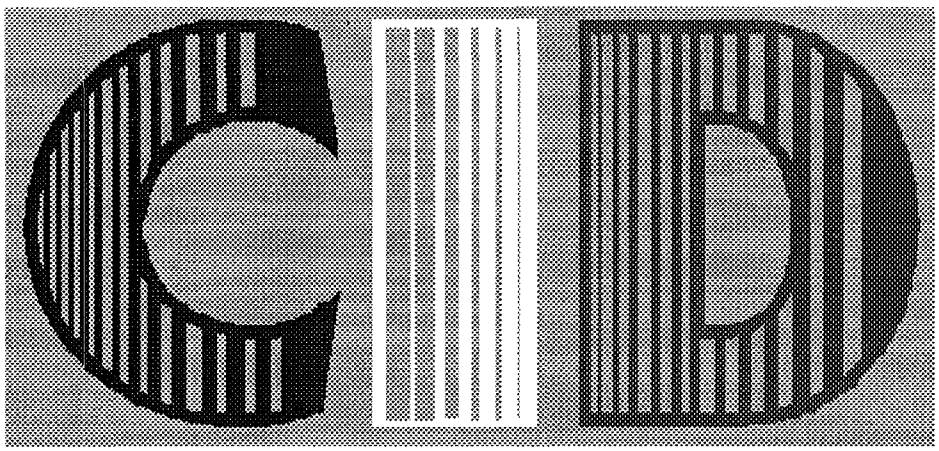
COLLEGE INTERARMEES



DE DEFENSE

SESSION 1997-1998

MEMOIRE DE GEOSTRATEGIE

LA GUERRE DE L'INFORMATION DANS LE CONTEXTE DE LA DEFENSE MILITAIRE

par :

LCL Mohamad Yusop bin Daud Gp A5

mars 1998

LA GUERRE DE L'INFORMATION DANS LE CONTEXTE DE LA DEFENSE MILITAIRE

INTRODUCTION

Des services télématiques sur micro-ordinateur, des téléphones mobiles, des caméscopes, et des télécopieurs sont capables de fournir des points d'entrée et des réseaux de diffusion pour propager la propagande de nos adversaires. Les cibles définies sont les structures stratégiques militaires, gouvernementales, économiques, même les comptes bancaires individuels des troupes déployées. Ce phénomène est inévitable car les systèmes d'information imprègnent notre vie militaire et civile. Voici des exemples de propagande ayant influencé le moral national et le soutien de forces armées de la nation. La guerre du Vietnam, apprit aux forces armées Américaines que rien ne servait de gagner chaque bataille si la guerre de l'information était perdue. Tout le monde connaît l'impact de l'échec de la capture de Mohamed Farah Aidid en Somalie par les États-Unis. Le potentiel de manipulation des multimédias par des gouvernements, des militaires, ou des parties politiques ou religieux dans une guerre civile telle que la Bosnie est un enjeu stratégique majeur. Ce qui conditionne les opérations militaires futures. Autrement dit, aujourd'hui nous devons investir non seulement dans les personnels mais aussi dans la planification, le matériel, et la recherche si nous voulons que nos ambitions puissent devenir des réalités.

Pourquoi, alors, devrions-nous penser à cette nouvelle et peut-être étrange idée ? La raison principale est que nous nous rendons compte que la guerre de l'information est quelque chose important. Dans le développement suivant nous nous attacherons à définir quatre notions : une définition de la guerre de l'information, la relation entre la guerre de l'information et la guerre de la commande et contrôle (C2), l'importance de la guerre de l'information, et le développement d'une stratégie de guerre de l'information.

LA DEFINITION DE LA GUERRE DE L'INFORMATION

Un nouveau facteur important dans la guerre de l'information est la couverture mondiale de la télévision et de la radio. La guerre de l'information au niveau stratégique est la « bataille en dehors du champ de bataille ». Elle définira le nouveau « espace de bataille ». Nous le confronterons dans un « champ de bataille intégré », pas dans le sens habituel c'est a dire d'avoir un système récepteur de positionnement global (GPS) dans chaque char ou chaque avion mais dans le sens de Clausewitz où la guerre est intégrée dans le politique presque simultanément avec la bataille.

La guerre de l'information, dans son sens le plus large, est simplement l'utilisation d'informations afin de réaliser nos objectifs nationaux. Comme la diplomatie, la compétition économique, ou l'utilisation de la force militaire, l'information en soi est un aspect majeur de la puissance nationale et devient une ressource nationale essentielle qui supporte la diplomatie, la compétition économique, et l'emploi pertinent des forces militaires.

La guerre de l'information est une notion complexe. Elle est complexe parce que les armes utilisées ont toujours en commun des mots, des photos, et des images, bien qu'aujourd'hui, ceux-ci puissent être transformés ou manipulés par des moyens sophistiqués. Elle est complexe parce que les attaques sont réalisées par des esprits pour affecter d'autres esprits. En outre, elle est compliquée parce que les attaques peuvent être directes ou indirectes, visant des organisations internes ou externes. La seule constante réside dans l'effet recherché. Dans la guerre de l'information l'effet désiré doit influencer et changer ce que l'adversaire croit ou ce que l'adversaire décide.

Au plus haut niveau de la stratégie, les nations cherchent à saisir, exploiter, et protéger l'information pour atteindre leurs objectifs. Cette exploitation et cette protection peuvent se produire dans les arènes économiques, politiques, ou militaires. La connaissance de l'information de l'adversaire est un moyen de mettre en valeur nos propres capacités, de dégrader ou contrecarrer les capacités ennemies, et de protéger nos propres capitaux, y compris notre propre information. Ce n'est pas nouveau. La lutte pour découvrir et exploiter l'information a commencé la première fois qu'un groupe de personnes a essayé de gagner l'avantage sur autrui. La guerre de l'information, dans son sens le plus fondamental, est le " théâtre " émergeant o un conflit entre états au niveau stratégique est le plus de chance de se produire.

La guerre de l'information vise les capacités d'information de l'ennemi, tout en protégeant les nôtres. Ayant précisé le sens de l'information et les fonctions de cette information, nous définissons la guerre de l'information comme suit :

> « Toutes actions visant à nier, exploiter, pour altérer, ou détruire l'information de l'ennemi et ses fonctions, protection contre ces actions, et exploitations de nos propres fonctions d'information militaire ».

Cette définition sert de base aux affirmations suivantes :

> La guerre de l'information peut se traduire par une attaque contre une fonction de l'information, indépendamment des moyens. Le bombardement de moyens de distribution téléphonique est la guerre de l'information, la destruction du logiciel de distribution en est aussi un exemple.
>
> La guerre de l'information représente n'importe quelle action entreprise pour protéger nos fonctions d'information, indépendamment des moyens. Le durcissement et la défense de la facilité de distribution contre l'attaque aérienne sont une guerre de l'information, l'emploi d'un programme anti-virus pour protéger le logiciel du service aussi.
>
> La guerre de l'information est à l'instar de la guerre aérienne, un moyen, pas une fin. Nous pouvons utiliser la guerre de l'information simultanément avec la conduite de l'attaque ou de l'interdiction stratégique, de la même manière que nous employons la guerre aérienne pour conduire l'attaque et l'interdiction stratégiques.

Les forces armées toujours essayent d'obtenir ou d'affecter l'information de l'adversaire pour l'utiliser au bénéfice de leurs forces. Les stratégies anciennes sont axées sur la « déception » afin d'influencer les décisions des décideurs adverses. Ce qui est une attaque indirecte puisque ces stratégies influencent l'information en altérant le processus de perception. Pour que la déception soit rendue inefficace, l'ennemi doit agir selon le processus suivant : observer la déception et agir sur ce processus.

Cependant, les moyens modernes pour exécuter les fonctions de l'information sont vulnérables à l'accès direct et à la manipulation de l'information. La technologie moderne permet à un adversaire de changer ou de créer l'information sans compter sur l'observation et l'interprétation. Voici une liste des caractéristiques modernes des systèmes d'information qui crée cette vulnérabilité : la mémoire concentrée, la vitesse d'accès, l'information-transmission répandue, et la capacité accrue des systèmes. Les mesures de sécurité intelligentes peuvent réduire, mais pas éliminer cette vulnérabilité. Leur absence est un facteur de faiblesse flagrant.

Les forces armées ne sont pas tentées de laisser leur succès aux fortunes de la guerre. Aussi, nous devons diriger nos efforts de guerre de l'information non seulement pour obtenir l'information de l'adversaire mais également défendre notre propre information. L'armée dépend fortement des fonctions de l'information militaire, la rendant vulnérable à la guerre de l'information. L'intégrité des fonctions de l'information militaire, aussi bien que l'information elle-même, ont une grande influence sur le succès de nos opérations militaires.

LA RELATION ENTRE LA GUERRE DE L'INFORMATION ET LA GUERRE DU C2

Le centre de la guerre d'information se situe dans n'importe quelle fonction de l'information : cela peut être la C2 (commande et contrôle), le système de commande d'une raffinerie, ou une station de commutation de téléphone. Le C2 représente seulement une partie de l'univers des fonctions de l'information militaires. Une des définitions du commandement et du contrôle est la suivante :

> « L'exercice de l'autorité et de la direction par un commandement approprié afin que les forces assignées puissent accomplir leur mission ».

La guerre de l'information est parfois désignée incorrectement sous le nom de la guerre de la commande et du contrôle, ou la guerre C2. Le but de ce type de guerre est d'utiliser des attaques physiques et radio-électroniques contre les systèmes d'information ennemis pour séparer les liaisons entre les forces ennemies et leurs commandements. En théorie, la guerre de l'information est réellement un ensemble d'activités beaucoup plus complexe, visant à atteindre l'esprit et la volonté de l'ennemi.

La guerre du C2 ne s'adresse qu'aux activités contre la capacité de l'adversaire de diriger la mise en place et l'emploi de ses forces, ou celles qui protègent la capacité de commandemant de celui-ci. Comme nous l'avons illustré, la guerre de l'information non seulement s'interesse à l'attaque du processus C2, mais

aussi à la destruction de la puissance de combat de l'ennemi. Réciproquement, la guerre du C2 n'a pas pour but réduire ou d'annuler la capacité ou le désir des unités de combat d'exécuter leurs ordres. Les opérations psychologiques tactiques et de« contre-mesures électronique d'auto-protection» gênent la capacité des unités à exécuter leurs ordres. Mais elles n'affectent nullement la capacité des commandants d'émettre des ordres à ces unités, ni leur capacité de recevoir ces ordres.

Bien qu'extraordinairement important, la politique de la guerre du C2 devrait seulement être une application particulière de la guerre de l'information. C'est une erreur grave pour les armées d'ignorer les autres aspects de la guerre de l'information. Par conséquent, la guerre de l'information, avec son organisation propre est essentielle à une guerre du C2 efficace.

L'IMPORTANCE DE LA GUERRE DE L' INFORMATION APPLIQUEE A LA DEFENSE

Nous devrions nous attendre à ce que nos systèmes d'information soient vulnérables à l'attaque. Les attaques, quand elles surviennent, peuvent apparaître sans aucune déclaration formelle de l'intention hostile de l'état adverse. Quand elles viennent, les attaques seront poursuivies contre les systèmes de la connaissance et les systèmes de la croyance, destinés à influencer les choix de dirigeants. Les non-combattants, ainsi que les dirigeants seront des cibles.

Pourquoi la guerre de l'information est-elle importante pour la défense ? Il y a deux raisons. Premièrement, la guerre de l'information offre des moyens importants pour accomplir des missions militaires. Deuxièmement, l'intégration répandue des systèmes d'information dans des opérations militaires permet aux fonctions de l'information des militaires d'acquérir une réelle valeur.

Un exemple hypothétique utilisant l'attaque de l'information montre comment la guerre de l'information pourrait réaliser une mission typique dévolue en temps normal à l'Armée de l'air:

> Les missions de BAI empêchent ou retardent les approvisionnements des unités de combat. Une mission de bombardement détruit des travées de pont en utilisant des BGL. A la place, nous pourrions modifier l'information des planificateurs adverses, classant ainsi faussement les ponts comme détruits. Cette information pousserait les planificateurs à réorienter leurs forces et les approvisionnements. Tout le monde pense que la mission est exécutée; mais l'attaque de l'information offre la possibilité de réaliser notre but tout en consommant peu de ressources ou sans exposer nos forces à l'attaque.

On peut illustrer le besoin de défenses renforcés contre la guerre de l'information si on imagine le chaos qui s'ensuivrait si un adversaire parvenait à pénétrer notre base de données instantanées pour de déploiement de force. Les changements subtils apportés pourraient totalement alterer nos capacités de projection de puissance en temps réel.

Au niveau stratégique dans des états à la capacité technologie élevée, la cible pour la guerre de l'information est merveilleusement riche: les télécommunications et téléphonie, les capteurs espace basé, les systèmes de relais de transmissions, les aides automatisées aux banques et aux transactions commerciales, les systèmes de production et de distribution d'énergie, les systèmes culturels de toutes sortes, et la gamme entière de matériel et de logiciel qui constitue ce que l'adversaire sait et ce que l'adversaire croit. Les systèmes d'information stratégiques dans les états à la capacité technologie élevée reflètent souvent un niveau opérationnel de même complexité. Tous sont vulnérables à l'attaque.

La guerre de l'information n'a pas besoin d'être reportée jusqu'à ce que l'hostilité devienne ouverte. Les dirigeants adverses seront peu enclins à combattre s'ils croient une ou plusieurs des affirmations suivants : cette violence est mauvaise, ils seront sans alliés, ils feront face à des sanctions dures, ou leur base industrielle ne supportera pas une guerre prolongée, leurs forces armées ne sont prêtes. Si le combat réel éclate, les attaques au niveau opérationnel peuvent s'harmoniser avec des attaques au niveau stratégique.

UNE STRATEGIE DE LA GUERRE DE L'INFORMATION

Pour développer une stratégie de la guerre de l'information, il faut réfléchir sérieusement aux technologies et aux aspects de l'information qui pourraient être tournées vers un but stratégique. Ceci implique de penser à l'information sous une nouvelle approche : quelle information est nécessaire? Quels changements d'organisation se produiront dans la manière o nous nous réunissons, traitons, distribuons, et utilisons l'information ? Quels changements opérationnels information-base peuvent alors se produire?

Nous pourrions employer la stratégie suivante pour réaliser l'infrastructure information de la défense :

Redéfinir la protection des infrastructures, (non seulement la protection de système ou de réseau). La conception des systèmes et des réseaux est généralement basée sur des considérations d'efficacité. La protection des infrastructures doit, donc, elle aussi être basée sur des considérations d'efficacité contre les attaques liées à la guerre de l'information, particulièrement dans les domaines de la capacité de survie et du soutien des fonctions critiques, et sur l'indépendance des fonctions du contrôle de l'infrastructure.

Protéger l'information proportionnellement à son importance. Certaines informations non classifiées mais de circonstance, (des données de temps et de terrain) peuvent avoir une signification plus tactique que des informations secrètes (par exemple, évaluations périmées du renseignement).

Intégrer les aspects politiques, techniques, opérationnels, et de personnel. Chacun de ces aspects est traité séparément par diverses cellules. Ils doivent être intégrés pour améliorer leur compétence et leur efficacité.

Ajouter des programmes en cours. Utiliser les activités et les programmes courantes de sécurité de l'information, et les disciplines de sécurité connexes comme la base pour réaliser une capacité de défense de guerre de l'information.

Harmoniser la défense de guerre de l'information, l'offense de guerre de l'information, la sécurité de l'information, et les fonctions de support intelligence. Ces fonctions étroitement liées sont basées sur beaucoup de technologies et de processus communs qui ont besoin d'un support mutuel.

Conduire vigoureusement la coordination entre tous les organismes concernés. L'infrastructure information de la défense est fortement complexe et rapidement évolutive. Il est nécessaire de définir des mesures afin d'exclure la duplication des efforts et la poursuite de buts contradictoires.

CONCLUSION

Les progrès des technologies de l'information produisent des changements extrêmes dans la manière o une nation prépare les guerres de l'avenir. Elles permettent une vision de « l'espace de bataille » à diffuser jusqu'au niveau le plus bas. Pour cette raison, chaque professionnel des armées a la responsabilité de comprendre l'impact de la guerre de l'information sur son service. Pour assurer l'interopérabilité, un soldat, un marin, ou un aviateur, peut alors développer une compréhension identique de la façon d'employer la guerre de l'information.

La compréhension du concept de la guerre de l'information est essentiel car il aide à définir le champ de bataille sur lequel la défense doit fonctionner. Elle s'identifie non seulement à la propagande, la déception ou la guerre électronique traditionnelle mais aussi à la guerre politique intégrée, se déroulant simultanément avec la bataille. La guerre de l'information n'est pas nouvelle mais le système d'information est plus vulnérable aux attaques depuis l'arrivée de la technologie moderne.

Nous connaissons maintenant la condition pour développer la vision qui produit la stratégie. La stratégie identifiera les technologies, les changements d'organisation, et les nouveaux concepts des opérations. Le développement la stratégie de la guerre de l'information peut être basé sur les fondements existants quoiqu'il nécessite beaucoup de créativité.