MEMOIRE DE STRATEGIE

Stratégie

et

guerre de l'information

1998—98

CES de FONTENILLES
CID/B3

S2FONTEJ.DOC

édition du : 02/06/1998

SOMMAIRE

INTRODUCTION 2

1. LA GUERRE DE L'INFORMATION 3

1.1. Définitions 3

1.2. Les composantes de la guerre de l'information 4

2. LES MENACES 6

2.1. Les types d'attaque contre l'informatique 6

2.2. Les agressions d'ordre "psychologique" 7

3. QUELLE STRATEGIE ? 8

3.1. Formation et doctrine 9

3.2. Organisation et techniques 9

CONCLUSION 10

BIBLIOGRAPHIE 11

ANNEXE 12

La guerre du Golfe est souvent présentée comme un conflit d'un type nouveau. Cette impression de nouveauté, ressentie que ce soit chez les acteurs directs, dans les états-majors ou même au sein du grand public, a fait l'objet d'une tentative d'explication dans un ouvrage paru aux Etats-Unis en 1993, *War and Anti-war* [6]. Ce conflit aurait été le premier théâtre d'opération où une armée du type "deuxième vague" se serait trouvé confrontée à des actions menées par une force du type "troisième vague".

En effet, dans cet ouvrage, les auteurs, Heidi et Alvin TOFFLER, définissent trois types de civilisations que l'on peut symboliser par : la houe, la chaîne de montage et l'ordinateur. A chacun de ces symboles correspond un type de société ayant ces propres exigences économiques donc politiques et militaires. On obtient, alors, un découpage de l'histoire en trois vagues principales :

- à la houe correspond une société agricole et une armée de "Première Vague";
- avec la chaîne de montage, on obtient une société industrielle de masse et des forces de "Deuxième Vague";
- l'ordinateur induit une société d'information et des armes de "Troisième Vague".

Afin de bien s'imprégner du contexte, il importe de comprendre ce que comportent ces classes :

La Première Vague est celle de « l'âge agraire », ou période pré-moderne. Elle s'étend jusqu'au XVIII° siècle. L'activité économique principale est l'agriculture qui deviendra, avec la première révolution agricole, « matrice de guerre » pour deux raisons majeures. En premier lieu, les progrès dans le domaine de la productivité permettront le stockage des excédents. Ceux-ci deviendront des objectifs de guerre. En second lieu, le développement des sociétés pré-modernes puis de la notion d'Etat sera précipité par la révolution agricole.

La Deuxième Vague correspond à « l'âge industriel », ou période moderne. Elle s'étend du XVIII° au XX° siècle. L'économie industrielle obéit au principe de la production industrielle de masse. Cette période est marquée par une recherche constante de la rationalisation dans tous les domaines.

Enfin, la Troisième Vague est celle de « l'âge de l'information », ou période post-moderne. La connaissance devient le noyau dur de l'économie. La valeur réelle des sociétés repose avant tout sur les idées, les informations stockées et les brevets. Selon les TOFFLER, « Savoir est désormais la ressource centrale de la capacité de destruction, de même qu'il est la ressource centrale de la productivité » Cette époque est caractérisée également par la « démassification », la flexibilité, ainsi que par la spécialisation et la qualification croissantes de la main d'oeuvre.

Ainsi, pour les époux TOFFLER, le type de guerre pratiquée n'est ni plus ni moins que le reflet de la façon de travailler à une époque donnée. Elle change donc en fonction de l'évolution des principes qui régissent l'économie. De façon schématique, le tableau comparatif en annexe met en parallèle les différents aspects liés à la guerre au cours des âges. Il est à noter que la nature des conflits devient de plus en plus en complexe au fur et à mesure du déroulement de l'histoire. S'il existe une vague dominante à une époque donnée, le type de société correspondant aux vagues précédentes subsiste. Il en résulte aujourd'hui une multiplication des types de conflits avec toutes les conséquences qui en découlent, notamment pour les sociétés relevant de la Troisième Vague.

A partir de là, il est clair que les sociétés appartenant à cette Troisième Vague sont celles qui ont développé et qui maîtrisent la communication. L'enjeu des conflits futurs résidera, donc, dans la conquête, le contrôle, voire la destruction des moyens de communication ou de leur contenu (le contenu et tout ce qui s'y réfère sera désigné sous le même vocable d'information).
Quelles sont les modalités de ce changement et quelle influence peut avoir ce dernier sur la stratégie française actuelle ?
Pour répondre à cette interrogation, il convient d'étudier, dans un premier temps, la guerre de l'information en essayant de la définir et en indiquant ses composantes. Ensuite, il faut préciser quelles peuvent être les menaces existantes contre les moyens informatiques servant de support à la maîtrise et au traitement de l'information, puis les agressions pouvant être menées contre les personnels. Et enfin, il serait souhaitable d'essayer d'en déduire une orientation stratégique.

1. LA GUERRE DE L'INFORMATION

" ... l'information est un atout stratégique ... une guerre du savoir ... chaque camp s'efforcera d'infléchir les actions ennemies en manipulant la circulation des renseignements et des informations ... ".

Duane ANDREWS
Secrétaire adjoint à la défense US, 1993.

1.1. Définitions

Pour certains, la guerre de l'information est un concept fou, sorte de "fourre-tout" à la mode. Pour l'Etat Major des Armées (EMA) c'est une notion qui recouvre trois domaines : la guerre pour, par et contre l'information. La guerre pour l'information repose sur l'exploitation des informations disponibles, que ces dernières proviennent de sources ouvertes ou secrètes, de moyens humains ou techniques. La domination par l'information repose sur la maîtrise de la bataille médiatique, de l'action psychologique et de la désinformation. La contre-guerre consiste à protéger nos informations et à être en mesure d'agir contre le flux d'informations qui nous intéressent. Elle s'appuie sur la sécurité des systèmes d'information et sur un certain nombre d'outils offensifs et défensifs.

En élargissant, on peut remarquer qu'initialement la notion de guerre de l'information se situait sur un terrain avant tout économique et commercial. Et qu'actuellement, ce sont les américains qui ont le plus avancé non seulement dans la réflexion mais également dans la mise en oeuvre à grande échelle. Il est, alors, intéressant de regarder la définition de ce nouveau type de guerre que donne le Département de la défense américaine : Il s'agit de « l'ensemble des actions menées pour imposer sa supériorité dans le domaine de l'information en soutien de la stratégie militaire nationale, en attaquant l'information et les systèmes d'information de l'adversaire tout en se protégeant contre de telles attaques ».

Il faut noter que le terme d'information doit être pris dans un sens large. Comme le déclarait le chef du Centre de l'armement pour la sécurité des systèmes d'information (CASSI) : « Dès lors qu'il y a informatisation, le système mérite d'être sécurisé. Une simple carte téléphonique constitue au même titre qu'un réseau de commandement militaire, un système d'information et de communication. Tout comme un missile qui contient également des données stratégiques modifiables à distance ». En définitive, tout matériel qui capte, transmet ou traite des données entre dans cette catégorie.

1.2. Les composantes de la guerre de l'information

Plusieurs grandes composantes sont actuellement mises en évidence, dont certaines nous sont déjà familières. Bien qu'elles ne soient pas encore toutes établies avec précision, les définitions suivantes peuvent être retenues :

la guerre du commandement, « command and control Warfare ». Elle correspond à la stratégie développée pour isoler les unités engagées des structures de commandement et de contrôle. Elle apparaît donc comme l'application militaire de la guerre de l'information. Les cibles sont les systèmes C^4I([1]) et leurs moyens de communication associés. Les objectifs principaux sont la destruction physique et le brouillage.

la guerre électronique, « electronic warfare ». Elle est menée dans le domaine des ondes électromagnétiques. Les techniques développées concernent les mesures de recherche électromagnétique, les contre-mesures électroniques et les mesures de protection électronique.

la guerre psychologique, « psychological warfare ». Notion vieille comme le monde, le terme de guerre médiatique est plus approprié. Elle concerne toutes les techniques visant à utiliser l'information pour "gérer" l'opinion publique tant civile que militaire. La nouveauté de cette notion réside dans les technologies utilisées pour agencer les messages (image, son, texte) et pour transmettre ces messages (radio, télévision par satellite, etc.).

[1] C^4I accronyme de Command, Control, Communications, Computer and Intelligence

la guerre de l'informatique, « hackers war », (littéralement « la guerre des pirates en informatique »). Elle concerne les attaques visant le système informatique adverse et les mesures de protection de ses propres systèmes. Une multitude d'actions peuvent être menées, allant de l'espionnage au sabotage en passant par la prise sous contrôle de systèmes adverses gérés par informatique.

la guerre par l'information, « information based warfare ». La mise en oeuvre des systèmes d'armes est liée à la réception et à l'organisation d'un volume croissant d'informations. Plus la capacité de ces systèmes à exploiter et à synthétiser les informations sera grande, plus leur efficacité sera importante. Les parades pouvant être utilisée contre la guerre par l'information sont diverses. Elles peuvent être liées à la furtivité des objectifs potentiels, à la rapidité de déplacement des objectifs mais également à la capacité de neutraliser les capteurs ou les moyens de guidage ou à la possibilité de pirater les systèmes informatiques intervenant dans la mise en oeuvre des systèmes d'armes adverses.

le blocus de l'information, « information blockade ». Cette composante relève de la prospective. Partant de l'hypothèse de la dépendance toujours plus étroite de l'économie à l'égard des informations extérieures, elle vise à couper la nation adverse des sources d'informations, ou à lui fournir des informations erronées, et donc à l'affaiblir à moyen ou à long terme.

le conflit cybernétique, « cyber war ». Il s'agit là d'une approche futuriste de la guerre de l'information. Elle concerne en premier lieu la guerre des systèmes. Cette notion fait allusion aux systèmes cybernétiques, combinaison d'informatique, de robotique, d'intelligence artificielle et de communication conçus pour détruire les systèmes adverses. En second lieu elle concerne, de façon plus réaliste, la guerre par simulation. Cette notion est liée au développement des nombreux outils de simulation, en particulier d'aide à la décision ou d'évaluation opérationnelle.

Ces différentes composantes relèvent toutes de la guerre de l'information. De ce fait, elles sont intimement liées et leur interdépendance est évidente.

Il faut leur ajouter une composante, **la communication opérationnelle**, dont le but est de regrouper toutes les actions effectuées par des cellules de presse (Press Information Office) pour conseiller un décideur, agir dans ou contre le monde des médias.

2. LES MENACES

> Le 2 novembre 1988, Robert Morris Jr, diplômé de l'Université de Harvard, lâche un ver sur ARPANET[2]. Le ver se transmet de machine en machine grâce à une faille dans le système de messagerie électronique. Le ver sature les machines contaminées en se reproduisant. Très vite, l'ensemble des communications sur le réseau est très fortement ralenti. Les administrateurs systèmes n'ont pas eu d'autres choix que de déconnecter leurs machines du réseau. Le réseau ARPANET sensé être utilisé pour les communications militaires en cas d'attaque nucléaire, avait été "mis à genou" par un simple programme écrit par un étudiant ! [3]

Même si la guerre de l'informatique n'est, comme il a été écrit précédemment, qu'une des composantes de la guerre de l'information, l'outil informatique a envahi tous les secteurs de la société de "Troisième Vague". C'est la raison pour laquelle il a paru important de traiter d'abord de ce qui risque de paralyser son fonctionnement.

2.1. Les types d'attaque contre l'informatique

L'informatique de réseau, les nombreuses connexions, en particulier sur INTERNET, offrent de multiples accès dérobés aux systèmes d'information. Les formes d'attaque sont variées. Outre la simple intrusion en vue de dérober des informations, les techniques suivantes sont les plus couramment admises :

- **Le virus**, petit programme informatique qui se recopie dans un programme correct afin d'en perturber le fonctionnement. L'introduction d'une disquette contaminée dans un ordinateur est la technique la plus couramment utilisée.
- **Le ver**, programme autonome qui se reproduit puis circule dans un réseau afin de pénétrer d'autres ordinateurs. A la différence d'un virus, il ne modifie pas les programmes mais peut occuper l'espace mémoire d'un système jusqu'à paralyser son fonctionnement. De plus, un ver peut être facilement modifié pour effacer des données et des fichiers.
- **La trappe,** mécanisme de type « porte de service » prévu par le concepteur même d'un système et qui lui permet de s'y réintroduire en contournant les moyens de protection.
- **Le cheval de Troie**, programme dissimulé dans un autre programme, est capable de détruire le contenu d'un ordinateur.
- **La bombe logique**, dérivée du cheval de Troie, est utilisée pour injecter des virus et des vers dans un système informatique. Pouvant être dissimulée dans le système par son concepteur même, la bombe logique peut être activée depuis l'extérieur ou se déclencher lors de la mise en oeuvre de certains programmes ou de certaines commandes faisant office de détonateur.

[2] ARPANET est l'ancêtre d'INTERNET

Ces cinq sortes d'attaques sont dites à base logicielle, il faut leur ajouter deux types d'armes :
- **Le canon hyperfréquence,** émetteur spécifique capable de déclencher une impulsion radio qui a la caractéristique de perturber les composants électroniques.
- **L'impulsion électromagnétique** (I.E.M.), arme non létale qui, alimentée par une charge nucléaire ou classique, génère une impulsion électromagnétique de très courte durée et de grande puissance comparable à la foudre. L'I.E.M. peut paralyser un système électronique dans la zone couverte par l'impulsion, en détruisant ses composants.

Ces deux dernières armes relèvent davantage de la panoplie militaire et demandent des moyens plus importants. Cependant toutes ces techniques peuvent désorganiser gravement le processus décisionnel ou de production d'un pays, d'une entreprise ou d'un état-major. L'informatique est, de ce fait, devenue une arme de déstabilisation non négligeable.

2.2. Les agressions d'ordre "psychologique"

Dans le paragraphe précédent, il a été question d'attaques contre les moyens et matériels utilisables dans la guerre de l'information. On aborde, ici, des agressions plus complexes et plus subtiles. En effet, il va être question de menaces contre l'homme, contre sa raison et voire, même, contre son subconscient.

De plus en plus, les guerres se gagnent sur les écrans de télévision du monde aussi bien que sur les champs de batailles. Les armées se font pourvoyeuses de désinformations (mouvement d'une division anglaise complètement occulté pendant "Desert Storm"), d'informations trompeuses (image de missile "Patriot" interceptant un scud) et d'images médiatiques marquantes (cf. l'opération "Nautile", campagne du SIRPA contre Greenpeace).

Les stratèges du savoir devront, donc, tenir compte du champ de bataille des médias, lieu où risquent de ce dérouler, demain, les combats les plus acharnés.
Six outils sont utilisables pour "manipuler les esprits" :

- l'accusation d'atrocités;
- le gonflement des enjeux,
- la diabolisation ou déshumanisation de l'adversaire;
- la polarisation;
- l'invocation de la sanction divine;
- la meta-propagande (discrédit de la propagande adverse).

Il est intéressant de noter que ces outils relèvent de la Deuxième Vague et ont souvent été utilisés au cours des deux derniers conflits mondiaux mais, relayés par le développement de la télévision et par son omniprésence dans la société contemporaine, ils prennent une puissance considérable.

L'action psychologique a un champ d'action très vaste, allant de la simple distribution de tracts sur un marché civil à des actions de déception, de désinformation et de manipulation extrêmement sophistiquées.
A ce titre la guerre du Golfe est un exemple d'utilisation d'arme psychologiques : campagne de désinformation présentant l'armée américaine comme dotée de matériels trop sophistiqués et peu efficaces dans le désert, médiatisation de la partie propre des combats (frappes chirurgicales avec des armes guidées laser) et voile complet sur les bombardements classiques, lâché de millions de tracts sur les lignes irakiennes promettant un bon traitement en cas de reddition, manipulation de l'information diffusée via CNN.

Agir sur le mental de l'adversaire et de ses propres troupes est une donnée essentielle à l'ère de la communication, il suffit de voir le succès de la radio "Azur FM" mise en place par les forces françaises sur le théâtre de l'ex-Yougoslavie.

Que se soit contre les moyens ou les utilisateurs, les attaques utilisables par les "combattants de l'information" sont, donc, nombreuses et variées. En cas de maîtrise de ces capacités (même en partie) par une nation, elle aurait à sa disposition des outils très puissants lui permettant de bénéficier d'un avantage certains.

3. QUELLE STRATEGIE[3] ?

> Le terrorisme informatique doit être vu comme un acte proche d'un acte de guerre, il s'agit, pour être efficace d'établir une stratégie à long terme et d'avoir la maîtrise d'un très grand nombre de facteurs. [3]

Les deux parties précédentes ont permis de se rendre compte de l'importance des menaces qui risquent de peser sur les capacités d'une nation à recueillir des informations sûres, à les analyser et utiliser ses moyens de commandement en toute sécurité. Il est, alors, logique d'essayer d'inclure ces nouvelles données dans la réflexion de défense.

La guerre de l'information doit faire partie d'une stratégie globale et cohérente. Elle suppose, donc, pour être mise en œuvre dans le domaine militaire et diplomatique, l'existence au niveau de l'Etat, d'une volonté de l'utiliser au service d'un but. "*Si la guerre doit correspondre entièrement aux intentions politiques et si la politique doit s'adapter aux moyens de guerre disponibles, ...*"[4]

---

[3] "Partie de la science militaire qui concerne la conduite générale de la guerre et l'organisation de la défense d'un pays". Le petit Robert, édition 1977.
[4] CLAUSEWITZ, *De la guerre,* VIII, 6, p 708.

La guerre de l'information se jouant dès le temps de paix, le rôle des chefs militaires est de présenter aux décideurs les moyens d'action disponibles pour mener à bien leur politique. Elle doit viser de manière directe ou indirecte les structures politiques, sociales et économiques des cibles, dans un but d'influencer les acteurs et leur processus décisionnel.

Pour être efficace Il semble qu'il faille modifier "l'équilibre de l'information et du savoir"[5] en sa faveur; cela devrait pouvoir s'obtenir par une formation des différents acteurs, une doctrine claire et simple et des infrastructures techniques et humaines capables de faire fonctionner tous les systèmes vitaux.

3.1. Formation et doctrine

Dans la réflexion militaire française, ces doctrines de guerre du C^2 sont encore "primitives". Il convient de formuler un concept plus systématique et englobant de "stratégie du savoir". Ce que l'on peut rapidement résumer par la notion de fonctions cruciales devant être maîtrisées : acquérir, traiter, distribuer et protéger l'information, tout en la refusant à ses ennemis et en ne la distribuant qu'avec parcimonie à ses alliés.

Bien sûr, c'est un domaine qui a besoin d'une doctrine claire, de formations et de moyens. D'où, l'importance d'encourager l'étude et la réflexion en ce domaine dans les cycles de formation supérieure comme le font les Américains depuis 1993 avec la création d'un cours sur la guerre de l'information à la National Defense University de Fort McNair (DC) ou comme le préconise M. SERVENT, *"Les formations qui devraient être délivrées (Ecoles, CID, CHEM-IHEDN) devraient être particulièrement dynamiques pour être efficaces". Il ne faut pas s'imaginer pouvoir répondre aux besoins décrits ici avec une simple conférence alibi.*[4]

Cela permettrait de mieux définir les composantes de la guerre du savoir, d'identifier la toile complexe de leurs interrelations et d'élaborer des "modèles" ouvrant sur des options stratégiques, puis sur des schémas de mise en œuvre de moyens.

3.2. Organisation et techniques

La première étape est de savoir que cette menace existe et qu'il va falloir se protéger. Contrairement à ce que pense M. GÉRÉ [7], il ne s'agit pas de savoir si on débouche sur une transformation fondamentale de la conception des guerres futures, mais de se rendre compte que l'introduction des Systèmes d'Information et de Commandement (SIC) induit un changement dans la conduite des états-majors, et qu'une attaque ciblée sur ces systèmes perturbera le schéma de prise de décision pendant un temps, certes court, mais peut-être suffisant pour prendre l'ascendant sur l'autre.

[5] travaux de définition de la cyberguerre par David RONFELDT & John ARQUILLA à la RAND Corporation.

Ensuite, il faut sensibiliser tous les personnels et développer une série de parades, à la fois dans le domaine matériel (Firewall, etc. ...) mais surtout dans le domaine de la communication opérationnelle et des opérations psychologiques (les deux étant différents et ne devant surtout pas être mélangés). Pour ce champ, à la fois difficile et particulier, il est nécessaire que le décideur expose aux militaires les buts de sa politique afin que ces derniers ne se trompent pas de cible et débouchent sur des résultats militaires contre-productifs.

Enfin, ce domaine étant à la limite du réel et du virtuel, il convient de développer une capacité de simulation afin de contrôler la vulnérabilité des systèmes et d'imaginer puis de valider, de manière discrète, des concepts et des capacités spécifiques à ce type de conflit. D'ailleurs, le Département de la Défense américain a demandé à la société RAND Corporation de conduire des exercices de simulations stratégiques sur ce sujet (six exercices ont eu lieu en 1995. Les participants étaient des hauts responsables de la sécurité nationale et des industriels du secteur des communications).

CONCLUSION

Bien que pour beaucoup de personnes, la guerre de l'information ne soit qu'une mode, voire un avatar d'une théorie fumeuse, la révolution dans les affaires militaires (ou RMA en anglais), il serait dangereux pour la France de ne pas en tenir compte et surtout de ne pas l'étudier. De plus, le fait que les Américains soient en train de consacrer une part importante de leur budget de défense à ce sujet, devrait suffire à se persuader de l'intérêt de ce domaine.
Du point de vue de la réflexion stratégique, c'est un concept tout à fait cohérent avec la notion d'approche indirecte prôné par LIDELLHART, mais pour être pleinement efficace, il doit être pris dans sa globalité, non pas uniquement dans un but de destruction et de neutralisation, mais dans une notion d'influence sur les acteurs et sur leurs processus décisionnels.

La manière dont la réflexion et les tentatives de mise en œuvre ont eu lieu est assez typique. Le contraste avec le modèle anglo-saxon est frappant. D'un côté, il y a des lignes directrices extrêmement fortes et le plus souvent des moyens puissants adaptés et de l'autre des lignes plus floues et des moyens plus flottants.

Enfin, la guerre de l'information est une stratégie de puissance adaptée à un Etat ayant une puissance économique mondiale et l'utilisant au service d'une volonté politique. Il semble, donc, difficile à la France de pouvoir mener ce type de combat de façon totalement autonome. De la même manière qu'on envisage des coalitions tactiques modulaires où chaque allié apporte les forces armées et les technologies spécialisées qui feront défaut aux autres, ne faudra-t-il pas envisager une mise en commun de certains moyens et amorcer une approche stratégique européenne (sous contrôle français bien entendu !) ?

BIBLIOGRAPHIE

[1]CLAUSEWITZ Carl von
De la guerre, Les éditions de minuit, 1955 (réédition décembre 1988).

[2]OUGH Bryan, MUNGO Paul
La Délinquance Assistée par Ordinateur, DunodTech, 1993.

[3]GALLEY Patrick
Terrorisme informatique : Quels sont les risques ?,
Mémoire de projet, Ecole polytechnique de Lausanne, 30/05/96.

[4]SERVENT Pierre (CBA ORSEM)
Rapport de mission en Bosnie et en France
Service d'Information et de Relation Publique des Armées (SIRPA) 10/97.

[6]TOFFLER Alvin et Heidi
Guerre et contre guerre, Fayard, 1994.

[7]L'ARMEMENT n°60, décembre 97 - janvier 98
Revue de la Délégation Générale pour l'Armement (DGA).

[8]Perspectives stratégiques n° 24 (01/97) & 32 (11/97)
Fondation pour les Etudes de Défense (FED).

[9]Comment palier les vulnérabilités informatiques d'une force opérationnelle terrestre
Etude complémentaire opérationnelle à option, CSEM, 96-97.

Articles :
La nouvelle guerre froide
Planète Internet, Novembre 96.
Le firewall en sentinelle
Informatiques Magazine, Octobre 96.

Colloques & Conférences :
la guerre de l'information
Centre d'Etude en Sciences Sociales de la Défense (CE2SD), 6/11/97.
Les Etats-Unis, l'internet et la guerre de l'information
Centre des Hautes Etudes de l'Armement (CHEAr), 19/11/97

ANNEXE : LES THEORIES DE TOFFLER.

	Première Vague **« âge agraire »**	**Deuxième Vague** **« âge industriel »**	**Troisième Vague** **« âge de l'information »**
Facteurs déclenchants	.revendications locales de terres; .rivalités entre souverains.	.compétition géo-économique. .revendications régionales. .rivalités entre peuples, l'Etat-Nation se substitue au chef.	.ère de la géo-information, conflits liés à la compétition dans le domaine du savoir. .rivalités économiques. .rivalités entre idéologies.
Caractéristiques effets recherchés	.guerres limitées. .« affaire personnalisée du corps à corps », destruction de l'infanterie ennemie. **«attrition of infantry ».**	.guerre totale. .destructions massives. .destruction des équipements. **« attrition of machines ».**	.guerre plus complexe. .par la maîtrise de l'information, du savoir, destruction de la volonté et de la capacité d'agir de l'adversaire. **« attrition of will and capability »**
Les Armées.	.diversité dans leur dimension, capacité, moral, qualité des chefs et entraînement. .armées liées à un chef. .armement non normalisé et usage limité des armes tirées à distance.	.industrialisation de la guerre. .armées de conscrits liés à une nation. .standardisation tant dans le domaine de l'équipement que dans ceux de l'entraînement, de l'organisation que de la doctrine. .production industrielle des armes. .« opérations linéaires, de masse concentrées, conduites suivant la voie hiérarchique ».	.acquisition et gestion de l'information .« démassification »: équipements diversifiés et automatisés. Sélection et précision dans le traitement des objectifs. .baisse des effectifs: personnels moins nombreux mais spécialisés et plus instruits: « Les guerriers abrutis sont à la *Troisième* Vague ce que les ouvriers non qualifiés sont à l'économie de la Troisième Vague: une espèce menacée. » .« front fuyant »