COLLEGE INTERARMEES DE DEFENSE

Paris

7ième Promotion
(1999 – 2000)

MEMOIRE DE STRATEGIE

L'information en tant que facteur stratégique :

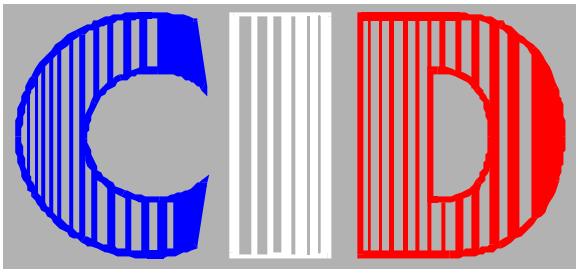
« INFORMATION WARFARE » - Importance et conséquences au niveau stratégique

Jürgen F. ZAHND
Major i.G. (Allemagne)

Division D - Groupe 6

Mars 2000

COLLEGE INTERARMEES



DE DEFENSE

7ième Promotion
Session 1999 - 2000

FICHE DE PRESENTATION

1 – Rédacteur : Jürgen F. ZAHND, Major i.G. (Allemagne)
CID Division D Groupe 6

2 – Titre générique : Mémoire de stratégie

3 – Sujet : L'information en tant que facteur stratégique
« Information Warfare » :
Importance et conséquences au niveau stratégique

4 – Rédaction : Paris, mars 2000

5 – Sommaire : Par rapport à l'évolution technique en général, les progrès en matière de technologie de l'information occupent une place importante. Dans tous les domaines, les sociétés à haute technologie dépendront de plus en plus des processus informatisés. Partout où la technologie de l'information intervient, la *guerre de l'information*, qui est la forme la plus agressive de la course à l'information, peut avoir lieu. De nouveaux risques et conflits potentiels émergent, mais il y a aussi de nouvelles chances offrant des marges de manœuvre pour régler les conflits par des moyens pacifiques grâce à l'utilisation précoce de la technologie de l'information. Le facteur *information* sera particulièrement important au niveau stratégique. Outre les tendances actuelles du développement de la technologie de l'information, le présent mémoire décrit son influence sur la société, l'économie, la politique et le domaine militaire. L'importance de la « guerre de l'information » pour un commandement stratégique efficace à l'âge de l'information est mise en évidence tout comme la nécessité de développer des concepts et des structures interministériels.

6 – Mots clés : Information, facteur(s) stratégique(s), « Information Warfare », guerre de l'information.

page

page

« Celui qui connaît son ennemi
et se connaît lui-même
mènera cent combats sans risque. »[1]

SUN ZI

(philosophe et général chinois,
il y a près de 2.500 ans)

[1] Dans « L'Art de la Guerre »
(édition 1990, page 107).

1. Introduction

Depuis le début des années quatre-vingt-dix, le débat sur *la guerre de l'information* (« Information Warfare (IW) »)[2] a pris une grande importance, en particulier dans l'hémisphère anglo-américaine. Aux Etats Unis, ce débat a déjà provoqué d'importants changements structurels et conceptuels.[3] En Allemagne en revanche, le facteur *information* joue certes un rôle clé au niveau opératif[4], mais une approche stratégique globale fait toujours défaut. Tandis que, d'une part, aux Etats Unis, on peut constater une véritable manie de l'information (« Information Mania ») et l'apparition d'une demande de changement de paradigme en matière de conduite de la guerre, d'autre part, des voix critiques s'élèvent désormais pour exprimer une attitude moins enthousiaste face à l'information et aux technologies de l'information.[5]

Le présent mémoire a pour but de décrire de manière critique l'importance que pourrait revêtir la *guerre de l'information* au niveau stratégique à l'aube du 21e siècle. Après une première *définition* du terme (chapitre 2) et un bref *historique* de l'évolution technologique jusqu'à nos jours (chapitre 3), l'étude sera consacrée aux *changements* qui en découlent en matière sociale, économique, politique et militaire (chapitre 4). Ensuite, la maîtrise du facteur *information* sera étudiée dans une optique stratégique (chapitre 5). Enfin l'analyse de l'*importance stratégique* de la guerre de l'information au 21e siècle sera abordée sur cette base (chapitre 6).

2. Terminologie

2.1 Définition de la guerre de l'information (« Information Warfare »)

L´expression « Information Warfare » est utilisée de manière très variée. Alors, pour éviter des malentendus, il faut poser une définition.[6] Traduire par « bataille pour et avec l'information » serait trop restrictif car cette formule suggère une application exclusivement militaire. Dans le cadre d'une analyse de la guerre de l'information dans une optique stratégique, une

[2] Le terme « Information Warfare » a été utilisé pour la première fois dans le contexte de la seconde guerre du Golfe. Cf. Campan (Gulf War, 1991), p. 81-84 ou aussi Le Bail (Bataille de l'information, 1992), pp. 14-15.
[3] C'est entre autre la raison pour laquelle le présent mémoire se réfère en premier lieu à des sources de langue anglaise.
[4] Dans sa nouvelle édition, le règlement de l'armée de terre 100/100 (Heeresdienstvorschrift der Bundeswehr HDv 100/100 « Truppenführung » (Commandement interarmes)) souligne l'importance particulière du facteur « information » au niveau opératif et tactique.
[5] Cf. Emmet (Information Mania, 1996), p. 19, et Alexander (Digitised Battlefield, 1995), p. 64.
[6] Les termes techniques utilisés dans les manuels anglo-américains sont reproduits tels quels.

approche globale semble être la plus appropriée.[7] Par conséquent, la définition à retenir est:

> *«guerre de l'information = toutes les mesures concourant à la supériorité en matière d'information grâce à la détérioration des informations, des processus informatiques et des systèmes d'information de l'adversaire tout en protégeant les informations, les processus et les systèmes informatiques amis. »*[8]

La guerre de l'information ne se limite donc pas au seul domaine militaire mais englobe toute la société dont les structures d'organisation et les individus représentent tant les objets (les cibles) que les sujets (les acteurs) de cette guerre. Ainsi, c'est l´ensemble de l'environnement d'un décideur au niveau du commandement stratégique qui peut être affecté. Non seulement, la guerre de l'information se superpose aux formes traditionnelles de conflits, mais, elle crée de nouvelles. Elle ne doit donc pas seulement être envisagée entre adversaires politiques ou militaires mais dans toute situation concurrentielle. Par ailleurs, la guerre de l'information s'étend également à la destruction d'installations adverses, la mise en œuvre de moyens immatériels et elle contient toujours un volet offensif et défensif.

2.2 Formes et modes d'action

Généralement, la littérature spécialisée distingue les formes suivantes de la guerre de l´information:[9]

La guerre du commandement (« Command and Control Warfare (C2W) »)

D'un point de vue militaire, cette forme représente la composante dominante de la guerre de l'information : « C2W » est « … the military strategy that implements information warfare on the battlefield »[10]. L'objectif consiste à priver totalement ou partiellement le commandement adverse d'information ou bien ne laisser passer que des informations incomplètes ou fausses sur sa propre situation et celle de son adversaire. L'intention du commandement de l'échelon supérieur est de ne pas communiquer l'information aux subordonnées ou bien de les tromper. Dans le langage militaire, le « C2W » est souvent complété par d'autres termes et devient « C3IW » (Command, Control, *Communication* and *Intelligence (renseignement)* Warfare) ou « C4W » (Command, Control, Communication and *Computers* Warfare). La lutte contre la capacité de commandement ad-

[7] Cette définition générale s'impose aussi progressivement dans la « Information Warfare Community », c.-à-d. dans les institutions dont le travail est consacré à la guerre de l'information.
[8] Cf. Büntemeyer (Dimension, 1996), p. 557.
[9] Les différentes formes de la guerre de l'information sont traitées dans le détail par Libicki (What is IW ?, 1995). Cf. aussi Büntemeyer (Dimension, 1996), p. 557, Amt für Nachrichtenwesen der Luftwaffe (L'office du renseignement militaire de l'armée de l'air fédérale) (Aktuelle Entwicklungen, 1996), p. 7, et Petersen (Krieg der Zukunft, 1995), pp. 783-788.
[10] Hutcherson (Command and Control Warfare, 1994), p. XIII.

verse n'est pas une notion fondamentalement nouvelle. Les installations de commandement ont toujours constitué un objectif central, par exemple dans le cadre de la désignation des cibles pour les forces aériennes. Mais, à l'avenir, cette guerre classique menée prioritairement avec des moyens de destruction physique (« Hard-Kill »), sera étendue de plus en plus à de nouvelles mesures de destruction immatérielle (« Soft-Kill »).

La guerre du renseignement (« Intelligence Based Warfare »)

Cette composante traditionnelle de la guerre de l'information comprend les méthodes d'acquisition de l'information utilisées depuis toujours or mieux connues aujourd'hui sous la désignation «renseignement humain» ou « HUMINT » (Human Intelligence). Certains affirment dire que les principes du renseignement d'origine humaine n´ont plus d'intérêt parce qu'aujourd'hui, on obtient des résultats équivalents plus vite et plus facilement grâce à d'autres moyens: « SIGINT », « IMINT » et « PHOTINT » (*Signals*, *Imagery*, *Photographic* Intelligence = renseignement par signaux, imagerie, photographie). En effet, ces methodes ont pris une grande importance ces derniers temps, grâce, entre autres, à de nouvelles plates-formes d'observation spatiale et aux développements dans le domaine des capteurs.[11] Certes, des voix critiques se font entendre pour mettre en garde contre l'exclusivité des composantes purement technologiques.[12] Mais au plan mondial l'importance des organisations qui, s'occupent de la recherche, de la mise à disposition et du traitement de l'information en temps quasi réel et au-delà de toute frontière nationale ou sociale, ne cessera pas de s'accroître.

La guerre psychologique (« Psychological Warfare »)

Cette forme de la guerre de l'information tient compte de l'aspect humain de la guerre de l'information. Le terme « perturbation venue de l'éther » désigne toute forme de propagande. Pour être efficaces, les mesures de propagande doivent être adaptées aux spécificités du groupe cible. Eventuellement, il peut s'avérer nécessaire d'appliquer des techniques de manipulation différentes en fonction du groupe cible. L'influence exercée à travers les médias, par exemple, prend une importance de plus en plus décisive.[13]

---

[11] Cf. sans nom d'auteur (Information Combat, 1995). p. 56.

[12] Mann (Desert Storm, 1994), pp. 4-14: "The US had satellites in place that could and did monitor military activity, but little was known about the regime's intentions. Consequently, there was no consensus on the probability of the Iraqi invasion before it actually occurred. Neither was there a consensus on Saddam Hussein's intentions beyond the occupation of Kuwait." Cf. aussi DiNardo (Cautionary Thoughts, 1995), pp. 69-79.

[13] La citation suivante illustre le rôle joué par les médias dans la perception des conflits par les gouvernements: "Aggressors hire public affairs firms to call attention to themselves, governments pay attention and militaries are invariably drawn into the conflict. The focus of world leaders is directed by the amount of media attention given to a crisis." Morris (Weapons, 1995), p. 17.

La guerre électronique (« Electronical Warfare »)

Cette forme représente l'élément de haute technologie de la guerre de l'information. Traditionnellement, c'est la supériorité dans le spectre électromagnétique qui est visée principalement. En particulier, l'intérêt est focalisé sur le matériel électronique, les logiciels des systèmes de commandement informatisé et les systèmes informatiques. Par ailleurs, la numérisation du champ de bataille et les nouveaux systèmes d'armes font partie de ce domaine.

La guerre de l'information économique (« Economical Information Warfare »)

Cette forme de la guerre de l'information traite de l'influence exercée sur les processus économiques. On peut penser à des manipulations de données boursières, de cours de change et de comptes bancaires qui pourraient provoquer l'effondrement de systèmes bancaires nationaux. La paralysie de certains systèmes de transport informatisés peut entraîner des perturbations importantes du cycle économique sans parler de l´inquiétude générale de la population civile qui pourrait penser que l´Etat est déstabilisé et alors adapter des comportements irrationnels.

La guerre des pirates informatiques (« Hacker Warfare »)

Les intrus dans les réseaux informatiques, appelés « Hacker », « Cracker » ou « Sniffer », exploitent de manière très diverse les failles des concepts de sécurité. Ces pirates informatiques pénètrent illégalement des réseaux protégés et arrivent à manipuler des données, c'est à dire à les modifier ou même à les supprimer.[14] A titre d'exemple, on peut citer la contamination par les dits bombes logiques (« Logical Bombs ») tels que virus, chevaux de Troie, Sweepers, vers, pièges ou par des puces manipulées (« Chipping »).[15]

La cyber-guerre (« Cyber Warfare »)

Ce terme désigne toutes les mesures qui mettent à profit la dépendance de la société vis-à-vis du monde virtuel des données pour prendre à partie des personnes ou des organisations. Les idées de manipulation des réseaux d'information ou de communication, de ce qu'on appelle le cyberespace, sont encore très futuristes et, dans la plupart, du domaine de la science fiction, même au 21^{e} siècle. Le règlement d'un conflit réel sur un micro-ordinateur personnel (« PC ») relève encore de l´imaginaire doit plutôt être considéré comme futuriste, tandis que, par exemple, la simulation du déroulement de conflits pour mieux pondérer les alternatives

[14] Au mois de février de cette année (2000) seulement, des inconnus ont réussi à « pirater » le site web du président américain et ont ainsi déclenché une alerte mondiale dans l'Internet.
[15] Cf. Grier (At War, 1997), p. 23, et Alexander (Digitised Battlefield, 1995), pp. 63-64.

d'action est devenue une réalité, du moins dans un environnement militaire (jeux de guerre (« war gaming »), modélisation (« modelling »)).[16]

L´illustration N° 1 (en annexe) constitue un résumé synthétique des formes principales de la guerre de l'information et de ses différents aspects. Notons qu´il est difficile de faire la distinction entre les formes et les procédures de la guerre de l'information décrites qui sont fonction des technologies utilisées. On observe en effet un chevauchement et une forte interdépendance des formes entre elles.

Afin de ne pas dépasser le cadre du présent mémoire, la restriction suivante est appliquée: les possibilités et évolutions techniques ne seront traitées que dans la mesure où elles auront probablement un impact au niveau du commandement stratégique. Au-delà du plus haut niveau stratégique (politique), le travail est focalisé en particulier – dans une optique propre aux forces armées - sur le niveau de la stratégie militaire. Les domaines d'application très variés de la guerre de l'information aux niveaux tactique et opératif ne seront analysés que dans la mesure où ils peuvent avoir des conséquences pour le niveau stratégique.[17]

3. Rétrospective : L'importance du progrès technique pour le commandement de niveau stratégique

3.1 Avant 1870

Depuis toujours, les développements technologiques ont eu une influence décisive sur la conduite de la guerre. Le chef militaire qui disposait le premier d'une arme plus moderne et plus performante a su, en règle générale, en profiter pour gagner la bataille. Jusqu'au milieu du siècle dernier, il est relativement facile d'apprécier l'influence qu'ont exercée les nouvelles technologies sur la conduite de la guerre car les chefs militaires et les souverains, c'est à dire la guerre et la politique étaient intimement liés. A titre d'exemple, on peut citer l'invention du fusil à aiguille en 1835, qui donna la supériorité à la Prusse (une puissance de feu triplée par rapport aux fusils à baguette) au cours des guerres menées par la Prusse en 1864 (contre le Danemark) et en 1866 (contre l'Autriche).[18] Depuis la guerre de Sécession[19] et au cours de l'industrialisation, qui suivit une différenciation en niveaux stratégique et tactico-opératif fut développée pour aboutir à la conception actuelle.

L'époque post 1871 est étudiée en trois phases.

---

[16] Cf. Kraus (IW in 2015, 1995), pp. 44-45.
[17] L'impact de la guerre de l'information aux niveaux opératif et tactique est analysé dans le détail par exemple par Hutcherson (Command and Control Warfare, 1994).
[18] Cf. Wirtgen (Zündnadelgewehr, 1991), pp. 180-184.
[19] Cf. Längin (US-Bürgerkrieg, 1998).

3.2 1871 – 1918

Pendant cette phase qui comprend aussi la première guerre mondiale, il faut citer comme étant les étapes clés du progrès technique, l'invention du chemin de fer, de la mitrailleuse, du télégraphe, du char de combat et de l'avion. L'extension du réseau ferroviaire à grande échelle a permis à la logistique militaire de mener pour la première fois des opérations de grande envergure. La mise en œuvre de l'arme blindée pendant la première guerre mondiale a certes apporté des avantages au niveau tactique, mais n'avait pas, au regard du dénouement de la guerre, encore une importance décisive au niveau stratégique. Enfin, la mise en service du télégraphe a permis au niveau du commandement supérieur de se détacher du champ de bataille. Malgré la multiplication des capacités de transmission de l'information, les réseaux des unités des transmetteurs sont longtemps restés insuffisamment performants pour permettre une intervention directe dans la bataille.[20] En parallèle, l'intégration du marché mondial fut lancée, car dans le domaine civil aussi, la transmission de l'information s'est accélérée et intensifiée. Ces conséquences dans le monde non-militaire ont de façon surprenante été longtemps négligées par les décideurs politiques.

3.3 1919 – 1945

Pour cette deuxième phase qui se termine à la fin de la seconde guerre mondiale, on peut constater que les inventions de la phase précédente ont pu être mises en œuvre avec succès au niveau opératif. A titre d'exemple, on peut citer la théorie de la guerre éclair, la bataille des chars, le combat interarmes et le commandement par objectif. Les moyens de transmission permettaient au commandement des forces armées par exemple de commander par radio la flotte des sous-marins à l'échelle mondiale. La banalisation des supports d'images et de sons ainsi que de la radio (« Volksempfänger », poste populaire) permettait au régime national-socialiste d'étayer ses objectifs politiques par la propagande. Alors que la fin de la guerre approchait, Hitler espérait encore pouvoir inverser le cours des évènements et éviter la défaite grâce à la mise en œuvre de ses *armes miracles* (« Wunderwaffen »), à savoir une avance technologique d'envergure stratégique. Mais ni la roquette V-2, ni l'avion à réaction Me 262, pour ne citer que les deux armes secrètes du troisième Reich les plus connues, ne purent être produites en quantités suffisantes pour des motifs logistiques.[21] Jusqu'à cette époque, ce n'était pas seulement l'invention en tant que telle, mais l'avance prise dans sa divulgation et rapidité de la mise en œuvre de nouveaux concepts qui décidaient de son succès.[22]

Suite à l'invention puis l´utilisation de la bombe atomique, le scénario de guerre s'est vu bouleversé d'un seul coup. Elle n'a pas seulement

[20] Dans ce contexte, on parle aujourd'hui aussi de « Micro-Management ».
[21] Cf. Ford (Geheimwaffen, 1996), pp. 39-57 et pp. 123-145.
[22] Cf. Dublik (Information Age, 1994), pp. 46-54.

contribué directement à mettre fin à la seconde guerre mondiale dans le Pacifique mais eut également un impact énorme sur la politique de l'après-guerre dans le sens global du terme. En effet, une nouvelle guerre entre les superpuissances put être évitée grâce à la politique de dissuasion stratégique. L'application militaire de la fission nucléaire peut être considérée d'ores et déjà comme le premier *saut technologique quantique* ayant un impact direct sur le commandement stratégique.[23]

3.4 Après 1945

L'invention la plus importante de l'après-guerre est probablement la microélectronique. Elle équipe aujourd'hui la presque totalité des matériels techniques. Renforcée par l'arrivée de la technologie des ordinateurs et en particulier de la technologie de l'information, elle a bouleversé tous les domaines sociaux, politiques et économiques en un temps record. La conduite de la guerre moderne est elle aussi profondément marquée par les nouvelles technologies, du moins à un niveau tactique et opératif.[24]

La transmission de l'information en temps réel par les média permet quasiment à la société civile de participer à une guerre qui n'est plus éloignée du spectateur que sur un plan physique. Ceci influença directement le commandement politique et militaire. Les récents conflits en Somalie et en ex-Yougoslavie ont montré très clairement qu'une avance technologique à elle seule ne suffit plus pour contrer toutes les formes de conflits imaginables. Néanmoins, en raison d'une dépendance accrue vis-à-vis des mécanismes de contrôle complexes de nouveaux risques ont émergé suite à la mise en réseau des systèmes d'information à grande échelle. En ayant recours aux moyens et procédures de la guerre de l'information cités ci-dessus, même des agresseurs de niveau inférieur sur le plan militaire arrivent à exploiter de manière décisive les failles des systèmes des Etats dotés de haute technologie.

Enfin, il a été démontré que les sauts quantiques en technologie ont un impact sur la conduite de la guerre à tous les niveaux. Ils n'ont pas toujours des conséquences directes et immédiates au moment de leur développement mais souvent dans la période suivant de leur divulgation et leur application généralisées (« Know How »). Pour acquérir un avantage stratégique décisif, il est donc impératif d'être le premier à saisir, dans une phase de développement technologique, les potentialités d'application ultérieures d´une nouveauté. Mais encore faut-il avoir la volonté et la capacité de mettre en œuvre et d'appliquer la nouvelle technologie en temps utile. En ce qui concerne l'utilisation de la technologie de l'information, nous nous trouvons déjà dans la phase de la divulgation et de l'application. Depuis des années, les Etats Unis ont pris une nette avance

[23] Cf. Buchholz (Quantensprünge, 1998), p. 9.
[24] L'avance stratégique prise par un des protagonistes grâce par exemple à la mise en œuvre de satellites d'observation ou des dits *armes intelligentes* équipées d'autodirecteurs (« Laser Guided Bombs »), a été démontrée avec grand fracas médiatique pendant la seconde guerre du Golfe.

dans le domaines structurel et conceptuel qu'ils arrivent même à accentuer progressivement. Pour les Etats européens, il importe de rattraper leur retard ou d'éviter au moins que l'écart ne se creuse davantage, tout en respectant ses propres objectifs stratégiques.

Nous pouvons observer que dans la domaine de la technologie de l'information, des poussées d'innovation absolument révolutionnaires qui auront un impact sur tous les domaines d'activités des individus se profilent à l'horizon. Dans leur analyse actuelle, les décideurs doivent en tenir compte dès aujourd'hui afin de pouvoir maîtriser les conséquences futures de *l'explosion de l'information* attendue. L'illustration N° 2 (en annexe) retrace les tendances actuelles en matière de technologie de l'information.

4. La technologie de l'information et ses influences

4.1 Influence sur la société

Dans un avenir proche, la plupart des ménages seront équipés d'un ordinateur personnel (« PC ») qui sera raccordé par des moyens de télécommunication toujours plus performants à des réseaux mondiaux tels que l'Internet.[25] L'utilisation de ces techniques aura une influence accrue sur la vie privée mais surtout sur la vie professionnelle. La réalisation d'achats (« Internet Shopping », « Cybercommerce »), d'opérations bancaires (« Telebanking », « Homebanking ») ou de réservation pour les vacances par ordinateur est devenue monnaie courante pour beaucoup.[26] Le téléenseignement et la télé université sont autant de formes nouvelles qui demandent aux écoles et aux universités le développement de nouveaux concepts pédagogiques. Le travail à domicile relié à l'ordinateur central de l'employeur (« Teleworking ») augmente quant à lui la flexibilité du marché du travail.[27] L'accès aux banques de données ouvertes au grand public, accès spontané, direct et global, pourrait évincer progressivement les média imprimés classiques. Le courrier électronique (« E-Mail ») simplifie également la communication individuelle. Des programmes numériques changeront la qualité des émissions de la radio et de la télévision. Grâce à des lunettes, casques et combinaisons 3-D, qui influe de manière réaliste sur les sensations de l'utilisateur, l'auditeur et le spectateur passifs d'hier auront la possibilité de bouger et d'agir de façon interactive dans des espaces artificiels (« Virtual Reality » (réalité virtuelle), « Cyber Space » (cyberespace)).[28] Grâce à la technologie de l'information, l'ordinateur personnel deviendra le moyen véhiculaire central de l'opinion publique. En même temps, l'influence exercée par les médias classiques diminuera. D'ores et déjà, les entreprises économiques adaptent leur stratégies à

[25] Cf. Gates (Weg, 1995), p. 297 (et suivantes).
[26] Cf. sans nom d'auteur (E-Commerce, 1999), p. 36 (et suivantes), ou Lübbe (Informationsgesellschaft, 1996), p. 7 (et suivantes).
[27] Gates (Weg, 1995), p. 223 (et suivantes) et p. 363 (et suivantes).
[28] Op. cit. p. 192 (et suivantes).

cette évolution en misant sur la vente par voie électronique, les services bancaires et la publicité « on-line ».

Une société fortement informatisée se verra soumise à de nouveaux risques et aura de nouveaux points vulnérables qu'un agresseur potentiel pourrait exploiter par les formes de la guerre de l'information décrites ci-dessus en déstabilisant, paralysant ou détruisant de vastes domaines de la vie d'une communauté. Un autre risque émane de la confiance aveugle qu'ont les citoyens en la véracité de l'information diffusée. Il est possible que, dans la perception subjective des choses, les limites entre la réalité virtuelle et la réalité réelle soient de plus en plus diffuses. Pour que les agences puissent s'imposer dans le flot des informations, le choix et la présentation de l'information qu'elles offriront seront soumis encore plus à la loi du bénéfice. On appelle ce phénomène *effet CNN* qui, à terme, pourrait aller jusqu'à la création délibérée de réalités fictives.[29]

Au niveau des dirigeants politiques, il convient d'en tirer les conséquences, de développer des concepts techniques et de mettre en place des instances de contrôle pour aller à l'encontre de ces menaces. Le débat sur l'interdiction de la diffusion d'images pornographiques d'enfants par l'Internet a démontré néanmoins à quel point des règlements nationaux deviennent caducs en présence d'un réseau mondial.[30] Pour que le contrôle soit efficace, il est donc impératif qu'il soit exercé au-delà des frontières qui séparent les pays et les organisations. Outre la mise en œuvre de mesures techniques et législatives, les dirigeants politiques ont pour tâche principale de développer, en matière de l'information, des concepts crédibles et originaux qui atteignent le citoyen en temps utile, à savoir, au moment où il se forge une opinion sur un sujet. Afin de s'imposer dans la diversité de l'information offerte, on peut imaginer tant des programmes actifs qui s'adressent directement au consommateur de l'information que des programmes passifs qui, en raison de leur attractivité, seront choisis par le consommateur lui-même.

4.2 Influence sur l'économie

Dans le domaine économique, on peut tirer des conclusions semblables. C'est le progrès technologique dans le domaine de la technologie de l'information qui a rendu possible la globalisation tant discutée. L'accès direct aux marchés des finances, des ressources et aux débouchés internationaux est de moins en moins soumis au contrôle national d'un Etat. En parallèle, le commerce de l'information occupe une part toujours plus importante dans le secteur des services qui connaît d'ailleurs une croissance

[29] « Broadcast news create a major new factor in warfare. it can create a fictive, rather than just fictional universe bacause while it can be shown to be true it is not the whole, relevant or contextual truth. There are many small countries involved in small conflicts that could have an interrest in creating a fictive universe in the interest of getting western attention ». Stein (Battlefield, 1995), p. 153 (et suivantes).

[30] Cf. Lübbe (Informationsgesellschaft, 1996), pp. 9,10,21 (et suivantes).

perpétuelle. Depuis de longues années, de vastes domaines de la production sont gérés par la technologie de l'information. Mais même des systèmes de transport et de distribution plus performants et décentralisés sont commandés par des moyens informatisés. Les structures des entreprises évolueront, et pas seulement suite à la décentralisation des postes mentionnés ci-dessus.[31] Rendre disponible la bonne information au bon moment sera la clé du succès pour les entreprises, pas uniquement dans les affaires quotidiennes mais surtout lorsqu'il s'agit de prendre des décisions stratégiques. Il est probable qu'à l'aube du nouveau siècle, l'*information* devienne le facteur de production décisif[32].

Dans le domaine économique, l'application renforcée de la technologie de l'information a entraîné une augmentation des chances mais aussi des potentiels de risques. Les organisations criminelles telles que le cartel international de la drogue, en profitant des possibilités offertes par la guerre de l'information, sont désormais capables de nuire gravement aux économies nationales. Des consortiums économiques tout à fait légaux, ayant acquis en fusionnant un énorme potentiel économique, peuvent, également par des transactions financières ou le choix d'implantation de leurs entreprises, beaucoup influer sur les intérêts politiques de certains pays. Ce phénomène démontre qu'à l'âge de l'information, sur un plan stratégique, des organisations et groupements non-gouvernementaux peuvent également se dresser politiquement contre des gouvernements.

4.3 Influence sur le militaire

Jusqu'ici, dans le secteur militaire, la technologie de l'information joue un rôle important en particulier au niveau tactique et opératif, ce qui fait même parler d'une révolution en matière militaire (« révolution in military affairs »).[33] Outre la mise en œuvre de systèmes d'armes intelligents tels que les missiles guidés par laser ou la munition *tire et oublie* (« Fire and Forget »), c'est surtout dans le domaine de la recherche de l'information (capteurs) et dans celui de la transmission de l'information (systèmes de commandement informatisé) que le plus grands profits ont pu être tirés. A cause du rapide développement technologique, les militaires se voient confrontés aux conséquences de phases de développement et d'expérimentation trop longues. En effet, au moment de leur mise en œuvre, les technologies ne correspondent plus à l'état de l'art technique et se révèlent trop onéreuses.[34] On essaie de contrer ce phénomène en appliquant dans le domaine militaire les technologies développées dans le civil. Les technologies duales, achetées sur étagère, dites de « Dual Use » ou

---

[31] Cf. Gates (Weg, 1995), pp. 225 et 226.

[32] En science économique, les facteurs de production sont tous les biens matériels et immatériels dont la combinaison permet la production ; la théorie classique distingue les trois facteurs *travail, sol* et *capital*.

[33] Cf. Haxlett (Revolution, 1994), p. 71 (et suivantes).

[34] En matière de la technologie de l'information, le cycle de développement dure moins de 18 mois, c'est à dire un système nouvellement acquis sera obsolète au plus tard après un an et demi. Cf. aussi Amt für Nachrichtenwesen der Luftwaffe (Aktuelle Entwicklungen, 1996), p. 19.

« Commercial off the Shelf » risquent d'être beaucoup plus vulnérables aux actions des mesures de la guerre de l'information (cheval de Troie p.e.) que les systèmes développés pour un usage militaire exclusif. Il convient par conséquent de focaliser les efforts sur le développement de mécanismes de protection supplémentaires appropriés.

Le flot d'information s´est accru de façon considérable. A titre d´exemple, pendant la phase de préparation de l'opération « Desert Storm » (tempête du désert), il fallait traiter quotidiennement plus de 700.000 appels téléphoniques, 150.000 télex et 35.000 fréquences.[35] Etant donné ce flot d'information, on n'a pas encore trouvé de réponse satisfaisante à la question de savoir comment il fallait trier les informations importantes pour les traiter au bon moment afin que le décideur militaire puisse les utiliser dans le processus de commandement. Dans ce contexte, on attend beaucoup du développement de logiciels intelligents qui ne soient pas seulement capables de traiter d'énormes quantités de données mais qui sachent aussi, de manière autonome, faire un premier tri des informations. La deuxième guerre du Golfe est communément considérée comme étant la première *guerre de l'information* (« Information War »). Cela s'explique, outre par l'emploi ponctuel de systèmes de roquettes, par la façon dont la guerre fut menée. Pendant la phase préparatoire de tempête du désert, une grande importance était accordée à la recherche et à l'évaluation de l'information afin de permettre une désignation de cibles (« Targeting ») appropriée. Les cibles des premières frappes aériennes furent les capteurs irakiens. Suite à leur destruction, Sadam Hussein était devenu dans une large mesure et même avant le déclenchement des opérations terrestres proprement dites, un commandant aveugle, sourd et muet.[36] Après avoir été découplé par la force du niveau stratégique, le niveau opératif n'était plus en mesure d'agir conformément aux intentions affichées par le niveau supérieur. Une nouvelle qualité dans la manière de mener un conflit est apparu. L'action est dirigée contre la machinerie d'information du commandement adverse afin d'établir un avantage stratégique au profit du commandement ami dans la lutte des forces dans l'espace et le temps. Il faut en particulier mettre en exergue l'importance de la lutte pour la supériorité en matière de l'information.

[35] Cf. Petersen (Krieg der Zukunft, 1995), p. 787.
[36] Op. cit. p. 787.

4.4 Influence sur la politique

Outre les conséquences mentionnées plus haut, au plan politique, ce sont trois tendances fondamentales qui se profilent à cause de l'emploi de cette technologie de l'information. D'abord, le maillage des réseaux et la transmission des données en temps réel réduisent le temps du processus décisionnel et de l'action. Ensuite, les possibilités d'influer sur le raisonnement de l'adversaire ont augmenté à l´instar de celles qui sont capables d'influer sur l'environnement stratégique ami. Troisièmement, à cause de l'exploitation des systèmes d'information intégrés dans des réseaux maillés, les Etats risquent de voir leur fonctionnement détérioré voire leur existence menacée. Cela explique la nécessité d'un commandement plus efficace au plus haut niveau politique et de stratégies aptes au plan *défensif* à assurer la protection contre les nouvelles menaces et capables d'autre part, sur le plan *offensif* de rechercher l'avantage pour imposer ses propres intérêts.

En résumé, on peut dire que la technologie de l'information a un impact sur tous les champs d'application du commandement stratégique. La base de toute gestion stratégique efficace d'un pays fortement informatisé consiste à profiter de toutes les possibilités offertes par cette nouvelle technologie. Une avance prise dans le développement et l'application de la technologie élargit les marges de manœuvre stratégiques. En même temps néanmoins, dans tous les domaines, surgissent de nouveaux risques et de points vulnérables face aux concurrents qui disposent eux aussi des capacités technologiques pour employer les moyens de la guerre de l'information. Parmi eux, il faut compter aussi des groupes de la société et des organisations qui jusqu'à aujourd'hui n'ont guère joué un rôle dans le raisonnement stratégique. Par conséquent, lorsqu'il s'agit de développer les concepts et les structures d'une stratégie globale, il faut accorder une importance toute particulière au phénomène de la *guerre de l'information*, surtout en matière de politique de sécurité.

5. Information - facteur stratégique déterminant

5.1 Définitions

Dans le présent mémoire, le terme *information* désigne la « connaissance sous forme de données, faits et concepts »[37]. Conformément à cette définition plutôt large du terme, l'information désigne la matière brute recueillie qui a déjà fait l'objet d'une évaluation.[38]

Les mongoles avaient déjà expliqué leurs succès politiques et militaires par l'application d'une stratégie qui consistait à connaître le plus précisément possible le raisonnement et les modes d'action de leurs adversai-

[37] Amt für Studien und Übungen der Bundeswehr (Auswirkungen, 1995), p. 28.
[38] Une définition plus étroite du terme est défendue par Mann (Desert Storm, 1994), p. 9.

res. En même temps, leurs propres intentions et techniques étaient soumises au plus grand secret.[39] Le mot de Sun Zi cité en introduction témoigne de l'importance qu'avait l'information dans les affrontements de l'époque : l'acquisition de l'information et l'avance prise sur l'adversaire en la matière, autrement dit, l'information acquise en temps utile et dont la véracité est établie fait depuis toujours partie intégrante de l'analyse de la situation. Elle constitue ainsi un paramètre crucial dans le processus de commandement et de décision, en particulier au niveau stratégique.

Quelles sont aujourd'hui les traits caractéristiques du commandement stratégique et quelle est l'importance accordée à la maîtrise de l'information ? Pour apporter des réponses à cette question, l'auteur se réfère, pour la suite du travail, à la définition de la stratégie proposée par Beaufre. D'après lui, la stratégie est l'art de «la dialectique des volontés employant la force pour résoudre leurs conflits ».[40] Dans ce contexte, la stratégie fait partie de la politique et comprend des moyens politiques, diplomatiques, économiques et militaires. Ses champs d'application sont la politique étrangère et de sécurité, la géo-économie, l'écologie, la technologie, la société, la culture et le militaire.[41] Autrement dit, la stratégie représente les principes d'une planification globale de l'emploi des ressources et instruments existants pour réaliser des objectifs politiques.[42] La stratégie globale est l'art et la science du développement et de la mise en œuvre des forces politiques, économiques, psychologiques et militaires d'une nation en vue d'un soutien maximal de la politique nationale en temps de paix et de guerre.[43]

Le niveau du commandement stratégique, ou plus correctement du commandement stratégique global, correspond donc au niveau gouvernemental de chaque Etat.[44] Dans l'Alliance de l'Atlantique Nord, l'organe correspondant est le Conseil de l'Atlantique Nord (« North Atlantic Council (NAC) »).[45] S'appuyant sur ses instruments militaires, la stratégie militaire, qui fait partie intégrante de la stratégie globale, tient compte des conditions géographiques, économiques, sociales, sociologiques, politiques et technologiques.[46] Le niveau de la stratégie militaire, située à la charnière du niveau stratégique, englobe donc sur le plan national, le ministre de la

---

[39] « Mongol leaders employed cyberwar principles ». Dans ce contexte, « Cyberwar » correspond à la guerre de l'information ; Cf. aussi Fischer (Entwicklungen, 1994), pp. 2 (et suivantes).
[40] Coutau-Bégarie (Traité, 1999), p. 73, Beaufre, André (Kriegskunst, 1964), p. 35, ou Chaliand (Dictionnaire, 1998), pp. 152 - 155.
[41] Cf. Vad (Gesamtstrategie, 1994), p. 290.
[42] Cf. Buchbender (Sicherheitspolitik, 1992), p. 137.
[43] Cf. Ruge (Politik und Strategie, 1967), p. 35.
[44] En Allemagne, il s'agit du Chancelier fédéral et des ministres. En matière de sécurité, la compétence incombe au Conseil fédéral de sécurité (Bundessicherheitsrat), en cas de crise, un état-major de crise est éventuellement mise en place au niveau de la chancellerie fédérale.
[45] Cf. NATO (Handbook, 1998), pp. 35 - 38.
[46] Cf. Buchbender (Sicherheitspolitik, 1992), p. 137.

Défense ainsi que l'organe de commandement militaire suprême.[47] A l'OTAN, il s'agit du Comité militaire (« Military Committee (MC) ») et des Commandants alliés suprêmes (« Major NATO Commanders (MNC) »).[48]

5.2 Les facteurs classiques forces, espace, temps et le facteur information

L'élément central du commandement stratégique consiste par conséquent à faire converger les forces, les moyens, l'espace et le temps sous une idée maîtresse qui dirige l'action pour imposer ses propres intérêts vis-à-vis d'un concurrent ou d'un adversaire. Cela peut se faire de façon active, passive, directe ou indirecte. Le pouvoir stratégique résultait jusqu'à nos jours de la maîtrise des facteurs stratégiques que sont « l'espace », « le temps » ainsi que « les forces » (morales et matérielles).[49] La lutte pour maîtriser ces facteurs fait à la fois partie du niveau opératif et du niveau tactique.[50] La différence se situe sur le plan de ordre de grandeur des moyens et des méthodes.

Tandis que pour Clausewitz, la valeur de l'information pour le succès d'une stratégie avait une moindre importance[51], les possibilités technologiques de l'âge de l'information offrent au commandement stratégique un instrument supplémentaire pour mener une stratégie active. L'exploitation exhaustive et active du facteur de l'information peut même contribuer à surmonter des distances physiques et à substituer des moyens matériels. Tout en réduisant le recours à la violence physique à un minimum, voire en y renonçant complètement, il devient possible de mettre un terme à un conflit ou même de l'éviter. A titre d'exemple, peuvent être cités dans ce contexte, l'avance prise en matière de l'information grâce à des moyens de renseignements plus performants et à la suppression des moyens de renseignement adverses, l'accès à des banques de données, la capacité de vérifier la véracité d'une argumentation pendant des négociations et l'influence exercée sur l'opinion publique chez l'adversaire.

D'un autre côté, il y les nouveaux risques tels que celui de se voir submergé par l'information, d'accuser un retard sur l'adversaire en matière d'information, de voir ses propres arguments vérifiés ou de rendre plus vulnérable son infrastructure et son propre système économique. Les

---

[47] En Allemagne, il s'agit, outre le ministre fédéral de la Défense, qui assure le commandement suprême en temps de paix, du chef d'état-major des Armées (Generalinspekteur) et du Conseil de commandement militaire.

[48] Cf. NATO (Handbook, 1998), pp. 234 -239.

[49] Au 19e siècle, Heinrich Lehr, professeur de stratégie à l'académie militaire impériale russe a déjà constaté ce lien.. « L'interdépendance entre ces éléments (éléments moraux et matériels ; note de l'auteur) et leur combinaison en fonction du temps et de l'espace constituent l'objet de la stratégie qui est la synthèse même de la guerre. » Cf. Fels (Strategiehandbuch, 1990), p. 12.

[50] Cf. Geyso, von (Strategie, 1996), p. 6.

[51] En ce qui concerne la valeur des renseignements, Clausewitz constate dans son premier livre « De la nature de la guerre » : « Une grande partie des renseignements qu'on obtient en guerre sont contradictoires, une partie encore plus grande sont erronés et de loin la plus grande partie sont soumis à une certaine incertitude. » Cf. Clausewitz (Vom Kriege, 1991), p. 258.

gouvernements des pays démocratiques deviennent de plus en plus tributaires de l'opinion publique. Grâce aux médias, la population d'un pays peut participer en temps quasi réel à ce qui se passe sur la scène politique mondiale et aux conflits qui se déroulent dans des théâtres lointains. Le retrait des soldats américains de Somalie en 1994, qui a eu lieu sur toile de fond d'une opinion publique provoquée par la diffusion d'images montrant un pilote américain tué et traîné dans le sable, démontre le pouvoir politique des grandes entreprises médiatiques exercent leur emprise et leur puissance politique sans faire l'objet d'un contrôle parlementaire. Une autre nouvelle dimension que peuvent avoir les conflits, provient de la capacité de petits pays ou des organisations non gouvernementales (O.N.G.), malgré un manque d'instruments conventionnels, à menacer ou attaquer des nations fortement industrialisées en utilisant les différentes formes de la guerre de l'information. Le commandement stratégique, dans ses réflexions conceptuelles et structurelles, doit tenir compte de ces risques.

5.3 La guerre de l'information - une dimension supplémentaire de la guerre terrestre, aérienne et navale

La guerre de l'information apporte une nouvelle dimension à la conduite future des opérations en intégrant les formes de la guerre classique dans ses aspects terrestre, aérienne et navale. A l'avenir, la maîtrise de l'information amie et ennemi revêtira une importance beaucoup plus grande que par le passé et imposeront de nouvelles exigences en matière de gestion de l'information. Ce terme générique de gestion de l'information comprend toutes les mesures visant à recueillir, transmettre, enregistrer, traiter et exploiter l'information. Par ailleurs, la qualité et l'importance de la lutte pour acquérir la supériorité en matière de l'information continueront à changer. La guerre de l'information au niveau stratégique sera caractérisée par la recherche permanente d'une avance décisive dans la possession de l'information stratégique pertinente. Par conséquent, il convient de compléter les facteurs stratégiques classiques cités ci-dessus par le facteur « information » qui sera placé sur le même pied d'égalité que les autres. A l'avenir, la capacité d'acquisition de la « supériorité en matière de l'information (Information Dominance) » sera peut-être le critère prédominant de la future stratégie gagnante.

6. L'importance stratégique de la guerre de l'information

6.1 Les objectifs stratégiques

Il a été démontré que les différentes formes et procédures de la guerre de l'information confèrent au commandant stratégique un instrument supplémentaire, qui lui permet de prendre un avantage stratégique en matière de recherche et de maîtrise de l'information pour faire valoir ses propres inté-

rêts. Ceci suppose la définition d'un objectif stratégique, c'est à dire la définition de ses propres intérêts.

Tandis que, aux Etats Unis par exemple, en 1996, les objectifs stratégiques ont fait l'objet d'une révision dans le cadre de la « National Security Strategy »[52], qui met en relief les nouveaux défis. Ceux-ci résultent de l'emploi de la technologie de l'information moderne au niveau stratégique ; en Allemagne, la définition explicite des intérêts et objectifs nationaux s'inscrivant dans une stratégie globale fait encore défaut. Le débat allemand sur la stratégie est régi par trois facteurs : « l'identité politique », « le rôle technologique et économique » et, en matière de politique étrangère et de sécurité, « l'intégration dans des structures internationales ».[53] Les valeurs et intérêts qui en découlent ont été formulés dans les Directives de politique de défense, publiées par le ministère de la Défense en 1992, et dans le Livre blanc du gouvernement fédéral de 1994.[54] Les lignes directrices des deux documents sont la démocratie, la stabilité, la protection, la modération et l'intégration. Les dirigeants politiques s'engagent à respecter ces valeurs qui constituent le cadre du champ d'action des hommes politiques dans les domaines de la société, de l'économie, de la politique étrangère et de sécurité ainsi que dans le domaine militaire. Les objectifs en matière de stratégie militaire nationale allemande n'ont pas encore fait l'objet d'un document publié séparément. Il est néanmoins possible de les déduire, tout comme le rôle et la mission des forces armées d'ailleurs,[55] des documents cités ci-dessus. Tandis qu'à l'après-guerre, l'action stratégique allemande était imprégnée surtout par une certaine retenue ; aujourd'hui, elle est caractérisée par une plus grande conscience d'elle-même et une mise en valeur plus claire des intérêts nationaux.

Le Concept stratégique de l'OTAN reprend, au niveau de l'Alliance, les objectifs nationaux. Les principes de sauvegarde de la paix, de la sécurité et de la stabilité en maintenant les liens transatlantiques et l'équilibre stratégique global, ont gardé toute leur validité. La déclaration de Rome, qui traduit l'approche très vaste qu'a l'OTAN d'une architecture de sécurité, tient compte de la nouvelle donne et dépasse l'ère post guerre froide (« Post-cold-war-era »). Elle reconnaît que la sécurité repose

---

[52] Ces objectifs sont regroupés sous le titre « Advancing our Interests Through Engagement and Enlargement ». Les Etats Unis justifient leurs objectifs par leur aspiration à un rôle de suprématie mondiale, légitimée par leur énorme pouvoir économique et militaire et la force de leurs valeurs démocratiques. Pour faire valoir leurs intérêts stratégiques, les Etats Unis s'engagent à employer des moyens pacifiques. Sur le plan de la stratégie militaire, ils maintiennent en même temps une forte capacité défensive, avec une présence à l'échelle mondiale, dans le but de dissuader d'éventuels agresseurs. Cf. chapitre II, White House (National Security strategy, 1996), p. 1 (et suivantes).

[53] Cf. Geyso (Strategie, 1996), p. 104.

[54] Cf. Bundesregierung (Weissbuch, 1994).

[55] Les missions de la Bundeswehr sont les suivantes : elle protège l'Allemagne et ses citoyens face au chantage politique et aux dangers extérieurs, elle apporte son soutien à la stabilité militaire et à l'intégration de l'Europe, elle défend l'Allemagne et ses Alliés, elle sert la paix mondiale et la sécurité internationale, en harmonie avec la charte des Nations Unies et elle apporte son aide en cas de catastrophes, assure des missions de sauvetage et soutient les actions humanitaires.

tant sur des aspects économiques, sociaux et environnementaux que sur une capacité de défense militaire. Voilà pourquoi la politique de sécurité de l'Alliance est fondée sur le dialogue, la coopération et la capacité de défense collective.[56] Sur le plan de la stratégie militaire, cela signifie le maintien d'une capacité de défense nucléaire et conventionnelle, y compris les structures militaires intégrées qui ont été adaptées au nouvel environnement stratégique. Désormais, il sera possible de réagir aux nouveaux conflits ou crises potentiels avec un volume réduit, certes, mais avec plus de flexibilité, une mobilité accrue et une structure adaptée.

Sur cette toile de fond, on peut évaluer les contraintes et les champs d'action des dirigeants politiques dans le domaine de la protection contre les nouveaux risques relatifs à la mise en œuvre de la guerre de l'information. Si on évoque l'élargissement du rayon d'action politique grâce à l'utilisation de la technologie de l'information moderne, celui-ci reste cependant restreint à cause des limites fixées par les stratégies globales des nations ou des alliances.

6.2 Les risques et conflits potentiels du 21e siècle

Les risques et conflits potentiels du 21e siècle peuvent être divisés essentiellement en trois catégories principales. Outre les conflits *classiques* inter-étatiques, il faut citer les conflits ayant des motifs ethniques nationalistes, religieux, idéologiques, historiques et/ou socio-économiques et qui, dans la plupart des cas, sont des conflits intra-étatiques. S'y ajoutent les risques potentiels qui résultent des grandes différences dans les niveaux de développement technologique des pays ou des groupes.

Les conflits inter-étatiques sont caractérisés par des protagonistes qui disposent de structures étatiques existantes, d'un leadership politique ayant des objectifs stratégiques, d'un monopole central du pouvoir et enfin, d'une culture de conflit qui, du moins dans la théorie, respecte les règles du Droit international. Bien que la plupart des Etats se soient engagés à régler leurs conflits par des moyens pacifiques, certains Etats défient toujours d'autres nations ou des alliances avec des moyens militaires. La guerre des Malouines, le conflit Iran-Irak, l'annexion du Koweït par l'Irak, les conflits armés entre l'Inde et le Pakistan à propos du Kashmir ou le conflit qui oppose les deux Etats coréens ne sont que quelques exemples de cette forme de conflit. Le règlement des conflits par des moyens pacifiques fait partie intégrante des objectifs stratégiques des démocraties fortement industrialisées. Afin d'y parvenir dans le cadre de ce type de conflit, il faut avoir en permanence une avance technologique permettant de dissuader à priori un agresseur potentiel tenté par le recours à la violence. Si, malgré tout, un affrontement militaire ne peut pas être évité, il faut disposer de suffisamment de capacités militaires permettant de contrer l'agression sans (*zéro morts*) ou avec un minimum de pertes. Quand le commandement stratégique dispose d'une avance technologi-

[56] Cf. NATO (Handbook, 1998) ; p. 59 (et suivantes).

que dans le domaine des armes intelligentes et dans l'application des différentes formes et procédures de la guerre de l'information, il est en mesure d'influer de manière décisive sur le déroulement des conflits comme en témoigne l'exemple de l'opération « Desert Storm ».

Depuis la fin de l'antagonisme est-ouest, l'importance de la deuxième catégorie de conflits a considérablement augmenté. Le grand nombre de conflits qui se déroulent en Afrique, sur les Balkans et dans les Etats de l'ex-U.R.S.S. témoigne de la brutalité avec laquelle s'affrontent les intérêts divergents. Ce type de conflit, dénommé le *choc des civilisations* (« Clash of Civilizations ») par Samuel Huntington[57], est souvent marqué par l'absence ou la disparition de structures étatiques et par l'inexistence d'un pouvoir efficace. Dans ce genre de conflits, les pays occidentaux, dont la politique vise la stabilité, le règlement pacifique des conflits et la protection des droits de l'homme, tiennent plus fréquemment un rôle de médiateur que d'acteur. A la table des négociations, les hommes politiques se voient souvent confrontés à des « seigneurs de la guerre (Warlords) » au comportement irrationnel. Dans un tel contexte, le commandement stratégique, pour faire valoir ses intérêts, doit employer ses instruments d'une manière complètement différente de celle utilisée dans des conflits classiques. L'engagement militaire, si jamais il a lieu, change en effet de qualité. L'emploi des technologies d'armement modernes ne joue qu'un rôle secondaire dans des conflits dominés par l'utilisation de kalachnikovs ou de machettes. En ce qui concerne la technologie et la gestion de l'information pourtant, la situation se présente différemment. Il devient par exemple beaucoup plus simple de diriger des négociations si les différentes déclarations des parties prenantes peuvent être vérifiées sans perte de temps par un réseau de communication performant que lorsque ces négociations ne reposent que sur la confiance mutuelle.

La troisième catégorie de conflits et de risques potentiels résulte, d'une part, des différences dans le développement technologique des civilisations et, d'autre part, du fait que des agresseurs potentiels, bien que ne disposant pas eux-mêmes d'un pouvoir économique ou militaire, arrivent à menacer des pays fortement développés en utilisant les technologies de pointe des différentes formes de la guerre de l'information. Cette théorie des conflits repose sur le modèle développé par Alvin et Heidi Toffler[58], qui a suscité un grand intérêt même au-delà des frontières des Etats Unis. D'après cette théorie, l'évolution complète des civilisations s'est faite en deux vagues, l'une agricole et l'autre industrielle. Les pays fortement industrialisés se trouvent au seuil d'une troisième vague, celle de l'ère de l'information. L'illustration N° 3 (en annexe) illustre le raisonnement des frères Toffler. En ce qui concerne l'évolution globale, la théorie dit que, pour un moment donné, les différentes civilisations sur terre atteignent différents états d'avancement dans leur développement. En fonction de

[57] Cf. Huntington (Clash of Civilizations, 1996), p. 22 (et suivantes).
[58] Cf. Toffler (War and Antiwar, 1993), p. 18 (et suivantes).

cet avancement, chaque civilisation a besoin d'un laps de temps spécifique avant d'entamer l'ère de l'information appelée « la troisième vague ».

D'après la théorie, le monde du 21e siècle, en ce qui concerne son niveau de développement, serait tripartite. D'un côté, il y aurait les civilisations progressistes appartenant en particulier à l'hémisphère occidental, qui disposent déjà des capacités de *l'âge de l'information* et qui continuent à les développer. D'un autre côté, il y aurait des civilisations appartenant encore à *l'âge industriel*, donc à la deuxième vague. Dans une certaine mesure, il y aurait également des sociétés qui se trouvent encore au niveau de développement de *l'âge agricole*. Enfin, entre ces niveaux, il y aurait des pays au seuil du niveau suivant qui, en fonction de leurs ressources, pourraient à terme franchir l'étape suivante. Le volume que prendrait le transfert technologique pourrait accélérer le développement du pays en question. Ce seraient ces différences dans le développement qui généreraient de graves conflits potentiels. Au sein des sociétés mêmes, on aurait affaire à des conflits résultant surtout de leur résistance au changement. Sur la scène internationale, il faudrait s'attendre en particulier à des conflits qui opposeraient, surtout pour des motifs économiques, les pays de la troisième vague aux pays moins développés. Eventuellement, des affrontements pourraient même apparaître mettant en cause des pays de la deuxième vague qui se servent déjà des moyens propres à l'âge de l'information, tels que des moyens de la guerre de l'information.[59] Certaines nations appartenant à la première ou à la deuxième vague pourraient tenter de compenser la supériorité des pays de la troisième vague en renforçant l'utilisation des moyens innovateurs des technologies de communication et d'information.

Par ailleurs, la théorie sur les conflits développée par les frères Toffler ne fait pas l'unanimité. Il faut notamment veiller à ne pas effectuer d'interpretation trop manichéiste des futurs scénarios de conflits.[60] En particulier, il est reproché à ce modèle de ne pas avoir prouvé la causalité du phénomène. La question se pose en effet de savoir si le modèle est vraiment apte à fournir des explications concernant les causes des conflits. Il faut aussi remettre en question l'hypothèse selon laquelle les seules différences de niveau dans le développement technologique des sociétés suffisent à provoquer des conflits. Pour autant, les propos sur la nouvelle forme que prendront les conflits peuvent faciliter une approche stratégique. Les dirigeants des pays disposant des technologies de pointe doivent donc focaliser leurs efforts en matière de politique économique et de recherche pour franchir le plus tôt possible le seuil de la troisième vague et maintenir leur avance technologique. Il importera par ailleurs de promouvoir les pays en voie de développement et les pays intermédiaires par une politique modérée dans les domaines de la sécurité, de l'économie et de l'aide au développement pour qu'ils se considèrent comme étant des par-

[59] Op. cit. p. 64 (et suivantes).
[60] Cf. DiNardo (Cautionary Thoughts, 1995), p. 70.

tenaires dans le processus du développement et non pas des concurrents perdants.

Le transfert technologique et la politique de l'information sont des piliers importants de cette stratégie. Comme il ne sera cependant pas toujours possible d'aboutir dans ces deux domaines, il convient, dans une première phase, d'identifier les risques découlant d'un éventuel échec et, dans une deuxième phase, de mettre au point des stratégies pour les maîtriser. Contrairement aux deux premières catégories de conflits, le camp des adversaires potentiels s'est élargi et comporte des organisations non-gouvernementales criminelles voire terroristes, des cartels économiques ou de la drogue, mais aussi des Etats à faible développement technologique parfois tout aussi criminels. Les menaces potentielles émanant de ces acteurs, des menaces tous azimuts, se dirigent tant contre les dirigeants, les ressources, l'infrastructure et la population d'un Etat que contre ses forces armées.

En conclusion, on peut dire que les trois catégories de conflits peuvent toutes se distinguer les unes des autres. S'il est difficile de déterminer clairement les causes des conflits et s'il faut admettre que certains types de conflits se superposent, le mode et l'intensité des conflits sont fonction de leur catégorie. L'importance de la technologie utilisée dépend également du type du conflit. Dans toutes les catégories de conflits, les agresseurs peuvent se servir des réseaux de communication globaux, qui ne sont soumis ni à un contrôle étatique ni social, pour attaquer « le talon d'Achille » des Etats à technologies de pointe. Des attaques menées contre les mécanismes informatisés de contrôle et de régulation de l'infrastructure étatique, contre des centrales d'énergie, des installations de communication ou des centres médiatiques, des incidents provoqués dans des systèmes de transport complexes, une paralysie dans des domaines économiques ou financières clés sont autant de facteurs qui peuvent déstabiliser des pays. Pour l'instant, on estime que le nombre de pays disposant d'ores et déjà de la technologie de l'information nécessaire à la mise en œuvre de la guerre de l'information s'élève à plus de cent. Dans ce contexte, on parle même d'une « seconde menace stratégique »[61], en parrallèle à la menace nucléaire. Par rapport à celle-ci, la différence fondamentale consiste dans le fait que les pays hautement développés, maîtrisant au mieux la guerre de l'information, soient en même temps les plus vulnérables.[62] Les formes de conflits classiques caractérisés par la violence physique pourraient évoluer, du moins en partie, vers des affrontements marqués par la violence immatérielle. Les forces armées conventionnelles ne seront plus placées au centre de l'intérêt, à moins que celles-ci ne s'adaptent tant au niveau conceptuel que structurel.

---

[61] Amt für Nachrichtenwesen der Luftwaffe (Aktuelle Entwicklungen, 1996), p. 4.
[62] Cf. Müller (Informationszeitalter, 1996), p. 8.

Sur le plan du commandement stratégique des pays à technologies de pointe, la vulnérabilité accrue demande une prise en compte des nouveaux risques émanant des nouvelles catégories de conflits en profitant des formes et des procédures offertes par la guerre de l'information. Il existe d'une part une réaction purement défensive qui consiste à prendre des mesures de protection contre les armes intelligentes de l'adversaire et à assurer en permanence la protection des systèmes économiques, de commandement et d'infrastructure amis contre les attaques ennemies. D'autre part, la guerre de l'information peut signifier aussi la nécessité d'une capacité d'action offensive pouvant s'étendre jusqu'à l'emploi des forces armées avec leur équipement hautement sophistiqué. Là encore, pour ce faire, des objectifs stratégiques clairs ainsi que des concepts et des structures dans les Etats et enfin des alliances pour les réaliser sont indispensables. Les responsabilités et les rôles deviennent flous et ne peuvent donc plus être attribués à des domaines isolés. La coopération et des institutions globales s'imposent.

6.3 Les facteurs d'influence au niveau du commandement stratégique

Les différents facteurs d'influence au niveau du commandement stratégique sont fonction de l'environnement complet du décideur. Nombreux sont les variables qui échappent dès à présent à l'accès et donc au contrôle de l'Etat national. L'illustration N° 4 (en annexe) est une illustration de la complexité des interdépendances.

Les *champs d'action stratégiques* d'un Etat résultent de son environnement stratégique qui peut restreindre mais aussi les élargir. Il existe des facteurs d'influence qui favorisent l'exercice du pouvoir étatique et il y en a d'autres qui le limitent. Ces facteurs peuvent certes être classifiés dans des catégories de politique intérieure, étrangère ou globale, mais en même temps, ils sont placés dans une interdépendance permanente et directe. Si, par exemple, une entreprise économique privée a l'intention de conclure avec un partenaire international un marché ayant un impact négatif sur le site économique ou menant à une perte d'emploi dans un des pays, les médias, la population et les groupes de pression du pays concernés ne tarderont pas à exercer une pression massive sur leurs dirigeants politiques afin de mettre en échec ce marché international. Dans le cas contraire, une politique économique nationale trop protectionniste fera très vite l'objet de vives critiques de la part des médias et des groupes de pression d'autres pays ; sur la scène internationale, le gouvernement ainsi critiqué sera mis sous pression, et des conflits inter-, mais aussi intra-étatiques ne seront plus à exclure.

Dans ce contexte, il faut regarder de plus près le rôle particulier que jouent les médias en tant que facteur d'influence au niveau stratégique. Les médias (la télévision, la radio, les journaux) ont un accès direct à la presque totalité des ménages. Il est cependant souvent impossible ou très

difficile de vérifier l'authenticité et l'actualité des informations traitées d'une manière sélective. Malgré cela, ils représentent souvent le seul moyen permettant de faire connaître les décisions gouvernementales au grand public national et international. Puisque notamment les médias privatisés jouissent dans leur travail journalistique d'une grande indépendance politique, un des défis à relever par le commandement stratégique consiste à mettre au point des concepts médiatiques efficaces. Le travail journalistique des médias visent à obtenir des parts de marché, un certain tirage, donc à réaliser du bénéfice et par ailleurs la volonté des décideurs de se présenter le plus positivement possible, sont à l'origine d'un conflit entre les médias et le dirigeant politique.[63] Un concept médiatique efficace développé par un Etat devrait reposer sur l'équilibre entre un *code de déontologie* auquel souscrivent volontairement les médias et des règles légales contraignantes tout en garantissant le libre accès même à des domaines sensibles. Des règles trop restrictives telles que des contraintes à la libre circulation, l'application de règles d'accréditation trop sévères voire la censure étatique sont à l'origine d'un travail journalistique partial caractérisé par la méfiance réciproque et des procès d'intentions.[64]

Tout commandement stratégique digne de ce nom connaît les mécanismes régulateurs, anticipe sur les développement menaçants et développe en temps utile - individuellement ou dans des coalitions politiques et des alliances internationales - des concepts afin de faire valoir ses propres intérêts au maximum grâce à une politique de l'avance et de l'équilibre. Cette exigence, formulée de manière quelque peu abstraite, vaut bien sûr pour tous les champs d'action, y compris donc pour la politique de sécurité. Suite au maillage de plus en plus étroit des réseaux de communication et d'information modernes et à la dissolution progressive des structures étatiques nationales, la complexité de l'environnement stratégique d'un Etat ne cesse de croître. Tout point d'accès à un réseau, chaque nœud dans les réseaux de communication permet d'une part la recherche et la transmission rapides de l'information, et, d'autre part, il rend également possible l'application des mesures de la guerre de l'information. Le degré de vulnérabilité, qui, comme cela a été démontré auparavant, a considérablement augmenté, ou les délais de réaction extrêmement réduits sont autant de défis à relever dans le processus décisionnel stratégique qui nous étudierons par la suite.

6.4 L'importance de la guerre de l'information pour le processus décisionnel

La méthodologie de la prise de décision stratégique s'effectue dans un cycle régulateur auquel les militaires sont familiarisés et comprend les phases bien connues *constat de la situation*, *l'évaluation de la situation*, *déci-*

[63] Cf. Reeb (Kampf um Informationen, 1991), pp. 1, 5 (et suivantes).
[64] La discussion à propos de la politique médiatique menée pendant la guerre du Golfe est un exemple parlant de ces déficits. Cf. par exemple Beham (Kriegstrommeln, 1996) ou MacArthur (Schlacht der Lügen, 1993).

sion et mise au point de la stratégie, *réalisation* et finalement *contrôle,* suivi par une nouvelle évaluation de la situation. L'illustration N° 5 (en annexe) reprend en modèle le processus décisionnel stratégique.

A l'âge de l'information, c'est en particulier le *constat de la situation* qui dépend dans une large mesure des technologies utilisées. La technologie permet qu'une situation soit perçue à l'échelon mondial (« Global Situational Awareness ») en temps quasi réel et en incluant tous les champs d'action stratégiques. Dans ce contexte, la composante de la guerre de l'information qui repose sur le renseignement (« Intelligence Based Warfare ») joue un rôle particulier dans le but de prendre une avance pour ce qui est du recueil de l'information. Dès cette première phase, toutes les voies par lesquelles transitent les flux d'information dans le cadre de la transmission de données se réunissent et forment ainsi le talon d'Achille vis-à-vis d'éventuelles attaques contre les systèmes d'information amis. Il importe donc, dès cette étape, de contrer les attaques ennemies contre les données et les logiciels de traitement amis. Un autre problème qu'on sous-estime encore souvent est causé par l'introduction de l'information dans notre système. Puisque ce n'est que l'information pertinente et, en plus, disponible en temps utile qui permet d'avoir un avantage d'information exploitable et de prendre les bonnes décisions, l'analyse et le traitement de l'information doivent notamment répondre à des critères d'efficacité.[65] Ainsi apparaît la nécessité d'établir un ordre de priorités de l'information stratégique pertinente. Cependant le tri dans l'information ne pourra pas être effectué par le seul système *homme*. Dans ce domaine, des logiciels intelligents, qui aident à gérer les flots d'information selon des critères de tri prédéfinis, peuvent être mis en œuvre.

L'*évaluation de la situation* est un processus principalement cognitif. Dans cette deuxième phase, le décideur stratégique est assisté par des états-majors conseillers qui, eux, fournissent des contributions à la préparation de la décision en établissant par exemple des analyses de risques. En pondérant les chances et les risques, l'évaluation stratégique de la situation s'inscrit premièrement dans une approche globale et doit tenir compte de la complexité de l'environnement stratégique décrite ci-dessus. L'évaluation de la situation débouche sur des alternatives de réaction, dont il faut analyser les chances d'aboutir. Pendant cette phase, le rôle de la technologie de l'information est double : d'une part, en se servant de l'intelligence artificielle et des techniques de simulation, les organes conseillers disposent d'outils permettant d'évaluer les événements et la probabilité d'un succès, d'autre part, par les moyens de communication,

[65] Si, pendant la seconde guerre mondiale, le transfert de données par télexe ne comprenait que 66 mots par minute, pendant la guerre du Golfe, les ordinateurs transmettaient 192.000 mots par minute. La maîtrise de ces flots d'information s'est avérée par ailleurs comme étant un des problèmes cruciaux du conflit. Cf. sans nom d'auteur (Bits & Bites, 1996), p. 204, et Mann (Desert Storm, 1994), p. 8.

l'environnement stratégique peut influer directement sur le processus décisionnel en cours.[66]

Une fois que la décision a été prise, dans une troisième phase, il faut *formuler la stratégie*. Dans la quatrième phase, il faut *mettre en œuvre* par les responsables politiques compétents qui en déduiront concepts, structures et directives. A plusieurs reprises, l'importance fondamentale de la politique de l'information a été mise en relief. Dans ce contexte, l'idée de créer un ministère responsable en la matière mérite encore plus d'attention.

L'emploi de la technologie de l'information moderne augmente aussi considérablement l'efficacité de la cinquième et dernière phase, la phase du *contrôle*. Grâce aux sondages d'opinion, on peut dire, par exemple, comment sont accueillies des décisions stratégiques. Le développement des cours des actions et des devises sur les marchés internationaux, qui sert d'indicateur pour le succès des décisions économiques stratégiques, constitue un autre exemple.

Le processus décisionnel stratégique est donc soumis à l'influence croissante de la technologie de l'information, y compris ses chances et ses risques. Ayant fait ses preuves, le déroulement du processus décisionnel reste certes essentiellement inchangé, mais l'application des procédures d'évaluation, d'analyse et de mise en œuvre continuera à le modifier progressivement. La course à l'avantage décisif en matière de l'information changera en particulier le facteur *temps*. Un dit *créneau d'opportunité* (« Window of Opportunity »), qui ne se présente que pendant une courte durée, impose une réaction rapide, tout comme des risques émanant d'un *créneau de vulnérabilité* (« Window of Vulnerability »). Les cycles de prise de décision auront donc tendance à s'accélérer.[67] Voilà pourquoi, les décisions d'une moindre envergure doivent être prises de plus en plus à des niveaux décentralisés. Le système *homme* devenant de plus en plus le facteur critique, il faudrait que le décideur stratégique et ceux qui préparent ses décisions (états-majors) répondent à des critères plus exigeants. Les décisions ne sont pas seulement prises de plus en plus vite mais aussi sur de grandes distances, et ces décisions sont constamment soumises à l'appréciation des médias internationaux présents en permanence. Outre la capacité de se concentrer sur les décisions stratégiques pertinentes, il faut avoir en particulier le « talent de prendre sa décision en temps utile », une aptitude qui fut déjà mise en évidence dans des siècles antérieurs.[68]

---

[66] Cf. Fels (Strategiehandbuch, 1990), p. 481.
[67] Cf. Sullivan (Land Warfare, 1993), p. 51, et sans nom d'auteur (Russian Views, 1994), p. 45.
[68] Cf. Clausewitz (Vom Kriege, 1991), p. 359.

6.5 La réalisation des buts stratégiques à l'âge de l'information

A la lumière de ce qui a été dit jusqu'ici, quatre conditions doivent être réunies pour mettre en œuvre les objectifs stratégiques fixés. Outre la *volonté* politique d'exprimer ses propres intérêts puis de les réaliser dans un environnement stratégique donné, il faudra que les *moyens* appropriés soient disponibles, que des *concepts* et des *structures* existent et que soit maintenue l'*avance prise dans la lutte relative aux facteurs stratégiques* que sont les forces, l'espace, le temps et l'information.[69]

La condition sine qua none pour développer sa propre *volonté* est l'état d'esprit du chef stratégique, ce que Clausewitz a appelé les « valeurs morales »[70]. La perception d'une situation stratégique doit initier une résolution. Cette capacité requiert une méthodologie adéquate et des instruments d'analyse appropriés. L'objectif prioritaire doit être d'influer sur la perception et la résolution de l'adversaire en question pour les diriger dans le sens souhaité. Comme pour une approche tactique, les adversaires stratégiques tenteront d'appliquer des éléments tels que *la ruse* ou *la surprise*.[71] Là aussi, la mise en œuvre des moyens de la guerre de l'information offre de nouvelles possibilités technologiques. On peut imaginer par exemple d'introduire une situation synthétique dans le système d'information de l'adversaire en l'incrustant dans la situation réelle pour la remplacer complètement ou partiellement (« Electronical Warfare »).

Certes, les *moyens* classiques pour faire valoir sa volonté au niveau stratégique persisteront, mais ils seront élargis par toute la gamme des moyens de la guerre de l'information. Même à l'âge de l'information, un principe bien connu gardera toute sa valeur : « La force suffisante doit être concentrée sur le point décisif ».[72] Même si l'on ne dispose pas de la technologie de la dernière génération, il est possible d'infliger des pertes décisives à un adversaire dès lors qu'on a procédé auparavant à une analyse précise de ses failles.[73] Si un acteur arrive à percer les dispositifs de protection adverses, il pourra faire valoir ses intérêts stratégiques grâce à l'application des moyens de la guerre de l'information, même si, d'un point de vue technique et conventionnel, cet acteur est clairement en position inférieure.

Une fois que la volonté politique a été définie, que la stratégie globale a été formulée et que les dirigeants stratégiques disposent d'instruments suffisants pour exercer leur pouvoir, il importera que, dans la phase suivante, les différents responsables aux niveaux subordonnés développent *les concepts et les structures* en vue de la mise en œuvre des moyens. Maintenir *l'avantage* pris sur l'adversaire en termes de *for-*

---

[69] Dearth (Information War, 1997), p. 11 (et suivantes).
[70] Clausewitz (Vom Kriege, 1991), p. 356 (et suivantes).
[71] Op. cit. pp. 385 et 379.
[72] Op. cit. p. 403.
[73] Cf. Amt für Studien und Übungen der Bundeswehr (Auswirkungen, 1995), p. 45.

ces, espace et *temps* reste une tâche permanente. A l'âge de la technologie de l'information, ces intentions sont cependant complétées voire supplantées par le facteur *information*. Seul le dirigeant stratégique qui, au cours du processus décisionnel, dispose de la bonne information au bon moment, aura une marge de manœuvre élargie et saura employer de manière prometteuse ses dispositifs dans l'espace et le temps. Les concepts et les structures devront répondre de plus en plus répondre à la nécessité de prendre un *avantage dans le domaine de l'information.*[74] Etant donné que le développement technologique continuera, le seul avantage quantitatif ou qualitatif ne suffira plus. Pour être sûr du succès au niveau stratégique comme au niveau opératif, il sera désormais indispensable de viser la *supériorité globale dans le domaine de l'information*.

La réalisation des objectifs stratégiques à l'âge de l'information répondra donc aux principes classiques de la théorie stratégique, mais ces principes seront progressivement complétés ou imprégnés par l'aspiration à la supériorité globale dans le domaine de l'information. Les facteurs qui influent sur le commandement stratégique auront une autre valeur. A l'heure actuelle, la *gestion de l'information* (« Information Management ») est assurée individuellement par les différents ministères, mais on ne peut plus exclure que, suite à l'élargissement des champs d'action stratégiques, un ministère complet s'occupe exclusivement de la *politique de l'information*.

7. Conclusion

Bien que le débat théorique sur le facteur *information* ne soit pas fondamentalement nouveau, il faut reconnaître que de profonds changements dans tous les domaines de la société se dessinent au seuil du 21e siècle en raison de l'accélération du développement de la technologie de l'information.

Ces changements affectent également le niveau du commandement stratégique, car la guerre de l'information risque d'avoir lieu partout où la technologie de l'information est présente ! Certes, la guerre de l'information est dirigée en premier lieu contre les forces armées, mais aussi contre les structures civiles des sociétés à technologies de pointe, ce qui les rend très vulnérables. Non seulement de nouveaux risques potentiels émergent mais apparaissent également de nouvelles méthodes de

[74] Là aussi, les Etats Unis sont les pionniers. Les Etats Unis n'ont pas seulement reformulé leurs objectifs stratégiques, mais, en matière de guerre de l'information, ils sont également en train de créer les structures censées développer des programmes défensifs et offensifs. Les institutions CIA, DIA, NSA, CIO, DISA, DOD et des établissements civils tels que le FBI, le DOJ et le DOE participent au développement de ces programmes (pour les abréviations voir en annexe). Un « Centre de la guerre de l'information » (« Information Warfare Center »), doté d'un budget annuel d'un milliard de dollars environ, a été mis en place il y a quelques années au sein de la NSA par exemple. Cf. Amt für Studien und Übungen der Luftwaffe (Aktuelle Entwicklungen, 1996), p. 5 (et suivantes).

conduite de conflit. Cette menace pour le citoyen individuel, ses valeurs, ses normes juridiques et son système économique demande un élargissement du concept traditionnel de sécurité. Puisque les nouveaux risques de l'âge de l'information menacent les domaines les plus divers au-delà de toutes les frontières, une stratégie globale s'impose, une stratégie avec une expression des besoins conceptuels et structurels en matière de guerre de l'information qui permette une convergence des forces et des moyens. Une *manie de l'information* (« Information Mania ») n'est cependant pas de mise.

En revanche, l'application de la technologie de l'information offre aussi l'opportunité de prévenir des conflits et de contribuer à les résoudre avec des moyens pacifiques. Au niveau stratégique, il importera d'en tenir compte pour que les objectifs politiques puissent être réalisés. A l'avenir, l'information sera le facteur stratégique décisif. Dans ce contexte, la guerre de l'information constitue la forme la plus agressive de la course à l'information. Au niveau stratégique, la lutte permanente pour prendre l'avantage dans la détention de l'information à valeur stratégique sera au cœur de l'action. La guerre de l'information sera la plus efficace chaque fois qu'elle dissuadera un agresseur potentiel de s'engager dans un conflit, grâce à la mise en place de protection de qualité.

Pour y arriver, des capacités technologiques, des stratégies offensives et défensives ainsi que des concepts, des mécanismes décisionnels et des structures d'organisation interministériels et entre les alliances sont indispensables. Ces éléments doivent converger et être optimisés au niveau des centres décisionnels et tenir compte de l'environnement stratégique complet du décideur. Une approche du haut vers le bas (« Top-Down-Approach ») où le développement de concepts stratégiques sert de base à l'élaboration de concepts opératifs individuels est souhaitable. Leur réalisation concrète demandera encore un travail de recherche et d'étude intense. Dans ce contexte, les partenaires européens de l'Alliance ont tout intérêt à rechercher une étroite coopération transatlantique.

« Soumettre l'ennemi sans combattre est ce qu'il y a de mieux. »[75]

SUN ZI

[75] Dans « L'Art de la Guerre » (édition 1990, page 105).

ANNEXES

Abréviations

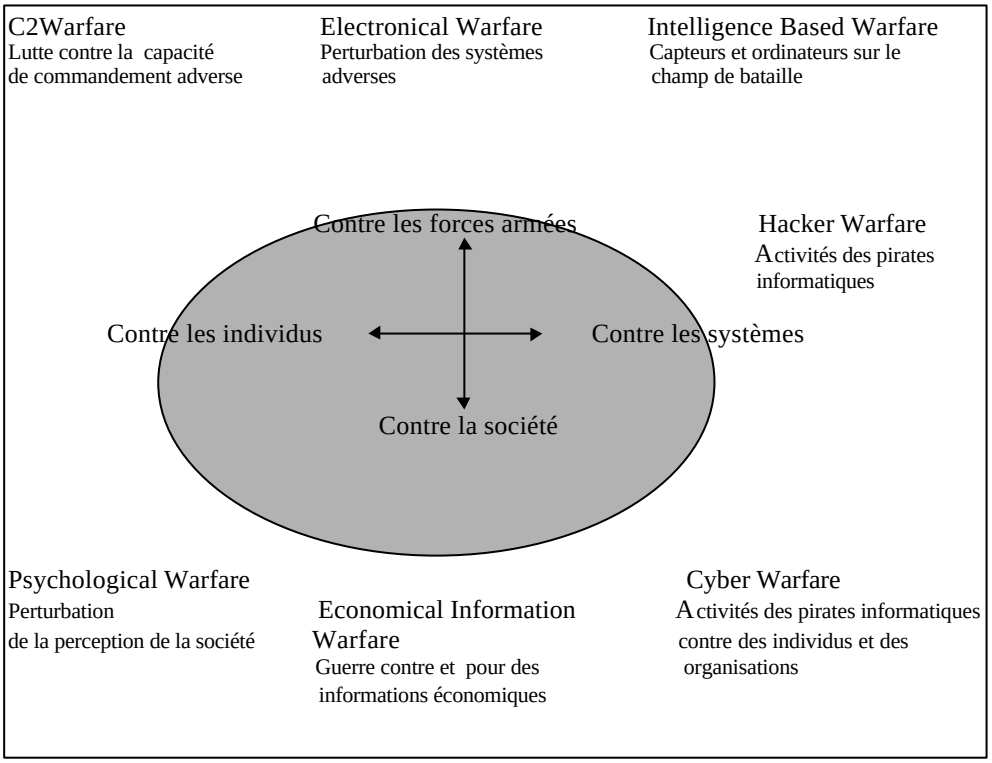
BMVg	Bundesministerium der Verteidigung *(ministère fédérale de la Défense)*
C2W	Command and Control Warfare
C3IW	Command, Control, Communication and Intelligence Warfare
C4W	Command, Control, Communication and Computers Warfare
c.-a.-d.	c'est-à-dire
Cf.	confer (latin) *(voir)*
CIA	Central Intelligence Agency (US)
CIO	Central Imagery Office (US)
CNN	Cabel News Network (US)
DIA	Defense Intelligence Agency (US)
DISA	Defense Information Systems Agency (US)
DOD	Department of Defense (US)
DOE	Department of Energy (US)
DOJ	Department of Justice (US)
EMP	Elektromagnetischer Impuls *(impulsion électromagnétique)*
FBI	Federal Bureau of Investigation (US)
HDv	Heeresdienstvorschrift (Bundeswehr) *(règlement de l'armée de terre allemande)*
Id.	Idem (latin) *(le même auteur)*
Ibid.	Ibidem (latin) *(au même endroit)*
IMINT	Imagery Intelligence
IW	Information Warfare *(guerre de l'information)*
MA	mode(s) d'action
MC	Military Commitee (NATO) *(Comité militaire, O.T.A.N.)*
MNC	Major NATO Commander (SACEUR, SACLANT) *(Commandant allié suprême, O.T.A.N.)*

NAC	North Atlantic Council (NATO) *(Conseil de l'Atlantique Nord, O.T.A.N.)*
NATO	North Atlantic Treaty Organisation *(Organisation du traité de l'Atlantique Nord, O.T.A.N.)*
NGO	Non Governmental Organization *(organisation non gouvernementale, O.N.G.)*
N°	numéro
NSA	National Security Agency (US)
Op. cit.	Opere citato (latin) *(ouvrage cité)*
p.	page
PC	Personal Computer *(ordinateur individuel)*
p.e.	par exemple
PHOTINT	Photographic Intelligence
pp.	pages
RECO	Reconnaissance
SACEUR	Supreme Allied Commander Europe (NATO) *(commandant suprême des forces alliées en Europe, O.T.A.N.)*
SACLANT	Supreme Allied Commander Atlantic (NATO) *(commandant suprême allié de l'atlantique, O.T.A.N.)*
SIGINT	Signals Intelligence
TRS	Transmission(s)
U.R.S.S.	Union des Républiques Socialistes Soviétiques
US(A)	United States (of America) *(les Etats-Unis d'Amérique)*

Table des illustrations

Illustration N° 1 :

Formes et dimensions de la guerre de l'information



Cf. Buchholz (Quantensprünge, 1998), p. 6.

Illustration N° 2 :

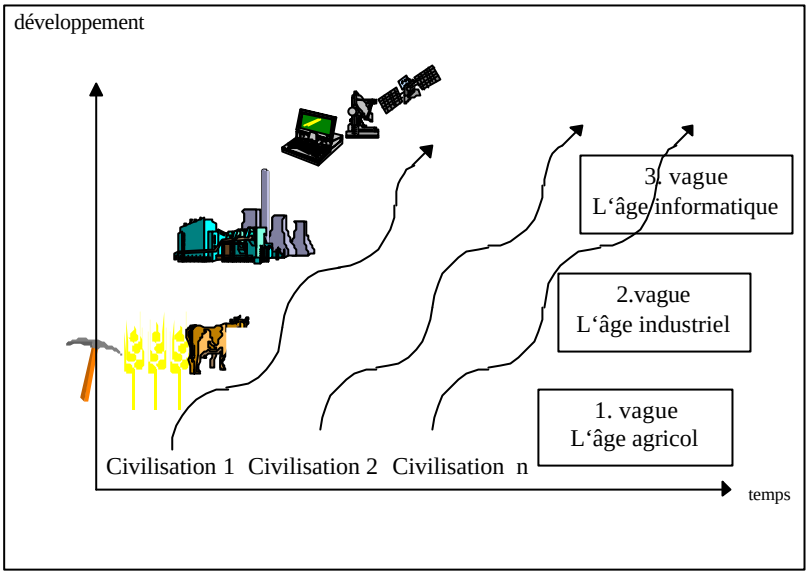
Tendances de développement en matière de la technologie de l'information

Technologie	Description
Informatique Matériels (Hardware)	• Augmentation de la performance suite à la miniaturisation des puces de silicium à structure tridimensionnelle. • Ordinateurs performants à parallélisme massif • Les limites mécaniques dans la production seront surmontées par des ordinateurs optiques et biologiques. • Elargissement de la robotique • Maillage complet des réseaux à l'échelon mondial
Logiciels (Software)	• Langages informatiques intelligents • Dialogue homme-machine simplifié • Fiabilité accrue des programmes • Traitement de la voix • Intelligence artificielle permettant l'exploitation et le tri d'importants volumes de données en temps utile
Electronique et capteurs Composants électroniques	• Micro-ondes monolithiques servant de technologies pour pilotes de périphériques • Eléments électroniques supraconducteurs • Transistors sous vide miniaturisés • Mémoires informatiques • Puces numériques de traitement de signaux • Technologie informatique à processeurs multiples • Technologie de réseaux neuronaux • Nouvelles techniques de traitements et de représentation d'images
Systèmes de capteurs	• Radars d'imagerie à haute résolution • Capteurs acoustiques et magnétiques • Radars d'observation et de détection spatiales • Accélération de la vitesse de traitement des signaux jusqu'à 10^{12} opérations par seconde
Haute énergie à effet dirigé	• Les impulsions crêtes du rayonnement électromagnétique provoquent la défaillance de composants électronique • Miniaturisation des éléments générant l'IEM (impulsion électromagnétique)
Armes et instruments non-létaux	• Armes détruisant des systèmes mais épargnant les vies humaines

Cf. Büntemeyer (Dimension, 1996), p. 555 (et suivantes), et aussi Amt für Studien und Übungen der Bundeswehr (Auswirkungen, 1995), p. 21 (et suivantes).

Illustration N° 3 :

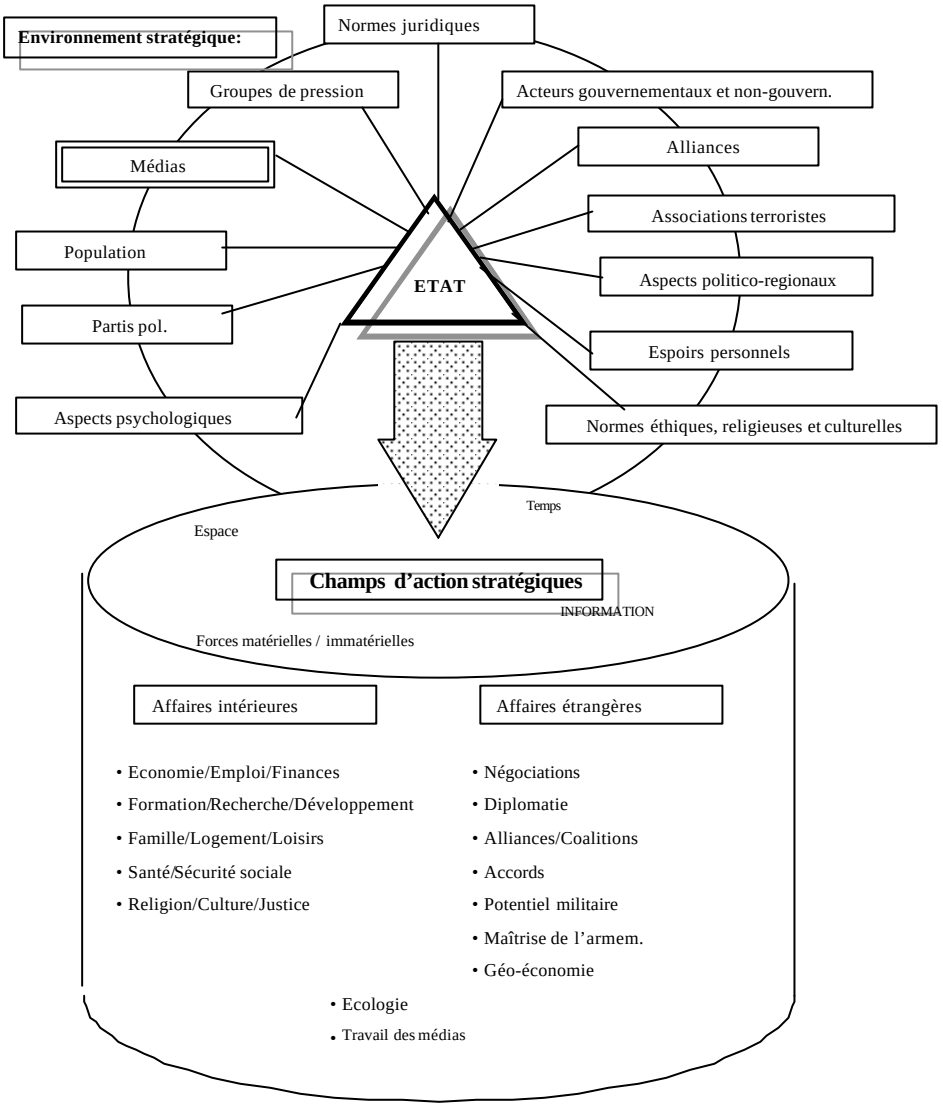
Modèle des civilisations (d'après Toffler)



Cf. Amt für Studien und Übungen der Bundeswehr (Auswirkungen, 1995), p. 16.

Illustration N° 4 :

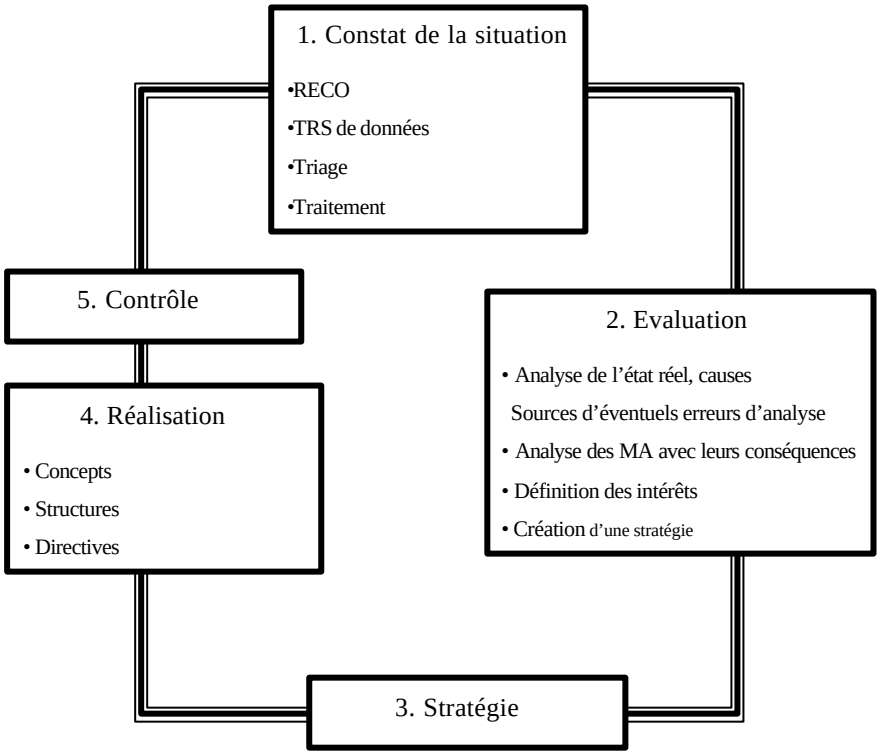
Facteurs d'influence au niveau du commandement stratégique



Cf. Buchholz (Quantensprünge, 1998), p. 30, en combinaison avec Fels (Strategiehandbuch, 1990), Ruge (Politik und Strategie, 1967), chapitres 2 et 3, ou aussi Collins (Grand Strategy, 1973), p. 2.

Illustration N° 5 :

Processus décisionnel stratégique



Cette présentation correspond dans le fond à la méthodologie de Carrel (Lagebeurteilung, 1994), pp. 227-228. Cf. aussi le modèle d'analyse mathématique chez Koman (Strategische Analyse, 1975), p. 30 (et suivantes).

Bibliographie

Abegglen, Christoph. *« Information Warfare – strategisches Mittel der Zukunft »,* dans : Allgemeine Schweizerische Militärzeitschrift. N° 12/1997, pp. 9-14.

Alexander, David. (Digitised Battlefield, 1995). *« Information Warfare And The Digitised Battlefield »*, dans : Military Technology. 1995, pp. 57-64.

Amt für Studien und Übungen der Bundeswehr. (Auswirkungen, 1995). Sicherheits- und militärpolitische Auswirkungen neuer Waffentechnologien unter besonderer Berücksichtigung des « Information Warfare ». Initialstudie. Waldbröl : 1995.

Amt für Nachrichtenwesen der Luftwaffe. (Aktuelle Entwicklungen, 1996). Information Warfare – Aktuelle Entwicklungen -. A2-Informationen 18/96. Cologne : 1996.

Arquilla, John J. ; Ronfeldt, David F. *« Cyberwar and Netwar : New Modes, Old Concepts, of Conflict »,* dans : Internet (http://www) : <.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html>

Beaufre, André. (Kriegskunst, 1964). Totale Kriegskunst im Frieden – Einführung in die Strategie. Berlin : 1964.

Beham, Mira. (Kriegstrommeln, 1996). Kriegstrommeln : Medien, Krieg und Politik. Munich : Deutscher Taschenbuch-Verlag (DTV), 1996

Brom, Gerard P. *« C4IEWS in the US Army – Issues, Analysis and Trends »*, dans : NATO'S Sixteen Nations. N° 3/97, pp. 64-66.

Buchbender ; Bühl ; Kujat. (Sicherheitspolitik, 1992). Wörterbuch zur Sicherheitspolitik. Herford et Bonn : Mittler, 1992.

Buchholz, Harald ; Michel, Markus. (Quantensprünge, 1998). « Quantensprünge » in der Informationstechnologie. Hambourg : Führungsakademie der Bundeswehr, 1998.

Bundesregierung der Bundesrepublik Deutschland. (Weissbuch, 1994). Weissbuch 1994 : Weissbuch zur Sicherheit der Bundesrepublik Deutschland und zur Lage und Zukunft der Bundeswehr. BMVg (éditeur). Bonn: 1994.

Büntemeyer, Fredi. (Dimension, 1996). *« Information als entscheidende Dimension der Auseinandersetzung im 21. Jahrhundert »*, dans : Soldat und Technik. 9/1996, pp. 555-559.

Buse, Uwe. *« Die Zukunft des Krieges (Serie : Spiegel des 21. Jahrhunderts, Teil 1) »,* dans : Spiegel : reporter (Monatsmagazin für Reportage, Essay Interview). N° 11/1999, pp. 82-87.

Campan, Alan. (Gulf War, 1991). *« Gulf War's Silent Warriers Bind US Units Via Space »*, dans : Signal. 1991, pp. 81-84.

Carrel, Laurent F. (Lagebeurteilung, 1994). « *Sicherheitspolitisch-strategische Lagebeurteilung : Herausforderungen an die Methodik »*, dans : Österreichische Militärzeitschrift (ÖMZ). Volume 32, 1994, pp. 227-234.

Chaliand, Gérard ; Blin, Arnaud. (Dictionnaire, 1998). Dictionnaire de stratégie militaire des origines ànos jours. Perrin, 1998.

Cimbala, Stephen J. *« Information Warfare and Nuclear Conflict Termination »*, dans : European Security. Volume 7, N° 4 (Winter 1998), pp. 69-90.

Clausewitz, von, Carl. (Vom Kriege, 1991). Hinterlassenes Werk : Vom Kriege. 19° édition. Bonn : Dümmlers, 1980 et 1991.

Cobbold, Richard. *« Information Warfare : Un Underview»,* dans : The New International Security Review. 1998, pp. 66-76.

Collins, John M. (Grand Strategy, 1973). Grand Strategy, Principles and Practices. Annapolis: United States Naval Institute, 1973.

Coutau-Bégarie, Hervé. (Traité, 1999). Traité de Stratégie. 2e édition. Paris : Economica, 1999.

Id. (Directeur). Stratégie, Information, Communication. N° 1/98 / 9. Institut de Stratégie Comparée. Paris : Economica, 1998.

Covault, Craig. *« Cyber Threat Challenges Intelligence Capability : NSA director warns of 'fundamental new danger', cites changung role of defensive systems and intelligence »,* dans : Aviation Week and Space Technology. N° 146, 1997, pp. 20-21.

Dearth, Douglas H. (Information War, 1997). *« Information War : Re-thinking the Application of Power in the 21st Century »*, dans : Military Intelligence. Volume 23, Number 1, January-March 1997, pp. 11-43.

DiNardo R.L. ; Hughes, D.J. (Cautionary Thoughts, 1995). *« Some Cautionary Thoughts on Information Warfare »*, dans : Airpower Journal., N° 4 (Winter 95, Volume IX), 1995, pp. 69-79.

Dublik James ; Sullivan Gordon. (Information Age, 1994). « War in the Information Age », dans : Military Review, Volume 74 (1994), pp. 46-54.

Emmet, Peter. (Information Mania, 1996). *« Information Mania : A new manifestation of Gulf War Syndrome ? »*, dans : RUSI, Journal Royal United Serve Institute for Defence Studies. N° 141 (1996), pp. 19-26.

Fabiszisky, Markus. Information Warfare : eine neue Form der strategischen Kriegsführung. Francfort/Main : Oberprüfungsamt für die höheren technischen Verwaltungsbeamten (2 VI - 1376), 1997.

Feaver, Peter D. *« Blowback : Information Warfare and the Dynamics of Coercion »*, dans : Security Studies. Volume 7, N° 4 (Summer 1998), pp. 88-120.

Fels Gerhard ; Huber, R. K. ; Kaltefleiter, W. ; Pauls, R. F. ; Schulze, F. J. (Strategiehandbuch, 1990). Strategiehandbuch. Volume 1 et 2. Herford, Bonn : Mittler, 1990.

Fischer. (Entwicklungen, 1994). Entwicklungen im Bereich « Information Warfare Operations ». Heereshauptverbindungsstab 1 (TRADOC), Fort Monroe, Virginia : 1994, pp. 2-19.

Ford, Brian. (Geheimwaffen, 1996). Der Zweite Weltkrieg : Die deutschen Geheimwaffen. Traduit de l'anglais par H. Weilguni. 3° édition. Rastatt : Moewig, 1996.

Freedman, Lawrence. *« Britain and the Revolution in Military Affairs »,* dans : Defense Analysis. London : Volume 14, N° 1/1998, pp. 55-66.

Fulghum, David A. *« Information Warfare : Cyberwar Plans Trigger Intelligence Controversy : U.S. national intelligence agencies, military at odds over what can be attacked in a computer war »,* dans : Aviation Week & Space Technology. N° 19, 1998, pp. 52-54.

Gates, Bill. (Weg, 1995). Der Weg nach vorn. Hambourg : Hoffman und Campe, 1995.

Geiger, Gebhard. Verteidigung im 'Cyberspace' : Internationale Probleme, nationale Aufgaben. Ebenhausen : Stiftung Wissenschaft und Politik : Forschungsinstitut für Internationale Politik und Sicherheit, 1997.

Geyso, von. (Strategie, 1996). Reader Strategieseminar. Hambourg, Führungsakademie der Bundeswehr : 1996.

Gompert, David C. *« Keeping Information Warfare in Perspective »,* dans : Internet (http://www) : <.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html>

Grier, Peter. (At War, 1997). *« At War With Sweepers, Sniffers, Trapdoors and Worms »*, dans : Air Force Magazine. 1997, pp. 21-24.

Id. (Information Warfare, 1995). *« Information Warfare »,* dans : Air Force Magazine. N° 78. 1995, pp. 34-37.

Habermeyer, Helmut. *« Information Warfare – die neue Dimension,* dans : Österreichische Militärische Zeitschrift. N° 5/1998, pp. 559-566.

Haxlett, James ; Libicki, Martin. (Revolution, 1994). *« The Revolution in Military Affairs »*, dans : Strategic Forum. Istitute for National Strategic Studies (N° 11), 1994, pp. 71-74.

Hobson, Sharon. *« Canada's information ops in defensive role : The Canadian Forces are reshaping their information operations capabilities »,* dans : Jane's Defence Weekly. N° 15, 1997, pp. 29-30.

Huntington, Samuel P. (Clash of Civilizations, 1996). The Clash of Civilizations. New York : Simon & Schuster, 1996.

Hutcherson B. Norman. (Command and Control Warfare, 1994). Command and Control Warfare - Putting Another Tool in War-Fighters Data Base. Alabama, Maxwell Air Force Base: Air University Press, 1994.

Jones, Harry E. *« Information Dominance for Army XXI : Battlefield Visualization »,* dans : Military Intelligence. January-March 1997, pp. 8-10.

Koman, Peter. (Strategische Analyse, 1975). *« Strategische Analyse »*. Dans : Österreichische Militärzeitschrift (ÖMZ). Volume 1, 1975, p. 30 (et suivantes).

Kopeinig, Arnulf. *« Information Warfare : Versuch eines definitorischen Zugangs im Rahmen politikwissenschaftlicher Untersuchungen »,* dans : Österreichische militärische Zeitschrift. N° 1/99. Vienne : 1999, pp. 23-36.

Kraus George. (IW in 2015, 1995). « *Information Warfare in 2015 »*, dans : United States Naval Institute. Volume 121, 1995, pp. 42-45.

Kretschmer, Thomas ; Euting, Thomas. *« Information War : Kriegs- und Konfliktbild der Zukunft »,* dans : Soldat und Technik. N° 10 :1997, pp. 557-560.

Kruglov, V. V. *« Über den bewaffneten Kampf der Zukunft (O vooruzennoj bor'be buduscgo) »,* dans : Militärische Futurologie (Voennaja futurologija). Traduction allemande. Moscou : N° 5/1998 /10, pp. 54-58.

Längin, Bernd G. (US-Bürgerkrieg, 1998). Der amerikanische Bürgerkrieg. Augsbourg : Bechtermünz, 1998.

Le Bail, Pierre-Yves. (bataille de l'information, 1992). *« La bataille de l'information : Les médias dans la guerre du Golfe »*, dans : Armées d'aujourd'hui. N° 157 (1992), pp. 14-15.

Lewis, Brian C. *« Information Warfare »,* dans : Internet (http://www) : <.fas.org/irp/eprint/snyder/infowarfare.html>

Libicki, Martin. (What is IW ?, 1995). What is Information Warfare ? National Defense University. Institute for National Strategic Studies. Washington : 1995.

Lübbe, Herrmann ; Neumann, Bernd. (Informationsgesellschaft, 1996). Informationsgesellschaft – Quo vadis ?. Konrad-Adenauer-Stiftung. Aktuelle Fragen der Politik. St. Augustin : 1996.

Mackubin, Thomas Owens. *« Technologie, the RMA (Revolution in Military affairs), and Future War »*, dans : Stategic Review. Washington D.C. : United States Strategic Institute. Spring 1998, pp. 63-70.

Malterre, Thibauld. *« L'information, reine des batailles »*, dans : Armées d'aujourdhui. N° 246 (12/99 et 01/00), pp. 71-73.

Mann, Edward. (Desert Storm, 1994*). « Desert Storm : The First Information War? »*, dans : Air Power Journal*.* N° 4, 1994, pp. 4-14.

Mann, Paul. *« 21st Century Security : Government / Industry Alliance Urged Against Cyber Threats »,* dans : Aviation Week & Space Technologie. N° 13/1998, pp.65-67.

MacArthur, John R. (Schlacht der Lügen, 1993). Die Schlacht der Lügen. Munich : Deutscher Taschenbuchverlag (DTV), 1993.

Müller, Niklaus. (Informationszeitalter, 1996). *« Krieg im Informationszeitalter »*, dans : Schweizer Soldat und MFD. N° 71, novembre 1996, pp. 7-9.

Müller von Blumencron, Mathias. *« Hacker : Dämonen im Datennetz »,* dans : Der Spiegel. N° 7/2000, pp. 108-110.

Molander, R. C. ; Riddle, A. S. ; Wilson, P. A. *« Strategic Information Warfare : A New Face of War »,* dans : Parameters. Autumn 1996, pp. 81-92.

Möller-Gulland, Niels. *« Information Warfare »,* dans : Allgemeine Schweizerische Militärzeitschrift. N°. 12/1997, pp. 2-8.

Mommsen, Klaus. *« Information Warfare »,* dans : Rissener Rundbrief. Hambourg : N° 2-3/1998, pp. 103-112.

Morris, Chris ; Morris, Janet ; Baines, Thomas. (Weapons, 1995). *« Weapons of Mass Protection: Information Warfare and Airpower in the Age of Chaos »*, dans : Air Power Journal. Volume IX (Spring), 1995, p. 17.

NATO. (Handbook, 1998). The Nato Handbook. 50th Anniversary Edition. Bruxelles : 1998.

Nerlich, Uwe. *« Strategische Dimensionen der Informationskriegführung »,* dans : Europäische Sicherheit. N°. 4/98, pp. 40-43.

Petersen, Kurt ; Pracht, Kurt. (Krieg der Zukunft, 1995). *« Information Warfare : Der Krieg der Zukunft hat bereits begonnen : Wer heute den Einstieg verschläft, wird morgen manipuliert », dans* : Soldat und Technik. N° 38/1995, pp. 783-788.

Ravier, Eric. *« Science et Défense : Informatique et nouvel échelon stratégique »,* dans : Défense Nationale. N° 11/1997, pp. 145-149.

Reeb, Hans Joachim. (Kampf um Informationen, 1991). Der Kampf um Informationen in Krisen und Kriegen. Coblence : Zentrum für Innere Führung, 1991.

Rodgers, James L. *« Information Warfare : Nothing New Under The Sun »,* dans : Marine Corps Gazette. April, 1997, pp. 23-29.

Ruge Friedrich. (Politik und Strategie, 1967). Politik und Strategie: Strategisches Denken und politisches Handeln, Francfort: Bernhard und Graefe Verlag für Wehrwesen, 1967.

Sans nom d'auteur. (E-Commerce, 1999). *« Person of the Year : Amazon.com's Jeff Bezos : E-Commerce is changing the way the world shops »*, dans : Time : The weekly newsmagazine. Volume 154, N° 26 (December 27, 1999), titre et pp. 36-89.

Sans nom d'auteur. *« Cornerstones of Information Warfare »,* dans : Internet (http://www) :
<.af.mil/lib/corner.html>

Sans nom d'auteur. *« Information Warfare : A Two-Edged Sword »,* dans : Internet (http://www) :
<.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html>

Sans nom d'auteur. *« Chapter 8 : Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance »,* dans : Internet (http://www) :
<.fas.org/man/docs/adr_99/chap8.html#top>

Sans nom d'auteur. *«Report of the Defense Science Board Task Force on information Warfare – Defense (IW-D) : November 1996 : Office of the Under Secretary of Defense for Acquisition & Technology (Washington D.C. 20301-3140) »,* dans : Internet (http://www) : <.jya.com/iwdmain.html >

Sans nom d'auteur. (Bits & Bytes, 1996). *« Bits & Bytes statt Bomben »*, dans : Focus : Das Moderne Nachrichtenmagazin. N° 44. Munich, 1996, pp. 204-207.

Sans nom d'auteur. (Information Combat, 1995). Information Warfare / Information Combat. Arbeitspapier der Führungs-akademie der Bundeswehr. Hambourg : 1995.

Sans nom d'auteur. (Russian Views, 1994). *« Role of new Technologie : Russian Views on 'Non-Traditional' Weapons »*, dans : RUSI White Hall Paper. N° 26, 1994, S. 21-52.

Schenker, Jennifer L. *« Internet Wars : The battle for the future of Kosovo is also being waged via E-mail and ovver the Web »,* dans : Time : The weekly Newsmagazine. N° 26, 1999, pp. 40-41.

Scherz, Reimar. *« Die Digitalisierung des Gefechtsfeldes : Der Ansatz des deutschen Heeres »,* dans : Europäische Sicherheit. N° 11/1998, pp. 14-19.

Scott, William B. *« Information Warfare Policies Called Critical to National security »,* dans : Aviation Week and Space Technology. N° 28, 1996, pp. 60-64.

Steele, Robert D. *« Information Peacekeeping : The Purest Form of War »,* dans : Internet (http://www) : <.fas.org/irp/eprint/cyberwar-chapter.html>

Stein, George J. (Battlefield, 1995). *« Information War - Cyberwar – Netwar," Battlefield of the Future: 21st Century Warfare Issues"*. Barry R. Schneider et Lawrence E. Ginter (éditeurs), dans : Air War College Studies in National Security (N 3). Air University, Maxwell Air Force Base, Septembre 1995, pp. 153-170.

Stockfisch, Dieter. *« Information Warfare oder Information Assurance ? »*, dans : Soldat und Technik. N° 12/1998, pp. 804-805.

Id. *« Joint Vision 2010 »,* dans : Soldat und Technik. N° 1/1998, pp. 75-76.

Sullivan, Gordon R. ; Dubik, James M. (Land Warfare, 1993). Land Warfare in the 21st Century. Strategic Studies Institute, U.S. Army War College, February 1993.

Sun Zi. (L'Art de la guerre, 1990). L'Art de la guerre. Bibliothèque Stratégique. Dirigée par Lucien Poirier et Hervé Coutau-Bégarie. Paris : Economica, 1990.

Sunzi. Die Kunst des Krieges. James Clavell (éditeur). Traduit de l'américain par Jürgen Langowsky. Munich : Droemer Knaur, 1988.

Thomas, Timothy L. *« Russia's Information Warfare Structure : Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military »,* dans : European Security. Volume 7, N° 1 (Spring 1998), pp. 156-172.

Toffler, Alvin et Heidi. (War and Antiwar, 1993). War and Antiwar : survival at the dawn of the 21st century. Boston : Little Brown Company, 1993.

Vad, Erich. (Gesamtstrategie, 1994). *« ,Gesamtstrategie und nationale Führungsfähigkeit* », dans : Europäische Sicherheit. N° 06/94, p. 290-316.

White House. *« White Paper : The Clinton Administration's Policy on Critical Infrastructure Protection : Presidential Decision Directive 63 May 22, 1998 (Presidential Directives and Executive Orders) »,* dans : Internet (http://www) : <.fas.org/irp/offdocs/paper598.html>

Id. (National Security Strategy, 1996). National Security Strategy of Engagement and Enlargement. Washington D.C. : 1996.

Will, Thomas. *« Information als Waffe »,* dans : Truppenpraxis / Wehrausbildung. N° 1/1998, pp. 7-11.

Wirtgen, Rolf. (Zündnadelgewehr, 1991). Das Zündnadelgewehr : Eine militärtechnische Revolution im 19. Jahrhundert. Herford et Bonn : Mittler, 1991.

Yeary, Lon M. *« Hackerwar and Its Influence on the Marine Expeditionary Force Commander »,* dans : Internet (http://www) : <.fas.org/cp/eprint/96/yeary.html>

Youssouf, Ammin. *« La guerre sur Internet : 21e siècle – l'ère des cyberconflits »,* dans : Terre Magazine. N° 106, jul/août 1999, pp. 42-43.