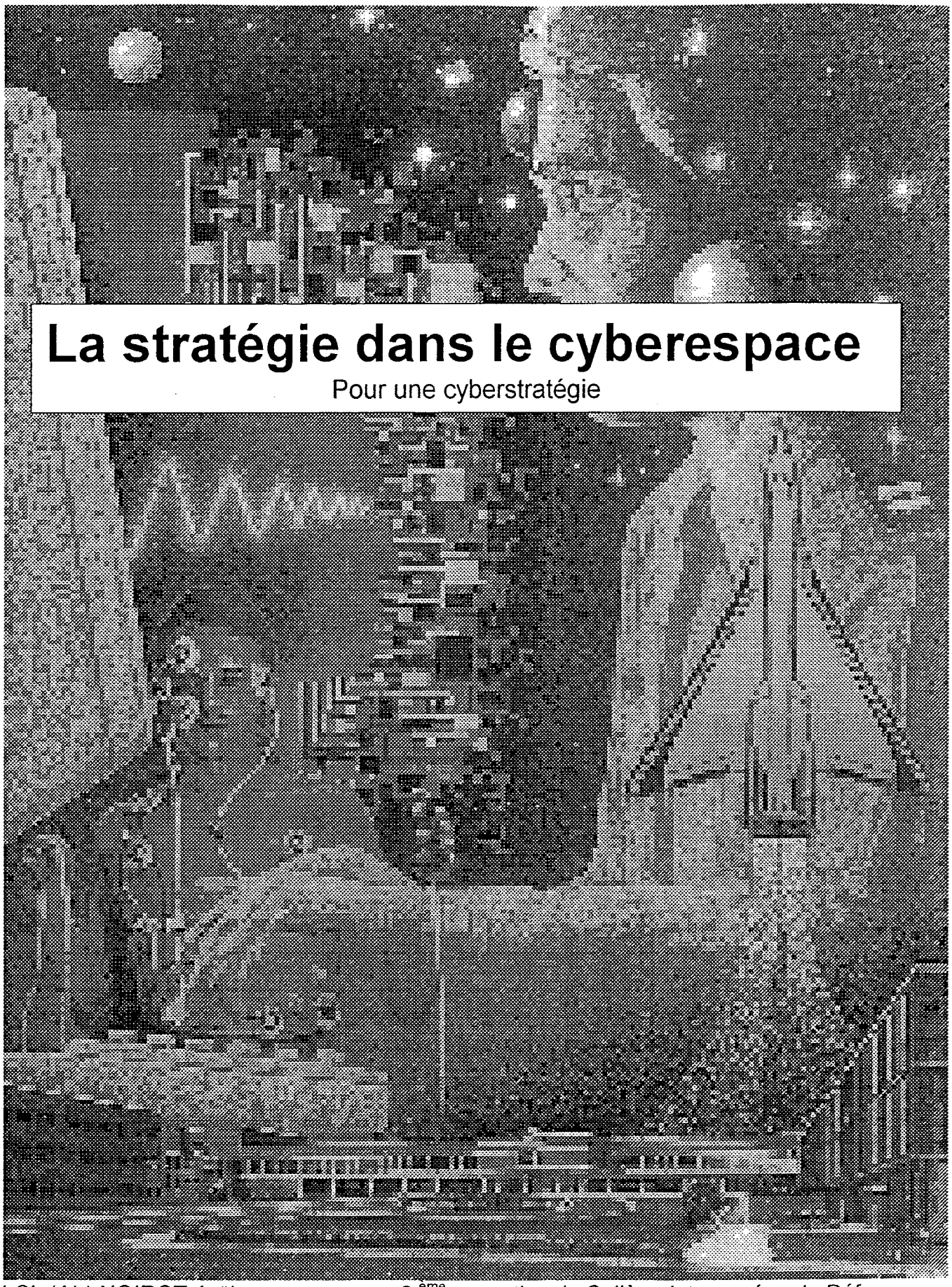


La stratégie dans le cyberespace

Pour une cyberstratégie

LCL (Air) NOIROT Joël

6 ème promotion du Collège Interarmées de Défense

SOMMAIRE

La stratégie dans le cyberespace

- Pour une cyberstratégie -

Introduction

Le cyberespace. Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques...Une représentation graphique des données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumière disposés dans le non-espace de l'esprit, des amas et des constellations de données[1].

C'est par cette définition, tirée d'un roman de science-fiction, que le mot cyberespace est apparu pour la première fois. Avec le passage à un monde de l'information qui envahit notre vie quotidienne, ce mot de science-fiction perd de son vernis futuriste, pour devenir un mot de notre temps. La matérialisation de ce passage à un monde de l'information est illustrée par le réseau *Internet*.

Le réseau *Internet* n'est qu'un sentier de terre comparé aux autoroutes de l'information promises. Les autoroutes de l'information sont le chemin privilégié vers ce qu'il est convenu d'appeler le **cyberespace**. Il s'agit de l'espace dans lequel évoluent les informations, les images, le renseignement. *C'est un espace immatériel mais dont les liens avec le réel sont bien présents*[2]. Le développement de celui-ci repose sur la volonté de ses promoteurs de conserver la domination mondiale

La conflictualité[3] est le carburant de la géopolitique. La géopolitique s'est, depuis des siècles, bâtie sur trois facteurs immuables :

- la lutte pour les ressources ;
- l'accroissement de son espace géographique ;
- l'affirmation d'une identité collective ;

Au cours du XX^{ème} siècle, une quatrième source de conflictualité est apparue : l'idéologie, dont les plus importantes et les plus meurtrières furent le communisme et le nazisme. L'idéologie, source de conflictualité, semblerait avoir disparu avec l'écrasement du nazisme et l'écroulement du communisme. Cependant, le libéralisme à la mode anglo-saxonne, n'est-elle pas une forme nouvelle d'idéologie, source de conflictualité ?

Le cyberespace est devenu un facteur géopolitique majeur de cette fin de siècle[4] et se pose comme une nouvelle source de conflictualité. *Internet, les autoroutes de l'information et le cyberespace possèdent, dès l'origine, les germes des conflits*[5]. Cette conflictualité se résoud par le temps qui atténue les différends, la diplomatie, la duperie, la menace, la coercition, la violence. La guerre n'est pas uniquement la manifestation d'une violence physique. Elle peut se manifester sous les formes décrites ci-dessus.

Mais comment cette nouvelle source de conflictualité peut-elle modifier la guerre et la stratégie ?

---

[1] Cyberespace : mot inventé par William GIBSON dans "Neuromancien" 1985 Ed. J'ai Lu S-F n° 2325 P.64
[2] Michel WAUTELET, *Les Cyberconflits*, Ed. GRIP
[3] Aymeric CHAUPRADE, *Cours Traité de géopolitique*.
[4] *La géopolitique traditionnelle prise dans la toile du cyberespace?*, Mémoire de l'auteur, 6ème promotion CID
[5] Michel WAUTELET, *Les Cyberconflits*, Ed. GRIP

De la nature de la guerre

Les facteurs de la géopolitique sont source du conflit. Ils en sont le but politique. Sans but politique il ne peut y avoir de conflit, de guerre.

La Guerre, matrice de l'histoire

Au commencement était la guerre. Aux temps anciens de l'Antiquité, les philosophes grecs voyaient en la guerre un constituant naturel de la vie des hommes. Chez les Grecs, la guerre est omniprésente, que ce soit dans leur mythologie, avec les dieux de l'Olympe qui s'opposent les uns aux autres, ou chez les philosophes. Héraclite[6] est le philosophe du " feu ", entendu comme l'élément primordial dont tout est issu et où tout doit finir. Il dit : *La guerre est le " père[7] " de toutes choses.* Il ajoute : *Ce sont les contraires qui forment la plus belle des trames et c'est de leur querelle que sont issues les choses.* Cette façon de voir en la guerre quelque chose de naturel est très marquée chez Héraclite. *L'originalité de l'intuition héraclitéenne réside dans le fait d'avoir imaginé le monde comme un gigantesque champ de bataille, où s'affrontent des forces plus ou moins équivalentes. Cette lutte ne constitue pas l'exception, mais la norme de la vie, et même la vie elle-même que les hommes doivent accepter comme une forme de justice naturelle[8].* Des philosophes pouvaient être aussi des chefs de guerre, l'un des plus célèbres fut Xénophon. Il est assez inattendu de voir les Grecs, inventeurs de la démocratie, considérer la guerre comme un élément naturel de la vie pour résoudre les conflits.

Avant les Grecs, les Chinois avaient réfléchi à la manière de conduire la guerre. Sun Zi[9] et Sun Bin en sont le meilleur exemple.

Les Romains ont fondé la puissance de leur empire sur les conquêtes militaires. L'Empire romain, à son apogée, englobait tous les pays entourant la Mer Méditerranée et la Mer Noire, plus l'Angleterre. Cette domination a duré près de cinq siècles et curieusement peu d'écrits de stratégie militaire ont été laissés par les Romains. Dans ses " Commentaires " Jules César parle plus de politique que de stratégie militaire.

La perception de la guerre va évoluer au fil du temps, au même rythme que la stratégie, art supérieur de conduire la guerre.

La guerre, témoin de son temps

Clausewitz définit la guerre de plusieurs manières. Selon un niveau politique croissant, il se place au niveau du duel entre Nations et dit que *La guerre est un acte de violence qui doit contraindre l'adversaire à exécuter notre volonté[10].* Clausewitz voit dans les opérations militaires, le moyen d'atteindre le but fixé. Il ne conçoit atteindre le but politique, notre volonté, que par la violence des armes.

Cependant la violence n'est pas la force. *Aveu de faiblesse, la violence est toujours une destruction qui n'est utilisée que lorsque la force a échoué[11].* La force c'est le pouvoir, la

---

[6] Héraclite l'Obscur, 576-480 av. J.-C., philosophe grec de l'école ionienne né à Ephèse.
[7] En grec guerre, polemos, est masculin
[8] Luciano de Crescenzo, *Les grands philosophes de la Grèce Antique,* ed. Claude Lattès
[9] Sun Zi, IV^e^ siècle av. J.-C,.*L'art de la guerre,*
[10] Carl von Clausewitz, *De la guerre, livre 1*
[11] Véronique Chesneau, Violence et conflictualité : Approche sociologique, Article de la revue *Le Trimestre du monde,* p.61-80, N°35 - 3^e^ trimestre 1996

puissance, l'influence. La force est un moyen de résolution de la conflictualité, un moyen qui n'est pas nécessairement violent. La force est un moyen d'imposer sa volonté à l'ennemi sans pour cela utiliser la violence physique des armes. Il existe un moyen d'atteindre ses objectifs politiques sans avoir à faire usage de ses armes.

Nous avons là, dans cette première définition de la guerre de Clausewitz, une limite aux principes généraux de la guerre. A mon sens ceux-ci ne sont valables que pour l'époque à laquelle ils ont été écrits. Cependant, des principes généraux et universels de haute volée, peuvent être dégagés de ces écrits. Ils sont en nombre limités car les objectifs politiques d'une guerre et les moyens d'y parvenir sont étroitement liés à l'environnement et à l'époque. Il est assez frappant de constater que les traités des plus grands auteurs de stratégie dictent quelques principes stratégiques avant de continuer par de nombreux conseils qui relèvent plus de la tactique du moment, quand ce n'est pas de l'utilisation des armements et de la manœuvre à pied du fantassin.

Antoine Henri Jomini dans son *Précis de l'art de la guerre* distingue d'abord cinq branches purement militaires, avant d'ajouter un chapitre sur le but politique de la guerre. Il distingue ainsi six parties qui forment selon lui l'art de la guerre. Parmi ces six formes la première concerne la politique de la guerre. Nous retrouvons là un des grands principes de toute stratégie : la nécessité d'un but politique à la guerre. La seconde forme s'attache à la stratégie, que Jomini définit ainsi : *La stratégie ou l'art de bien diriger les masses sur le théâtre de la guerre, soit pour l'invasion d'un pays, soit pour la défense du sien*[12]. Nous avons là la limite qu'imposait le cadre de la guerre au XIXè siècle, en limitant la stratégie à un cadre strictement militaire et souvent tactique. Les autres formes se situent à un niveau conceptuel inférieur et ne concernent pas l'objet de cette étude.

Les deux guerres mondiales vont élargir le champ de la guerre (donc le spectre de la stratégie). La guerre devient une guerre totale, militaire mais aussi une guerre " des civils[13]" où tous les moyens d'une Nation sont mobilisés. La stratégie telle qu'elle fut pratiquée pendant des siècles va trouver son élargissement dans le développement technique des outils de la guerre. L'avènement de l'avion va bouleverser la manière de conduire la guerre, donc la stratégie. Le bombardement stratégique va apparaître et donner à la guerre une dimension économique, psychologique et morale.

Clausewitz nous donne une définition de la guerre qui semble plus adaptée au monde moderne et médiatique dans lequel nous vivons : *La guerre est une simple continuation de la politique par d'autres moyens*[14]. Il ajoute : *la guerre n'est pas un simple acte politique mais l'exercice de la politique*. Nous avons là une définition de la guerre qui convient tout à fait à l'homme du XX^{ème} siècle. Celui-ci peut imposer sa volonté à son adversaire par d'autres moyens que ceux des armes classiques. On parle maintenant de guerre économique, de guerre l'information !

Cependant Clausewitz ajoute que ce qui reste propre à la guerre, c'est le caractère tout à fait particulier des moyens. Ces moyens, jusqu'à une époque récente, étaient uniquement constitués de moyens militaires de violence physique. Et c'est en ce point que la théorie de Clausewitz trouve sa limite.

Clausewitz nous rappelle qu'il n'y a pas de limite à la manifestation de la violence (premier extrême). Ce principe trouve ses limites dans le monde médiatique dans lequel nous vivons. Lors de la guerre du Golfe, la violence envers les soldats irakiens a été limitée.

---

[12] Antoine Henri Jomini, *Précis de l'art de la guerre*

[13] Il faut comprendre une guerre où les civils sont aussi acteurs de la guerre, sans porter l'uniforme et les armes

[14] Carl von Clausewitz, *De la guerre, livre I*

On les considérait plutôt comme les victimes d'un régime, que comme les auteurs et acteurs belliqueux d'une guerre d'invasion du Koweït. Ce qui n'était pas le cas de la Garde Républicaine, qui constite le bouclier du régime de Saddam Hussein. Cependant, les opérations, très violentes contre cette Garde, ont été limitées afin que le régime irakien en place ne soit pas détruit. Il fallait que l'Irak ne soit pas livré à la convoitise de ses voisins et démantelé. Nous avons là un exemple où le premier principe extrême de Clausewitz n'a pas été appliqué. Ceci a été accompli de manière totalement réfléchie. Les buts politiques l'ont emporté sur les principes militaires.

Il y a vingt cinq siècles, Sun Zi énonçait déjà que l'art ultime de conduire la guerre était de la faire sans utiliser la violence des armes : *C'est pourquoi remporter cent victoires en cent combats n'est pas ce qu'il y a de mieux ; soumettre l'ennemi sans combattre est ce qu'il y a de mieux*[15]. Napoléon Bonaparte en a fourni un brillant exemple à la bataille d'Ulm où le général autrichien Mack dut se rendre sans avoir pu combattre.

L'industrialisation de notre société et son passage à un monde de l'information entraînent le changement de nature de la guerre. Ils nous conduisent à envisager d'autres moyens, en sus des moyens militaires, pour gagner la guerre. Il ne s'agit pas ici de nier la place des armes, mais de prendre en considération d'autres moyens pour multiplier l'efficacité des armements actuels afin de parvenir aux buts politiques poursuivis. Les moyens militaires perdent une partie de leur importance relative au cours d'un conflit. Mais ils restent indispensables pour terminer une campagne, qui deviendra la plus limitée possible, ou imposer une menace physique sur l'adversaire pour conclure la guerre.

Le Chinois Xu Zhen Zhou disait : *Les batailles ne représentent qu'un cinquième de l'importance de la guerre*[16]. Avec l'avènement de l'ère de l'information cette proportion va encore diminuer.

La philosophie de la guerre de Clausewitz est de rendre l'ennemi impotent en détruisant ses forces armées. Il a fortement mis l'accent sur la friction et la bataille décisive sans trop s'intéresser à la manœuvre stratégique. Le résultat probable sera une bataille qui se terminera en bain de sang. Ceci n'est plus acceptable dans le monde actuel.

Clausewitz a soudainement bien vieilli !

Toutes ces évolutions ont des conséquences sur l'art de conduire la guerre : la stratégie.

De la stratégie et de son évolution

De la stratégie

Ce mot serait apparu pour la première fois en 1771 sous la plume de Joly de Maizeroy[17] dans ses commentaires des *Institutions militaires* de l'empereur Léon le Philosophe. L'étymologie du mot stratégie viendrait de la juxtaposition de *agos*, l'armée qui campe, et de *agein*, pousser en avant, avancer[18].

---

[15] Sun Zi, *L'art de la guerre*, De l'offensive par les plans, Traduction de Valérie Niquet, Ed. Economica
[16] Xu Zhen Zhou, *l'Art de la politique chez les légistes chinois*, p.229, Ed. Economica
[17] Hervé COUTAU-BÉGARIE, *Traité de stratégie*, Ed. Economica
[18] Ibid.

Que recouvre le mot de stratégie ? C'est une vaste tâche à laquelle de nombreux auteurs se sont attelés avec, au bout du compte, autant de définition que de stratégistes.

Voici la première définition que donne Joly de Maizeroy de la stratégie dans sa *Théorie de la guerre (1777) : La conduite de la guerre est la science du général, que les Grecs nommaient stratégie, science profonde, vaste, sublime, qui en renferme beaucoup d'autres, mais dont la base fondamentale est la Tactique... Pour former des projets, la stratégie combine le temps, les lieux, les moyens et les divers intérêts*[19]

Une définition très intéressante me semble être celle qu'aurait pu donner Sun Zi, si le mot eut été inventé à son époque : *la stratégie est l'art de conduire la guerre*. Cette définition est assez générale pour avoir toute sa pertinence aujourd'hui, si dans le mot guerre on y inclut la guerre économique, industrielle et la guerre de l'information.

Ces premières définitions de la stratégie nous la montrent sous l'aspect de la science du général pour gagner la guerre. D'autres définitions, mêlant art, science ou théorie, vont être inventées pour affiner le concept de stratégie et le faire correspondre à son époque. Mais celles-ci restent centrées sur la bataille..

Une définition moderne et complète nous est donnée dans le Traité de Stratégie de Hervé COUTAU-BÉGARIE : *La stratégie est la dialectique des intelligences, dans un milieu conflictuel, fondée sur l'utilisation ou la menace d'utilisation de moyens violents à des fins politiques*[20]. Si on inclut les moyens électroniques et informatiques dans les moyens violents, on peut utiliser cette définition dans notre monde moderne dominé par l'information.

Le perfectionnement des armements a imposé de nouvelles tactiques. Le nombre sans cesse croissant de combattants engagés nécessite leur dispersion pour faciliter le ravitaillement. Mais aussi leur concentration pour la bataille. Tout cela a conduit le commandement à créer les divisions. Ce qui a entraîné une évolution de l'art de la guerre, en élevant le niveau de réflexion. Le maréchal de Saxe parle *des grandes parties de la guerre*. On passe de la tactique améliorée à la grande tactique. La conduite de la guerre prend une autre dimension.

Une définition de la stratégie, qui paraît mieux correspondre au monde actuel, serait la suivante : **La stratégie est l'art de gagner la guerre, à moindre coût**[21]**, en utilisant des moyens inférieurs**[22] **à ceux de l'ennemi.**

De l'évolution de la stratégie

Au cours de la première partie du XX^{ème} siècle, la stratégie a pris une dimension d'un niveau supérieur avec la guerre totale et les énormes effectifs engagés. La seconde partie de ce siècle voit arriver les armes de précision, les systèmes d'information et de commandement (SIC) de plus en plus intégrés et sophistiqués. Il devient tentant de s'attaquer à ces systèmes d'information pour priver l'ennemi de sa capacité de connaître notre dispositif et de commander ses propres forces. La stratégie d'anéantissement selon Clausewitz cède la place à la frappe chirurgicale qui ne détruit que le centre nerveux de l'ennemi.

---

[19] Joly de Maizeroy, *Théorie de la guerre*, Paris, Chez la Veuve Leclerc

[20] Hervé COUTAU-BÉGARIE, *Traité de stratégie*, Ed. Economica, p. 73

[21] Concept de la guerre à zéro mort

[22] C'est-à-dire sans grandes masses humaines, ni moyens matériels nombreux et imposants

Le concept de paralysie stratégique a été remis au goût du jour, récemment, avec les travaux des colonels John BOYD et de John WARDEN de l'US Air Force. Les idées de Warden ont été mises en application, avec le succès que l'on connaît, pendant la guerre du Golfe. Mais avant d'aborder les nouveaux concepts stratégiques que permettent les nouvelles technologies des armements dits " intelligents " et de l'information, il convient tout d'abord d'étudier ce que recouvre le mot cyberguerre traduction littérale du mot anglais "cyberwar". Les auteurs francophones utilisent le mot de cyberconflits. Ce mot recouvre tous les types de conflits : économiques, financiers, technologiques, culturels et militaires. J'emploierai le mot de cyberguerre pour limiter mon propos aux conflits militaires (les cyberconflits sont déjà en cours, mais cela dépasserait le cadre de ce mémoire).

De la guerre à la cyberguerre

Les trois vagues des Toffler

Pour Avin et Heidi Toffler, les gourous de la futurologie américaine, les autoroutes de l'information constituent l'élément technique de domination du monde. Au départ il s'agissait, selon eux, de redynamiser la société américaine[23]. Les idées des Toffler, depuis la publication de leur best-seller, *Le choc du futur*, en 1970, ont profondément marqué les esprits des dirigeants et économistes américains et mondiaux.

Selon les Toffler, le monde est en train de passer (à mon sens le mouvement est déjà bien engagé) d'un monde dual (Nord-Sud, riches et pauvres, industrialisé et agricole) à un monde triséqué. Selon un ordre historique, le monde est divisé en secteurs de plusieurs vagues. La Première vague est le monde rural qui offre les ressources agricoles et minérales. La Deuxième vague est celle de la main-d'œuvre bon marché et de la production industrielle en série. Quant aux secteurs de la Troisième vague, ils vendent au monde : de l'information et de l'innovation, du management, de la technologie avancée, des logiciels, de l'éducation et de la formation , des services médicaux et financiers. Dans leur livre "War and Anti-War", paru en 1993, ils démontrent que, après la guerre à cheval, reflet d'une civilisation agraire, après l'affrontement de chars et d'avions, caractéristique de la société industrielle, surgit aujourd'hui la guerre de la "Troisième vague" ; celle de la suprématie du savoir[24].

Cette dernière vague, basée sur l'information et la connaissance, a besoin, pour continuer à se développer, d'outils spécifiques. Ces outils commencent à prendre forme et prennent pour nom : Internet, multimédia, autoroutes de l'information. Développer les autoroutes de l'information est indispensable à une nation pour appartenir aux pays de la Troisième vague, afin de faire partie du groupe de pays qui conserveront la domination économique, intellectuelle et culturelle du monde. A cet égard, les propos des Toffler, des politiciens américains, de nombreux industriels concernés ne peuvent laisser aucun doute. Pour d'autres, développer les autoroutes de l'information n'est que l'opportunité d'être le premier dans un secteur de haute technologie, afin d'en tirer des profits qui peuvent être énormes. Mais au bout du compte, le résultat n'est-il pas le même ?

---

[23] Avin et Heidi Toffler, *Les nouveaux pouvoirs*, Arthème Fayard, Paris, 1991

[24] Cité par le quotidien Les Echos du 14 janvier 1999

La lutte pour les ressources

La chute du mur de Berlin a mis fin à la Guerre Froide et au danger mortel d'holocauste nucléaire. On pensait en avoir fini avec les guerres. Mais à cette Guerre Froide (ou paix armée) a succédé un nombre impressionnant de conflits ethniques (la troisième source de conflictualité de l'école géopolitique) dont un sanglant et cruel au cœur même de l'Europe. Ces crises bouleversent la carte géopolitique du monde en ce sens que de nombreux conflits se déroulent dans des pays riches en matières premières. Celles-ci deviennent indisponibles à cause des combats. Ces conflits sont intolérables à la Grande Puissance qui a décidé de devenir, plus encore, le gendarme du Monde. Son arrivée en Afrique, qui était traditionnellement dans la sphère d'influence de la France, pourtant son alliée, en est le meilleur exemple. A part quelques conflits ethniques comme en ex-Yougoslavie[25], ou religieux comme en Algérie[26], la plupart des conflits ethniques sont des conflits instrumentalisés par : des Etats qui veulent s'assurer un approvisionnement sûr en matières premières ou de puissantes compagnies qui paient des armées de mercenaires pour protéger leurs (colossaux) intérêts financiers[27].

Cette lutte pour les ressources devient de plus en plus âpre, car c'est la condition sine qua non du développement économique des Etats. Par exemple, pour ce qui touche les besoins en pétrole, il faut savoir que les USA consomment 3 tonnes par personne et par an, la France 1,5t et la Chine 0,12t. Quand la Chine consommera autant de pétrole que la France (on ne parle pas de la consommation des USA), **la consommation de la seule Chine sera supérieure de 25% à la production TOTALE de l'OPEP**[28]. La lutte sera terrible pour le contrôle des ressources en pétrole. Le problème des ressources en l'eau se posera avec la même acuité.

Dans cette lutte pour les ressources, la domination de l'information va donner un avantage considérable à celui qui l'exercera. Ce nouveau facteur est en train de modifier le paysage géopolitique. Cette information prend une importance capitale dans notre environnement économique, militaire, technologique et culturel. La première étape de l'influence énorme de l'information s'est d'abord manifestée dans l'économie.

De l'influence de l'information numérique

Les techniques numériques, permettant de mettre l'écrit, les sons et l'image sous forme de code binaire universel, transmissible instantanément en tous lieux, ont transformé notre univers en s'affranchissant du temps et de l'espace.

La Terre est devenue un village global.

L'explosion de la micro-informatique, en permettant l'accès au plus grand nombre aux techniques numériques à faible coût, a révolutionné le monde de l'information. Nous pouvons affirmer que notre monde est passé dans l'ère de l'information numérique et que

[25] Le conflit purement ethnique n'existe pas. Il s'agit le plus souvent d'une lutte économique pour les richesses d'un pays ou d'une lutte pour le pouvoir entre ethnies. L'ONU devrait renégocier avec les Etats les frontières issues du colonialisme ou des guerres, afin de créer des entités ethniques homogènes qui correspondent à des Nations (dans un premier temps, car on peut imaginer que la non-viabilité de certains Etats trop petits les incitera vite à se regrouper, mais cette fois-ci volontairement, dans des marchés économiques plus vastes).

[26] Il ne s'agit pas d'un conflit purement religieux (affirmation identitaire) mais plutôt d'une lutte pour le pouvoir et par ricochet le pouvoir économique. C'est aussi le cas du conflit afghan.

[27] Exemples africains.

[28] Calculs effectués à partir des données du QUID

celle-ci recouvre tous les domaines de l'économie et de la géopolitique. Ce passage dans l'ère de l'information a commencé avec le développement de l'électronique qui a permis le boom des médias de masse : la radiophonie, la télévision, les disques, la vidéo.

Une accélération de ce processus de passage à un monde de l'information a été causée par l'avènement du tout numérique, de l'informatique individuelle et la démocratisation du PC[29]. Après le disque CD, le disque vidéo, le DVD[30] arrive dans les foyers. Il procure une qualité d'image sans égal, un son de très haute qualité à 6 canaux numériques, tout cela grâce aux traitements informatiques des signaux. Le marché est immense et recouvre tous les supports : sons, images et écrit[31]. La télévision devient numérique avec les bouquets de programmes[32] transmis par des satellites de faible puissance type ASTRA.

Les sommes en jeu sont considérables. Le contrôle de ces moyens de diffusion de l'information, des divertissements ou de la culture est devenu un enjeu économique gigantesque, un levier énorme du pouvoir et de la culture planétaires.

Les bourses mondiales sont informatisées, les transferts d'argent entre banques se font de manière immatérielle grâce au réseau SWIFT[33]. Chaque jour, des milliards de dollars sont échangés de part le monde via des réseaux informatiques. Dans les bourses, on estime que les mouvements spéculatifs des capitaux sont de cinquante à soixante fois plus importants que le montant des transactions réelles.

L'économie et la finance mondiales sont passées du monde réel au monde de l'information virtuelle : le cyberespace.

De l'influence de l'immatériel sur les conflits

Toutes les branches de l'économie sont touchées par l'information et l'économie est devenue le nouveau champ de bataille planétaire. Le contrôle de l'information est vital car elle est devenue une richesse inestimable :

- en elle-même avec les médias ;
- pour participer et gagner la guerre économique ;
- pour accroître son influence politique, sociale et culturelle ;
- pour gagner de nouvelles places stratégiques (en possédant et en contrôlant cette information) comme les Anglais contrôlaient les détroits et les routes maritimes.

Un nouveau facteur de conflictualité est apparu : la guerre pour le contrôle de l'information : l'information warfare (préféré au terme cyberwar[34] limité à quelques formes de guerre de l'information).

Le lieu de cette conflictualité est le cyberespace dont une représentation est donnée ci-après[35].

---

[29] Personal Computer ou " micro-ordinateur ". Il est difficile de parler de micro-ordinateur quand ceux-ci, coûtant moins de 10 000F, sont aussi puissants que des gros systèmes classiques coûtant 500 fois plus ! Ce sont des micro-ordinateurs par leur taille et leur prix, pas par leur puissance de calcul.

[30] Digital Versatile Disk

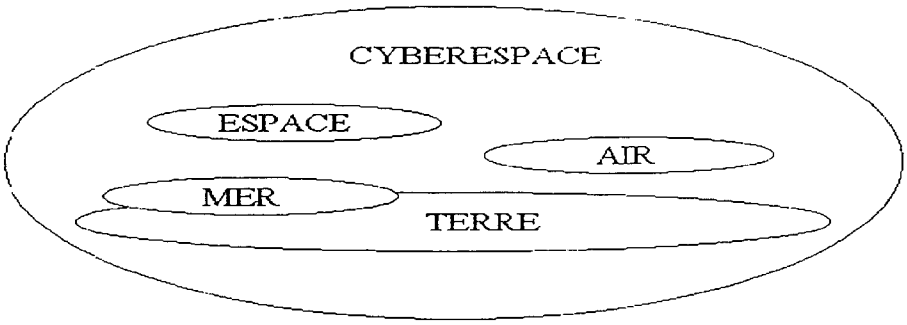
[31] Les journaux de la presse écrite ont un site INTERNET dans lequel on peut consulter les articles publiés.

[32] Canal+ satellite, TPS et AB satellite sont les principaux acteurs sur le marché français.

[33] Réseau mondial interbancaire de compensation (très protégé évidemment).

[34] Terme de ARQUILLA et RONFELDT de la RAND qui le préfèrent à Information Warfare

[35] Représentation inspirée de celle de "Les cyberconflits" de Michel WAUTELET Ed. GRIP



Nous voyons que le lieu du conflit n'est plus un espace physique, l'espace géographique, mais un espace virtuel.

Cet espace, le cyberespace[36], n'a pas d'existence physique mais il englobe les espaces physiques qu'il entoure et qu'il relie.

L'information est devenue une richesse économique et un outil de la guerre économique. Elle est un enjeu technologique et de domination. Elle est un vecteur culturel extrêmement puissant, elle est l'épine dorsale de tout conflit militaire. Nous voyons aussi qu'elle couvre tous les domaines de la puissance. *L'acquisition de la supériorité aérienne est une priorité absolue. La supériorité aérienne est liée à la maîtrise de l'information*[37].

On peut donc affirmer que l'information est le cinquième facteur de la puissance, au même titre que la puissance économique, technologique, culturelle ou militaire[38].

L'information et le cyberespace possèdent ainsi, dès l'origine, les germes de conflits. Vouloir dominer, ou tout simplement posséder un instrument de domination, va inciter les autres à vouloir acquérir cet instrument. Vous essaierez de l'empêcher de l'acquérir afin de conserver votre avantage. Alors, cet adversaire essaiera de détruire ou de rendre inopérant vos moyens.

Lorsqu'on parle de domination économique, technologique, culturelle ou intellectuelle, on ne peut s'empêcher de penser à la domination militaire. Bien que le concept de réseau ait été, au départ, créé par l'ARPA[39] pour des besoins militaires[40], le réseau Internet, embryon des autoroutes de l'information, est né au CERN[41] et il échappe actuellement aux militaires. Mais les militaires pourront-ils laisser ce puissant moyen de communication en dehors de leur sphère de réflexion et d'action ?

De plus, sur le champ de bataille, le général doit savoir comment est organisé le dispositif ennemi afin de pouvoir en tenir compte. **Il doit s'affranchir de l'incertitude et dissiper le "brouillard de la guerre".** *Comment un homme peut-il dire ce qu'il doit faire si il*

---

[36] Les Américains parlent aussi d'Information Battlespace.
[37] Mémento de Commandement et de Conduite des Opérations Aériennes, CDAOA
[38] Les quatre dimensions de la puissance selon Gérard CHALIAND
[39] Advanced Research Project Agency
[40] Il s'agissait pour les militaires américains, dans les années 60, de pouvoir riposter à une frappe nucléaire soviétique. Pour cela ils ont imaginé d'interconnecter tous leurs ordinateurs, en une immense toile d'araignée, afin de pouvoir continuer à combattre après une frappe surprise soviétique. Ainsi les protocoles informatiques Transport Control Protocol (TCP) et Internet Protocol (IP) ont été créés et sont utilisés aujourd'hui par Internet.
[41] A l'origine : Conseil Européen pour la Recherche Nucléaire

ignore ce que son ennemi prépare ?[42] *J'ai passé ma vie à essayer de deviner ce qu'il y avait de l'autre côté de la colline*[43].

Pour emporter la décision, il faut agir avec rapidité. *Comme il est vrai que dans toute opération militaire le temps est tout*[44]. Les télécommunications permettent de réduire les délais et de maîtriser le temps. *Je préfère perdre une bataille que perdre une minute*[45].

La représentation du cyberespace ci-dessous, limité au monde militaire, est tirée d'un site Internet de l'USAF[46] où nous voyons que le cyberespace est un espace immatériel, celui de l'information, qui englobe les autres espaces. Cet espace virtuel est contenu dans les systèmes informatiques et dans les systèmes de transmissions informatiques.

Le cyberespace militaire

Au plan militaire, " la supériorité de l'information est l'épine dorsale de la révolution des affaires militaires (RMA) "[47] . L'US Air Force, dans son document " Global Engagement : A vision for the 21st Century Air Force ", parle "d'Information Dominance" comme l'une de ses priorités et de ses compétences les plus élevées. *C'est en puissance de calcul, en brouilleurs et en capteurs, via satellites et radar, que les stratèges raisonnent désormais pour assurer la "dominance par l'information"*[48].

---

[42] Antoine Henri Jomini
[43] Duc de Wellington
[44] Duc de Wellington
[45] Napoléon Bonaparte
[46] Document USAF : Information Superiority, http://www.af.mil/lib/afissues/1997/issues31.html
[47] Rapport 98 de William S. COHEN, secrétaire d'état US à la Défense, devant le Congrès américain. Internet : http://www.dtic.mil/execsec/adr98/message.html. La Revolution in Military Affairs (RMA) est une action du DoD prenant en compte la révolution de l'information. Théorisé dès 1975 par le maréchal soviétique Orgakov !
[48] Quotidien Les Echos, jeudi 14 janvier 1999

De la fiabilité et de la robustesse de ce cyberespace dépend la puissance des Nations de la Troisième vague.

De la paralysie stratégique

C'est le rôle de la Grande Stratégie de découvrir et d'exploiter le talon d'Achille de la nation ennemie[49].

Basil Liddell Hart, en choisissant un titre suggestif, *Pâris ou l'avenir de la guerre,* rappelle la victoire mythique de Pâris qui a battu son adversaire Achille, grâce à une flèche bien tirée. Comme ce titre le suggère, *l'attaque des vulnérabilités de l'ennemi (par opposition à ses forces) est préférable. La technologie l'a rendu possible*[50].

De la paralysie stratégique

La notion de paralysie stratégique remonte loin dans le temps. Sun Zi en fut le meilleur apôtre : *Selon toutes les méthodes pour conduire une guerre, sauvegarder un pays vaut mieux que le détruire, sauvegarder une brigade vaut mieux que la détruire,...C'est pourquoi remporter cent victoires en cent combats n'est pas ce qu'il y a de mieux ; soumettre l'ennemi sans combattre est ce qu'il y a de mieux*[51].

Plus près de nous, John Frederick Charles Fuller, général britannique, premier organisateur d'une offensive blindée en 1917 à Cambrai, a dit : *La force physique d'une armée réside dans son organisation, contrôlée par son cerveau. Paralysez ce cerveau et le corps cesse de fonctionner*[52].

Le concept de paralysie stratégique est redevenu d'actualité car il a été rendu possible par la mise au point des armes de précision ou "intelligentes[53]". Elles permettent de détruire la cible, de haute valeur stratégique, en limitant les effets collatéraux. Ces armes sont des armes aériennes. C'est la raison pour laquelle ce sont les aviateurs qui ont le plus réfléchi, ces dernières années, à l'emploi de la puissance aérienne. Ils ont essayé d'en tirer des enseignements pour une nouvelle stratégie. Parmi ces penseurs qui ont dépoussiéré la stratégie il faut citer les colonels John Warden et John Boyd de l'US Air Force.

Le major David S. Fadok, ancien stagiaire à l'Air University, a effectué une comparaison intéressante entre les approches de Boyd et de Warden[54]. Fadok montre la convergence de leurs théories qui se rejoignent sur la paralysie stratégique par la puissance aérienne. Fadok relie la pensée de chacun des auteurs aux philosophies de Clausewitz et de Jomini. Mais cependant sans apporter d'éléments nouveaux à une stratégie nouvelle.

---

[49] B.H. Liddell Hart, *Pâris ou l'avenir de la guerre*

[50] David S. Fadok, *La paralysie stratégique par la puissance aérienne,* Institut de stratégie comparée

[51] Sun Zi, *L'art de la guerre*, De l'offensive par les plans, maxime n° 14, Trad. Valérie Niquet, Ed. Economica

[52] J.F.C. Fuller, *The foundations of the science of war*, cité par David S. Fadok

[53] Les armes qui peuvent se diriger seules sur leur cible

[54] David S. Fadok, *La paralysie stratégique par la puissance aérienne,* Institut de stratégie comparée

La paralysie stratégique selon Warden

Le colonel John Warden est un adepte de la paralysie stratégique. *Comme stratèges et hommes de l'art opérationnel nous devons nous débarrasser de l'idée que la partie principale de la guerre est le heurt de forces armées. Dans la guerre stratégique ce heurt peut certes se produire mais il n'est pas toujours nécessaire, devrait normalement être évité, et constitue presque toujours un moyen pour une fin et non une fin en lui-même*[55]. Il est partisan d'une guerre aérienne stratégique, de nature plus politique qu'économique ou anti-forces. Attaquer la direction ennemie est le moyen le plus efficace, le plus rapide et le moins coûteux pour parvenir à ses objectifs. Il est un héritier de Fuller.

Warden, dans *The Air Campaign,* est un ardent défenseur de la puissance aérienne, qui, selon lui, possède une capacité unique à réaliser les objectifs stratégiques de la guerre, avec une efficacité maximum à un coût minimum. La flexibilité, l'allonge et la vitesse permettent à l'avion de dépasser le champ de bataille pour aller frapper dans la profondeur, toutes les capacités de l'ennemi, de manière vive et décisive. L'ubiquité de la puissance aérienne multiplie théoriquement le nombre de centres de gravité stratégiques (nous retrouvons le concept clausewitzien du centre de gravité de l'ennemi) vulnérables aux attaques (par comparaison avec le nombre de ceux accessibles aux forces de surface), dotant ainsi les forces aériennes d'une capacité stratégique décisive plus grande. Warden définit le centre de gravité de l'ennemi comme *le point où l'ennemi est le plus vulnérable et sur lequel une attaque aura le plus de chance d'être décisive.* Le problème qui se pose est d'identifier ces centres de gravité. Warden prône l'utilisation de la puissance aérienne, qui seule peut atteindre **tous** les centres de gravité ennemi pour les détruire.

Cependant cette affirmation repose sur deux postulats :
- il faut que les centres de gravité soit de nature matérielle ;
- il faut que cet ennemi possède des centres de gravité vulnérables à une attaque.

Dans le premier cas, si le centre de gravité d'une guérilla est le soutien populaire, l'occupation du terrain par des forces terrestres aura l'avantage sur les attaques aériennes. Dans le second cas, si l'ennemi a prévu un système souple, facilement reconfigurable et redondant, il sera peu vulnérable.

Warden nous dit que *les meilleurs modèles au niveau stratégique sont ceux qui nous donnent l'image globale la plus simple possible. A mesure que nous avons besoin de plus de détails, nous agrandissons des parties de notre modèle de manière à voir les détails, de manière de plus en plus fine. Il est cependant important, qu'en construisant et en utilisant notre modèle, nous partions toujours de l'ensemble avant de descendre au détail*[56]. Il a ainsi présenté le système ennemi sous une forme *systémique*[57], pour :
- avoir une représentation globale et complète plus facilement compréhensible ;
- pouvoir descendre à un niveau de détail plus fin, sans perdre la vue d'ensemble ;
- chercher et trouver ses points *de vulnérabilité et de décision.*

Il a défini un modèle systémique en cinq cercles qui décrit une représentation de l'organisation d'une Nation. Parmi ces cinq cercles, représentant chacun une fonction vitale d'un pays, il s'agit d'identifier les centres nerveux à l'intérieur de chaque cercle et de les détruire.

---

[55] John A. Warden, *L'ennemi en tant que système*, Air Power Journal, printemps 95

[56] John A. Warden, *L'ennemi en tant que système*, Air Power Journal, printemps 95

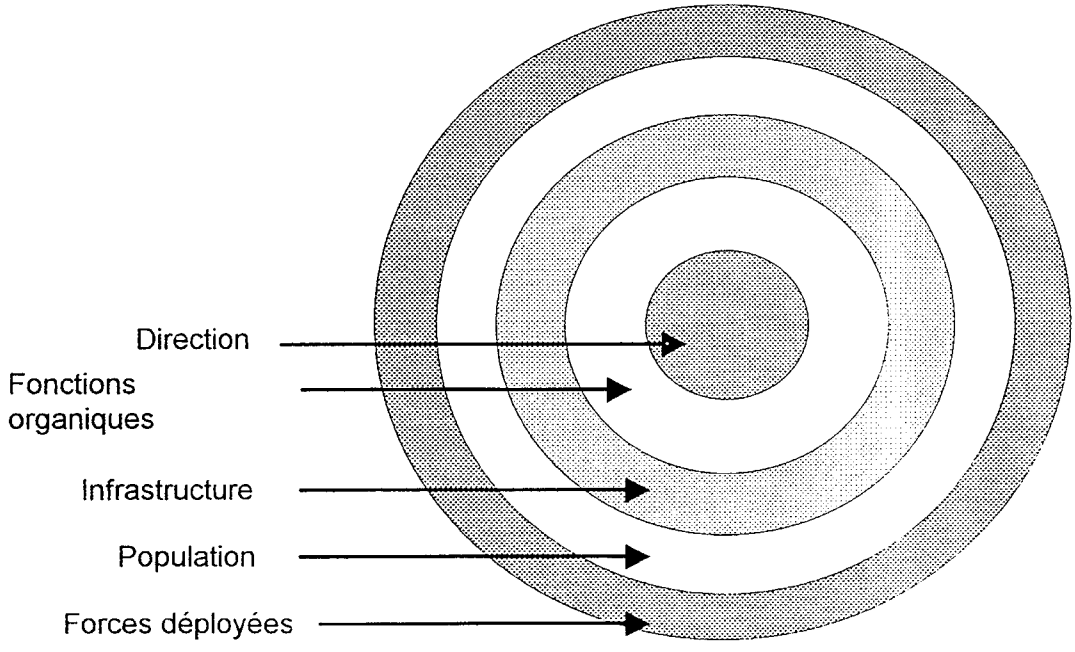
[57] La systémique est une technique permettant de décrire un système (social, militaire, économique..) sous une forme simplifiée, pour en faire l'analyse et comprendre le fonctionnement. Un système est représenté sous forme de "boîte" qui possède des propriétés, avec des flux en entrée et sortie, et une réaction entre la sortie et l'entrée.

L'intérêt de ce modèle est qu'il montre qu'il faut rechercher les attaques contre les centres de gravité et que celles-ci pourront s'effectuer de manière parallèle. Warden utilise une analogie biologique, en prenant le corps humain comme modèle, pour expliquer son modèle. Il l'étend ensuite à un Etat, à un cartel de la drogue et au réseau de distribution d'électricité. Le tableau suivant illustre ces analogies.

	Corps	Etat	Cartel de la drogue	Réseau électrique
Direction	Cerveau - Yeux - Nerfs	Gouvernement - Transmissions - Sécurité	Chef - Transmissions, - Sécurité	Centre de contrôle
Fonctions organiques essentielles	Transformation de la nourriture et de l'oxygène dans les organes vitaux	Energie (électricité, pétrole, nourriture) et monnaie	Production et transformation de coca	Agents (chaleur, eau) Production (électricité)
Infrastructures	Os, muscles, vaisseaux	Routes, Aérodromes, Usines	Laboratoires, routes, voies aériennes et maritimes	Lignes électriques Centrales
Population	Cellules	Habitants	Cultivateurs, Fabricants, Distributeurs	Employés
Mécanismes de lutte	Leucocytes	Armée, Police, Pompiers	Membres armés	Techniciens

Concept du système ennemi

Warden, avec la représentation suivante, montre que les entités stratégiques d'un pays peuvent être décomposées en cinq éléments. L'apparence de cible du modèle n'est pas neutre. Il s'agit bien de viser le centre de la cible pour gagner.



Le modèle en cinq cercles

Le premier cercle, celui du centre, est l'élément primordial du modèle, car il représente la direction nationale, le commandement. C'est le niveau qui prend les décisions. On peut le comparer au cerveau d'un organisme vivant. La transmission des ordres est essentielle. Quand les transmissions sont endommagées, les chefs ont les plus grandes difficultés pour mener la guerre.

Le second cercle représente les fonctions organiques essentielles. Il s'agit des installations et des processus sans lesquels l'Etat et son organisation ne peuvent continuer à fonctionner. Warden cite la production d'électricité, le raffinage du pétrole.

Le troisième cercle est celui des infrastrucures. Il comprend ainsi les systèmes de transport (chemins de fer, compagnies aériennes, autoroutes, ponts...). Warden parle aussi de transporter l'information. On peut penser qu'il s'agit des infrastructures lourdes de communications et non pas la fonction communication des systèmes d'information. En effet, chaque entité incluse dans chaque cercle comprend son propre système d'information.

Le quatrième cercle est celui de la population. Le soutien populaire peut être le centre de gravité d'une guérilla. L'attaque de la population n'est pas moralement acceptable. De plus, la seconde guerre mondiale a montré son inefficacité.

Le cinquième cercle est celui des forces militaires déployées de l'ennemi. C'est le cercle extérieur qui protège l'organisation des attaques extérieures. Si on attaque ce cercle en détruisant les forces de l'ennemi, on le soumet à notre volonté.

Une image représentant une analogie avec ce modèle pourrait être celle du système solaire. Pour le détruire, on peut imaginer détruire les planètes les unes après les autres. On peut imaginer détruire le soleil, plus de gravité et le système solaire s'effondre. On peut aussi mettre un écran entre le soleil et la Terre : plus de rayonnement, plus de vie sur Terre.

Une attaque contre le cerveau, paralyse l'organisme. C'est bien plus rapide et efficace que d'essayer de s'attaquer aux cercles extérieurs. L'attaque du cerveau peut se faire de manière physique. Mais un somnifère, propagé par les vaisseaux sanguins, peut être aussi une solution aussi efficace. Comme un virus dans un réseau informatique.

A l'intérieur de chaque cercle, existent plusieurs centres de gravité. La difficulté tient à l'identification et à la localisation de ces centres de gravité. Warden préconise, pour trouver les centres de gravité de l'ennemi, de décomposer chaque cercle jusqu'à ce que l'un d'eux laisse apparaître le facteur clé qui permettra d'obtenir la paralysie stratégique.

Warden propose trois manières pour imposer notre volonté à l'ennemi par :
- Une *stratégie de coût imposé* (coercition). Il s'agit de rendre la poursuite de la guerre trop coûteuse pour le commandement ennemi ;
- Une *stratégie de paralysie* . Cela consiste à rendre toute poursuite de la guerre impossible du point de vue commandement ennemi ;
- Une *stratégie de destruction*. C'est la recherche de l'anéantissement de la totalité du système ennemi. Cependant pour des problèmes de morale, Warden écarte cette stratégie militaire, politiquement non acceptable pour les guerres du XXI^{ème} siècle.

En dépit de la remarque de Napoléon, qui attribuait trois fois plus d'importance au moral qu'au physique, Warden se concentre uniquement sur les aspects physiques de la guerre. Il utilise la formule suivante :

Efficacité au combat = Force physique X Force morale

Cela lui permet de dire qu'on peut éliminer totalement l'efficacité au combat de l'ennemi en s'attaquant *exclusivement* aux composantes physiques de sa puissance.

Les défauts de ce modèle sont les suivants :

- Les centres de gravité ennemi doivent être de nature matérielle. Ceci est une sérieuse limite au modèle. Il dit qu'il est plus facile de détruire des cibles matérielles que le moral de l'ennemi. Warden justifie cette option en disant : *Il est conceptuellement possible de connaître le physique , donc, théoriquement, si je connais tout au sujet de l'ennemi, je peux réduire le terme physique de l'équation à zéro. Le moral, je ne connais à peu près rien de son état*[58]. Il est cependant très difficile de réduire à zéro la puissance d'un ennemi pour des raisons de moyens et de morale.
- Ce modèle est un peu simple (mais il peut être considéré comme le point de départ pour une analyse d'ordre supérieur) et surtout c'est un **modèle qui ne fait pas apparaître la dynamique des échanges** (décisions et transmissions des ordres). L'aspect temporel et la prise en compte des réactions inévitables de l'ennemi n'apparaissent pas non plus.
- Ce modèle ignore le monde de l'information et ne privilégie que l'attaque physique de l'adversaire.

Une stratégie fondée sur la cyberguerre, devrait permettre de s'affranchir des défauts identifiés. Pour cela, il faut définir un modèle, inspiré de celui de Warden, mais qui prendra en compte le cyberespace. Puis, définir les moyens pour trouver facilement, presque automatiquement, les centres de gravité et les paralyser. Pour cela, il faut étudier la paralysie stratégique selon Boyd, avec le concept de la boucle Observer-Orienter-Décider-Agir (OODA).

La paralysie stratégique selon Boyd

Le colonel John Boyd est un pilote de chasse qui a arpenté la « Mig Alley » en F-86 Sabre pendant la guerre de Corée. Il a, de manière intuitive, établi le concept de « manœuvres de transition rapide ». Il s'agissait de passer, plus rapidement que son adversaire, d'une manœuvre à une autre. A la fin de la guerre il fut affecté à la Fighter Weapons School de Nellis au Nevada, où il codifia ses leçons du combat air-air en un manuel tactique intitulé *Aerial Attack Study*. Quelques années plus tard, il quantifia ses idées tactiques sous forme de la théorie de l'énergie et de la manoeuvrabilité. Expert reconnu, il fut affecté au Pentagone, où il apporta son concours au projet d'avion de combat FX, alors en mauvaise posture. Les modifications qu'il apporta firent de ce demi-échec le meilleur avion de supériorité aérienne : le F-15. Cependant ce fut son travail pour le F-16 qui confirma ses affinités pour les manœuvres de transition rapide. Cet état d'esprit fut très important pour la suite de sa carrière et sa théorie de la paralysie stratégique.

Après avoir quitté le service actif, Boyd fit évoluer son concept tactique de manœuvre aérienne de transition rapide en une théorie plus générale du conflit. « *Destruction and Creation* » fut le premier essai d'une quinzaine de pages qu'il écrivit en 1976. Ensuite il poursuivit la diffusion de ses idées par une série de cinq articles sous le titre collectif : « *A Discourse on Winning and Losing* »[59].

Boyd s'attache à analyser le processus décisionnel de l'ennemi afin d'en déceler les failles pour s'y introduire, le ralentir, l'empêcher de fonctionner ou le corrompre. Il s'agit de faire preuve d'une « agilité mentale » supérieure à celle de l'ennemi (on retrouve la philosophie de manœuvre de transition rapide, appliquée à la théorie du conflit). Boyd insiste

[58] Interview de Warden rapportée par Fadok

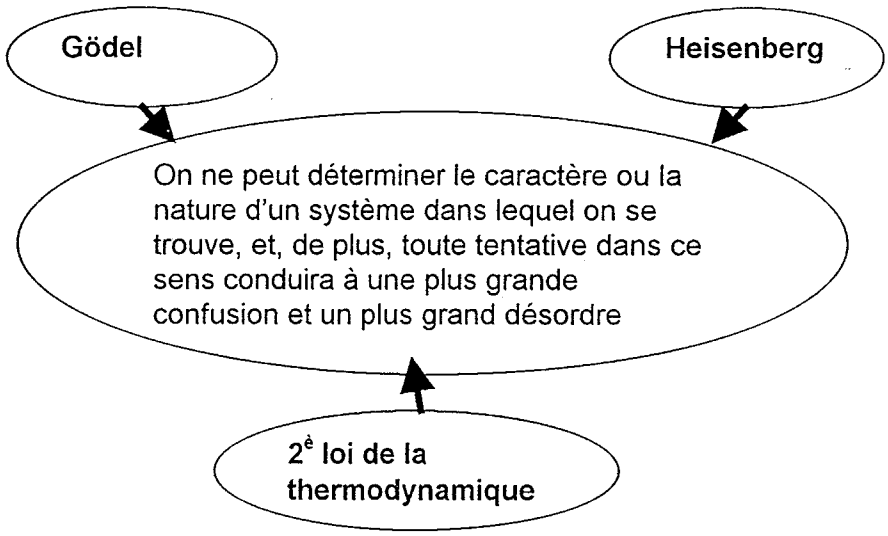
[59] John R. Boyd. *A Discourse on Winning and Losing*. Air University Library , document M-U 30352-16

sur l'importance critique de ce processus cognitif vital pour gagner dans un monde imprévisible et marqué par la compétition.

Dans *Destruction and Creation*, Boyd relie trois théories scientifiques issues des mathématiques, de la physique et de la thermodynamique pour servir de base à sa théorie :

- Les théorèmes d'incomplétude de Gödel[60]. *Ainsi, la démonstration de Gödel montre indirectement que pour déterminer la consistance de n'importe quel nouveau système, nous devons construire ou découvrir un autre système au delà de ce nouveau système*[61].
- Le principe d'incertitude d'Heisenberg[62]. *Les valeurs de l'incertitude ne représente pas seulement le degré d'intrusion de l'observateur dans l'observé mais aussi le degré de confusion et de désordre perçu par cet observateur*[63].
- La deuxième loi d'entropie[64]. *...l'entropie doit croître dans tout système clos, ou dans tout système qui ne peut pas communiquer de manière ordonnée avec d'autres systèmes ou environnements extérieurs à lui-même*[65].
-

Tout ceci conduit à résumer la pensée de Boyd sous la forme du diagramme suivant :



De cette proposition de base Boyd construisit une théorie générale du conflit liant la victoire au repli de l'adversaire sur lui-même (de façon à augmenter son entropie, son désordre intérieur, donc son incapacité à poursuivre le combat de manière efficace). Il dit : *...l'incertitude et le désordre générés par un système replié sur lui-même peuvent être*

---

[60] En 1931 Kurt Gödel a développé le postulat selon lequel il est possible, pour tout système symbolique formel, de construire une proposition qui ne peut être ni prouvée ni réfutée, dans le cadre du même système. Les théorèmes d'incomplétude de Gödel posent un problème scientifique beaucoup plus général. En effet, ils montrent qu'une théorie scientifique ne peut expliquer l'ensemble des phénomènes observés, et que deux théories radicalement opposées peuvent coexister et s'appliquer aux mêmes phénomènes naturels.

[61] John Boyd, *Destruction and Creation*, traduction de l'auteur

[62] Werner Heisenberg a énoncé le principe, dit d'Heisenberg, de mécanique quantique selon lequel il est impossible de spécifier simultanément et avec précision la position et la vitesse d'une particule, tel un électron.

[63] John Boyd, *Destruction and Creation*, traduction de l'auteur

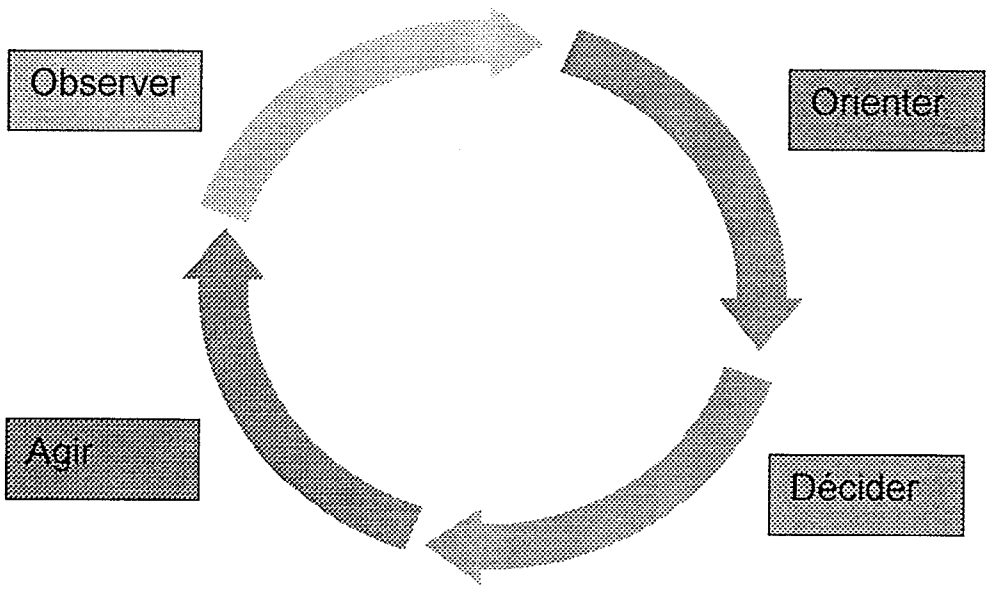
[64] Appelé aussi principe de Carnot, ce deuxième principe de la thermodynamique fait intervenir une grandeur d'état, l'entropie *S*, qui mesure le désordre du système à l'échelle moléculaire. Le deuxième principe énonce que l'entropie d'un système isolé ne peut que croître. En conséquence, lorsqu'un système a atteint son état d'équilibre, son entropie est maximale. La nature semble donc «préférer!» le désordre à l'ordre.

[65] John Boyd, *Destruction and Creation*, traduction de l'auteur

compensé par une ouverture vers l'extérieur et en créant un nouveau système[66]. Il s'agit donc d'obliger l'adversaire *à se replier sur lui-même* et à l'empêcher de s'ouvrir vers l'extérieur. Le but militaire de Boyd est de « *briser l'esprit et la volonté du commandement ennemi en créant des situations stratégiques ou opérationnelles surprenantes et dangereuses* »[67]. Il s'agit d'opérer à une cadence plus rapide que celle de l'adversaire pour ne pas lui laisser le temps de s'adapter mentalement à l'enchaînement rapide des évènements incertains d'un conflit. Il s'agit de désorganiser l'adversaire en lui présentant de manière répétitive *un mélange d'évènements ambigus et menaçants, et d'autre part d'évènements non menaçants visant à le leurrer*[68].

Nous avons là une différence fondamentale par rapport à l'approche de Warden qui considère un modèle statique. A l'inverse de Clausewitz, qui recommande de détruire les « centres rayonnants de mouvements et de puissance », Boyd recommande de créer des centres de gravité non coopératifs, en attaquant les liaisons morales-mentales-physiques qui lient ces centres les uns aux autres. Le résultat final est la destruction de l'harmonie de l'organisation interne de l'ennemi, en détruisant ses connexions avec le monde extérieur.

Boyd soutient que tous les comportements relationnels humains, individuels ou en groupe, peuvent être décrits par un cycle de quatre tâches : l'observation, l'orientation, la décision et l'action.

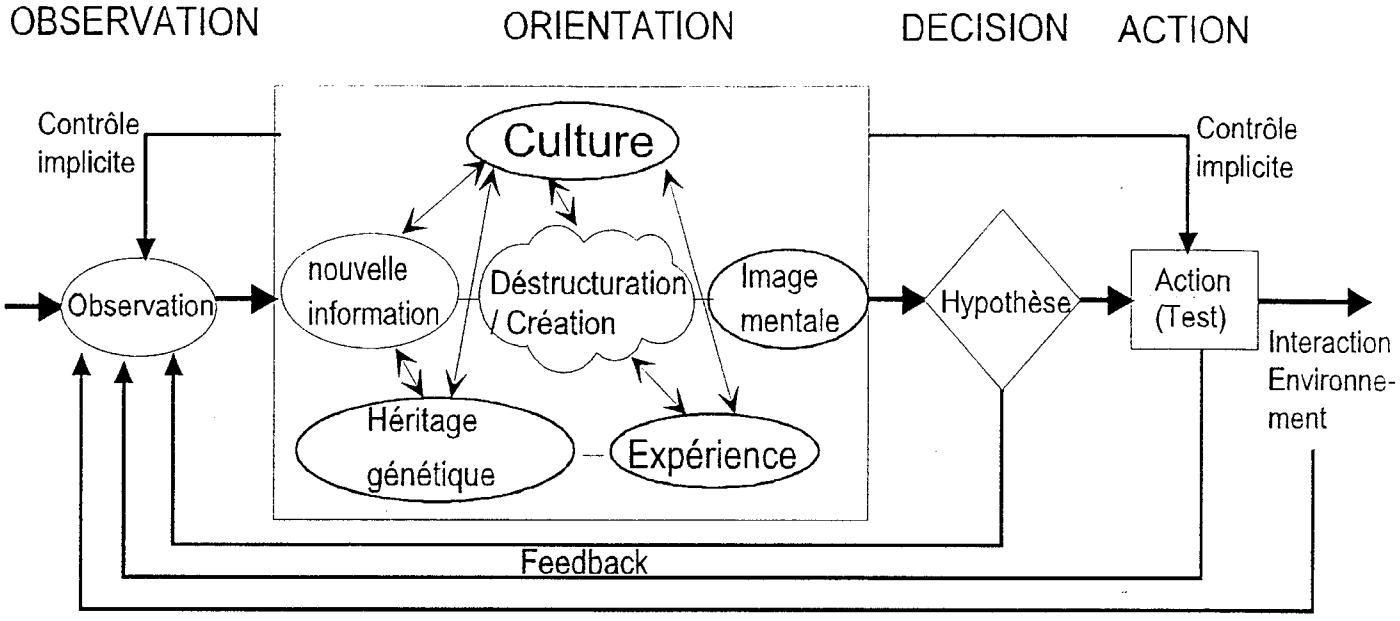


Ce processus décisionnel a été représenté d'une manière systémique sous la représentation de la boucle Observation – Orientation – Décision – Action (OODA). Cette analyse est plutôt une théorie du conflit qui met l'accent sur les processus mentaux et temporels de l'ennemi.

Le schéma suivant présente la boucle OODA telle que Boyd l'a décrite. Le nuage « déstructuration/création » correspond à une forme moderne d'analyse/synthèse.

---

[66] John Boyd, *Destruction and Creation*, traduction de l'auteur
[67] William Lind cité par D. Fadok dans *La paralysie stratégique par la puissance aérienne*
[68] John Boyd, *Patterns of Conflict*, traduction de l'auteur



Le cycle OODA de Boyd

Le second O, Orientation, dépositaire de notre héritage génétique, de nos traditions culturelles et expériences passées, est la part la plus importante de la boucle OODA car il modèle notre façon d'observer, de décider et d'agir[69].

La grande force de la théorie de Boyd est l'importance de la dimension temporelle. C'est aussi sa faiblesse. Un ennemi peut ne pas vouloir entrer dans ce jeu. C'est le cas des adversaires qui *ralentissent sciemment* le tempo de la guerre. Par exemple, ce fut le cas de la guerre de résistance que Mao Ze Dong livra aux Japonais. Il proposa le concept de guerre prolongée pour venir à bout du Japon.

C'est aussi le cas des guérillas. Le centre de gravité peut être le soutien de la population. Le moyen d'en venir à bout consistera à faire une communication de propagande. C'est aussi une forme de guerre de l'information !

Complémentarité des deux théories

Boyd et Warden ont chacun établi une théorie qui s'attache à rechercher la paralysie stratégique de l'adversaire. Ils soutiennent que la cible doit être le commandement ennemi. Pour cela, le moyen le plus efficace et le plus sûr, pour transformer les opérations militaires en succès politique, est de paralyser ce commandement.

Warden développe dans son modèle en cinq cercles une théorie pratique : l'attaque rapide et simultanée des forces physiques ou les centres de gravité de l'ennemi.

Boyd décrit, dans son modèle de la boucle OODA, une théorie plus abstraite : la manœuvre à l'intérieur du processus intellectuel de l'ennemi.

[69] John Boyd, *Organic Design*, p. 26, Air University Library, Traduction de l'auteur

Les théories de Boyd et Warden se complètent. Boyd parle d'opérer sur un rythme décisionnel plus rapide que celui de l'ennemi, Warden prône la guerre de haute technologie. Lorsque Boyd cherche à s'immiscer dans la boucle OODA de l'ennemi (dans son C4I[70]), Warden cherche à trouver ce C4I et le détruire *physiquement*.

Il est intéressant de noter que les travaux de ces deux aviateurs ont redonné à l'arme aérienne conventionnelle une dimension stratégique qu'elle avait perdue.

A côté de la puissance et de la force militaire, **la guerre de l'information est un nouveau moyen de parvenir à la paralysie stratégique**.

Il s'agit d'utiliser le modèle de Warden, en y apportant quelques aménagements en précisant la place des systèmes d'information dans chaque cercle. Ce modèle clarifié sera ensuite complété des fonctions stratégiques du cyberespace. Ces fonctions sont mises en oeuvre dans les centres de gravité. Il s'agira ensuite, suivant en cela la philosophie de Boyd, de rechercher des moyens d'action cybernétiques pour mettre hors d'usage ces centres nerveux, soit en les détruisant, selon Warden, soit en entrant dans la représentation mentale des images de l'ennemi, selon Boyd, par des moyens de guerre informatique.

Il s'agit d'imaginer une stratégie de l'ère du cyberespace : la cyberstratégie qui sera une stratégie de paralysie, utilisant des moyens cybernétiques, qui plongera ses racines chez Sun Zi, Fuller, Hart et plus près de nous, Boyd et Warden.

De la cyberstratégie

La guerre de l'information dans *Air Force 2025*

Les études sur la guerre de l'information ou *Information Warfare* sont déjà lancées depuis longtemps outre-atlantique. Le nombre de publications lui étant consacrées est considérable. On y parle d'opérations de l'information, d'attaques de l'information...Ce sont essentiellement des écrits de tactique pour gagner des batailles de la guerre de l'information.

Dans *Air Force 2025*, plusieurs documents de recherche ont été publiés qui concernent la guerre de l'information à l'horizon 2025. Un document a particulièrement retenu mon attention : *Information Operations : Wisdom Warfare for 2025*[71].

Dans ce document, les opérations de l'information, dans le cadre de la puissance aérospatiale, y sont décrites. La guerre de l'information recouvre tous les domaines où s'exerce la puissance militaire.

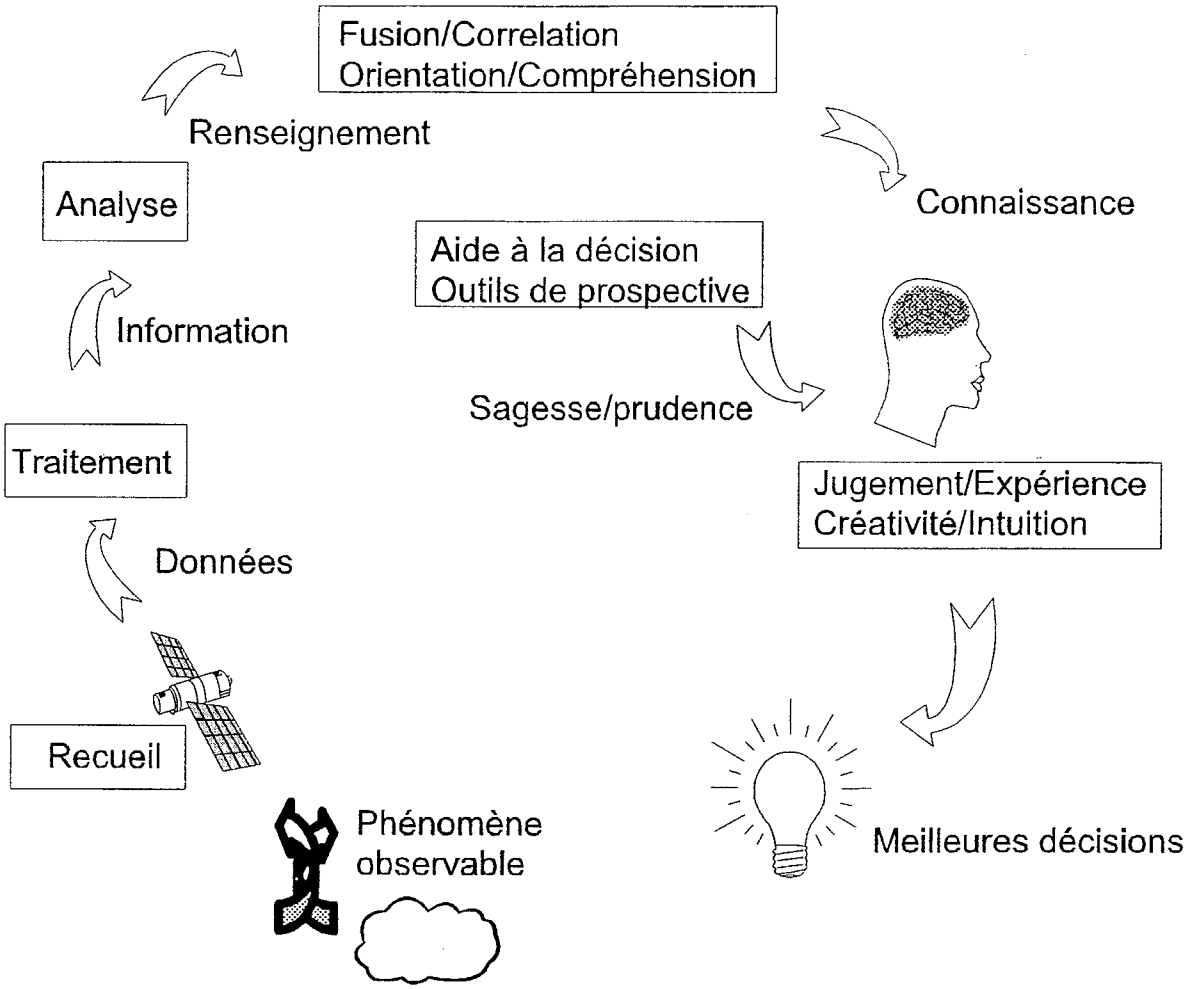
Une notion importante est la *sagesse* (wisdom) définie comme le savoir (knowledge) assorti d'un bon jugement (good judgment). Il s'agit de mettre en place une « architecture de sagesse » pour conduire la guerre et cette architecture, va aider, de manière considérable, le combattant à prendre les bonnes décisions.

---

[70] Command, Control, Communications, Computers, Intelligence

[71] Information Operations : Wisdom Warfare for 2025, Research paper, April 1996, Air University.

Il faut tout d'abord décrire le processus de traitement d'une donnée brute (qui s'apparente à la boucle OODA de Boyd sans la partie « feedback »).

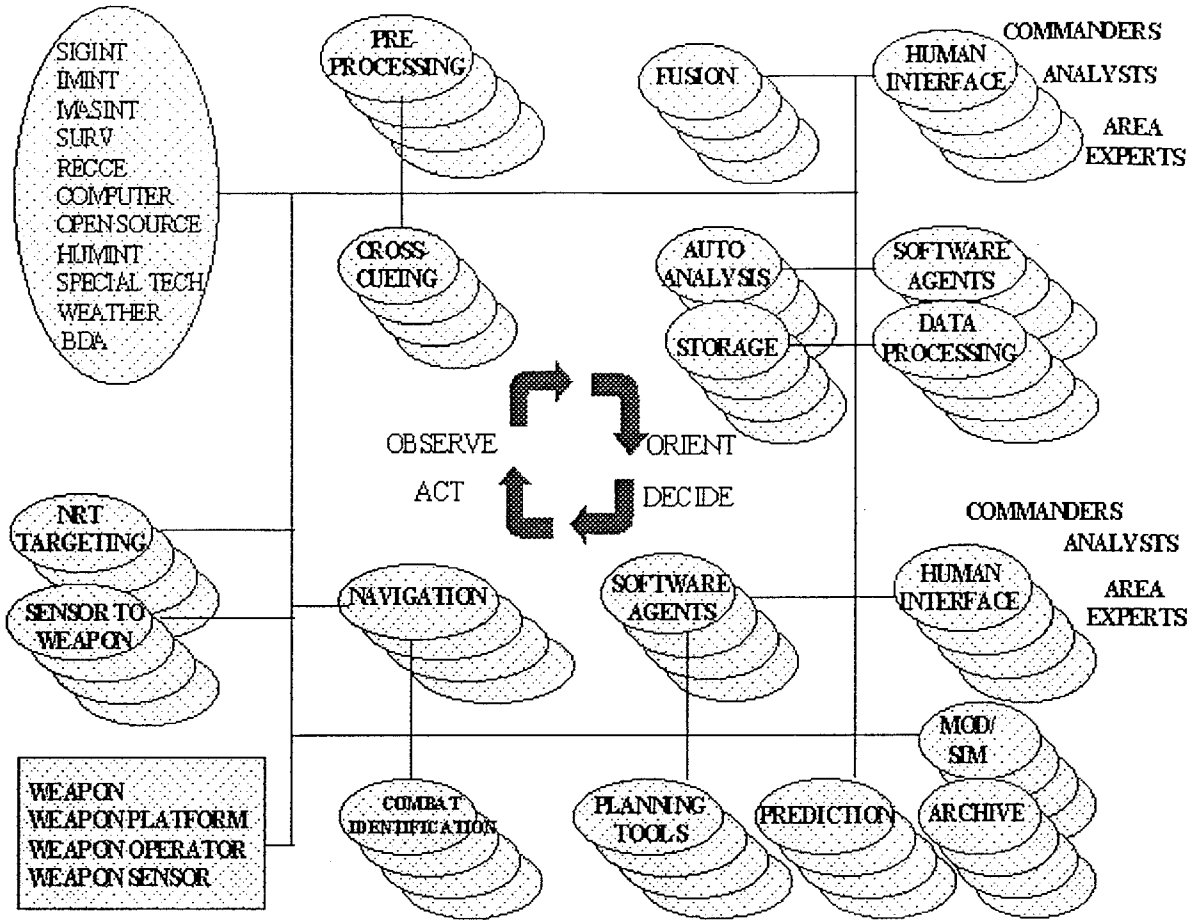


Le processus de « la décision avisée » [72] [73]

Dans ce circuit de l'information, nous pouvons identifier plusieurs grandes fonctions : recueil, transmission, traitements à divers moments et endroits.

Ce processus de la sagesse débouche sur une architecture de la guerre avisée : « Wisdom Warfare Architecture ». Le schéma suivant montre l'architecture imaginée.

[72] "Décision avisée" me semble plus adapté que "Décision de la sagesse"
[73] Information Operations : Wisdom Warfare for 2025, Research paper, April 1996, Air University,



Wisdom Warfare Architecture[74]

Cette architecture est articulée autour des quatre fonctions du modèle OODA de Boyd (les auteurs disent que ce découpage des outils autour des fonctions de Boyd n'est qu'une illustration car il est difficile de catégoriser formellement ceux-ci). Cependant on peut remarquer que ce qui forme l'environnement OODA est constitué **de modules qui comprennent tous une fondation informatique.**

Curieusement, dans ce document et tous ceux consacrés à la guerre de 2025, une stratégie globale pour conduire une cyberguerre n'est pas envisagée. Il n'existe pas de cyberstratégie. J'entends par cyberguerre, une lutte des moyens informatiques : l'attaque ou la défense de l'informatique par l'informatique.

Les fonctions invariantes du cyberespace

Chacun des modules du précédent schéma (fonctions, outils, tâches, armements) comporte une partie qui traite de l'information de manière automatique[75]. Un moyen d'empêcher le module de remplir sa tâche, donc de paralyser son adversaire, est d'attaquer la fonction informatique qui soutient la fonction du module.

[74] Information Operations : Wisdom Warfare for 2025, Research paper, April 1996, Air University,
[75] Traitement automatique de l'information = définition de l'informatique

Une analyse de ces modules, nécessaires à la conduite des opérations selon la boucle OODA, conduit à identifier dans le substrat informatique, plusieurs fonctions qui manipulent de l'information. Identifions les.

Dans la fonction « **OBSERVER** » de l'architecture, il s'agit de collecter l'information. On retrouve les éléments traditionnels du renseignement (SIGINT, IMINT, MASINT, HUMINT[76]), de la surveillance et de la reconnaissance. Les capteurs météorologiques et les capteurs de numérisation du terrain en font partie.

Se trouve là un élément récurrent : le **recueil** de données. Pour réduire le temps de transfert de ces données (accélération de notre propre boucle OODA), celle-ci est traitée au niveau des capteurs. Il y a donc une fonction **traitement**.

Ces données traitées deviennent alors une information. Cette information doit être ensuite transmise vers le sol ou le centre de commandement. D'où la fonction **transmission**.

Pour que cette information ne soit pas interceptée et lue (l'adversaire sait ce qu'on sait et peut en tirer des conclusions : intrusion dans notre propre boucle OODA), altérée (ralentissement de notre boucle OODA), ou interceptée, modifiée et retransmise à notre insu (intrusion dans notre propre boucle OODA et modification de notre image mentale de la situation), il faut la chiffrer. D'où la fonction **protection**.

Avant de parvenir au décideur, l'information doit être fusionnée et corrélée avec d'autres afin de gagner en pertinence. D'où un nouveau **traitement** (souvent lourd et coûteux en ressources informatiques).

Lorsque cette information sera enfin parvenue au chef, en temps utile et en ayant gardé toute sa pertinence, celui-ci l'analysera et en tirera des conclusions. Par exemple il jugera qu'il est indispensable de la faire connaître à ses subordonnés. Il y a là une fonction de **partage** (différente de celle de transmission)[77].

La fonction « **AGIR** » est étroitement liée à la fonction « Observer ». Il y a un lien direct entre le système d'arme et le capteur. Ce lien (liaison de données en temps quasi réel), permettra à l'armement tiré de se diriger vers sa cible grâce à des systèmes de guidage évolués comme par exemple le recalage GPS[78] (sensor-to-weapon). Une autre liaison de données permettra aux senseurs (AWACS, satellites, drones, avions de reconnaissance...) de fournir au tireur une situation tactique à jour au moment du tir (sensor-to-shooter). Les systèmes d'armes devront donc utiliser les fonctions identifiées pour la fonction « Observer » : recueil, traitement, transmission, protection et partage.

Le composant « **ORIENTER** » de l'architecture décrite, réalise la fonction « Connaissance » des opérations[79] de l'information. Cela inclut les nœuds où les fonctions de fusion, d'analyse, de stockage et de recherche des données sont exécutées. Cette quantité énorme d'information est trop grande pour que des êtres humains puissent la maintenir à jour et la retrouver facilement sans l'aide de l'informatique. Par exemple la fusion de données est cruciale pour maintenir cette énorme quantité d'information disponible et la

---

[76] SIGnal INTelligence : renseignement d'origine éléctromagnétique ; Imagery INTel : renseignement à partir d'images (spatiales, aériennes ou autres) ; Measure And Signature INTel : renseignement basé sur la mesure et la signature des signaux électromagnétiques ; Human INTel : renseignement d'origine humaine

[77] Le partage de l'information comprend le stockage, l'autorisation d'accès (via un réseau) aux personnes autorisées (d'où gestion de serveurs, réseau locaux ou étendus, profils utilisateurs, mots de passe et chiffrement)

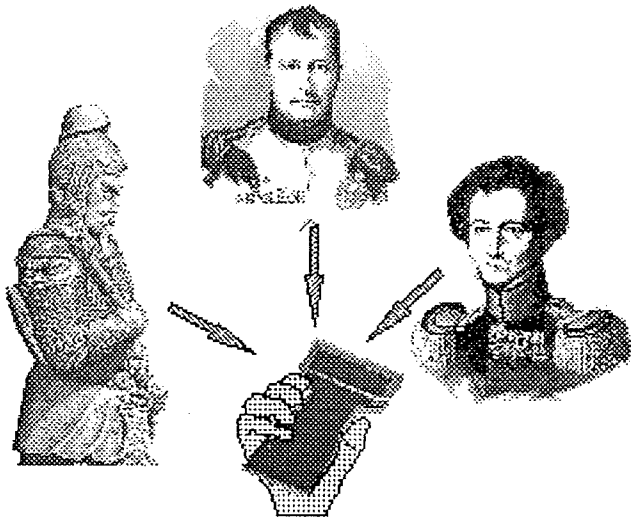
[78] Global Positioning System : système de positionnement par satellite permettant une navigation précise

[79] Au sens opérations militaires

transformer en une information utile sans saturer aussi bien les cerveaux des décideurs que les systèmes informatiques eux-mêmes. Une nouvelle fonction est apparue : la fonction **archivage/stockage**.

La fonction « **DÉCIDER** » constitue le niveau « sagesse »[80] de l'architecture. Pour décider, le chef a besoin d'outils de modélisation, de simulation, de prévision, d'aide à la décision, de planification. Pour cela, il a besoin de l'information qui a été archivée et qui constitue la mémoire . Apparaît à nouveau la fonction **archivage**.

Un outil, très puissant, du composant « Sagesse » de l'architecture est d'utiliser le «fantôme des génies[81]». Il s'agit d'utiliser les concepts inventés par de grands stratèges historiques. On leur soumet les conditions de la situation actuelle. Puis on en tire les évènements les plus probables (COA)[82] que ces stratèges auraient retenus.



"Genius Ghosting" : Sun Zi, Napoléon, Clausewitz[83]

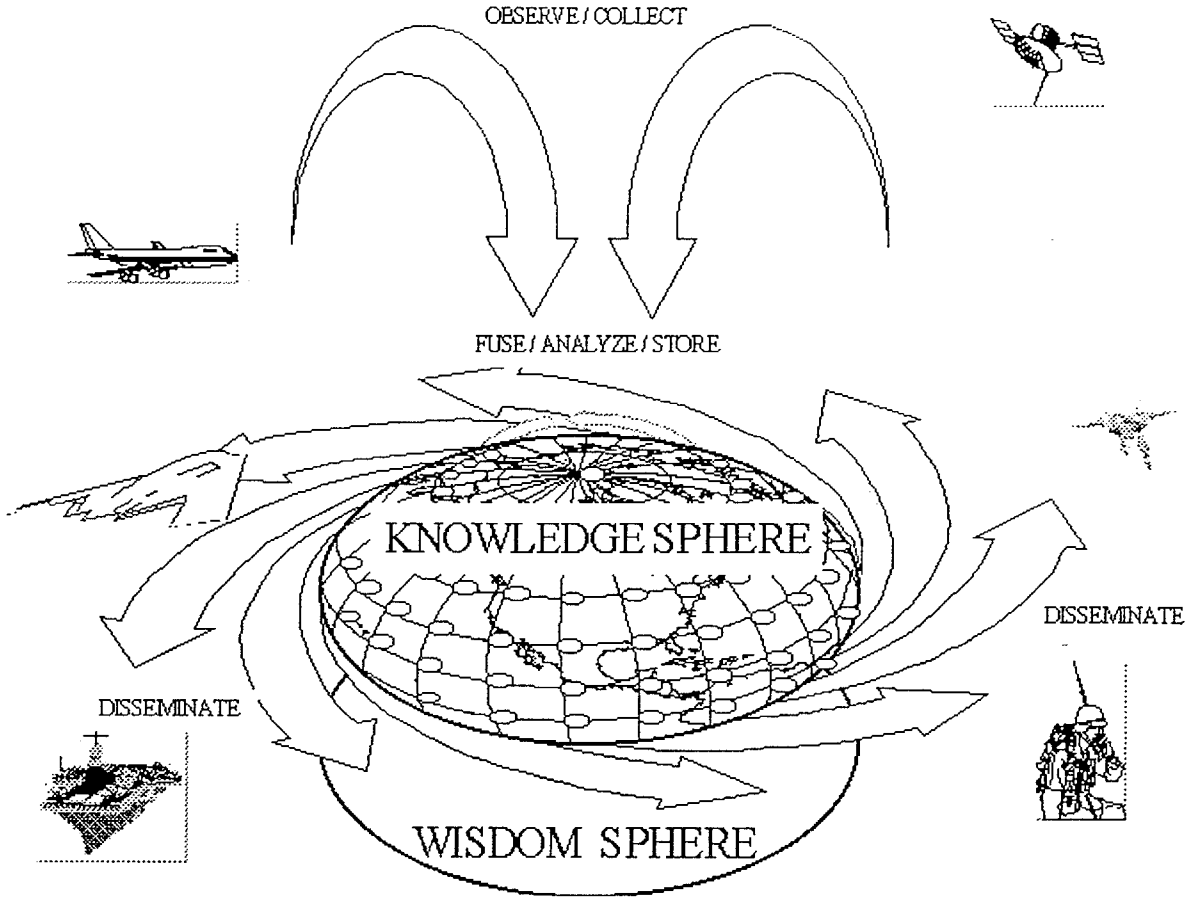
Il suffit d'introduire ces actions dans des simulations pour calculer la probabilité d'occurrence de chacune de ces actions probables. Les institutions académiques peuvent fournir le cadre historique. Le composant « Connaissance » fournit le contexte courant. Les modèles donnent la marche des évènements. La simulation donne la probabilité d'occurrence. En comparant les résultats des simulations issues des COA des différents «fantômes des génies», le chef pourra donc choisir entre une grande variété de solutions.

Cependant le décideur a un parti pris ou un penchant avec l'information qu'il utilise pour prendre sa décision. Et cela aucune architecture décisionnelle ne peut l'empêcher. De plus, comme l'architecture tend à se rapprocher de l'esprit humain, le décideur aura tendance a se reposer sur celle-ci.

Le schéma suivant, tiré du document de recherche de l'USAF, donne une représentation des échanges entre le monde réel et celui des domaines de la connaissance et de la sagesse.

---

[80] « Wisdom Sphere » dans le texte original
[81] « Genius Ghosting »
[82] Course Of Action dans le texte original (COA)
[83] Information Operations : Wisdom Warfare for 2025, Research paper, April 1996, Air University



Les domaines de la Connaissance et de la Sagesse[84]

Que ce soit aujourd'hui ou encore plus à l'horizon 2025, le cyberespace sera bâti sur des systèmes informatiques de plus en plus puissants, disséminés au plus près du recueil de l'information. Ils seront omniprésents et omnipotents. Pour utiliser ce cyberespace à notre avantage, il faut protéger ses fondations. Pour combattre un adversaire, il suffit d'attaquer les fondations de son cyberespace. Et toute son organisation s'écroule !

L'analyse précédente a permis d'identifier six fonctions :
- Recueil ;
- Archivage/stockage ;
- Traitement ;
- Transmission ;
- Protection ;
- Partage[85].

Ces six fonctions constituent les six axes stratégiques de la cyberwar.

Comment intégrer ces six fonctions à un modèle qui représente ce concept ?

[84] Information Operations : Wisdom Warfare for 2025, Research paper, April 1996, Air University
[85] Nous appelerons ces cinq fonctions RAT^2P^2 pour plus de commodité

Le modèle de la roue

Comme nous l'avons vu précédemment, les six fonctions RAT^2P^2 identifiées constituent le socle du cyberespace. Nous avons aussi vu que le cyberespace est un espace virtuel qui contient tous les autres espaces physiques. Il contient donc toutes les composantes d'un système ennemi. Warden a défini un modèle en cinq cercles décrivant le système de l'ennemi. Utilisons ce modèle comme base, en précisant la place de l'information dans chaque cercle et en lui adjoignant les fonctions invariantes du cyberespace.

Le schéma suivant montre le modèle des cinq cercles, complété de six rayons. **Dans ce nouveau modèle, chaque cercle possède ses propres systèmes d'information.**

Le premier cercle, celui de la direction nationale, est le niveau où se prennent les décisions. Il comprend donc son propre système d'information avec une partie transmission pour donner ses ordres et recevoir les informations des autres cercles.

Le second cercle, celui des des fonctions vitales, possède les systèmes d'information propres à chaque activité. Par exemple, si on s'attaque au système de commandement ou de contrôle d'une raffinerie, celle-ci ne pourra remplir sa tâche et l'approvisionnement en carburants des forces ne sera plus assuré.

Le troisième cercle, celui des infrastructures, comprend tout ce qui participe aux transports. Les systèmes d'information de ce cercle sont très sensibles. En effet, si on s'attaque au système de circulation des trains, cela suffit pour complètement paralyser la fonction de transport ferroviaire. Puis, par transfert des passagers et du fret vers le transport routier, il y aura engorgement de ce type de transport, saturation et blocage.

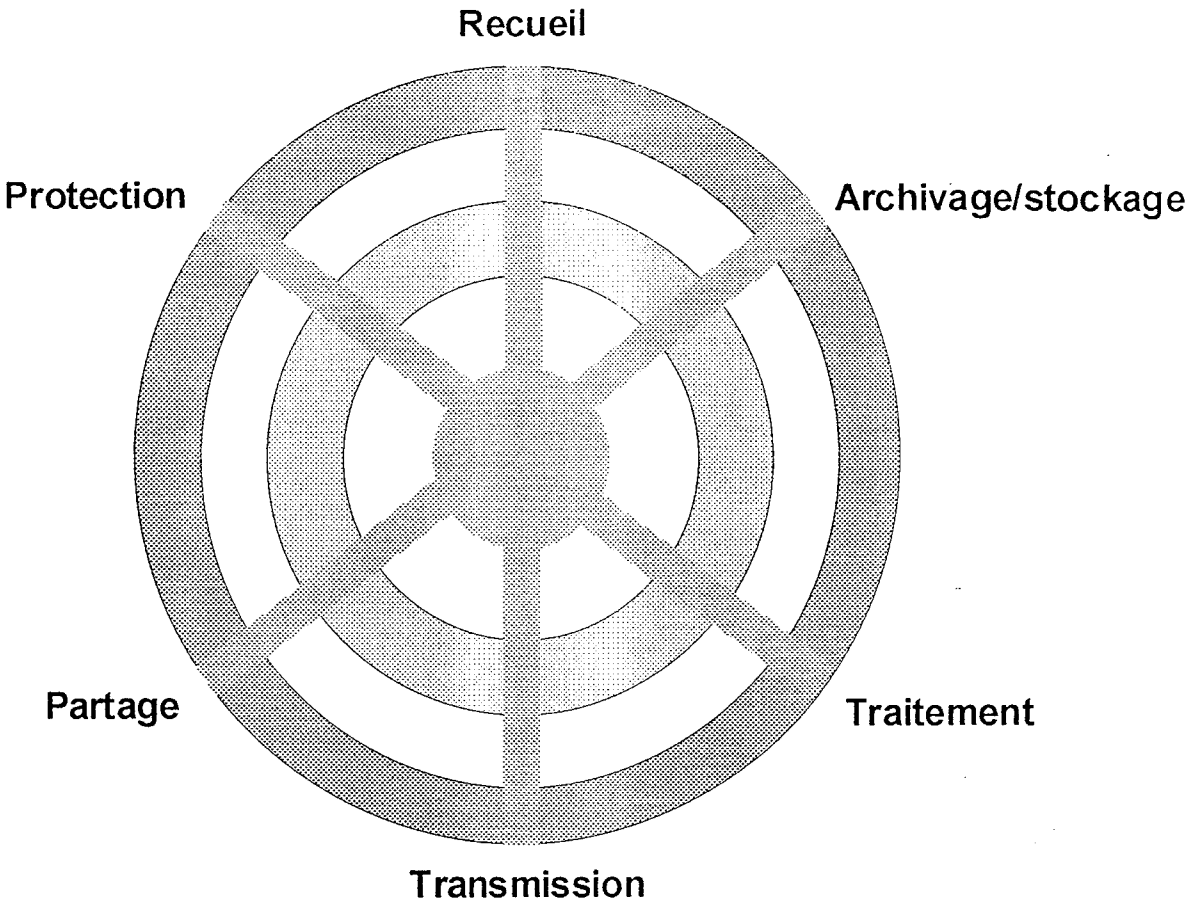
Pour ce cercle, Warden parle de transport d'information. Dans le modèle revisité, il faut comprendre : infrastructures de communications tels que câbles téléphoniqes, fibres optiques ou faisceaux hertziens. Cela n'aurait aucun sens de mettre tout ce qui concerne les systèmes d'information dans un seul cercle. Il faut distinguer les systèmes d'informations et les systèmes qui les supportent, propres à chaque cercle, des infrastructures lourdes de transport de cette information.

Le quatrième cercle, celui de la population, possède aussi ses propres systèmes d'information. La presse et les médias constituent des systèmes d'information de ce cercle et des centres de gravité. On le voit chaque jour, l'action des médias vis-à-vis de l'opinion publique est essentielle lors d'opérations militaires comme en Iraq ou au Kosovo.

Le cinquième cercle, celui des forces armées ennemies déployées, est le cercle qui nous intéresse au premier chef. Ce cercle comprend de nombreux systèmes d'information, qui constituent autant de centres de gravité.

Les six rayons de la roue, représentent chacun une fonction stratégique du cyberespace.

Les six fonctions stratégiques du cyberespace recouvrent ainsi toutes les entités stratégiques d'un adversaire. Il s'agit d'une représentation conceptuelle, et non pas d'une représentation physique. En effet, la fonction « Recueil » est toujours couplée à la fonction « Transmission » (et parfois à la fonction « Protection »). Physiquement, elles sont confondues, conceptuellement elles sont séparées.



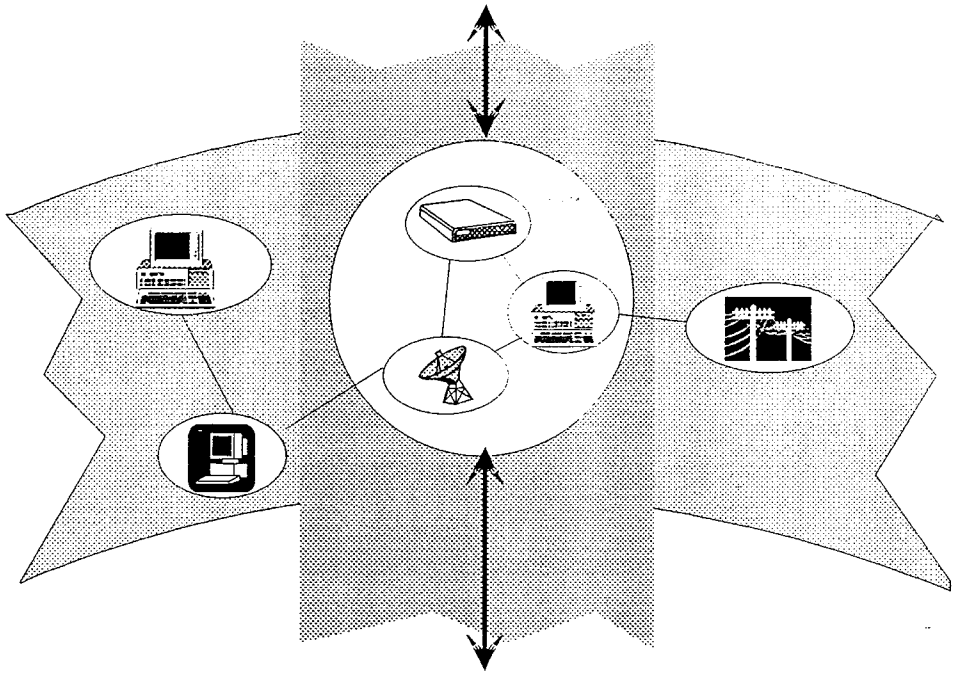
Le modèle de la Roue

Tous les rayons ont été représentés avec le même diamètre. Si chaque fonction n'a pas la même importance en termes de ressources humaines, informatiques ou financières, l'attaque de l'une d'elle suffit à atteindre et détruire, par effet cumulatif, le cyberespace de l'adversaire. Donc toutes les fonctions ont la même importance dans ce modèle conceptuel.

Etudions comment s'effectuent les connexions entre les rayons (les fonctions stratégiques) et les cercles représentant les entités stratégiques.

Dans chaque cercle stratégique, il existe des centres de gravité liés à la nature de ce cercle. Souvent ces centres de gravité sont difficiles à trouver ou extrêmement protégés. Se pose alors le problème de trouver ces centres nerveux et les attaquer.

La nouvelle approche proposée, consiste à rechercher non pas ce centre nerveux, mais plutôt ses connexions avec le reste du cercle, et les connexions avec les autres cercles. Il s'agit d'isoler le cerveau de ses forces. Il existe un espace de l'information propre au cercle, qu'on pourrait appeler un sous-cyberespace, et le cyberespace est l'ensemble de ces espaces connectés ensemble. Le schéma suivant montre les centres nerveux d'information (CNI) d'un cercle connecté au CNI du cyberespace (il s'agit là aussi d'une représentation conceptuelle).



Il suffit d'attaquer une seule de ces fonctions pour s'introduire dans l'espace de manœuvre temporel et intellectuel de l'adversaire.

Si on attaque, par exemple, la fonction « Transmission » à quelque niveau que ce soit, l'information ne pourra irriguer les autres cercles et, surtout, la direction nationale, le « cerveau » du système. Pour attaquer la fonction « Transmission », on peut attaquer le centre de télécommunication de l'entité visée (du cercle). On peut aussi couper la liaison en coupant physiquement le support de transmission. S'il s'agit d'un système radio, on peut brouiller le signal.

Avec l'omniprésence des moyens informatiques dans les systèmes de transmission, il suffit de s'attaquer au système informatique (les moyens sont nombreux et seront développés plus loin) pour empêcher la fonction « Transmission » de remplir sa tâche. On peut couper la connexion qui existe entre un cercle et une des fonctions RAT^2P^2. Dans ce cas, le cercle stratégique ne pourra communiquer avec les autres cercles, et surtout avec le cercle central de la direction nationale. Le cercle sera déconnecté des autres cercles. On aura créé des **centres de gravité non-coopératifs**, tel que le recommande Boyd. Le système ennemi complet ne recevra, ni ne transmettra d'information. Il sera sourd et aveugle. Selon la dialectique de Boyd, il se retrouvera « replié[86] » sur lui-même. Son entropie augmentera, sa capacité à donner les réponses adéquates à nos propres actions sera perdue. Il sera paralysé, incapable de suivre le rythme des opérations que nous lui imposerons, tel que l'exige le concept de la boucle OODA. Nous aurons effectué la paralysie stratégique de notre adversaire et atteint notre but, c'est-à-dire gagner la guerre.

Ce mode d'action fonctionne avec toutes les autres fonctions de la même manière, avec une petite différence pour la fonction « Protection ». La fonction « Protection » est une fonction particulière, car en l'attaquant, on peut s'introduire dans la boucle OODA de l'adversaire sans que celui-ci ne s'en aperçoive. On pourra alors savoir ce qu'il projette et surtout le duper. En effet, en interceptant ses transmissions, en les déchiffrant, on peut

[86] "...to fold adversary back inside himself..." John Boyd. *Strategic Game*, p. 44, traduction auteur

connaître ses plans. On peut aussi "rejouer" la transmission en modifiant son contenu. On aura ainsi modifié les images spatio-temporelles de son cyberespace.

Ce modèle de la roue peut être vu, par les Anglo-saxons, comme une cible de jeu de flèchettes (Information Dart Board).

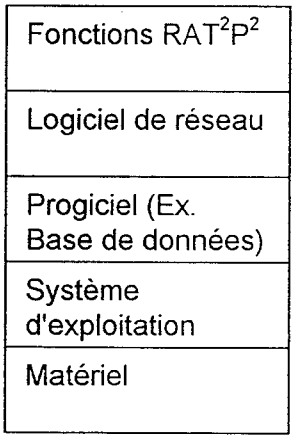
Nous avons vu que les six fonctions RAT^2P^2 constituent le socle du cyberespace. De l'attaque de ces fonctions, dépend la paralysie stratégique de l'adversaire. Nous devons nous prémunir également d'une attaque contre notre propre cyberespace. Nous allons étudier les stratégies d'attaque et défense d'un cyberespace.

Axes stratégiques d'attaque et de défense du cyberespace

Le moyen de paralysie stratégique de l'adversaire repose sur l'attaque des six fonctions RAT^2P^2. Nous allons voir en détail, fonction par fonction, les axes stratégiques d'attaque. Auparavant, il faut cependant noter que ces fonctions RAT^2P^2 s'exécutent dans des systèmes informatiques qui comprennent :

- du matériel (HardWare) constitué de circuits logiques intégrés, de mémoires de divers types et de microprocesseurs ;
- de logiciel de base ou encore appelé Système d'Exploitation ou SE, (ex. : DOS, Windows 95, UNIX[87]...).

Une architecture plus évoluée comprend, au dessus de la partie matérielle et logicielle de base, un progiciel (par exemple un système de gestion de base de données). Et dans le cas du partage de cette information, un progiciel de réseau (ex. : NETWARE ou Internet). Cette architecture informatique, somme toute assez classique, est représentée dans le schéma ci-dessous. Il s'agit de l'empilement de couches logicielles, au-dessus du matériel.



Les axes stratégiques d'attaque et de défense comprennent donc les fonctions RAT^2P^2, qui s'exécutent sur un système informatique. L'attaque du cyberespace adverse et la défense du nôtre doivent donc prendre en compte, les fonctions RAT^2P^2 et le système informatique, constituant leur socle.

[87] Il en existe plus d'une centaine, mais Windows 95/98/NT et la famille UNIX sont les plus répandus

L'attaque et la défense de ces axes stratégiques du cyberespace, d'un niveau plus tactiques, seront discutées en annexe.

Ces fonctions RAT^2P^2 se retrouvent dans différents types de guerres de l'information. Regardons ensemble quelques exemples.

Quelques catégories de conflits de la cyberwar.

Martin Libicki, un auteur prolifique pour tout ce qui concerne la guerre de l'information ou Information Warfare[88] a défini plusieurs domaines :

- Command and Control Warfare (la guerre du commandement et des opérations) ;
- Intelligence Based Warfare (la guerre du renseignement) ;
- Electronic Warfare (la guerre électronique) ;
- Psychological Warfare (la guerre psychologique) ;
- Hacker Warfare (la guerre informatique [piratage]) ;
- Economic Information Warfare (la guerre de l'information économique) ;
- Cyberwar (la cyberguerre ou guerre des systèmes cybernétiques) ;
- Information Blockade (le blocus de l'information) ;
- Information Based Warfare (la guerre des SIC[89]).

La cyberstratégie, que nous venons de définir, s'applique sans aucun problème à la plupart de ces catégories de conflit. Elle est particulièrement adaptée à la guerre des SIC et à la guerre des systèmes cybernétiques.

Universalité du modèle de la Roue

Les colonels Boyd et Warden ont redonné à la stratégie un nouvel élan. Les progrès fulgurants de l'arme aérienne ont peut-être été le phénomène qui a déclenché ce besoin de rajeunissement de la stratégie.

Le modèle de Warden est bien adapté à une campagne aérienne. La campagne d'Iraq est là pour le confirmer.

En introduisant le concept de paralysie stratégique par la guerre cybernétique, le cyberespace envahit la stratégie. Le cyberespace englobe tous les autres espaces ainsi que nous l'avons vu précédemment. Le but de la cyberstratégie est de s'introduire dans l'espace temporel et mental de l'adversaire. Le modèle de la Roue peut donc s'appliquer à n'importe quel type de campagne. Que ce soit une campagne terrestre, aérienne ou maritime.

Structures pour la cyberwar

Le Pentagone prend très au sérieux ce nouvel espace de puissance et de lutte. En 1993, l'USAF a créé l'Information Warfare Center. Le 1er octobre 1995, est créé le 1er escadron de guerre de l'information (609th IWS) sur la base aérienne de Shaw. Le 9 octobre 1998, le général Hugh SHELTON a signé un document créant un organisme chargé

[88] Martin LIBICKI, *What is Information Warfare*, NDU press. Les auteurs américains, devant le clair axe politique donné par le DoD, sont très actifs dans l'étude de la guerre de l'information.

[89] Systèmes d'Information et de Commandement

d'étudier, au niveau du DoD, l'attaque des réseaux informatiques et la conduite de l'Information Warfare.

Il conviendrait, au niveau de l'Etat-Major des Armées, de mettre en place des structures comparables à celles mises en place aux Etats-Unis. Il s'agirait de créer un bureau chargé de la guerre de l'information. Ce bureau comporterait deux divisions :

- l'une chargée de la partie offensive, avec l'étude de l'attaque des réseaux et systèmes d'information de l'adversaire ;
- l'autre chargée de la partie défensive. Cette division reprendrait les attributions des divisions de sécurité informatique des Etats-Majors des différentes Armées.

Limites à la cyberwar

Nous venons d'étudier une stratégie qui s'applique essentiellement au monde militaire. La guerre de l'information fait aussi partie d'une stratégie de guerre, mais celle-ci est à la frontière du militaire et du civil. La guerre de l'information en direction du monde civil est une réalité qu'il convient de prendre en compte le plus tôt possible. Il s'agit d'expliquer aux opinions publiques la légalité et la justesse des opérations militaires menées. Il peut aussi s'agir de propagande. "*Si tu veux détruire ton ennemi, détruis ses traditions*". C'est exactement ce que nous subissons avec l'information unique diffusée par CNN. Nous recevons une information unique, une version des faits unique, une analyse unique. Nous atteignons là le sommet de la pensée unique. "*L'ONU regarde CNN*" titrait le journal Libération du 17 décembre 1998. Un ambassadeur russe se demandait dans cet article, pourquoi le Conseil de sécurité de l'ONU était-il obligé de regarder CNN pour savoir ce qui se passait en Iraq, pendant l'opération "Renard du désert" ?

Lorsque la source de l'information est unique, la pensée devient unique. Il y a là un grave danger de manipulation des opinions publiques. Ceci peut avoir de grandes répercussions sur la stratégie militaire et la conduite d'une guerre. Nous devons y prendre garde. Mais ceci dépasse le cadre de ce mémoire.

Conclusion

La "Revolution in Military Affairs" n'est pas un nouveau concept du complexe militaro-industriel pour revitaliser ce secteur et contrecarrer la réduction des budgets de la Défense. La RMA est le fruit de l'évolution technologique et de la révolution de l'information qui frappe notre monde. *Il est devenu vital de gérer la chaîne de l'intelligence, depuis la collecte d'informations jusqu'au guidage des munitions et même à la gestion médiatique du conflit*[90]. La RMA est le fruit de la prise en compte du cyberespace

L'information est devenue la pierre angulaire du conflit. Nous devons réfléchir à une stratégie qui prenne en compte le cyberespace. La puissance aérienne a permis de mettre en œuvre le concept de paralysie stratégique. Les aviateurs BOYD et WARDEN ont joué un grand rôle dans le renouvellement de la pensée stratégique. Leur outil, pour parvenir au résultat escompté, est l'avion. Celui-ci devait permettre aux autres Armées de terminer le conflit à moindre coût.

Une nouvelle étape est à franchir : obtenir la paralysie stratégique de l'adversaire par une cyberstratégie. Le préalable à toute opération militaire d'envergure est la conquête de la supériorité aérienne. Une cyberstratégie doit permettre à l'aviateur de mener sa tâche avec un minimum de danger et un maximum d'efficacité. La tâche des autres Armées s'en trouvera facilitée. Cette cyberstratégie s'appliquera de la même manière au profit de la Marine et de l'Armée de terre. Elle leur permettra d'obtenir la victoire à moindre coût et avec le minimum de risques. Les modèles de BOYD et WARDEN ont fourni une solide base pour définir une cyberstratégie ; une stratégie avec comme instrument de lutte : l'outil informatique. Le modèle de la Roue a permis de mettre en évidence les six fonctions qui constituent les axes de cette cyberstratégie : Recueil, Archivage/stockage, Traitement, Transmission, Protection, Partage de l'information.

Sur un mode défensif, la sécurité informatique est la pierre angulaire de la défense de notre cyberespace. Cependant, des vulnérabilités importantes subsistent. Celles-ci sont liées à la prédominance de l'industrie logicielle américaine. On peut néanmoins diminuer cette dépendance en utilisant des logiciels dont on peut avoir les codes source afin de contrôler leur innocuité. Le dernier logiciel n'est pas forcément la panacée. Un logiciel, un peu moins récent mais sûr, est une solution préférable. LINUX en est un excellent exemple. Le chiffre est aussi un domaine essentiel et la France doit conserver son autonomie de décision. Il faut privilégier l'utilisation d'algorithmes nationaux (la France possède des mathématiciens parmi les meilleurs du monde[91]). PGP constitue aussi une alternative intéressante. Le logiciel constituant les fondations du cyberespace, pour conserver notre liberté de décision et d'action, il faut diminuer notre dépendance à l'égard de l'industrie logicielle américaine. Les Etats-Unis sont nos alliés, cependant il ne faut pas perdre de vue que les intérêts vitaux des Etats-Unis ne sont pas forcément les nôtres. Il faut éviter qu'une affaire comme celle de Suez[92] puisse se reproduire.

L'accent mis sur l'emploi du GPS me paraît être dangereux pour notre autonomie d'action. Il faut privilégier d'autres voies.

Pour ce qui concerne l'offensive, les solutions sont innombrables et la France possède suffisamment d'informaticiens qualifiés capables d'imaginer des solutions pour pénétrer le cyberespace d'un éventuel adversaire.

---

[90] Paul Ivan de Saint Germain, directeur de la Fondation pour les Etudes de Défense, cité par les Echos du 14 janvier 1999

[91] Cf. les nombreuses médailles Fields (Nobel des mathématiques) que les mathématiciens français ont reçues

[92] Lire à ce sujet l'excellent "*Diplomacy*" de Henry Kissinger, Ed. Simon & Schuster

La critique, qu'on peut faire de cette théorie, est qu'elle ne peut s'appliquer qu'à des adversaires d'un niveau technologique équivalent. Que la cyberwar ne peut agir contre une guérilla, dont le centre de gravité est le soutien du peuple.

La cyberguerrilla est déjà lancée. Les adversaires de Kabila ont un site Internet. Les cyber-rebelles[93] sont là. La liste des sites Internet des différents mouvements rebelles ou islamistes s'allonge. Pour démontrer cette affirmation voici quelques sites :

- www.congo.co.za : Rassemblement congolais pour la démocratie
- www.afard-unita.asso.fr : Union nationale pour l'indépendance de l'Angola (Unita)
- www.kdp.pp.se : Parti démocratique Kurde d'Irak

Le cyberterrorisme est aussi lancé. En réponse à la condamnation à mort de deux *hackers*[94] (pirates des réseaux), un groupe a créé le Hacker Emergency Response Team (HERT) qui a lancé une offensive contre tous les sites chinois[95]. *Le petit y (dans le cyberespace) redevient un partenaire important et potentiellement très dangereux*[96].

Le cyberespace est une réalité. Tous les domaines de lutte sont concernés. Des domaines, comme la guérilla, qui semblaient ne pas devoir appartenir à ce cyberespace, l'utilisent pour faire triompher leur cause. Afin d'éviter ce que les Américains appellent un "Waterloo électronique"[97] ou un "Pearl Harbour cyberspatial"[98], il est urgent et vital pour les Armées de prendre en compte le cyberespace. La France doit, à l'instar du DoD, mettre sur pied une structure de cyberguerre et approfondir la réflexion stratégique sur la guerre de l'information. Le coût humain et financier sera important, mais c'est un investissement nécessaire à l'indépendance nationale. *Plus l'investissement matériel est grand, plus l'investissement intellectuel est important*[99].

En paraphrasant le maréchal Foch qui disait : *L'art de la guerre est, en définitive, l'art de garder sa liberté,* on peut dire : *La cyberstratégie, est la stratégie qui permet de conserver sa liberté de décision et d'action, sur le champ de bataille d'aujourd'hui : le cyberespace.*

Il ne faut pas tomber dans l'excès de l'Américain William Murray, qui donnait comme titre à l'un de ses articles : "*Clausewitz Out, Computers In*", voulant ainsi montrer le recul de la stratégie devant la technologie : la technologie ne peut s'affranchir de la stratégie. Cependant, celle-ci doit évoluer et s'adapter aux moyens de son temps. La maxime qui correspondrait le mieux à la philosophie de ce mémoire serait :

Les ordinateurs avec Sun Zi pour une cyberstratégie[100]

---

[93] Enquête parue dans Jeune Afrique, *Dans les pas des cyber-rebelles*, du 26 janvier 1999

[94] le mot "hacker" a pris le sens de pirate alors que sa signification était plutôt celle d'un passionné qui "pioche" au fond des choses

[95] *"Frappes informatiques" sur Internet*, Figaro du 14 janvier 1999

[96] Michel Wautelet, *Les cyberconflits*, Ed. Grip

[97] "*Averting an electronic Waterloo*", Rapport du Center for Strategic &International Studies (CSIS), adresse Internet : www.csi.org

[98] Article du journal Le Monde

[99] Hervé COUTAU-BÉGARIE, *Traité de stratégie*, Ed. Economica

[100] **Computers in Sun Tzu for a cyberstrategy**

ANNEXE

Nous avons vu que les six fonctions RAT^2P^2 sont les axes stratégiques de la cyberwar. Ces fonctions sont exécutées sur des systèmes informatiques. Avant d'étudier la manière de s'attaquer à ces fonctions, il faut se pencher sur l'attaque des fondations sur lesquelles ces fonctions s'appuient : les moyens informatiques.

Le système informatique

Le matériel

Le matériel informatique moderne est composé d'ordinateurs, de modems, de réseaux de transmissions. Ceux-ci comprennent des mémoires "flashables". C'est-à-dire qu'on peut effectuer la mise à jour du logiciel inclus dans celles-ci par un autre logiciel. Par exemple on peut améliorer les caractéristiques d'un modem, en changeant le logiciel contenu dans sa mémoire, par un nouveau logiciel, pour lui permettre de transmettre à une vitesse plus élevée. On charge le logiciel de mise à jour maintenant souvent à partir du réseau Internet.

On peut imaginer, provoquer l'effacement du logiciel contenu dans la mémoire de l'équipement. Alors celui-ci ne pourra plus fonctionner. On peut aussi charger un logiciel qui ferait une tâche supplémentaire[100] (d'espionnage des données transmises par exemple) et qui resterait indétectée, car l'équipement continuerait à fonctionner normalement.

Une autre forme d'attaque consisterait à envoyer un code au microprocesseur pour que celui-ci se bloque définitivement. Auparavant, il faudra implémenter cette fonction secrète au moment de la conception de celui-ci. Pour l'instant, seuls les industriels américains sont concepteurs et fabricants de microprocesseurs ou de microcontrôleurs. Connaissant la main mise de la NSA[101] sur toutes les technologies sensibles, on peut imaginer que ces fonctions d'autodestruction ou d'espionnage sont déjà implantées dans les composants des ordinateurs et périphériques.

Pour se protéger de ce type d'attaque, il faut faire produire les composants par sa propre industrie. Thomson produit des microprocesseurs sous licence Motorola. Il convient donc d'analyser les composants pour détecter une telle fonction. Il faut aussi tester et certifier les logiciels de bas niveau contenus dans les mémoires des matériels informatiques.

Le système d'exploitation

Pour fonctionner, un ordinateur a besoin d'un logiciel qui contrôle son fonctionnement : le Système d'Exploitation (SE). Ce logiciel gère l'allocation et l'utilisation des ressources matérielles, telle que la mémoire, l'unité centrale de traitement, les disques durs et les périphériques. En un mot, il exécute les tâches domestiques dans l'ordinateur : lire une donnée en entrée, décoder la fonction à exécuter, fournir le résultat...

---

[100] On appelle ce type de fonction discrète, sans rapport avec la fonction première du logiciel : un Cheval de Troie

[101] National Security Agency. Leur devise officieuse est : "En Dieu nous croyons, tout le reste nous le surveillons"

En prenant le contrôle du SE, en utilisant un profil utilisateur caché et mis en œuvre par un code spécifique et secret[102], on peut empêcher ce logiciel de fonctionner, donc l'ordinateur de remplir sa tâche. On peut aussi lui faire exécuter des opérations qui détruiront une partie importante du matériel (par exemple le disque dur, en faisant faire des allers et retours incessants au bras de lecture[103]).

Un autre moyen, plus subtil, consisterait à lui faire exécuter une fonction supplémentaire, non autorisée[104]. Par exemple demander au logiciel de base de faire une copie des données manipulées dans une zone protégée du disque dur, afin qu'elles puissent être récupérées plus tard discrètement ou les envoyer sur un réseau par MEL[105] à une adresse électronique où nous pourrons consulter tranquillement ces données.

La maîtrise de conception et de développement d'un système d'exploitation (UNIX, WINDOWS, NT...) est essentielle pour avoir un moyen d'attaque très performant du cyberespace. Cependant, on s'aperçoit que sur le marché, tous les systèmes d'exploitation sont américains. Nous sommes donc en situation de vulnérabilité d'un point de vue défensif et en situation de faiblesse d'un point de vue offensif.

Un moyen de se protéger de ce risque, est d'utiliser un SE dont on détient le code source. Les éditeurs de SE refusent de donner leurs codes source, ou même les déposer chez un tiers de confiance tel un notaire (protection de secrets industriels disent-ils). Il existe cependant un SE de la famille des UNIX (son nom est LINUX), créé par un programmeur finlandais, Linus Torvalds, dont le développement est assuré gracieusement par des informaticiens du monde entier et dont le code source est disponible. C'est un système performant, fiable, gratuit, dont la disponibilité et la transparence sont assurées. L'Etat-Major des Armées doit se pencher sur ce produit, lancer une étude pour envisager éventuellement son utilisation, en lieu et place des SE coûteux dont nous n'avons pas le code source.

Les progiciels

Les progiciels[106] sont des logiciels paramétrables conçus pour être fournis à plusieurs utilisateurs, en vue d'une même utilisation. On en trouve plusieurs types :

- bureautiques : traitements de textes (Word...), tableurs (Excel...), outils de présentation (PowerPoint...), gestion de fichiers (Dbase, Access...) ;
- Systèmes de Gestion de Bases de Données ou SGBD (Ingres, Oracle, ...)
- Outils divers : gestion de courrier, de stocks, de clients...

Ces logiciels sont de plus en plus gros et complexes à mettre en œuvre. L'utilisation et la maintenance d'un SGBD nécessitent les connaissances de plusieurs informaticiens très spécialisés. Un disfonctionnement est difficile à détecter et à analyser. On peut facilement semer le désordre dans un tel produit et il sera extrêmement difficile et coûteux d'y remédier. Le système SOCRATE de la SNCF est basé sur un SGBD. Si les données des horaires ou des réservations ou des tours de service des cheminots ou la composition des trains sont modifiées, ce système de transport vital pour la Défense sera paralysé. Imaginons que la même attaque se produise contre EDF, Air France et France Télécom ! Les SGBD fournissent donc une cible privilégiée aux attaques du cyberespace. Il suffit de disposer d'une « Back Door » pour contourner les dispositifs de sécurité de ces systèmes. Un moyen

---

[102] Appelé "Back Door" dans le jargon informatique. Ce code peut être envoyé via les réseaux.
[103] Certains virus possèdent aussi cette fonction
[104] un Cheval de Troie
[105] Message ELectronique, traduction du mot anglais E-Mail
[106] Provient de la contraction de produit et de logiciel

plus dangereux consisterait à modifier certaines données vitales, en leur laissant un semblant de cohérence, et de laisser le système fonctionner « normalement ». Les dégâts seraient considérables, car on prendrait des décisions sur des données erronées, sans s'en apercevoir. Les progiciels sont américains. Ceci est dû au fait que l'industrie logicielle américaine possède une masse critique et un énorme marché qui lui permettent d'entreprendre des développements logiciels coûteux.

Dans le cadre d'une attaque effectuée grâce à des progiciels, on peut facilement programmer des « patchs[107] » qui implémenteront des Chevaux de Troie, dont la fonction sera de paralyser le SGBD, de modifier certaines données ou d'espionner.

Pour se défendre contre de telles menaces, il faut utiliser des SGBD développés nationalement, en sacrifiant peut-être quelques fonctions sophistiquées ou des performances, mais en gagnant en sécurité.

Les réseaux informatiques

L'informatique moderne, le cyberespace est là pour le prouver, est basée sur les réseaux. La technologie des réseaux est complexe et il faut plusieurs spécialistes de haut niveau dans différents domaines, pour couvrir tout le spectre de ce métier. Nous nous bornerons donc à une description très sommaire, pour montrer l'extrême vulnérabilité des réseaux. **Pour que la sécurité d'un réseau soit assurée, il est obligatoire d'utiliser le chiffrement, qui, outre l'aspect protection de la confidentialité des données transportées, permet de mettre en place des mécanismes de sécurité physique et logique du réseau.** L'aspect confidentialité des données sera développé dans le chapitre « Protection des données »

Pour mieux comprendre comment on peut aisément attaquer un réseau, il faut tout d'abord savoir comment celui-ci est constitué. Le schéma suivant représente un modèle dit "d'interconnexion des systèmes ouverts", ou OSI *(Open Systems Interconnection)* qui a été défini par l'ISO *(International Standards Organization).* Le modèle OSI répartit les protocoles informatiques utilisés selon sept couches, définissant ainsi un langage commun pour le monde des télécommunications et de l'informatique. Il constitue aujourd'hui le socle de référence pour tous les systèmes de traitement de l'information.

N°couche	Niveau	Fonction
7	Application	Fournit l'ensemble des services compréhensibles aux programmes
6	Présentation	Fournit les représentations syntaxiques de référence communes à deux applications(traduction entre machines différentes)
5	Session	Spécifie les règles de synchronisation du dialogue entre deux processus d'application
4	Transport	Fournit un transfert de données transparent et fiable de bout en bout. Masque la topologie du réseau. (niveau Message)
3	Réseau	Assure le routage des données et le choix d'un chemin entre nœuds (niveau Paquet)
2	Liaison	Assure le transfert de données entre relais adjacents avec détection des erreurs de transmission (niveau Trame)
1	Physique	Permet la transmission physique des signaux électriques codés (l'unité d'information transportée est le Bit)

[107] Morceau de logiciel qu'on ajoute à un autre logiciel, pour corriger des bogues

Mis à part la couche Physique, où se trouvent du matériel et du logiciel de bas niveau, toutes les autres couches sont des couches logicielles. Les remarques faites pour le matériel s'appliquent pour cette couche n°1 dite « Couche Physique ».

La couche Liaison est sensible à la détection des erreurs. On peut handicaper le fonctionnement d'un réseau en empêchant le mécanisme de détection/correction des erreurs de transmission de fonctionner. Cela pourrait apparaître à un adversaire comme une mauvaise liaison, sans qu'il ne se doute qu'il est l'objet d'une attaque. C'est un moyen d'augmenter la friction dans sa boucle OODA.

La couche Réseau est essentiellement chargée du routage (le choix d'un chemin entre divers nœuds de communication). En contrôlant ce logiciel, on peut empêcher l'acheminement des données. On peut aussi demander qu'une « copie » nous soit envoyée. On peut envoyer plusieurs fois le même paquet, pour mettre à mal le mécanisme de réassemblage des paquets (pour en faire un message cohérent) ou tout simplement saturer le système en réception et ainsi créer ce qu'on appelle un *déni de service*.

La couche Transport manipule les messages complets. Si la couche 3 ne fournit pas tous les paquets, la couche 4 ne peut reconstituer le message complet. D'où demande de retransmission. Ce qui permet de surcharger le réseau par des retransmissions inutiles.

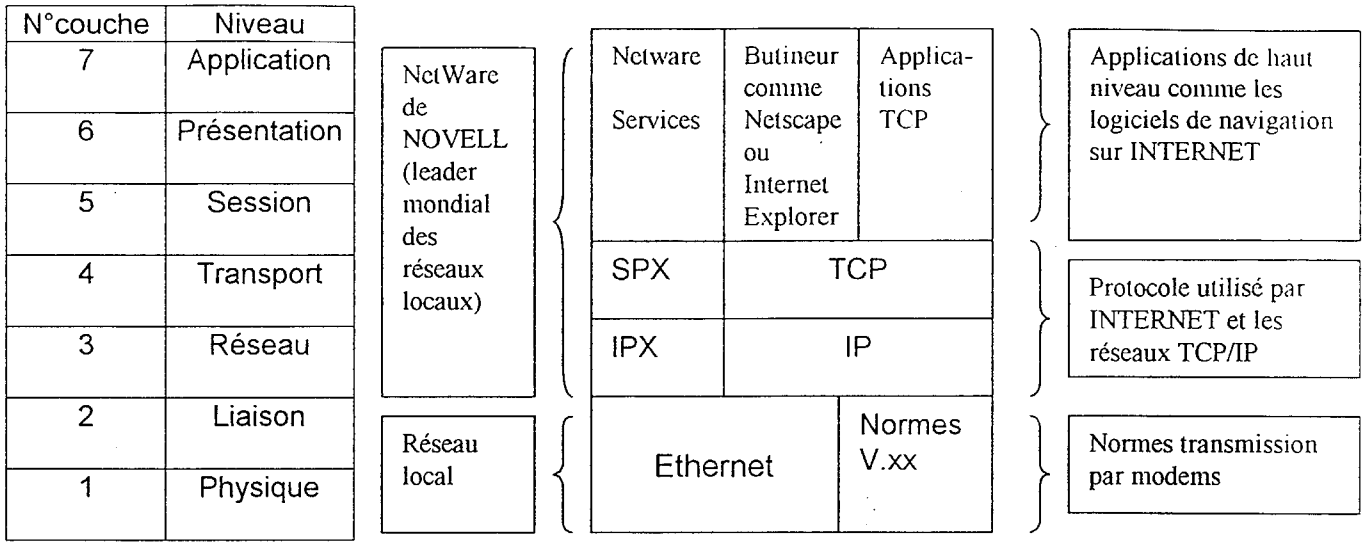
La couche Session assure un dialogue correct entre applications (établissement et interruption de la communication, cohérence et synchronisation des opérations). Si on empêche l'enchaînement correct des opérations nécessaires à une communication, celle-ci ne peut se dérouler.

La couche Présentation traite les formes de représentation des données, permettant la traduction entre machines différentes. Si ce mécanisme de traduction de format entre machines hétérogènes est touché, il ne sera plus possible de faire dialoguer des machines différentes.

On peut imaginer, pour rester discret, changer la traduction, en employant le « langage » d'une autre machine. Par exemple, si un ordinateur A dialogue avec une machine B, on peut empêcher ce dialogue, et faire passer cela pour une panne et non pas une attaque (afin de rester discret ou de retarder le diagnostic) en faisant passer la machine B pour une machine qui comprend le langage d'une machine C. On se sera introduit dans la boucle OODA de l'adversaire et fortement augmenté la friction de sa boucle.

La couche Application rassemble toutes les applications qui ont besoin de communiquer par le réseau : messagerie électronique, transfert de fichiers, gestionnaire de bases de données. Elle est source et destination de toutes les informations à transporter. Par exemple, c'est là que se trouvent des outils de transfert de fichiers *File Transfert, Access & Management*, la messagerie X400. Se trouvent là des cibles potentielles importantes.

Après ces considérations générales sur la vulnérabilité des différentes couches qui constituent un réseau, pour illustrer la contemporanéité du problème, mettons quelques noms dans ces couches



Exemple simplifié de pile OSI

Première remarque : Nous n'avons pas intégré dans ce modèle les protocoles d'administration et de gestion du réseau (de type SNMP[108]). L'administration du réseau consiste à paramétrer le réseau pour que l'utilisateur des applications puissent accéder aux programmes et données dont il a besoin dans de bonnes conditions de sécurité. Il s'agit d'un travail qui nécessite la connaissance fine des applications. Il faut connaître les ressources du réseau à mettre à la disposition des utilisateurs des programmes. Les couches basses (1 & 2) peuvent être de la compétence des techniciens des télécommunications. Au dessus, les couches 3 et 4 sont de la compétence des informaticiens spécialistes des réseaux et les couches 5 à 7 de la compétence des informaticiens programmeurs.

Seconde remarque : Les logiciels qui constituent les différentes couches d'un réseau sont des logiciels d'origine américaine. Nous nous trouvons dans ce domaine dans une situation de vulnérabilité aussi dangereuse que celle des systèmes d'exploitation ou des SGBD.

La fonction "Recueil"

Cette fonction comprend le recueil :

- de l'information du champ de bataille. Il s'agit d'avoir une vision globale de la situation tactique du théâtre d'opérations.
- de l'information de la boucle OODA de l'ennemi. Il s'agit là d'espionner le système d'information de l'adversaire.

Le recueil de la situation tactique fait souvent appel à des capteurs électroniques embarqués[109], dont la part du traitement du signal augmente de façon vertigineuse. Ce qui conditionne la performance du capteur, c'est la vitesse et la puissance du traitement de la donnée recueillie.

Par exemple, dans le cas d'un radar aéroporté de type AWACS[110], la performance du système de détection est directement liée :

---

[108] Simple Network Management Protocol

[109] radars de tous types, écoute électronique, photographie numérique satellitaire ou aéroportée

[110] Airborne early Warning And Control System

- aux performances du radar, qui comprend une très grande part de traitement du signal (par exemple pour éliminer les échos fixes) ;
- au logiciel de traitement des données issues du radar afin d'en faire une information ;
- au système de transmission pour mettre le plus rapidement possible cette situation tactique à la disposition de ceux qui ont à en connaître (liaison 11 et bientôt liaison16).

Nous avons là à notre disposition de nombreuses cibles potentielles pour rendre l'adversaire aveugle (à condition que celui-ci possède une panoplie de niveau technique comparable à la nôtre). Les logiciels embarqués peuvent faire l'objet de bombes logiques[112] ou de chevaux de Troie. Il faut posséder le code source pour détecter de telles menaces[113].

Le recueil de l'information peut être aussi, pour un système de navigation, la réception d'information de recalage de type GPS par exemple. Pour ma part, je pense qu'il faut s'affranchir du système GPS pour toutes les applications militaires françaises. Le système GPS, propriété du DoD américain, possède deux types de précision : une précision moyenne à usage civil et une précision élevée pour les applications militaires. Cette dernière nécessite la possession d'une clé cryptographique pour bénéficier de cette précision. Le centre de contrôle des satellites NAVSTAR de Falcon AFB[114], peut décider d'occulter une région du monde. Nous ne sommes donc pas libres de l'utilisation du GPS. Les fréquences sont connues. Une société russe, *Aviaconversia*, commercialise une petite mallette capable de brouiller le GPS dans un rayon de cent kilomètres.

La fonction "Archivage/stockage"

Dans un système d'information, supporté par un système informatique, les données sont stockées à chaque étape, pour pouvoir subir les traitements appropriés qui leur donneront une valeur plus importante.

Dans le processus par lequel le chef bâtit sa "décision avisée", celui-ci fait appel à des fonctions de fusion/corrélation de données. Les données recueillies sont correlées avec d'autres données, qui auront dû être archivées auparavant, pour être disponibles pour ce traitement de corrélation. Ces archives numériques sont donc stockées, de manière sûre, pour être disponibles au moment opportun.

Lorsque ces données perdront de leur valeur pour le moment présent, car trop anciennes, elles seront archivées pour servir de mémoire du système d'information : elles deviendront des archives.

Le stockage de l'information s'effectue sur les disques magnétiques des ordinateurs.

La mise hors service d'un disque peut avoir de graves conséquences :
- sur le fonctionnement de ces ordinateurs, si le disque contient le système d'exploitation ;
- par la perte des données, ou des programmes, inscrits sur ce disque ;
- par le temps passé à utiliser les sauvegardes pour remettre les données ou les programmes sur le disque.

La mise hors service d'un disque peut s'effectuer par l'attaque du logiciel qui le gère, mais aussi par une attaque sur les commandes qui ont un effet mécanique (faire effectuer

[112] Logiciel qui, lorqu'il est exécuté, détruit tout ou partie des données du système informatique
[113] L'Armée de l'air possède les sources du logiciel AWACS développé par BOEING
[114] Air Force Base, Falcon AFB est au Colorado dans la Cheyenne Mountain

des allers et retours rapides et incessants au bras de lecture pour provoquer un "atterrissage des têtes de lecture") et détruire ainsi physiquement le disque. Ceci peut être réalisé grâce à l'utilisation de virus informatiques ou de chevaux de Troie. Un autre moyen d'attaque très efficace est de mettre hors service la climatisation des salles informatiques.

L'archivage s'effectue le plus souvent sur des bandes magnétiques. Les données sont compressées pour tenir le moins de place possible. Une attaque du logiciel d'archivage est une bonne solution pour empêcher la relecture de ces bandes. Un changement de l'ordre du marquage physique des bandes est aussi un moyen subtil et efficace.

Cette fonction d'archivage et de stockage est donc aussi importante que les autres fonctions. Il convient d'appliquer avec rigueur les recommandations de sécurité informatique concernant les sauvegardes.

La fonction "Traitement"

La donnée brute, pour devenir une information qui conduit à une décision pertinente, a besoin de suivre le circuit décrit précédemment dans "le processus de la décision avisée". A divers niveaux, elle subit donc divers traitements. Ces traitements sont réalisés grâce à l'aide d'outils informatiques.

Si on réussit à s'introduire dans les systèmes informatiques utilisés dans ce processus, on peut :

- connaître l'information dont dispose l'ennemi ;
- modifier la perception qu'a l'ennemi de cette information et le conduire à prendre des décisions erronées ;
- lui donner des éléments d'analyse et d'aide à la décision erronés, toujours pour le conduire à prendre de mauvaises décisions ;
- ralentir ou même casser son processus de décision par divers moyens d'attaque de son système informatique. On augmente de manière considérable la friction à l'intérieur de sa boucle OODA. On opacifie son "brouillard de la guerre".

Les moyens d'attaque sont donc des moyens de guerre informatique :

- attaque du matériel ;
- attaque des logiciels utilisés :
    - système d'exploitation ;
    - progiciels ;
    - logiciels spécifiques : Ce sont des logiciels développés pour remplir une tâche définie. Ces logiciels sont moins vulnérables à des bombes logiques car développés souvent par l'industrie nationale. Le moyen d'attaque de ce type de logiciel sera l'emploi de programmes informatiques malins, véhiculés par les réseaux comme des chevaux de Troie, bombes logiques, virus, ou vers[115].

La fonction "Transmission"

Le centre de gravité de la boucle OODA est le temps. Il s'agit de faire tourner sa boucle plus rapidement que celle de l'ennemi. Nous avons vu dans "le processus de la décision avisée" que la donnée navigue entre différents niveaux de compétence et de responsabilité. Nous avons aussi vu dans le schéma qui décrit les "domaines de la

[115] Petit programme qui circule et se réplique dans un système jusqu'à le saturer. Le plus célèbre (involontairement) a été "Christmas Tree".

connaissance et de la sagesse" que l'information entre dans le domaine par "Observation/collection", il s'agit de la fonction Recueil, et qu'ensuite, quand la décision est prise, il faut la transmettre et la disséminer vers les acteurs du champ de bataille. L'utilisation des réseaux est donc indispensable pour diminuer les temps de transmission de l'information (pour diminuer la friction de notre boucle OODA).

On peut augmenter de manière considérable la friction de la fonction Transmission de l'adversaire, par du brouillage électronique (qui comprend une part importante de logiciel), par la destruction de ses centres de transmission, la coupure physique des supports de transmission. Cependant, un adversaire averti aura bâti un système de transmission souple, redondant et facilement reconfigurable. Pour augmenter de manière significative et **durable** la friction de ses transmissions, une attaque par des moyens informatiques est la plus efficace. En effet, l'emploi de virus, ou de vers, permet d'inoculer le "poison" dans tout le réseau de transmission, par propagation de ceux-ci. On n'a pas à se soucier de les introduire dans tous les endroits à bloquer, le virus se propagera de lui-même, dans toutes les branches de transmission qu'il pourra découvrir. Y compris les plus secrètes. De plus, la dépollution sera difficile, longue et coûteuse en ressources.

La fonction "Protection"

La protection des informations traitées dans notre boucle OODA est indispensable pour éviter que l'adversaire ne s'introduise dans celle-ci :

- pour connaître nos informations (en s'introduisant dans notre schéma mental);
- pour ralentir (augmenter la friction de) notre boucle OODA en la saturant d'informations inutiles ;
- nous tromper en modifiant les informations circulant dans cette boucle ;
- nous amener à prendre de mauvaises décisions en introduisant de fausses informations.

Le chiffrement des données est le moyen incontournable pour se protéger de ces attaques. Il rend nos transferts d'information confidentiels, il permet de s'assurer de l'identité de notre interlocuteur sur les réseaux[116], il interdit à l'adversaire de s'introduire dans notre boucle OODA pour la submerger de données inutiles, modifier ou ajouter de l'information destinée à nous faire prendre de mauvaises décisions. Dans certains systèmes d'armes utilisant l'évasion de fréquence, une clé de chiffrement sert aussi à définir les lois des sauts de fréquence[117], rendant l'intrusion dans les réseaux radio encore plus difficile.

La maîtrise du chiffre est donc une priorité absolue.

Il faut cependant s'interroger sur les algorithmes de chiffrement utilisés. Les plus répandus, et les plus utilisés dans le monde occidental (souvent pour des problèmes de compatibilité entre pays de l'OTAN) sont :

- le DES (Data Encryption Standard) normalisé en 1977 par le National Bureau of standards[118], dont la sécurité est mise en cause ; il est remplacé par le triple DES ;
- le système à clés publiques RSA (du nom de leurs auteurs du MIT[119]: Rivest, Samir et Adleman).

---

[116] Par un système de signature électronique chiffrée

[117] Dans le MIDS-LVT (terminal Liaison 16), une clé Transmission SECurity (TSEC) donne la loi d'évasion de fréquence, la gigue et l'interfoliation des message. Une clé Message SECurity (MSEC) protége les données

[118] Maintenant le National Institute of Standards and Technology (NIST)

[119] Massachusetts Institute of Technology

Aux Etats-Unis, la NSA[120] est chargée d'écouter tout type de communications. Un réseau d'écoute mondial, *Echelon*, regroupant les Etats-Unis, la Grande Bretagne, l'Australie et la Nouvelle Zélande a été récemment mis à jour. La NSA, par l'intermédiaire du National Computer Security Center, aurait aidé de nombreuses entreprises informatiques américaines, dans leurs programmes de développement logiciel[121]. L'incroyable affaire de la société suisse Crypto AG est révélatrice de la puissance de la NSA pour agir auprès des sociétés étrangères qui s'occupent de cryptographie. A mon avis, lorsque les Etats-Unis mettent à la disposition de leurs Alliés un logiciel ou un matériel de chiffrement, il faut penser que la NSA possède le moyen de casser le chiffre. Ils fournissent aussi des clés et refusent de nous donner les moyens de générer nous-même les clés.

Des citoyens américains se sont émus de la toute puissance de l'administration (en ce qui concerne la protection de leur vie privée). Les agences de renseignement US utiliseraient le logiciel *PROMIS*, pour surveiller les activités des gens, leurs mouvements, leurs dépenses, affiliations politiques[122]. L'un d'eux, Phil Zimmermann a développé un logiciel de chiffrement, Pretty Good Privacy (PGP), indépendamment de la NSA. Il a subi les foudres de l'Administration US qui le poursuit en justice, avec beaucoup d'acharnement. Ce logiciel regroupe trois algorithmes de chiffrement dont la robustesse n'a pas encore été mise en cause :

- IDEA, (International Data Encryption Algorithm), chiffrement classique mis au point en 1990 par Lai et Massey de l'Institut Fédéral de Technologie Suisse ;
- RSA, pour le chiffrement à clé publique ;
- MD5, algorithme de mélange des données, créé par Rivest du MIT (le R de RSA).

Ce logiciel semble extrêmement robuste et pratiquement impossible à « casser » en attaquant la clé. C'est sans doute la raison de la fureur de l'administration US. Il utilise des clés de 128 bits, ce qui donne 2^{128} combinaisons. Ce qui demanderait $5,4 \times 10^{24}$ années pour trouver la clé avec un ordinateur qui décrypterait 1 millions de clés à la seconde. Autre avantage, le code source est disponible et donc on peut l'analyser pour voir s'il n'existe pas de pièges cachés ou de "back door".

Pour protéger notre boucle OODA, il faut donc chiffrer en utilisant un chiffre national. Cependant il conviendrait d'étudier l'utilisation de PGP. Il faut, de plus, chiffrer **TOUTES** nos transmissions afin de surcharger un éventuel "voyeur". Celui-ci sera obligé de décrypter tout notre trafic afin de trouver nos informations de valeurs, noyées dans un grand flot d'informations sans valeur. Il ne pourra pas suivre le rythme de notre boucle OODA, car il s'épuisera à essayer de décrypter notre flux d'information.

La fonction "Partage"

L'information doit être partagée.

Il arrive souvent que le contexte d'une situation particulière soit connu, mais que celui qui en a besoin n'en a pas été averti. Par exemple le capitaine O'Grady, dont le F16 fut abattu en Bosnie, n'avait pas été mis au courant de la présence de batteries anti-aériennes dans son secteur.

Pour exécuter cette fonction "Partage" il faut :

- prévenir le combattant ou le décideur que l'information dont il a besoin existe ;

---

[120] Surnommée le "Puzzle Palace" aux USA. On utilise en France : Les Grandes Oreilles

[121] Enquête de Valeurs Actuelles du 16 janvier 1999

[122] Préface de Zimmermann dans "*Protect your Privacy*". William Stallings, Ed. Prentice-Hall, traduction auteur

- mettre cette information à la disposition de ceux qui en ont besoin dans des conditions de rapidité et de confidentialité optimum ;
- gérer l'accès à cette information par contrôle d'accès aux SGBD, aux serveurs et aux réseaux (fonction d'administration que nous n'avons pas abordé dans ce mémoire).

Cette fonction "Partage" a besoin des outils informatiques suivants : les réseaux locaux ou étendus, les SGBD, la fonction "Protection" et les outils d'administration des systèmes informatiques.

Bibliographie

Neuromancien, William GIBSON, Ed. J'ai Lu S-F n° 2325

Les cyberconflits, Michel WAUTELET, Ed. GRIP

Cours Traité de géopolitique, Aymeric CHAUPRADE, Polycopié de cours du CID

La géopolitique traditionnelle prise dans la toile du cyberespace ?, Mémoire de l'auteur

Les grands philosophes de la Grèce Antique, Luciano de CRESCENZO, Ed. Claude Lattès

L'Art de la guerre, SUN ZI, Traduction de Valérie NIQUET-CABESTAN, Ed. Economica

De la guerre, livre I, Carl von CLAUSEWITZ,

Violence et conflictualité : Approche sociologique, Véronique CHESNEAU, Revue Le Trimestre du Monde n°35 – 3è trimestre 1996

Précis de l'art de la guerre, Antoine Henri JOMINI,

L'Art de la politique chez les légistes chinois, XU ZHEN ZHOU, Ed. Economica

Théorie de la guerre, Joly de MAIZEROY, Ed. Chez la Veuve Leclerc

Traité de stratégie, Hervé COUTAU-BÉGARIE, Polycopié de cours du CID

Les nouveaux pouvoirs, Avin et Heidi TOFFLER, Ed. Fayard

Anthologie mondiale de la stratégie, Gérard CHALIAND, Ed. Robert Laffont

Information superiority, site Internet USAF : www.af.mil/lib/afissues/1997/issues31.html

Rapport 1998 de William COHEN, secrétaire d'Etat US à la Défense devant le Congrès, adresse Internet : www.dtic.mil/execsec/adr98/message.html

La paralysie stratégique par la puissance aérienne, David S. FADOK, Ed. Institut de stratégie comparée (ouvrage remarquable)

The foundations of the science of war, J.F.C. FULLER

L'ennemi en tant que système, John A. WARDEN, Air Power Journal, printemps 1995

A Discourse on winning and losing, John R. BOYD, Document de l'Air University Library

Destruction and Creation, John R. BOYD, Document de l'Air University Library

Patterns of conflict, John R. BOYD, Document de l'Air University Library

Strategic Game, John R. BOYD, Document de l'Air University Library

Organic Design, John R. BOYD, Document de l'Air University Library

Information Operations : Wisdom warfare for 2025, Research paper collectif, avril 1996, Air University, Adresse Internet : www.au.af.mil/au/2025/volume1/chap01/v1c1-1.html

What is Information Warfare, Martin C. LBICKI, Ed. NDU Press

Guerres dans le cyberespace, Jean GUISNEL, Ed. La Découverte

Le nid du coucou, Clifford STOLL; Ed. Albin Michel

Virus, la maladie des ordinateurs, Burger, Ed. Micro Application

Diplomacy, Henri KISSINGER, Ed. Simon & Schuster

Le grand échiquier, Zbigniew BRZEZINSKI, Ed. Bayard

Protect your privacy, a guide for PGP users, William STALLINGS, Ed. Prentice-Hall

Averting an electronic Waterloo, Rapport du Center for Strategic &International Studies (CSIS), adresse Internet : www.csis.org

Dans les pas des cyber-rebelles, Enquête parue dans Jeune Afrique, du 26 janvier 1999

NSA, quand l'Amérique espionne le monde, enquête de valeurs Actuelles du 16 janvier 1999