ont transformé le radiotéléphone en outil de travail permettant de joindre le monde entier. Son avenir s'annonce encore plus brillant. On retiendra qu'il a constitué le cadeau phare de Noël 97 avec 850 000 exemplaires vendus pour un parc national de 5,8 millions d'unités.

Le radiotéléphone sonne-t-il le glas du téléphone à fil ? Déjà, à certaines heures, une communication Paris - province coûte moins cher par l'intermédiaire du GSM que sur le réseau traditionnel. De plus, la déréglementation, en 1998, du secteur des télécommunications en faisant jouer la concurrence a dynamisé ce secteur.

Cette vulgarisation de la téléphonie mobile modifie les comportements des usagers. Il est maintenant communément admis de disposer en permanence et en tout endroit de moyens de télécommunication. L'homme devient même, dans certain cas, esclave

de son téléphone. Il suffit d'observer le comportement de certains, dans les lieux publics, pour se convaincre de cette évolution des comportements.

1.2.3. La radio diffusion

La couverture globale offerte par le satellite intéresse de plus en plus les opérateurs de radio ou de télédiffusion. Cette couverture mondiale de qualité est en effet inaccessible aux moyens classiques terrestres de diffusion du fait de la nécessité de multiplier les réémetteurs, ce qui entraîne des problèmes d'implantation, de maintenance (en particulier dans les pays du tiers - monde) et de sécurité de fonctionnement (brouillage, contrôle des stations ...).

Si la diffusion d'images ne s'adresse dans un premier temps qu'à des pays dotés de revenus importants (coût des installations de réception), la radiodiffusion en revanche est exploitable à destination des pays du tiers - monde. Plusieurs projets sont en cours de réalisation ou d'étude comme les projets Worldspace et SATIVOD [voir annexe].

Le projet Worldspace notamment, dont le lancement est suivi très attentivement par la communauté internationale des radiodiffuseurs, devrait cohabiter et, à terme, remplacer les systèmes existants d'émission par ondes courtes en raison de son coût compétitif, de sa couverture mondiale et de la qualité du son diffusé. Il faut noter que dans ce type de diffusion il est quasiment impossible de brouiller les émissions et virtuellement impossible de contrôler les stations d'émission ou de réémission. De plus la réception du son ne dépend plus des caprices de la propagation et l'on peut être assuré d'une couverture de qualité sans faille. Dans le cadre d'une information bien " canalisée ", ce type de diffusion prend une dimension indéniable.

Un formidable outil de communication est ainsi mis à la disposition de tous, avec ses avantages et inconvénients. Ce genre de système associé à des possibilités de cryptage (dans les pays où cela est possible : USA en particulier) équivaut à la mise en place à bon compte d'un réseau de commandement fiable, rapide et difficile à contrôler ou à mettre en défaut. Il est évident, là aussi, que le caractère de facilité offert à tous peut profiter à des entreprises dont les buts, lucratifs ou non, peuvent s'éloigner quelque peu de la morale communément admise.

1.2.4. La télévision

La diffusion des émissions de télévision analogique atteint aujourd'hui ses limites : la diffusion hertzienne ne couvre pas toutes les zones; celle par câble a des difficultés à s'imposer en particulier en France; la diffusion par micro-ondes est encore en expérimentation et celle par satellite est coûteuse et limitée en capacité et en qualité.

Il faut donc faire appel à d'autres techniques. Après l'échec de la norme D2Mac, on se tourne vers les techniques de numérisation et de compression de la radio et de la télévision ainsi que vers un concept de télévision interactive.

Il est désormais possible de diffuser avec une meilleure qualité cinq à huit fois plus de programmes sur un même transpondeur. Le nouveau concept " d'interactivité ", que les médias évoquent souvent, à propos du numérique ou des autoroutes de l'information représente l'évolution majeure de ces dernières années. Il permettra aux usagers de dialoguer avec le diffuseur, lui permettant ainsi d'agir sur le contenu de l'information émise. Au total, les possibilités d'échanges seront alors multipliées et par voie de conséquence les coûts réduits pour l'usager. Les intérêts commerciaux engagés sont colossaux et les changements qui vont intervenir dans l'audiovisuel mondial durant les années qui viennent vont bouleverser toutes les habitudes des téléspectateurs.

Le passage au numérique est donc un phénomène planétaire dont les conséquences vont inéluctablement modifier en profondeur notre consommation et notre environnement culturel : nombre de chaînes, contenu des programmes, exception culturelle et communautés diverses...

Aujourd'hui, le développement de la télévision a transféré sur l'image la crédibilité accordée naguère à l'écrit. On ne dit plus " j'ai lu dans le journal ", mais " j'ai vu à la télévision ". L'image est devenue une accréditation sans faille de la réalité car elle bénéficie d'une forte note de crédibilité. C'est l'image qui crée l'information, elle est " l'imprimerie de la vie ". L'individu regarde l'événement comme un fait tourné vers lui alors qu'il est destiné au plus grand nombre. En 30 ans, l'image est devenue le média le plus accessible car il ne demande qu'une attention passive. L'individu recherche la facilité et évite la réflexion. Cela est encore plus vrai pour les couches les plus défavorisées de la société qui ne peuvent accéder à la connaissance que par l'image et le son. Mais quelle connaissance ? Celle de l'œil de la caméra qui tend à reconstruire la Société à coup d'électrons, qui manipule, qui submerge l'individu par des flots d'informations toujours plus variés qu'il n'arrive plus à trier. Cette situation régulièrement dénoncée entache son aura parce que des professionnels peu rigoureux préfèrent façonner voire créer l'information plutôt que de la véhiculer brute, ce qui pousse certains professionnels de l'image à constater : " on n'est plus informé, on se croit au spectacle en permanence ".

Paradoxalement, bien que l'audiovisuel, enjeu économique majeur de l'information, soit appelé à se développer, il peut engendrer un phénomène de désinformation de plus en plus difficile à contrôler et à combattre.

1.2.5. Internet

Alors que le schéma de distribution de l 'information est toujours plus ou moins centralisé (journaux, radio, télévision), ou limité en volume et vitesse de diffusion (courrier, téléphone), Internet est le premier média qui permet à un être humain de correspondre très vite avec un grand nombre d'individus.

L'Internet est né en 1969, à partir du réseau ARPAnet du département de la défense US. C'était un réseau expérimental destiné aux recherches militaires en particulier, capable de fonctionner pendant des attaques physiques, et, devant résister à une

destruction partielle, notamment d'origine nucléaire. Avec la création vers la fin des années 1980, par la National Science Foundation américaine (NSF), d'un réseau de cinq super ordinateurs mis à la disposition de la recherche universitaire, allait vraiment débuter la formidable aventure d'Internet qui autorisait un accès universel.

Aujourd'hui, l'interconnexion de dizaines de réseaux différents en termes de supports, de structures ou de services couvrant plus de 130 pays et raccordant plusieurs millions d'ordinateurs constitue un réseau mondial qui utilise le protocole TCP/IP pour ses relations. Cet ensemble a reçu par simplification le nom d'Internet.

Il n'existe pas d'autorité unique régnant sur l'Internet dans sa globalité. La seule autorité reconnue est celle de l'Internet Society ou ISOC. L'ISOC est une organisation de volontaires (Gouvernements, associations et particuliers y sont représentés) œuvrant pour la promotion des transferts d'informations via les technologies Internet. Il entretient un conseil des sages, appelé Internet Architecture Board (IAB), qui a la responsabilité de la gestion technique et de la direction de l'Internet. Les utilisateurs expriment leur opinion au travers d'Internet Engineering Task Force (IETF), autre organisation bénévole chargée des problèmes techniques opérationnels du réseau. Chaque réseau possède son propre central opérationnel (NOC pour Net Operational Central) pour résoudre les problèmes techniques de son niveau.

De même, il n'existe pas de financement centralisé pour Internet. Chaque réseau est indépendant financièrement : NSF finance NSFnet, la NASA finance le NASA Science Internet, et les universités ou les sociétés privées paient pour leurs connexions au réseau régional qui lui, paie un fournisseur national pour son accès.

Internet offre une gamme très étendue de services dont le plus connu est le World Wide Web (WWW) ou plus simplement le Web (toile d'araignée). Surfer sur l'Internet, c'est surtout surfer sur le Web, la partie multimédia de l'Internet. Parmi les autres services, citons : les forums thématiques de discussion, le transfert de fichiers, la messagerie électronique, etc. L'ensemble constitue un " village global "

Le prodigieux essor de l'Internet affecte en premier lieu le monde commercial, où il constitue un avantage compétitif de premier ordre pour l'entreprise. Rationalisation de la production, supervision des automates, veille technologique et commerciale, systèmes experts, secrets de fabriques, fichiers clients etc. Le savoir est l'actif stratégique le plus convoité de notre ère industrielle, son support est désormais électronique, et la globalisation de ses vecteurs de circulation engendre, de fait, de nouvelles opportunités et de nouvelles menaces.

L'évolution en termes de machines connectées est réellement exponentielle. A travers le monde, il y a un nouvel abonné toutes les deux secondes, avec un taux de croissance de 10 à 15% par mois ce qui conduit le WEB à doubler actuellement tous les 3 mois. A la fin du premier semestre 1995, il y avait 6 millions et demi de machines raccordées, soit plus de 40 millions d'utilisateurs. Bien que l'évaluation devienne de plus en plus difficile à établir car de très nombreux sites sont protégés

par des murs coupe - feux (firewall), on estime qu'un milliard de personnes devraient avoir une adresse électronique d'ici la fin de la décennie.

Ainsi toutes les prévisions, même les plus optimistes ont été dépassées. Le développement d'Internet connaît aujourd'hui autant de succès que celui du téléphone portable. On constate le plus formidable taux de croissance jamais observé. Pour atteindre 50 millions d'utilisateurs il a fallu 38 ans à la radio, 13 à la télévision, 10 au câble et 5 seulement à Internet.

Et malgré l'explosion inimaginable tout s'est bien passé, car l'adhésion des consommateurs est au rendez-vous, en dépit de l'image quelque peu terrifiante que les médias ont véhiculé malgré eux vers le grand public.

En fait les réseaux cybernétiques constituent une banque d'informations mondiales qui représente l'équivalent de 100 millions de pages sur un nombre gigantesque de sujets distincts. Contrairement à la radio ou à l'audiovisuel, ils demandent à l'individu de produire un effort beaucoup plus important pour accéder à une information particularisée. Actuellement ils engendrent les plus grands bouleversements socio-économiques de la planète. Par leur apparition soudaine pour le grand public et les effets produits on peut parler de révolution du 20ème siècle. La stratégie de développement et le succès commercial sont aujourd'hui dictés par l'individu consommateur qui fait son choix de produits et rejette les technologies qui ne l'intéresse pas.

1.2.6. Principales conséquences de cette modification du monde de l'information

En ce qui concerne l'ensemble des médias, on peut dire qu'aujourd'hui on évolue d'un schéma plus ou moins centralisé de diffusion de l'information où la gestion du flux est assurée par une autorité responsable identifiée, à un autre complètement déréglementé sans responsabilité clairement affichée. Ainsi deux mondes différents cohabitent et se séparent peu à peu. D'un côté la presse écrite, la radio et la télévision, de l'autre un système immatériel véhiculé par le réseau dans lequel il n'y a plus de hiérarchie, plus de réglementation.

Ce dernier constat conduit certains experts à présager que des déviations de plus en plus graves vont se produire, car l'individu peut maintenant contacter des millions de personnes sur la planète et s'attribuer un pouvoir qui va peser sur la société.

En même temps un fossé important se creuse parce que le système évolue trop rapidement. Non seulement la population des illettrés et analphabètes ne pourra jamais accéder à ces technologies, mais aussi de nouvelles catégories vont être écartées en particulier celle des personnes âgées dépassées par la technique et celle plus jeune d'un niveau intellectuel modeste. Toutes ces couches de la société seront exclues même si un effort d'éducation important est réalisé et même si des moyens sont mis en place pour leur permettre d'acquérir ces équipements à bas prix.

Par ailleurs, l'écart déjà considérable entre les pays du Nord et ceux du Sud va continuer de s'accentuer.

Par rapport à ce mouvement dont la dynamique paraît irréversible, il est souhaitable de ne pas aller trop loin, trop vite, afin de ne pas tendre vers une uniformisation de la société. Sans être innocentes ces évolutions touchent aux problèmes fondamentaux de la société en particulier ceux relatifs à la mutation des modes de communication. Ainsi faut-il conserver des instruments d'observation et de contrôle.

2. Risques et menaces à moyen terme

Les Nouvelles Technologies d'Information et de Communication (NTIC) favorisent l'émergence de nouveaux risques et de nouvelles menaces.

En termes de risques, le déséquilibre économique Nord - Sud pourrait s'aggraver d'un déséquilibre, en matière d'information et de communication, renforçant une logique revendicative de nature à devenir agressive.

En termes de menaces, les NTIC offrent aux États, groupes de pression ou d'intérêt politique, religieux ou économique, une arme accompagnant efficacement des opérations militaires, terroristes ou mafieuses, soit à travers la transmission rapide de données secrètes, soit grâce à la diffusion d'informations tendancieuses destinées à influencer les opinions publiques ou les élites d'un pays ou d'une zone géographique, soit enfin grâce à la captation, puis au détournement du capital technologique ou culturel d'un pays. L'information, objet de toutes les convoitises et de toutes les stratégies est une cible privilégiée. Car celui qui la possède, détient le pouvoir

2.1. Menaces pour l'individu

Que ce soit sur le Web ou sur les réseaux satellites de télévision, l'information est-elle objective?

La vie en direct de situations tendues relatées par des journalistes au cœur même de l'événement n'est-elle pas de nature à le susciter, voire à le provoquer ? Créer en quelque sorte le scoop face à la demande pour satisfaire la course à l'audimat ? Si la plupart des organismes ou des grandes entreprises prennent la précaution de signer l'information sous peine de perdre leur crédibilité, la méfiance doit être extrême quand il s'agit d'informations non " sourcées ", car le risque de trucage est tentant. Rappelons nous que certains ténors du journal télévisé nous ont présenté un montage de fausses situations à des heures de grande écoute. Le phénomène de désinformation est toujours d'actualité et doit être rappelé à chaque occasion; car il conditionne l'avenir même des médias.

On citera aussi les dangers potentiels introduits par la technologie numérique capable de modifier sans traces tout texte, image ou son numérisé, ou encore l'impact des messages subliminaux adroitement placés dans certains messages publicitaires pour mieux nous conditionner.

La part croissante de la publicité, l'affaiblissement du message médiatique se traduisent par un nivellement des cultures et l'abrutissement du consommateur.

L'impact de ces menaces sur l'individu est renforcé par le caractère fugitif de l'information qui empêche toute réflexion approfondie. La vitesse de circulation de l'information et la concentration entraînent une " déculturation ". Une information chasse l'autre, immédiatement oubliée elle ne suscite plus la réflexion.

2.2. Menaces pour l'entreprise

L'absence de culture de protection du patrimoine de l'entreprise est l'une des causes de perte de marchés, en particulier pour nos PME et PMI. Le peu d'efforts de formation consentis tant au niveau scolaire pour les futurs cadres commerciaux qu'au sein des entreprises qui les emploient tend à les rendre trop " bavards " ou à offrir parfois des informations stratégiques à des concurrents formés à l'intelligence économique.

2.2.1. L'espionnage économique

Qu'il soit d'ordre scientifique ou industriel, il est en plein essor et les pertes des entreprises françaises sont considérables. Il est principalement caractérisé par des interceptions de conversations, de télécopies et de transmissions informatiques, puis par le vol de matériels ou encore par l'intrusion dans les systèmes d'information. Ces actes de malveillance informatique ont des conséquences importantes qui entraînent une perte de compétitivité.

Certains d'entre eux comme le sabotage visent la destruction des systèmes informatiques de l'entreprise. Dans ce cas le préjudice causé peut être énorme au point que 80% d'entre elles déposent le bilan dans les deux ans qui suivent. Les coupables s'appellent virus, modification de logiciels, bombes logiques,... Il est opportun de rappeler que l'utilisation de programmes personnels, de jeux notamment, sur les postes de l'entreprise représente le plus fort pourcentage de pollution par virus informatique. Les conséquences sont encore plus importantes lorsque l'entreprise est sur réseau interne type Intranet.

Dans le cas de " Piratage " d'informations, il faut savoir que 80% des cas de malveillance bénéficient d'une complicité interne à l'entreprise.

2.2.2. La sécurité des échanges électroniques n'est pas parfaitement assurée

La médiocre sécurité offerte par les NTIC aux échanges électroniques suscite et entretient les actes de " piratage " extérieurs et autres formes de détournements. Ceux-ci sont opérés en toute tranquillité dans un climat de relative impunité. La généralisation de l'utilisation de l'Internet au dépend d'autres réseaux plus fiables(TRANSPAC, TRANSFIX) accroît la vulnérabilité. Plus de 18% des messages informatiques arrivent à leur destinataire de façon incomplète ou farfelue (un message émis est découpé en paquets qui partent simultanément mais empruntent des routes différentes jusqu'au destinataire et de ce fait n'arrivent pas au même moment). Cela a pour conséquence une dégradation de plus en plus importante du courrier électronique due à l'augmentation du trafic sur Internet et au nombre infini de routes de circulation possibles.

2.2.3. Interception d'informations sensibles et faiblesse de la cryptologie

Que ce soit par Fax, Internet ou tout autre support de messagerie, la protection des informations constitue un enjeu capital dans le commerce électronique.

Le cryptage consiste à transformer des informations électroniques de manière à les rendre indéchiffrables. Les Etats-Unis qui veulent être une force motrice pour le développement du commerce électronique sur le Web ont pris l'initiative dans ce domaine. Profitant des faiblesses d'une Europe encore frileuse, ils laissent loin derrière eux tous leurs adversaires économiques en adoptant une stratégie offensive. Pourtant le FBI, la CIA et la NSA *(National Security Agency-* organisme qui recense et diffuse les logiciels de codage) s'opposent pour des questions de sécurité nationale à toute exportation de logiciels de cryptage puissants.

Malgré cela, l'avance des Etats-Unis dans ce domaine est une réalité. L'Europe n'envisage pas avant la fin du siècle de cadre législatif définitif en matière de cryptage des logiciels.

La France est en retard parce qu'elle considère historiquement que la cryptologie est affaire de militaires. Le SCSSI (*Service Central de Sécurité des Systèmes d'Information*) contrôle l'utilisation et la distribution des outils de cryptologie. Tout système de chiffrement doit être soumis à cet organisme qui, à son gré et dans des délais laissés à son appréciation, rendra sa décision sans avoir à se justifier en cas de refus. Même si les codes actuels sont de plus en plus facilement cassés, le SCSSI refuse la légalisation de chiffrements performants (clés de plus de 128 bits), car l'État veut pouvoir déchiffrer toutes les communications.

2.2.4. Les actions criminelles

Les actions contre les entreprises, conduites par la petite délinquance ou la criminalité organisée, sont nombreuses. Par contre le montant du préjudice subi est mal connu et le plus souvent sous-évalué, ces délits étant rarement signalé par des entreprises, notamment bancaires, qui n'ont pas intérêt à faire connaître à leurs clients leurs faiblesses dans le domaine de la sécurité de leurs comptes.

Parmi elles, on peut citer :

- Le chantage sur le fonctionnement des systèmes informatiques consistant à réclamer de fortes sommes pour éviter leur destruction après avoir déclenché une action mineure démontrant le savoir-faire .
- Le clonage des téléphones cellulaires et des cartes bancaires ; les éléments d'identification de l'abonné, les codes d'accès et de sécurité obtenus frauduleusement sont utilisés pour fabriquer de fausses cartes à mémoire pour le téléphone ou des pistes magnétiques de cartes bancaires .
- Les vols et détournements financiers ; le hold-up électronique rapporte beaucoup plus que le braquage d'agences bancaires (dans le rapport de 1 à 140 selon le FBI américain) alors que la probabilité d'être pris est nettement plus faible (plus de 40 fois). C'est ainsi que des informaticiens russes ont pu en deux mois au début 1996, prélever 300 millions de dollars dans des banques américaines grâce à Internet et aux codes des comptes qu'ils avaient pu trouver.
- Le dysfonctionnement des réseaux de transfert de fonds ; chaque jour des millions de dollars en monnaie électronique se perdent sur le réseau mondial interbancaire SWIFT .

2.3. Menaces pour l'État

Les médias et les Nouvelles Technologies d'Information et de Communication sont un facteur de développement économique en même temps qu'ils constituent une fatalité qui expose un pays au regard des autres pour étendre son rayonnement ou pour accroître sa vulnérabilité.

Les conséquences d'une attaque délibérée sur nos systèmes d'information peuvent être dramatiques.

Imaginons par exemple que les systèmes des entreprises de transports publics soient pénétrés, que les paramètres de guidage des trains et des métros soient modifiés, que ceux de la régulation du trafic aérien soient altérés. Que les banques nationales ou les grandes organisations financières perdent le contrôle des réseaux de transfert de fonds et des systèmes de gestion des comptes. Plus généralement que ces attaques provoquent des coupures générales de certains services essentiels utilisés au quotidien : standards téléphoniques saturés, distributeurs de billets en panne, distribution du courant électrique interrompue... La sécurité civile du pays et l'économie tout entière seraient alors sérieusement menacées.

2.3.1. Uniformisation des valeurs diffusées par les médias et appauvrissement des diversités culturelles

C'est le risque de la pensée unique. Qui détient l'information, détient le pouvoir. S'en suit assurément une lutte d'influence pour tenter d'asseoir ou de contrecarrer un pouvoir. Et là, la lutte peut aussi bien opposer les États, des groupes d'États, des cultures (American Way of Life, intégrisme islamique...) ou des entreprises.

La guerre du Golfe a été la première illustration de ce phénomène : l'information CNN, c'est à dire l'information américaine, a pratiquement monopolisé les images diffusées dans le monde. Dans cette affaire, l'opinion publique française, mais aussi certains décideurs français avaient-ils réellement un libre arbitre ? " A l'époque, ne nous sommes nous pas trompés d'ennemi ?...." s'interrogent aujourd'hui certains. Il semble en effet évident aujourd'hui que, lors de la guerre du Golfe, les américains se sont permis de tester les effets de la manipulation et de la désinformation chez leurs partenaires, en usant de divers procédés médiatiques et psychologiques pour rallier tous les publics à leur cause.

Un des secteurs actuellement menacé par ce phénomène est notre presse écrite. Le danger d'une main mise par des groupes étrangers de l'information, pouvant de ce fait mettre en cause l'indépendance et la culture du pays n'est pas à écarter.

2.3.2. Menées mafieuses ou déviantes

Pour les groupes mafieux, les révisionnistes, les bandes de trafiquants en tous genres (en particulier de chantage au virus, de blocage des systèmes, de trafics financiers ou de médicaments interdits en France,..), le Web est une aubaine d'anonymat.

Le récent démantèlement par les gendarmes de Reims d'un réseau pédophile qui fonctionnait sur Internet est une exception. Par ailleurs, et à titre d'exemple complémentaire, sur le site Yahoo, le plus fréquenté avec 14,5 millions de visiteurs par mois (chiffre septembre 97), sept des dix mots - clés les plus recherchés sont liés au " charme "; le premier portant tout simplement le nom de " Sex ". Selon le journal USA Today, la fréquentation des sites Web pour adultes est, aux Etats-Unis, en forte hausse : 10 à 20% des recherches ayant trait à la pornographie.

Côté mafia, la Sacra Corona Unita aurait pu avoir accès à des données bancaires confidentielles lui permettant d'identifier l'existence de salaires doubles afin de les racketter.

2.3.3. Interception des rayonnements électromagnétiques

Tout rayonnement électromagnétique (émissions laser, micro-ondes, ondes courtes, ondes moyennes ou grandes ondes, ...) peut être intercepté à plus ou moins grande distance (en fonction de la fréquence) à condition de disposer d'un récepteur adéquat. A partir de plusieurs récepteurs, on peut relever la direction de l'émetteur et donc, par triangulation, procéder à sa localisation.

Là où le problème se complique, c'est lorsque il faut démoduler l'onde interceptée et éventuellement la décoder pour la rendre compréhensible. Ceci est d'autant plus difficile que l'émission est dite "exotique", c'est-à-dire différente des modulations classiques comme les modulations d'amplitude, de fréquence ou temporelle. Ce type d'opération nécessite des équipements plus sophistiqués, qui dépassent les possibilités d'un individu ou même de certains États.

A titre d'exemple d'interceptions, on peut citer :

- La possibilité d'écouter les réseaux radio des services de sécurité (police, gendarmerie, pompiers,...) avec un simple scanner permettant de balayer rapidement des gammes entières de fréquence.
- La capture, sur écran vidéo, de tout caractère tapé sur un terminal informatique situé à moins d'une centaine de mètres.
- L'interception à partir de stations terrestres, d'avions ou de navires spécialisés ou de satellites de toutes les émissions hertziennes d'un pays ou d'une zone donnée ....
- L'interception et l'écoute des communications par satellites.

2.3.4. Agression par un État étranger ou par un groupe de pression

" Une large proportion des systèmes d'information des Etats-Unis est vulnérable à des attaques incluant des interruptions de services, l'introduction de fausses données, des virus informatiques, des vols d'information. Contrairement aux autres menaces pour la sécurité nationale, le " coût d'entrée " pour les agresseurs potentiels est très faible, ce qui peut permettre des attaques initiées par des pays étrangers, des pirates informatiques, des terroristes, des fanatiques, des criminels et des organisations commerciales ".

Les nouvelles technologies (satellites et Internet notamment) peuvent permettre à un pays donné, comme aux organisations mafieuses ou terroristes, de conduire contre un autre pays des agressions de toute nature en dissimulant le plus longtemps possible leurs implications. Ces actions dirigées à partir de sites sans rapport direct avec l'agresseur ; pourraient par exemple être élaborées par des 'hackers' de talent recrutés parmi les nouvelles générations d'informaticiens formés à l'Est.

Parmi ces attaques, on peut citer :

- La diffusion de fausses informations opportunes, telles que celles véhiculées sur le faux site Web sur l'Elysée .
- La propagande directe ou indirecte contre les valeurs nationales ou au profit d'une idéologie .
- La modification de dossiers et le vol de données dans le Système Informatisé Schengen (SIS).
- La vente de logiciels piégés comme dans le cas d'un logiciel US vendu à la Jordanie ayant permis à la CIA de relever les fichiers de terroristes palestiniens.
- Les actions subversives ou de terrorisme.

Même si aujourd'hui on s'accorde à penser que le risque de terrorisme informatique commandité par un Etat est peu probable, il en est tout autrement, en revanche, de celui émanant d'organisations extrémistes. Ces dernières pourraient, à moindre coût, porter une attaque significative contre notre pays. La détection par les services français, il y a quelques années, d'offensives informatiques suspectes provenant d'organisations étrangères qui se servaient de " hackers " du *chaos computer club* prouve que cette menace n'appartient plus au domaine de science fiction.

La place essentielle des systèmes d'information dans nos sociétés modernes, le rôle croissant qu'ils sont appelé à jouer dans les secteurs économiques et au sein même du fonctionnement de l'État les rendent particulièrement vulnérables aux menaces qui nous venons de le souligner sont nombreuses.

Les agissements contre ces systèmes de communications ou la manipulation des informations constituent de fait des actions agressives qui peuvent être assimilées à des actions de guerre.

Dans le domaine militaire, l'omniprésence de l'information et la nécessité d'en conserver la maîtrise dans les crises ont conduit à formaliser la notion de guerre de l'information. La Défense a de tout temps été tributaire de la connaissance de l'environnement; les mutations géopolitiques, technologiques et sociales du mode contemporain n'ont fait qu'accroître de façon considérable cette situation.

L'importance croissante des fonctions C4I (Command, Control, Communication, Computer, Intelligence) et la place prioritaire qui leur est accordée dans le livre blanc sur la Défense, ainsi que dans les lois de programmation en fournirait la preuve si c'était nécessaire.

3. guerre de l'information

La guerre de l'information pourrait être selon certains la guerre du futur, le 'cyber-espace' en étant le champ de bataille privilégié.

La conduite d'une politique, d'une entreprise ou d'une opération militaire ne peut plus se concevoir sans utilisation de systèmes de communications et d'information performants.

La réflexion sur les implications stratégique de ce nouveau concept est récente. Toutefois nous nous attacherons à montrer qu'il existe une continuité entre les grands principes décrits par les stratèges chinois et le concept doctrinal et stratégique actuel.

3.1. Définition.

La guerre de l'information couvre un domaine très large, groupant plusieurs concepts tels que la guerre électronique, la guerre psychologique, le renseignement et la guerre des hackers (hacker warfare ou hackerwar).

La prise en compte de ce domaine et l'apparition d'une réflexion sur les implications des nouvelles technologies de l'information au niveau stratégique et tactique date des années 1980.

Le livre d'Alvin TOFFLER " The third Wave " , paru en 1980, pose les bases du concept de guerre de l'information.

" *Pour attaquer une nation, on peut procéder par rétention du flux d'information - couper le contact entre le siège d'une société multinationale et ses filiales à l'étranger .., élever des barrières informatives autour d'elle... Le vocabulaire international s'est enrichi d'une expression nouvelle : "la souveraineté de l'information.* "

La réflexion américaine, ininterrompue depuis lors, est passée du concept de *Manoeuver Warfare* applicable à une guerre conventionnelle à celui de *Strategic Information Warfare (SIW)* soulignant ainsi la forte implication stratégique de la guerre de l'information considéré dès lors comme une notion globale.

Pour définir plus précisément la guerre de l'information nous emprunterons la définition de Richard POWER figurant dans un document du *Computer Security Institute :*

" *La guerre de l'information consiste en des actions prises pour parvenir à la supériorité informationnelle dans le cadre de la stratégie militaire nationale ; ces actions consistent à affecter l'information et les systèmes d'information adverses, tout en augmentant et protégeant nos propres informations et systèmes d'information. La guerre de l'information, qui comprend un volet offensif et un volet défensif, est une intention précise permettant de déployer notre architecture de C⁴I pour améliorer l 'élaboration de la décision en acquérant la supériorité informationnelle dans les conflits.* "

3.2. La guerre de l'information : un concept stratégique ancien

Renseignement et propagande constituent depuis les origines un des fondements de toute stratégie militaire.

Le grand stratège chinois Sun Zi, il y a 25 siècles, considérait déjà que ces principes devaient occuper une place déterminante dans toute réflexion stratégique.

Dans le premier chapitre de son essai l'Art de la Guerre il écrit " *la guerre, c'est l'art de duper* ". Pour Sun Zi, cet art doit permettre de transformer les faiblesses en forces. Dans notre contexte contemporain, ce principe de " *ruse* "fait partie du domaine des actions psychologiques. Ces dernières revêtent en effet diverses formes parmi lesquelles les différents types de propagande constituent une pratique courante. L'avènement des Nouvelles Technologies d'Information et de Communication offre aujourd'hui aux États et groupes de pression divers de nouvelles opportunités en matière de guerre psychologique.

L'exemple du traitement médiatique américain de la guerre du Vietnam souligne l'importance à accorder à ce domaine.

" *L'action psychologique doit donc devenir une activité naturelle, tirant parti des développements techniques de notre époque (...).* "

Elle a pour objectif d'influencer les attitudes et les comportements afin de permettre la réalisation des objectifs politiques et militaires.

Le chapitre consacré au recueil de l'information souligne le caractère fondamental du renseignement dans l'art de la guerre. Selon Sun Zi, en effet, la connaissance parfaite de l'ennemi constitue un préalable à la victoire.

Ainsi lorsque le Livre Blanc sur la défense précise que le renseignement est un " *instrument stratégique (...), fonction essentielle de la stratégie de défense de la France* ", il ne fait que réactualiser un concept très ancien.

Si, du temps de la guerre froide notre vigilance se portait principalement en direction d'un ennemi parfaitement identifié, aujourd'hui la prise en compte de la mutation géostratégique résultante de la décomposition du bloc de l'Est nous pousse à porter notre attention dans toutes les directions. A cet égard, le renseignement est amené à jouer un rôle central dans le cadre d'une stratégie de prévention et d'action.

3.3. intérêt stratégique de la guerre de l'information

Le général Mermet au sujet de l'information note que " *le XXI^{ème} siècle sera celui où la bataille de l'information jouera un rôle déterminant (...). L'information est devenue une véritable matière première stratégique désormais indispensable aussi bien aux chefs d'entreprise pour assurer la conquête des marchés qu'aux gouvernements pour garantir leur liberté d'appréciation préalable, indispensable à l'autonomie de décision et au succès de toute politique* ".

A l'évidence, l'information ou plutôt la maîtrise de l'information représente aujourd'hui un enjeu stratégique de premier plan.

Disposer de l'information, c'est disposer de la connaissance. Le principal enjeu de la maîtrise de l'information consiste en la capacité à lever l'incertitude au moment de la décision.

La complexité croissante des situations de crises et de conflits, l'intervention d'acteurs non-étatiques toujours plus nombreux et la " sur-médiatisation " conduisent à multiplier les facteurs à prendre en compte ainsi que l'impact des décisions prises. Celui qui détient la maîtrise de l'information dispose d'un avantage stratégique majeur.

De l'étude précédente sur l'évolution des Nouvelles Technologies d'Information de Communication et des menaces qui en découlent ; nous pouvons dégager trois caractéristiques essentielles de la guerre de l'information qui renforcent cette perception de l'information comme un critère majeur de la stratégie. Il s'agit de la permanence, la transversalité et la dualité.

- Permanence : La menace contre nos systèmes d'information ne se limite pas aux périodes de conflit. Il est par conséquent vital, dès le temps de paix, de

mettre en œuvre tous les moyens nécessaire à la protection de l'information, de ses supports et de ses moyens de traitement.

- Transversalité : L'information n'existe que pour être échangée. Sa validité repose sur ses possibilités d'exploitation. Ce n'est pas l'information en elle même qui est intéressante mais bien l'exploitation qui en est faite. Elle doit donc à ce titre être au dessus des systèmes et au service de l'efficacité globale. Si le recueil des éléments est spécifique à chaque type d'équipements, l'information est la forme élaborée à partir de la synthèse de ces renseignements primaires.

- Dualité : Comme nous l'avons mis en exergue dans la deuxième partie de ce mémoire, la guerre de l'information n'est pas l'apanage de la défense. Elle concerne aussi directement les domaines médiatiques, culturels, scientifiques, économiques et politiques.

La guerre de l'information doit donc faire partie d'une stratégie globale et cohérente. Les enjeux liés à la maîtrise de l'information dépassent en effet le strict cadre de la gestion des crises pour devenir le préalable à toute politique extérieure.

En effet, comme l'écrivait Clausewitz, " *la guerre doit correspondre aux intentions politiques et la politique doit s'adapter aux moyens de guerre disponibles* ".

La guerre de l'information se joue donc dès le temps de paix. C'est effectivement bien en amont des périodes de crises que les chefs militaires doivent concevoir les moyens d'actions relatifs à cette nouvelle forme de guerre.

Les armées y ont un rôle majeur à jouer dans l'élaboration de la stratégie.

L'information n'est pas une fin en soi, " *elle donne un avantage décisif mais n'implique pas forcément le succès* ". De cette affirmation découle une vérité : la collaboration et la concertation doivent être très étroites entre les dirigeants politiques et les militaires.

3.4. Les formes de guerre de l'information

Aujourd'hui, l'électronique et l'informatique sont au coeur de tous nos systèmes d'armes. La complexité croissante de nos matériels et la nécessité de les adapter à un cadre d'emploi de plus en plus variable conduisent à réaliser des équipements

toujours plus sophistiqués intégrants les toutes dernières technologies (avion Rafale, char Leclerc, ...)

En outre, nul ne conçoit plus aujourd'hui un système de commandement qui n'intégrerait pas un usage généralisé des systèmes informatiques et des moyens de télécommunications performants. Les efforts développés par les armées françaises pour se doter d'un système d'information et de commandement (SICA) illustrent cette nécessité.

La réalisation des grandes fonctions de notre cadre d'emploi: dissuasion, prévention, protection et projection demande en permanence la mise en oeuvre de ces moyens matériels.

La conservation de la maîtrise de l'information est donc un aspect vital de notre défense.

Que penser en effet de la crédibilité d'une stratégie de dissuasion qui ne comprendrait pas la garantie d'un bon acheminement des ordres de tir ?

Toutefois il serait très réducteur de limiter la réflexion stratégique sur la guerre de l'information à ce seul aspect de maîtrise de l'information.

Les armées ont un rôle majeur à jouer dans la guerre de l'information, tant dans l'élaboration de la stratégie que dans la mise en oeuvre aux niveaux opératifs et tactique des systèmes d'information et de communication.

Ainsi, nous pouvons définir trois formes de guerre de l'information:

- La guerre **pour** l'information.
- La guerre **contre** l'information.
- La guerre **par** l'information.

3.4.1. La guerre pour l'information.

Elle repose sur l'exploitation des informations disponibles, qu'elles proviennent de sources ouvertes ou secrètes, d'origine humaine ou technique.

La mutation géostratégique oblige désormais à une compréhension des situations pouvant déboucher sur des crises d'intérêt militaire par la prise en compte de facteurs bien plus nombreux que l'État et la nature des forces en présence. Au-delà du renseignement purement militaire, il s'agit aujourd'hui d'inclure toutes les données de contexte, indispensables pour appréhender l'ensemble de la situation.

Le nombre d'informations susceptibles d'être ainsi recueilli croît exponentiellement et nécessite des ressources humaines et techniques performantes pour les traiter. L'information, en effet, n'est pas la connaissance. Une information complète du champ de bataille qui ne consisterait qu'en une accumulation de données ne serait pas d'une grande utilité pour prendre des décisions militaires. Les informations doivent être filtrées et intégrées dans une vision d'ensemble. L'afflux d'informations peut avoir un effet paralysant en raison non seulement de leur nombre, mais aussi de leur nécessaire ambiguïté. Elles peuvent tout simplement être fausses parce que l'ennemi les aura falsifiées ou aura utilisé des leurres afin de détourner nos centres d'intérêts. Enfin, dans les conditions modernes des conflits, la rapidité est de plus en plus décisive pour l'issue des combats, renforçant la nécessité de moyens automatisés de traitement.

Le renseignement militaire recouvre donc la notion de recueil des informations facilité par le perfectionnement des systèmes d'écoute électromagnétique, les progrès réalisés dans le domaine de la cryptographie, l'explosion des systèmes d'observation (satellites, avions, drones, ...) et par le développement de mécanismes de veille automatique du réseau Internet permettant de synthétiser toutes les informations utiles véhiculées par le réseau (TAIGA et NOEMIE pour la DGSE). Outre cet aspect de recueil de l'information, le renseignement militaire regroupe aussi tous les aspects liés au traitement et à l'analyse de ces sources d'information.

3.4.2. La guerre contre l'information

Elle consiste à protéger nos informations et à se donner la capacité d'agir contre les flux d'information qui nous intéressent. Elle se base sur l'ensemble des mesures de protection des systèmes d'information et sur la maîtrise d'un certain nombre d'outils offensifs et défensifs. Elle inclut notamment les contre-mesures informationnelles destinées à protéger nos systèmes contre les manipulations possibles.

En temps de crise, cette forme de guerre de l'information comprend entre autre la guerre du commandement. Elle a pour objectifs d'interdire à l'adversaire d'acquérir de l'information, de l'influencer, de dégrader ou de détruire ses capacités de commandement tout en assurant la protection de nos propres moyens de commandement.

Pour ce faire, elle fait appel à un certain nombre de moyens et de modes d'action parmi lesquels nous pouvons citer:

- La guerre électronique qui a pour but de conquérir et de conserver la maîtrise du champ de bataille électromagnétique. Elle comprend au niveau offensif les actions pour que les communications, les réponses radars et les signaux soient au moins perturbés et, au mieux inopérants.
- Une guerre de piratage dans laquelle les processeurs et autres procédés automatisés des systèmes ennemis sont dégradés, modifiés ou espionnés par le biais d'un accès illicite aux ordinateurs en vue d'y insérer des virus et autres logiciels pirates.
- Une guerre directe contre les centres de commandement visant à leur destruction par l'application de feux, favorisée par l'acquisition de renseignements sur la localisation et le type de poste de commandement.
- Une guerre de neutralisation des systèmes de commandements visant à détruire les systèmes électroniques ennemis à l'aide de rayonnements électromagnétiques qui peuvent être générés par l'explosion en haute altitude d'une bombe nucléaire (IEM)

3.4.3. La guerre par l'information.

Elle repose sur la maîtrise de la bataille médiatique, de l'action psychologique et de la désinformation.

Comme nous l'avons souligné dans la première partie, l'information médiatique est aujourd'hui planétaire. Tous les événements font l'objet d'une large couverture et son influence sur les populations naturellement disposées à s'émouvoir et à s'indigner est importante. Dès lors, les médias apparaissent comme un moyen d'action indispensable, non seulement aux autorités politiques, mais aussi au chef militaire qui doit savoir en user pour la réussite de sa mission. La victoire et la défaite ne procèdent pas seulement du succès des moyens militaires. Le jugement des médias, porté sur le bien fondé de l'intervention, sur la valeur des moyens employés et sur la justification des résultats obtenus, pèse aussi d'un poids considérable sur l'opinion publique nationale ou internationale.

Les actions psychologiques peuvent être définies comme l 'ensemble des opérations, qui par la transmission d'informations et de signes sélectionnés en direction d'un auditoire étranger cible ont pour objectif d'influencer ses émotions, ses intentions et son raisonnement. Elles agissent ainsi sur le comportement des gouvernements étrangers, des organisations, des groupes et des individus.

La désinformation, enfin, consiste en la diffusion d'informations erronées ou, plus subtilement, d'une multitude d'informations. Ces dernières peuvent être plausibles et ne doivent pas entrer en contradiction avec des données observables. Elles ont pour objectifs de masquer les informations pertinentes et d'impliquer des pondérations fausses dans l'importance à accorder aux diverses informations de telle sorte à fausser les décisions stratégiques adverses

4. Conséquences stratégiques

L'éventail stratégique de la guerre de l'information englobe donc l'ensemble des opérations de désinformation et toutes les autres formes de guerre psychologique, la pénétration et le sabotage des systèmes informatiques, le brouillage électronique des radars ennemis et la destruction des équipements de communication et des points stratégiques du dispositif adverse.

La part de l'information dans l'économie et, progressivement, dans les systèmes de défense, connaît une véritable explosion, un accroissement de la demande, une multiplication des supports et prend donc comme nous l'avons montré précédemment une importance stratégique déterminante dans la prise de décision. " *L'idée centrale est que la guerre a désormais radicalement changé de mode de fonctionnement, sinon de nature, avec l'avènement des nouveaux moyens de surveillance, de repérage et de transmission et la mise au point d'armes à grande portée et de grande précision* ".

Dans un système de tensions à l'échelle planétaire, les décideurs doivent avoir une connaissance poussée de leur environnement, des perspectives d'évolution de celui-ci, des opportunités qui s'y présentent, mais également des menaces qui les guettent, et ce quasiment en temps réel.

Intégrées aux dispositifs de défense, les potentialités des nouvelles technologies ont précisément la faculté de décupler les capacités d'anticipation au sein d'un environnement fondamentalement instable et incertain. Elles apparaissent de la sorte comme un élément stratégique de l'arsenal offensif dont dépend la survie des pays occidentaux. Elles nécessitent par conséquent une profonde adaptation de notre outil de défense.

Aujourd'hui, la double incidence des bouleversements géostratégiques et des sauts technologiques fait apparaître un vaste panel de menaces asymétriques et d'opportunités technologiques. Il s'agit, pour les milieux stratégiques, désemparés par ce que général Lucien Poirier nommait déjà la " *Crise des fondements* ", d'affronter le double enjeu que constitue l'effondrement de l'empire soviétique, donc la disparition de l'ennemi désigné, et le basculement d'une société industrielle vers une société " immatérielle " essentiellement basée sur l'information.

Car les changements de cette amplitude ne sont bien sûr pas sans incidence sur la façon de conduire la guerre.

Le nouvel environnement économique et stratégique, les ressources pour le moins réduites accordées à la Défense, nécessitent une véritable refonte de l'outil de défense, dans la perspective d'une menace diffuse et globale. Ces mutations se caractérisent notamment par le passage d'un monde où le risque (programmé) de guerre mondiale dérivait en conflits régionaux, à un monde de conflits régionaux risquant de dériver en guerre mondiale non programmée. Elles nécessitent la mise en œuvre de nouvelles stratégies.

Des administrations militaires aux théâtres d'opération d'autre part, l'application massive des nouvelles technologies pourrait considérablement modifier - à terme - notre façon de collecter, trier, traiter et diffuser l'information, et, corrélativement, les objectifs et les moyens de la guerre.

Les compétences nécessaires à la gestion de crise reposant essentiellement sur les capacités de réactivité et de maîtrise de l'information, la révolution des NTIC peut dés lors être considérée comme un élément stratégique de l'accroissement des capacités des forces armées : " un multiplicateur de puissance ".

4.1. La double incidence des bouleversements géostratégiques et des sauts technologiques:

4.1.1. Les conséquences de l'effondrement du bloc soviétique : les impératifs de réactivité et de maîtrise de l'information;

Premier facteur de changement d'ordre politique, économique et social, l'effondrement du bloc soviétique a conduit à une relative diffusion de la puissance et à un changement brutal des acteurs susceptibles d'occuper un rôle sur la scène internationale. Les nouveaux acteurs sont non seulement des États Nations, mais également des organisations internationales et un vaste panel d'organisations non - gouvernementales (ONG), mais aussi comme nous l'avons souligné dans la seconde partie un certain nombre d'acteurs transnationaux comme les médias, les mouvements religieux, les groupes terroristes ou les mafias.

Les changements économiques (globalisation et mondialisation des économies - durcissement de la compétition) et sociaux (développement de réseaux virtuels transnationaux) bouleversent les hiérarchies traditionnelles.

De même, si la lutte entre les deux superpuissances est révolue, l'éclatement de l'URSS en communauté d'États Indépendants a provoqué de graves tensions (menace de fondamentalistes islamistes, tendances indépendantistes, conflits territoriaux) parmi les zones autrefois couvertes par l'empire soviétique, comme le Caucase, l'Asie centrale (constituée de cinq républiques de forte tradition islamiste), la Turquie ou l'Iran qui constituent autant de facteurs de crise.

La résurgence de l'intégrisme musulman en Afrique du Nord et l'enlisement du conflit israélo-palestinien depuis l'arrivée au pouvoir de B.Netanyahou, partisan d'une doctrine " révisionniste " juive , peuvent également présager d'une vaste série de crises régionales dont l'ampleur reste pour le moins incertaine et préoccupante.

Se pose alors le problème du maniement d'une frappe massive aux dommages insupportables à l'égard de proliférants qui menaceraient nos intérêts vitaux, mais pour lesquels le risque de dommages insupportables ne se situerait pas au même niveau de perception que le nôtre. L'ennemi est désormais mal localisé, imprévisible et d'une rationalité pour le moins différente de celle des pays occidentaux, ce qui remet en cause les fondements mêmes de notre doctrine.

Trois facteurs déterminent en fait les mutations de notre environnement géostratégique:

- L'effondrement de l'empire soviétique supprime la seule force apte à soutenir des conflits à l'extérieur de ses frontières et capable de procurer les armes conventionnelles les plus avancées aux pays en crise.
- En cas de crise régionale, les pays occidentaux - Etats-Unis en tête - ont à leur disposition un vaste ensemble de mesures non militaires éventuellement applicables - comme l'embargo ou les boycotts - sans craindre l'interférence d'une autre superpuissance. Au plan militaire stricto sensu, leur évidente supériorité technologique et tactique confirme leur capacité à assurer une dominance sans partage sur les compétiteurs régionaux dans un futur proche.
- La convergence des intérêts stratégiques au sein des différentes zones d'influence et la volonté réciproque de réduire les coûts d'interventions dans un contexte de budgets militaires réduits conduit à une augmentation des opérations menées en coalition. Cela implique de nouvelles façons de conduire la guerre et une interopérabilité croissante des différentes forces d'intervention.

Jusqu'en 1989, le coût économique global d'une menace nucléaire susceptible de dissuader les soviétiques d'attaquer s'avérait beaucoup moins élevé que celui qui aurait pu assurer une protection efficace de la population contre une éventuelle attaque soviétique. Mais la dissuasion est par nature binaire. Ou bien la menace est stratégiquement efficace et le risque de guerre est nul, ou bien elle ne l'est pas et ce risque est maximal. Le modèle de dissuasion ne vise pas à réduire, mais à éliminer le risque de guerre, il ne prend donc en compte que ces deux cas extrêmes.

Par conséquent dans le nouveau contexte international, le rapport " coût/efficacité " de la dissuasion nucléaire se trouve détérioré du fait de l'augmentation de la probabilité d'échec de la dissuasion et donc de l'occurrence du risque de guerre. Le défi auquel doivent désormais faire face les Etats-Unis et l'Europe est de maintenir un éventail de capacités suffisamment vaste pour faire face :

- A des menaces symétriques - peu probables - de la plus haute intensité;
- A des menaces asymétriques et à une multitude de conflits conventionnels de moindre intensité;
- A des situations intermédiaires mettant en cause des zones d'influence susceptibles de faire dégénérer un conflit armé en guerre nucléaire non programmée (Iraq, Chypre ou Corée du Nord par exemple)

Les mutations de l'environnement géostratégique imposent une évolution de notre système de défense, un recours aux forces conventionnelles n'étant pas à exclure comme l'illustrent les nombreuses interventions effectuées ces dernières années (Somalie, Rwanda, Yougoslavie,...). De la prise en compte de ces mutations dépendront tout à la fois les options stratégiques et la politique d'armement.

La stratégie de défense doit par conséquent impérativement gagner en flexibilité afin d'affronter les conflits les plus imprévisibles, quelque puissent être leur nature, leur origine ou leurs cibles. L'appréhension de ces caractéristiques des conflits constitue un préalable aux engagements. Elle nécessite l'acquisition de la maîtrise de l'information et la mise en oeuvre de ce que nous avons nommé la guerre pour l'information dont la doctrine, à l'instar de celle adoptée par les Etats-Unis, doit être élaborée.

4.1.2. De la sphère commercial au monde militaire, les conséquences de l'application massive des nouvelles technologies d'information et de communication :

L'essor des nouvelles technologies d'information et de communication s'est curieusement effectué en parallèle des bouleversements géostratégiques que nous venons d'évoquer.

C'est très précisément en 1989 que la mise au point du World Wide Web, fondé sur la navigation hypertextuelle, a provoqué le décollage massif de l'Internet.

Parce qu'ils constituent le point névralgique d'une " société de l'immatériel ", Internet et l'ensemble des réseaux de télécommunications peuvent être considérés comme des " armes par destination ", pouvant être dirigées aussi bien contre un individu, une entreprise ou un État.

Au cœur du nouvel empire électronique qui se dessine, l'infoguerre, ou guerre de l'information, représente une zone de guerre silencieuse sur laquelle s'affrontent les services de renseignement du monde entier.

L'idée d'une géostratégie moderne fondée sur le contrôle des réseaux cybernétiques et la maîtrise de l'information est à l'image, comme le remarquaient Alvin et Heidi Toffler, de la manière dont nous créons les richesses. A l'instar des entreprises, les armées ont également à stocker et à traiter une multitude d'informations, et leurs

performances dépendent de la nature, de la distribution, de la souplesse des systèmes de contrôles, et notamment de leurs liens avec les radars, les défenses aériennes, et les réseaux de satellites et de communication.

De la performance des systèmes d'information, du contrôle qu'ils exercent sur les réseaux, dépendent désormais la sécurité et la puissance des organes de décision. Cette guerre de l'information s'inscrit, ou est susceptible de s'inscrire dans une stratégie de déstabilisation et d'affaiblissement général. En tant qu'instrument d'appropriation de l'information, elle donne la maîtrise de secteurs stratégiques et corrélativement, occasionne la perte de leur contrôle.

Cette révolution nécessite non seulement un nouvel ensemble de capacités technologiques, ou de nouvelles conditions politiques, économiques et sociales, mais aussi, leur reconnaissance et leur exploitation . Les implications des nouvelles technologies sont rarement reconnues au premier abord. Il est fréquent que les organisations essaient de coller de nouvelles technologies dans de vieux systèmes au risque de créer de nouvelles inefficiences. L'intervalle est souvent long entre le renouvellement des armes et les changements de tactiques.

L'activité elle-même doit donc être restructurée, tant sur le plan opérationnel que sur le plan organisationnel, afin d'exploiter le potentiel des nouvelles technologies.

Martin Van Creveld, dans son ouvrage *Technology and war*, qualifie notre période d'âge de " l'automatisation " (après " l'âge des outils ", " l'âge de la machine " et " l'âge des systèmes "). Cette nouvelle ère prend place dans l'après-guerre, avec l'évolution drastique de la quantité d'informations nécessaires à la conduite des opérations et à la prise des décisions. Dans les armées cette automatisation est devenue indispensable pour combattre efficacement.

Toutefois, la technologie seule ne suffit pas à produire une révolution militaire. Ce qui importe, c'est la façon dont les organisations militaires adaptent, combinent et intègrent les nouvelles technologies, les systèmes d'armes et les concepts opérationnels afin d'en optimiser l'exploitation. La révolution des NTIC et le passage à un monde postindustriel impliquent un bouleversement des moyens et même des objectifs de la guerre. De même qu'ils favorisent l'émergence, au plan organisationnel, d'entités plus souples et plus réactives, mieux adaptées à l'évolution des menaces.

4.2. Les conséquences logiques de l'intégration des systèmes

4.2.1. De l'intelligence des systèmes à l'intelligence des situations :

La stratégie d'attrition, mise en œuvre dans les années 80, est la conséquence logique d'une série de développements technologiques, que ce soit au niveau des armes, des systèmes de détection ou encore des capacités déployées en matière de contrôle, commandement, communications et " d'intelligence " (C^3I) La destruction de l'ennemi se concevait grâce à une concentration massive des forces et à l'accumulation de succès tactiques remportés au cours d'une progression prudente sur un large front.

Pour les occidentaux, le problème était alors d'arriver à rassembler des ressources supérieures à celle de l'adversaire pour le détruire uniquement par la puissance de feu et le matériel. Cette stratégie visait, en pleine guerre froide, à contrer la puissance des forces du Pacte de Varsovie, en décuplant l'efficacité des vecteurs de frappe. Il s'agissait alors essentiellement de disposer de l'information sur la situation, le comportement et les intentions de l'ennemi.

La guerre du Golfe, en 1991, constitue le prototype des guerres futures: des vecteurs de haute précision, des systèmes de lancement de frappes massives contrôlés par des systèmes de surveillance en continu, une écrasante supériorité aérienne ainsi qu'une maîtrise totale dans le domaine du C^3I et de la guerre électronique. Dans ces conditions, d'après le général soviétique Bogdanov, *" l'Irak avait perdu la guerre avant même qu'elle ne commence "*.

Saddam Hussein avait déployé des échelons entiers de concentration d'hommes et de blindés. En face, deux systèmes armes redoutables furent déployées. Les AWACS (Airbone Warning and Control system) - et le J-STARS, son homologue à terre, capable de détecter jusqu'à 250 kilomètres de distance et d'instaurer le chaos parmi tous les échelons successifs des armées irakiennes.

Pour rattacher les multiples bases de données et réseaux américains des Etats-Unis à la zone de guerre, un ensemble de réseaux complexes fût mis en place, reposant sur 118 stations terrestres mobiles de communication par satellites et 12 terminaux de satellites commerciaux disposant de 81 commutateurs rendant disponibles 329 voies de conversations téléphoniques et 30 circuits de transmission de messages.

Au total, ces dispositifs traitèrent jusqu'à 700 000 appels téléphoniques et 152 000 messages par jour concernant les consignes des gestionnaires de l'espace aérien des six pays de l'alliance, la logistique de guerre, le suivi des cargaisons, etc...

La guerre du Golfe a vécu ce que l'on appelé " la plus vaste mobilisation de communication de l'histoire militaire

Fondée sur la pleine exploitation des technologies d'information et de communication et le règne de l'intelligence artificielle, cette guerre est la preuve que la victoire sur le front militaire dépend désormais des capacités d'adaptation de

l'infrastructure militaire et de l'interopérabilité des systèmes, voir de leur intégration complète.

Les systèmes d'armes intelligents, déployés lors de l'opération Tempête du Désert - munitions conventionnelles modernes (missiles et armes de précision), systèmes C^3I, communications spatiales et systèmes de détection en temps réel - ont permis d'assurer en toutes circonstances la domination de la coalition. dans ce type de conflit conventionnel de haute intensité.

La puissance de feu est devenue si précise que les nouveaux systèmes d'armes peuvent aisément identifier le bâtiment ou la pièce, mais également " *le coin de la pièce susceptible de provoquer l'effondrement du tout - et même le courant d'air qui va permettre à la bombe de s'y loger...* " Cela remet entièrement en question le traditionnel principe militaire de concentration de forces.

La pleine intégration des systèmes de détection aux systèmes de commandement et de contrôle permet de mettre en œuvre des synergies sans précédent.

Dans le passé, comme le soulignait Van Creveld, le commandement comptait sur l'accroissement des capacités individuelles des composants des forces militaires - masse, mobilité, puissance de feu, etc. - pour compenser les imperfections en C^3I.

La révolution de l'information devrait au contraire permettre d'exploiter toutes les potentialités des capacités militaires, tant sur le plan organisationnel que sur le plan opérationnel ou technologique.

Une fois collectée et traitée, l'information se traduit par une prise de conscience aiguë des caractéristiques d'une situation précise, préalable indispensable à une prise de décision appropriée. L'intelligence quant à elle, suppose non seulement une bonne compréhension de l'environnement et des situations, mais aussi et surtout une claire perception des implications potentielles des actions choisies. Il importe avant tout aujourd'hui de disposer de l'intelligence de la situation, préalable à toute action.

Les avantages de l'automatisation, des réseaux de communications globales et des systèmes modernes de détection donnent une importance sans précédent au management et à l'exploitation de l'information.

L'ampleur croissante du champ d'action, la précision et le pouvoir de destruction des munitions conventionnelles accentuent l'importance du C^3I à tel point que la domination dans ce seul domaine pourrait bientôt être une condition nécessaire de la victoire.

Grâce à cette " révolution cognitive ", la capacité existe désormais, pour la première fois, de détourner le C³I de sa traditionnelle fonction de support pour exercer un rôle d'orchestration, de synchronisation et de "focalisation" des différentes forces sur un point décisif.

4.2.2. La fusion des niveaux stratégiques, tactiques et opérationnels

Bien que nous ne puissions pas prédire exactement la tournure que pourraient prendre les futurs conflits, il est probable que l'on assiste à un vaste élargissement du champ d'action et à une certaine forme de fusion des niveaux stratégiques, opératifs et tactiques. L'utilisation des systèmes d'armes intelligents, des systèmes de surveillance et des armes de précision nécessite l'intégration des opérations et des différents éléments gages de l'efficacité du plan d'ensemble.

La révolution de l'information est la condition permissive, et non la cause, de ces transformations. Elle fournit deux aptitudes déterminantes, d'une part la capacité de remonter la hiérarchie cognitive définie précédemment (de la collecte des données aux décisions), et d'autre part la capacité de communiquer ces décisions en temps réel aux différents acteurs.

Auparavant, avec les imperfections des systèmes de commandement et de contrôle, et l'insuffisance des capacités de synchronisation, il n'y avait pas d'autre choix que de créer des processus et des organisations hiérarchiques pour faire parvenir les décisions du commandement aux échelons subordonnés.

Avec l'utilisation des NTIC (nouveaux systèmes C³I), les informations peuvent instantanément être transmises du plus haut de la hiérarchie au plus bas et, remonter de la même manière l'ensemble de la chaîne.

Les commandements subordonnés peuvent désormais participer à l'analyse globale des situations, quasiment en temps réel, via des systèmes intégrés de C³I, tirant alors profit de leurs connaissances de la situation locale.

Aujourd'hui notre pays a vocation à intervenir dans toutes sortes de crises à l'échelle planétaire, qu'il s'agisse de la défense de nos intérêts stratégiques et économiques, ou d'actions de maintien de la paix au sein des coalitions. La gestion de crise est donc devenue la norme, plaçant au premier plan les capacités de mobilité et de réactivité, tant sur le plan stratégique que sur le plan tactique.

La capacité de projeter et de soutenir les forces sur des zones éparses et éloignées conduit à assurer une supériorité aérienne et navale.

L'intégration des systèmes d'armes et des plates-formes ainsi que des systèmes de reconnaissance et de surveillance, l'automatisation des fonctions de commandement et de contrôle ainsi que leur association avec des vecteurs précis permettent de détruire un nombre significatif de cibles ennemies et de formations de combat, avant

que le contact ait eu lieu, et même avant que le ralliement des forces alliées ne se soit opéré.

L'amélioration des capteurs rend possible une utilisation à des fins tactiques de moyens jusque-là réservés au niveau stratégique. C'est ainsi, qu'avec l'augmentation de la résolution des satellites d'observation tels que Helios, l'imagerie spatiale est aujourd'hui exploitable au niveau tactique.

Les plates formes aéronavales sont capables de conduire une guerre où la notion de point stratégique ciblé se substitue à la traditionnelle distinction entre front avant et ligne arrière et rend superflu les vastes déploiements de troupes au sol. Les objectifs stratégiques seront réalisés par l'intermédiaire d'armes purement conventionnelles avec des frappes intensives précises, pilotées par des systèmes de reconnaissance capables de localiser n'importe quel objectif.

C'est donc de la maîtrise des réseaux d'information et de l'intégration des systèmes d'armes que dépend désormais, en grande partie, la victoire sur le front militaire. A la géostratégie classique, s'ajoute dorénavant une " infostratégie " qui en est le préalable nécessaire. La réalisation des objectifs stratégiques par l'emploi de moyens conventionnels, préalable à l'engagement terrestre, établi une très forte corrélation entre stratégique et tactique concourant ainsi à réaliser une forme de fusion de ces différents niveaux qu'il convient de prendre en compte au niveau organisationnel.

4.3. Ajustements fondamentaux en matière d'organisation militaire et de doctrine: Les mutations organisationnelles

Les commandements peuvent désormais exploiter les connaissances et les expertises d'autres organisations situées à des milliers de kilomètres pour formuler les plans d'action durant les heures suivantes.

Le système de commandement devient dépendant d'une multitude d'aménagements informels, ad-hoc. C'est ainsi que, lors de la guerre du Golfe, des officiers basés au Pentagone aidaient à repérer les cibles et à mettre au point des plans d'attaque, tandis que les commandements spatiaux alertaient les forces en cas d'attaques de missiles contre Israël ou l'Arabie Saoudite, et que les météorologistes traitaient les informations météo utiles aux mouvements de troupes sur les théâtres d'opérations.

L'organisation n'est plus une donnée immuable. L'étroite dépendance qui existe entre les structures organisationnelles et la gestion efficace des flux d'information doit être prise en compte dans la réflexion stratégique.

L'accroissement exponentiel de la masse et du débit d'informations à traiter est à la fois la cause et la conséquence d'une plus grande numérisation.

Il s'agit dès lors de concilier la gestion décentralisée des activités opérationnelles avec une centralisation rapide des informations nécessaires aux décisions stratégiques.

Ainsi, l'impact de la révolution de l'information affecte d'abord l'ensemble de la hiérarchie cognitive, à commencer par les données, l'information, la connaissance et l'intelligence.

Le raccourcissement des délais entre décision et action requiert une véritable décentralisation de ce qui représentait jusqu'ici le commandement central. Les innovations organisationnelles sous-tendues par les nouvelles technologies reflètent les changements observés dans les structures organisationnelles et les processus de décision du monde civil, notamment commercial. Ces changements, facteurs clés de succès, sont supposés améliorer à la fois la réactivité face aux nouvelles informations, et l'exécution des décisions.

Le passage des formes hiérarchiques traditionnelles à des réseaux d'unités de décision interconnectées est à la fois un gage de réduction des coûts en matière de collecte et de distribution des informations, le préalable à une efficacité accrue pour la diffusion de ces informations en temps réel.

A travers l'accroissement des capacités de contrôle et de commandement des opérations se trouvent en effet remis en cause la traditionnelle division du travail ainsi que l'attribution des rôles et des missions, au sein des organismes militaires eux-mêmes.

En outre, l'augmentation de la zone d'influence et d'intérêt que le commandement est à même de contrôler, compte tenu de la performance des systèmes de surveillance et de reconnaissance et de la puissance des systèmes d'armes, a pour conséquence logique une intersection croissante des différents organismes affectés aux missions de surveillance.

Il faut donc évoluer d'une organisation très hiérarchisée vers une nouvelle organisation. En effet, seule capable de concilier un niveau extrêmement élevé d'intégration avec la relative décentralisation des activités, une organisation de type réseau facilite la prise de décision et décuple les capacités des forces sur les théâtres d'opérations. Ce type d'organisation parfaitement adapté au partage de l'information n'est pas pour autant inadaptée au commandement. Le chef reste responsable de la décision et dispose toujours de la capacité à diffuser ses ordres.

Conclusion

L'évolution de l'information est considérée comme le fait majeur de cette fin de siècle et la suprématie du XXI^{ième} siècle sera détenue par ceux qui maîtriseront l'information et les médias.

La bataille du prochain siècle sera aussi celle de la connaissance et de l'innovation, et ce qu'aujourd'hui on nomme le multimédia va se normaliser, fusionner et se redéployer pour engendrer un espace unimédia où l'ensemble de tous les services de l'information sera supporté par un maillage de réseaux interactifs.

Pour la première fois dans l'histoire de la communication, l'apparition des nouvelles technologies, et plus particulièrement d'un langage commun : le numérique, génère un processus qui entraîne un changement rapide de modèle économique. Cela nous conduit vers une refonte totale du mode de pensée et du mode de diffusion de l'information, en particulier dans les secteurs de l'édition traditionnelle, de la radiodiffusion et de la télévision.

Cette révolution ne se limite pas à la multiplication des informations circulant sur support électronique, mais résulte de la maîtrise des processus cognitifs et de l'accroissement des capacités d'intelligence des situations.

Le savoir est l'actif stratégique le plus convoité de notre ère industrielle. La globalisation de ses vecteurs de circulation engendre, de fait, de nouvelles opportunités et de nouvelles menaces.

Au niveau militaire, les précédentes révolution ont décuplé l'échelle et l'intensité des conflits armés en améliorant l'efficacité des moyens: la protection, la puissance de feu, la portée des armes.

De la maîtrise de l'information dépend aujourd'hui notre capacité à agir dans un monde qui depuis l'effondrement du bloc soviétique peut être qualifié de très complexe.

La révolution en cours se manifeste par conséquent par un changement de paradigme visant, par la combinaison des effets rendue possible par ces nouvelles technologies , à obtenir des résultats immédiatement décisifs sur le champ de bataille.

L'adaptation de nos organisations, la formalisation d'une doctrine pour la guerre de l'information sont les enjeux majeurs de l'adaptation de notre stratégie au XXI^{ème} siècle.

Au niveau du monde civil, une démarche similaire doit être impérativement initiée pour faire face aux risques et menaces émergentes. La compétitivité de nos entreprises est en jeu.

Sans l'information adéquate, la connectivité requise et l'organisation adaptée, la France risque de rater le passage à la Société de l'Information.

Notre pays dans ce domaine dispose des compétences, et des moyens pour en devenir un acteur de premier plan. Même si la volonté politique tarde à se manifester, elle doit s'attacher à véhiculer et défendre, grâce aux dernières innovations technologiques, une information qui nous est propre, et, affirmer contre le système anglo-saxon son exception culturelle.

Pour ce faire, le pouvoir politique doit agir dans les aspects de la législation et de la réglementation, mais aussi dans celui réservé à la dimension humaine.

S'il faut admettre que les sciences exactes ont considérablement fait progresser les champs de la technologie, il conviendra désormais de laisser agir des sciences plus organisationnelles et donc humaines pour que cette évolution ne soit pas une révolution douloureuse.

C'est à ce prix que pourront cohabiter INFORMATION et DEFENSE.

Annexes

A - Bibliographie

Col **MOLINER** Jean - Luc : *La guerre de l'information vue par un opérationnel français*, L'armement. décembre 1997 - janvier 1998

COUTAU-BEGARIE Hervé : *Traité de stratégie*, Economica, Bibliothèque stratégique - février 1999

FISHER Addison : *Security and digital signature in electronic business*, Defense Electronics - août 1994

GERE François : *L'action psychologique à l'ère de l'hypermédiatisme* , L'armement. décembre 1997 - janvier 1998

GIBSON William : *Neuromancer*, La découverte. Paris 1985

GROUARD Serge : *La guerre en orbite. Essai de politique et de stratégie spatiales*, Economica, Bibliothèque stratégique - mars 1994

GUISNEL Jean : *Guerres dans le cyberespace*, La découverte. Paris 1995

LCL **CHAUVANCY** François : *La stratégie d'influence par la maîtrise de l'information*, Le Casoar - janvier 1999

LIBICKI Martin : *Defending cyberspace and other metaphors*. National Defense University - Washington DC 1997

McLUHAN Marshall : *Global Village*

POWER Richard : *Information warfare*, Computer Security Institute

TOFFLER Alvin et Heidi : *Guerre et contre-guerre. Survivre à l'aube du XXI*ème *siècle*, Fayard. Paris 1994

The Third Wave, Denoël. Paris 1980

VAN CREVELD Martin : *Technology and war*

VINÇ ON Serge : *Gestion des crises et guerre de l'information*, Le Casoar. janvier 1999

WODKA-GALLIEN Philippe : *Les opérations psychologiques: la doctrine et la pratique en vigueur aux États-Unis*, Le Casoar - janvier 1999

WOLTON Dominique : *War Game*, Flammarion - Paris 1991

B - Glossaire

- **Bombe logique** : programme illicite contenant une fonction malveillante généralement associée à un déclenchement différé. Elle se caractérise par l'unicité de

la cible, en l'occurrence le système informatique sur lequel elle est présente, et l'absence d'auto-propagation de l'infection.

- **Cheval de Troie** (Trojan horse) : c'est une forme particulière de virus Elle est utilisée pour pénétrer par effraction dans l'ordinateur, consulter, modifier ou détruire des informations. Elle peut toucher un grand nombre de systèmes puisque le programme modifié est réinjecté dans les circuits de diffusion.

- **Extranet** : Réseau d'une " grande " entreprise composée de plusieurs centres géographiquement distants et dont tous les sites peuvent communiquer entre eux de la même façon qu'un réseau Intranet (*à l'extérieur de l'entreprise)*. Ce type de réseau est très vulnérable aux actes de piratage informatique.

- **Fire Wall** : Mur coupe feu ou garde barrière. Dispositif permettant une séparation franche interdisant toute intrusion dans un système informatique.

- **Intranet** : Réseau informatique d'une entreprise implantée en un lieu unique sur lequel sont connectés tous les PC identifiés pour dialoguer entre eux afin de permettre l'échange de courrier, de notes de service, d'images, de documents bureautiques, du son ; en fait, tout ce qui est en format électronique (*à l'intérieur d'une même entreprise)*.

- **NTIC** : Nouvelles Technologies d'Information et de Communication

- **Tempest** : l'effet " tempest " est caractérisé par l'émission de radiations électromagnétiques produites par un appareil électronique sous la forme d'un signal radio. Sachant que tout composant électronique émet un signal radio, ce dernier peut être capté à l'aide d'un récepteur dans un rayon de plusieurs centaines de mètres et l'information est ainsi reconstituée avec une totale fidélité. La station réceptrice ne peut cependant que recevoir de manière passive sans être en mesure d'intervenir directement pour par exemple modifier le contenu. Un des moyens de défense consiste à enfermer la source d'émission dans une cage de Faraday afin de réduire fortement sinon d'empêcher toute émission de radiation.

- **TCP/IP** : (Transport Control Protocol/Internet Protocol). Norme de communication permettant d'accéder et de naviguer sur le réseau Internet.

- **Ver** : processus parasite qui consomme les ressources du système (mémoires, réseaux, etc...). Il possède la faculté de se reproduire et de se propager au sein de la mémoire des ordinateurs et à travers les réseaux informatiques. Il peut déclencher des actions malveillantes.

- **Virus** : infection générique se greffant sur un programme ou une zone système avec la possibilité de créer des répliques de lui-même. Il augmente la taille des fichiers et peut saturer un support magnétique. La plupart des virus contiennent des fonctions à déclenchement différé.

WEB : (littéralement : toile d'araignée) - En fait on parle de WWW (World Wide WEB : Réseau d'information mondial)

C - DIFFUSION DE PROGRAMMES PAR SATELLITE : Worldspace - SATIVOD

WorldSpace

Jusqu'à présent, la radiodiffusion classique par voie terrestre demeure relativement coûteuse et limitée. Les obstacles à la diffusion des NTIC à l'échelle du continent africain sont considérables. La diffusion numérique de programmes par voie satellitaire répond à ces impératifs et permet d'assurer une couverture globale, y compris dans les zones les plus isolées.

Le principe de la radiodiffusion numérique par voie satellitaire est assez simple. Le système achemine un signal d'une station de contrôle au sol à l'aide d'une petite antenne parabolique. L'antenne émet le signal vers un satellite géostationnaire couvrant la zone de réception, qui à son tour envoie le signal directement aux récepteurs d'émissions numériques portatifs de la zone considérée.

Projet industriel développé par WorldSpace

WorldSpace est un bon exemple de cette technologie. Il s'agit d'un projet de grande envergure, 80% de la population mondiale pouvant potentiellement être desservie par les émissions radio, en qualité numérique, sur la base des principes généraux énoncés plus haut. Worldspace entend offrir des services de diffusion de programmes audio et multimédia numériques en direct par satellite, vers les régions du monde émergentes et mal desservies : le Moyen-Orient, l'Afrique, le bassin méditerranéen, l'Asie, les Caraïbes et l'Amérique latine.

WorldSpace lancera trois satellites geostationnaires qui assureront une large couverture pour la radiodiffusion vers ces zones.

Le lancement du premier satellite, Afristar, a été effectué fin 1998. Le deuxième satellite, Asiastar, doit être lancé dans le premier trimestre de 1999 et le troisième satellite, Ameristar, en mai 1999. La diffusion des émissions est prévue pour décembre 1998.

L'accès direct aux programmes numériques en provenance des satellites WorldSpace nécessite un nouveau type de récepteur numérique. En plus des programmes satellitaires de WorldSpace, le récepteur portatif permet de recevoir des émissions sur ondes courtes ainsi que des émissions en AM et en FM.

Technologie

La technologie employée fait appel à des communications de bout en bout de la station terrestre au satellite jusqu'à l'utilisateur final. Les concepteurs et producteurs d'émissions et de programmes pourront bénéficier d'une grande qualité de service à un prix relativement raisonnable.

Les producteurs d'émission et de programmes pourront émettre directement vers les satellites à partir de petites stations au sol. L'interface entre les studios et les stations au sol peut se mettre en place en quelques heures.

Chaque satellite est contrôlé par des centres régionaux opérationnels de contrôle (Regional Operations Control Centers : ROCC). Chaque centre est relié à des stations de télémétrie, de commande et de correction (Telemetry, Command and Range : TCR) pour contrôler et gérer la maintenance de chaque satellite.

Chaque ROCC comprend en outre un centre de contrôle (Mission Control Center : MCC) qui facilite l'accès des nouveaux clients.

Le MCC gère tous les services d'émission à partir d'une station terrestre de gestion des systèmes de communication (Communications Systems Monitoring : CSM). Le retour instantané permet au MCC de prendre des actions correctives et d'assurer des communications ininterrompues.

Le composant clé du récepteur WorldSpace est un processeur qui démodule et décomprime les transmissions. La première génération de récepteurs satellitaires sera fabriquée à plus d'un million d'exemplaires.

SATIVOD

Alcatel Espace vient de mettre 50 ingénieurs au travail à plein-temps sur un projet concernant une constellation de 60 satellites dédiés à la fourniture de vidéo interactive et de communications multimédia. Le service débuterait vers 2000 ou 2001.

Pour ce projet estimé à 18 milliards de francs, Alcatel Espace compte trouver d'autres investisseurs. Quelques dizaines de MF sont déjà prévues pour les études préliminaires.

Chaque satellite pèsera 600 kg et sera placé sur une orbite basse à 1600 km. Ce système dénommé Sativod desservira les zones à faible densité de population, là où le câble n'est pas rentable.