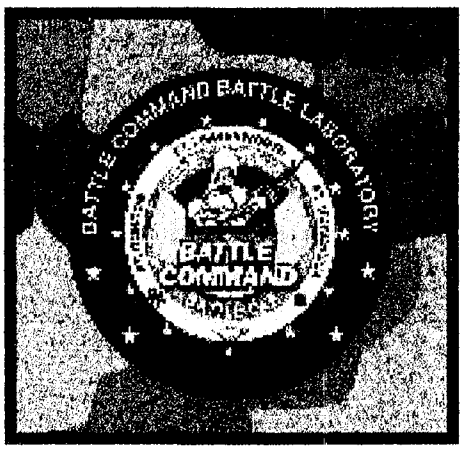
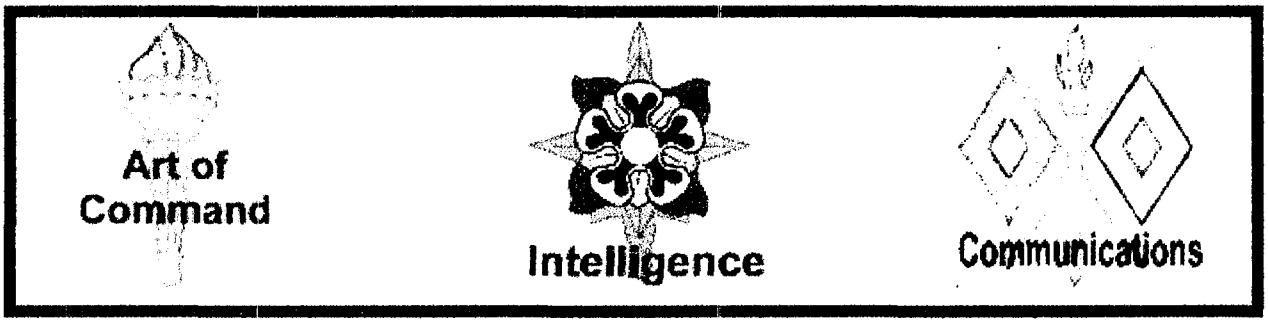
-1998-51

CBA SUATTON Christian
5eme PROMOTION
Div B / groupe B2

Paris, le 24 mars 1998

L'U.S.Army et les Opérations d'Information





Stratégie

SOMMAIRE

1. INTRODUCTION

Un constat s'impose : nos sociétés sont entrées de plain-pied dans " l'âge de l'information". Elles dépendent toujours plus de flots d'informations, soit que celles-ci transitent sur leur continent, par tous les médiums disponibles (Internet, faisceaux hertziens, satellites, câbles, etc.) , soit qu'elles soient stockées dans de gigantesques bases de données dans lesquelles piochent alors les services autorisés, gouvernementaux ou privés. L'utilisateur moyen n'a accès, par l'intermédiaire de son ordinateur et de son téléphone, qu'à ce que ces services veulent bien lui montrer ou lui communiquer : accès à ses comptes bancaires, publicités pour de nouveaux films, compte-rendu de séances de l'ONU entre autres.

L'explosion des technologies de l'information a ainsi initié un mouvement d'une ampleur que le grand public mesure encore assez mal. Bien que nous ne soyons qu'au début de cette nouvelle ère, les progrès technologiques rendent possibles l'accès, par les décideurs, à une information toujours plus complète, plus précise et dans des délais de plus en plus courts. Au fur et à mesure de la chute des coûts de traitement et de communication, il devient rentable pour des organisations publiques ou privées d'adopter et d'utiliser ses technologies dans des situations de plus en plus nombreuses.

Au niveau du D.O.D[1], cette explosion a été qualifiée de révolution, la R.M.A[2] :

<< Changement majeur dans la nature de la guerre découlant de l'utilisation de technologies innovantes qui, combinées à des changements décisifs dans la doctrine militaire et les concepts opérationnels, modifie fondamentalement le caractère et la conduite des opérations >>.

Pour la première fois de leur histoire, les Etats-Unis ne peuvent plus considérer le CONUS[3] comme un sanctuaire à l'abri de toute menace étrangère du fait de son parapluie nucléaire et de ses frontières naturelles que constituent ses océans. Pour répondre à ces menaces et aux défis de cette révolution, l'U.S.Army à développé le concept des opérations d'information[4].

---

[1] Department of Defense : ministère de la défense des U.S.A

[2] Revolution in Military Affairs

[3] CONtinental US : territoire des U.S.A. situé en Amérique du nord

[4] information : renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée une communication, un enregistrement ou un traitement.

2. MENACES

La dépendance de plus en plus grande de nos sociétés envers l'information, ses systèmes et ses réseaux, conjuguée au coût sans cesse diminuant de matériels de plus en plus performants, contribue à la vulnérabilisation des forces armées. Lorsqu'il est possible de s'offrir les services d'un ingénieur informaticien indien, aussi qualifié que son homologue occidental, pour 2000 Fr. par mois, le rapport coût/efficacité d'une attaque devient redoutablement intéressant.

Les menaces envers les infrastructures de l'information sont sérieuses, d'origines multiples et surtout grandissantes. Elles peuvent provenir d'individus ou de groupes motivés par des intérêts dans des domaines aussi variés que les affaires militaires, la politique, la société, la culture, l'ethnicité, les religions ou l'industrie et le commerce. Mais elles peuvent provenir simplement de vandales qui investissent les systèmes informatiques pour le plaisir et la reconnaissance de leurs capacités.

Les menaces envers les ordinateurs, les systèmes et les réseaux sont classées par niveau d'hostilité (temps de paix, crise, guerre), par niveau de capacité technique de l'agresseur et par sujet d'intérêt.

Elles sont présentes dès le temps de paix, leur niveau de gravité pouvant augmenter au fur et à mesure de l'aggravation de la situation

2.1. Modes d'action

Un adversaire potentiel dispose de plusieurs options pour influencer ou attaquer les S.I.C[5] et les services gouvernementaux. Les actions peuvent être immédiates - dégradation de capacité ou destruction physique - ou à effet retard tels que corruption de base de donnée ou prise de contrôle d'un programme. Parmi celles-ci, on trouve :

- accès non autorisé, afin de récupérer ou d'ajouter des données;
- implémentation[6] de logiciels "malveillants" destinés à engendrer, pour un programme donné, un fonctionnement différent prévu à l'origine[7]. Cette catégorie comprend les virus, les bombes logiques et les programmes destinés à contourner les contrôles de sécurité;
- utilisation d'attaques électroniques pour rendre les données fausses ou inutilisables;
- collecte de renseignements électroniques, signaux, rayonnements ou données;
- conduite d'attaques électroniques telles que brouillage, falsification de signal ou génération de rafales d'E.M.P;

---

[5] système d'information et de commandement

[6] terme informatique signifiant : mise en place d'un logiciel sur une plate-forme informatique

[7] C'est le cas du logiciel "Lotus Notes" dont le gouvernement suédois vient d'expliquer que ses services ont trouvé une porte dérobée, installée à la demande de la CIA, pour lui permettre d'espionner tranquillement ses utilisateurs à leurs dépens.

- emploi d'opérations psychologiques et de déception pour influencer ou s'opposer aux S.I.C adverses;
- attaques pour détruire physiquement, dégrader ou perturber les réseaux civils de contrôle et de communication dont dépendent les opérations militaires, soit par l'utilisation de missiles ou de bombes, soit par attentats terroristes;
- utilisation de moyens electromagnétiques pour brouiller les systèmes de communication commerciaux utilisés par les armées.

2.2. Sources

Ces menaces peuvent provenir d'une grande variété de sources allant de l'individu, utilisateur non autorisé ou interne à une société, aux services de renseignement étrangers, militaires ou civils. Les frontières entre ces groupes sont floues et il est souvent difficile de discerner les origines d'un incident particulier. Une action paraissant être le fait d'un " hacker[8]" peut en réalité être due à un service étranger.

Les **utilisateurs non autorisés**, tels que les hackers, sont la source la plus importante d'attaques en temps de paix. Leur menace envers les réseaux et les systèmes est sans cesse croissante.

Les **" internes "** , individus possédant un droit d'accès légitime aux systèmes, représentent la menace la plus difficile à contrer. Qu'il agisse sur commande ou par motivation personnelle , " l'interne " a accès à des systèmes protégés contre les attaques. Les périodes les plus propices à leurs agressions sont lors de la conception, la fabrication, la mise en place et l'entretien du système d'information[9].

Les **terroristes** ont un usage grandissant des S.I.C commerciaux, dont Internet. Leurs actions vont de l'accès illégal à un réseau d'information jusqu'aux attaques physiques de l'infrastructure. Ils font de même un usage important des systèmes commerciaux pour transmettre leurs renseignements.

Les **groupes non étatiques**, jusqu'alors peu coutumiers du fait, tels que cartels de la drogue ou activistes politiques, tirent avantage des possibilités offertes par "l'âge de l'information". Ils peuvent acquérir à bas prix les infrastructures commerciales, de communication de la Défense, aussi bien civiles que militaires. Ils peuvent utiliser les médias pour tenter d'influencer les opinions publiques et modifier la perception d'un conflit. La dernière campagne de GreenPeace contre les essais nucléaires français en est un exemple probant.

Les **services de renseignement** sont bien entendu les acteurs privilégiés de ces opérations, profitant de l'anonymat fourni par certains modes de fonctionnement des réseaux pour dissimuler leurs actions derrière la façade d'innocents "hackers". Mais leurs objectifs principaux sont plus souvent les réseaux commerciaux ou scientifiques civils que militaires.

---

[8] Hacker : nom moderne des pirates informatiques qui pénètrent par effraction dans les réseaux et les systèmes, le plus souvent par jeu.

[9] Pendant la guerre du Vietnam, les Américains ont constaté que 60% de leurs ordinateurs sur place étaient piégés. Les enquêtes ont déterminé que c'était pendant les opérations de révision que des dispositifs étaient installés.

On trouve enfin les **forces armées adverses** et les **adversaires politiques**, dont l'habileté à manipuler les médias peut leur procurer un avantage décisif dès avant le début du conflit, voire même empêcher le conflit. L'attitude de Sadam Hussein début 98 pour "enfoncer un coin" dans la coalition qui l'avait bouté hors du Koweït en est une preuve.

3. LES DEFIS POUR LE D.O.D

Il s'agit tout d'abord pour les U.S.A de protéger leurs communications. Selon la direction des systèmes d'information de la Défense (D.I.S.A : Defense Information System Agency) , plus de 95% des communications du D.O.D transitent par des réseaux commerciaux ne disposant pas de système de protection. De plus, ce sont ces mêmes réseaux qui véhiculent la plus grande partie de l'information ouverte.

Un autre aspect des opérations d'information est leur **permanence**. Il n'y a pas de discontinuité paix, crise, guerre. A l'image de la guerre sous-marine à laquelle se sont livrées les marines de l'O.T.A.N et du pacte de Varsovie durant la guerre froide, les actions relatives à l'information se déroulent à tout instant et les forces armées ne recevront jamais d'ordre préparatoire pour faire face à une menace plus ou moins précise. Il s'agit d'être constamment prêt.

Sur un autre plan, la vision globale de la planète que nous offrent les réseaux médiatiques, avec leurs images spectaculaires et leurs analyses en continu des opérations en cours par des "experts" militaires peuvent influer sur **l'opinion publique** et par conséquent sur la politique menée par les autorités américaines. Les chefs efficaces, civils et militaires, seront ceux capables d'anticiper la manière dont un adversaire pourra tenter de manipuler les médias afin d'éviter de voir le conflit se déplacer dans l'arène publique.

A l'influence exercée sur le peuple correspond celle qui touche au **moral des troupes** et l'on sait l'importance critique du moral dans le caractère américain. La volonté de vaincre, le dévouement au pays et la solidarité envers les camarades de combat pourraient être rapidement annihilées, soit par des actions psychologiques bien menées, soit par la simple propagation d'informations. A ce titre, les médias sont souvent plus rapides dans la diffusion de nouvelles, vraies ou fausses que ce qu'est en mesure de réaliser une chaîne hiérarchique militaire. L'exemple de Radio Mille Collines au Rwanda est suffisamment explicite, et il aurait été souhaitable de se donner les moyens de brouiller ou détruire la station. Une mauvaise nouvelle, une interprétation erronée, une information peu précise ou une désinformation peuvent influencer les familles, aussi bien que les troupes. La mise en place de constellations de satellites de communication en orbite basse, pouvant atteindre et surtout être atteints par un téléphone portable du type de ceux couramment employés constitue à ce titre une nouvelle menace par le lien direct qui peut être créé entre un soldat en opération et sa "base arrière" familiale. Et ce, où que ce soit sur le globe. Pourtant, l'U.S.Army n'envisage pas de retirer aux soldats leur libre accès aux radios, télévisions et journaux.

Terminons par un **point de vue légal**. Il existe aux U.S.A, et dans le monde entier en général, relativement peu de règles ou de lois gouvernant l'accès et l'utilisation des systèmes d'information et de leurs technologies, essentiellement en raison de l'éruption quasi permanente de nouveaux concepts informatiques et électroniques devant lesquels le législateur est débordé. Comment alors s'appuyer sur des lois pour définir des règles d'engagement ou des conventions complétant celles de La Haye en matière de droit de la guerre. Les U.S.A ne disposent pas d'une commission nationale informatique et liberté (C.N.I.L). leurs réseaux sont interconnectés, à l'image de l'Internet, et les lois définissant le contrôle du contenu et de sa diffusion sont encore à définir, à l'image de la tentative du président Clinton pour réguler le

Web qui s'est heurtée au **1er amendement**. De même, la mise à disposition du secteur public de produits jusqu'alors à usages strictement régulés par l'état, tels qu'images satellitaires à résolution métrique, peuvent mettre en danger les forces. La passation d'un contrat commercial avec une entreprise privée permet à un adversaire de se procurer des images d'une qualité suffisante, en temps quasi réel, de la situation sur le terrain.

Face à cet environnement, le D.O.D et les forces armées américaines ont défini le concept de maîtrise de l'information (I.D : Information Dominance). Mais l'acception de ce terme varie suivant les trois services. Qu'en est-il de celui de l'U.S.Army ?

4. L'U.S.ARMY ET LES OPERATIONS D'INFORMATION

L'U.S.Army est celui des trois services le plus prolixe en matière d'information, et peut être le plus en avance. Cela peut tenir au fait que son combat étant le plus tributaire du facteur humain, le contexte des I.O lui est apparu comme fondamentalement nouveau est extrêmement porteur.

4.1. Information Operations et Information Warfare

Le concept des I.O[10] de l'U.S.Army découle de celui de la guerre de l'information[11] du D.O.D, décrit dans le document C.J.C.S.I 3210.01 comme :

<< actions conduites pour obtenir la supériorité informationnelle en agissant sur l'information, les procédures basées sur l'information, les S.I.C et les réseaux informatiques de l'adversaire tout en protégeant nos propres capacités dans ces domaines >>.

L'objectif stratégique de l'I.W est de prendre et conserver un avantage décisif en attaquant la structure informationnelle nationale d'un adversaire par exploitation, interdiction et influence.

L'U.S.Army a ainsi défini son propre concept, les I.O pour se démarquer de celui du D.O.D plus orienté vers l'emploi en temps de guerre. Son approche est plus large, admettant que les questions relatives à l'information empiètent sur toutes les composantes des opérations militaires, en temps de paix, de crise ou de guerre. Les I.O de l'U.S.Army sont ainsi définies :

<< opérations militaires permanentes menées à l'intérieur de l'environnement informationnel militaire[12] qui permettent, favorisent et protègent les capacités d'une force amie à collecter, traiter et agir sur l'information pour en retirer un avantage dans tous les domaines des opérations. Les I.O comprennent l'interaction avec l'environnement informationnel global[13] ainsi que l'exploitation et l'interdiction des capacités de s'informer et de décider de l'adversaire >>.

Les I.O sont donc conduites de l'entraînement en temps de paix, pendant le déploiement et les combats, jusqu'au redéploiement final.

4.2. Composantes des I.O

Les champs d'action des I.O se composent de trois domaines interconnectés :

- les opérations,
- le renseignement et l'information utiles[14],

---

[10] Information Operations

[11] I.W : Information Warfare

[12] M.I.E : Military Information Environment

[13] G.I.E : Global Information Environment

[14] R.I.I : Relevant Information and Intelligence

- les S.I.C (INFOSYS).

4.3. Les opérations

Les opérations conduites par l'U.S.Army sont dénommées C2W (Command and Control Warfare), C.A (Civil Affairs operations) et P.A (Public Affairs operations).

4.3.1. Les opérations C2W

Les opérations relevant du domaine C2W correspondent intégralement à l'application du concept I.W du D.O.D. Offensives (C2-attack) ou défensives (C2-protect), leur objectif est d'influencer, priver, dégrader ou détruire les capacités C2 de l'adversaire tout en protégeant celles de l'U.S.Army. Même dans le contexte des opérations autres que la guerre[15], les C2W offrent au commandement des moyens létaux ou non de remplir sa mission. Les différentes composantes en sont les OPSEC (Operations Security), la déception, les opérations psychologiques (PSYOPS : Psychological Operations), la guerre électronique (E.W : Electronic Warfare) et la destruction physique.

Les **OPSEC** pourraient se résumer à assurer la sécurité des opérations. En réalité, il s'agit de déterminer les informations vitales qu'il faut protéger, d'identifier les actions que les systèmes de renseignement ennemis pourraient observer, de déterminer les signes qui suffiraient à l'adversaire pour reconstruire une information vitale, et enfin définir et conduire les mesures nécessaires à l'élimination ou la réduction à un niveau acceptable de la vulnérabilité des actions amies. Le principal défi des OPSEC est posé, comme nous l'avons dit, par les systèmes commerciaux disponibles en matière d'imagerie, de positionnement et de communications cellulaires[16]. Les médias constituent aussi un danger potentiel.

La **déception**, concept peu usité en France sans doute en raison de la quantité de moyens nécessaires à sa réalisation, est en revanche un paradigme de toute opération majeure américaine. Il suffit de se rappeler le positionnement d'une force amphibie du Marine Corps en face de Koweït City pendant l'opération Desert Storm. Les moyens informatiques modernes peuvent contribuer à la déception, en leurrant les systèmes adverses.

Les **PSYOPS** sont destinées à véhiculer des informations sélectionnées à destination d'audiences étrangères pour agir sur leur perception, sur leur motivation et, en définitive, sur le comportement de leur gouvernement, de leur organisation, de leur groupe ou des individus eux-mêmes. L'objectif avoué est d'induire ou de renforcer une attitude bienveillante à l'égard des responsables des opérations. Elles sont un outil essentiel des C2W et l'U.S.Army ne cache absolument pas leur emploi.

En ce qui concerne la **guerre électronique**, elle est tout à fait comparable au concept français.

---

[15] O.O.T.W : Operations Other Than War

[16] appelées ainsi en raison de la dénomination des paquets de données servant à véhiculer la communication, les cellules. Correspond au téléphone portable type GSM.

La **destruction physique** enfin fait partie intégrante des C2W, bien que ses effets soient radicalement différents de ceux des opérations précédemment citées. La guerre du Golfe a commencé, rappelons le, par la neutralisation des systèmes d'alerte avancée irakiens par un raid d'hélicoptères AH64. Il s'agissait bien là de priver l'adversaire de ses capacités de capter de l'information.

4.3.2. Les " Civils Affairs "

Les affaires civiles sont considérées comme un appui aux I.O. Leurs domaines d'activités permettent de faciliter les opérations par la mise en relation des autorités civiles, des O.N.G et des populations avec les troupes déployées, à l'image de l'opération " Restore Democracy " en Haïti.

Il est envisagé la mise en place, pour chaque opération, d'un C.M.O.C (centre d'opérations civilo-militaires) dont le but serait de créer ces relations et de les entretenir. De plus, le personnel des C.A joue un rôle important dans la collecte du renseignement.

4.3.3. Les " Public Affairs "

Les Américains ayant parfaitement mesuré l'importance croissante des médias d'information du grand public, le rôle des personnels des P.A est d'informer les commandants en chef des implications des opérations planifiées sur les opinions publiques. Elles contribuent de plus à protéger les soldats et leurs familles des conséquences désastreuses que pourrait avoir une mauvaise interprétation, volontaire ou non, d'événements en rapport avec les opérations en cours. L'actuelle polémique sur le syndrome du Golfe en fournit un exemple criant, se déroulant en temps de paix bien que l'origine vienne du conflit.

4.4. Renseignement et informations utiles (R.I.I.)

<< Les R.I.I sont les informations extraites du M.I.E qui influent, contribuent ou ont un rapport avec l'exécution d'une mission opérationnelle >>.

Au cours de toutes les guerres qui jalonnent l'histoire de l'humanité, les commandants en chef ont cherché à utiliser au mieux les informations dont ils pouvaient disposer. Dorénavant, compte tenu des flots toujours croissants d'informations disponibles, le problème n'est plus de collecter le renseignement , mais de traiter des masses de données pour en extraire la bonne information et s'assurer qu'elle parvienne bien à la bonne personne et au bon moment. Les avancées technologiques modernes engendrent ainsi des changements dans la manière dont les R.I.I appuient les opérations.

L'interconnexion des systèmes permet une large diffusion des informations . Cela comprend aussi bien la transmission d'informations brutes fournies par des capteurs placés à tous les échelons des forces que la dissémination d'analyses produites par des agences gouvernementales depuis le territoire national. Ces informations

pourront soit être transmises d'office (technologie "push"[17]), soit fournies à la demande (technologie "pull"[18]).

L'exploitation des quantités d'informations disponibles rend envisageable, à plus ou moins long terme, le concept de visualisation du champ de bataille en temps réel, le rêve de tout commandeur. Quel que soit leur échelon dans une opération, les leaders seront en mesure d'observer la situation tactique, opérative ou stratégique en quel qu'endroit que ce soit.

4.5. Les S.I.C (INFOSYS)

Les S.I.C collectent, traitent et répartissent les données relatives aux opérations en cours ou futures. Si l'automatisation a grandement facilité le traitement de l'information, l'homme reste le moyen le plus efficace pour apprécier la pertinence d'un renseignement. Les S.I.C permettent aux commandants et leurs états-majors de visualiser la situation courante, coordonner les opérations et les appuis navals et aériens, et diriger les différentes missions - au contact ou dans la profondeur - comme si elles n'étaient qu'une seule et même opération.

Les avantages que confèrent les S.I.C ne sont plus à présenter. Néanmoins, le concept de l'U.S.Army est celui d'une intégration à la fois verticale et horizontale afin d'offrir une souplesse tactique maximale à tous les acteurs de " l'espace de bataille ". Ainsi, on pourrait imaginer que deux chefs de section appartenant à des unités différentes mais se retrouvant proches l'un de l'autre sur le terrain puissent se communiquer directement des renseignements, sans l'intermédiaire de la chaîne hiérarchique, néanmoins automatiquement informée. Cette révolution dans les mentalités ne pourra se faire qu'à la condition d'une formation très stricte afin d'éviter les dérives rencontrées avec le système R.I.T.A lorsque les cadres découvrirent les possibilités de connexion au réseau téléphonique civil.

De plus, il est souhaité une connectivité globale de tous les S.I.C, civils et militaires, afin de permettre l'exploitation de l'ensemble des facettes des I.O, à tous les niveaux et sur la planète entière.

---

[17] L'information est poussée à tous les utilisateurs pour qui elle peut s'avérer utile.

[18] L'information est expédiée si elle fait partie d'un domaine d'intérêt sélectionné par le destinataire.

5. CONCLUSION

<< **la guerre de l'information : un concept " fourre-tout "** >> titrait l'IGA P. KLEINKNECHT dans son éditorial de " L'Armement ". on peut certes lui donner raison si l'on considère que de tout ce qui vient d'être évoqué, rien ne semble fondamentalement nouveau. Mais on peut déjà rapprocher le concept des I.O de celui du " zéro mort " en ceci qu'ils sont tous les deux politiquement corrects et font miroiter l'utopie d'une guerre propre dont les seules destructions seraient celles de matériels.

Si l'on considère maintenant l'Armée de terre des U.S.A, car c'est bien d'elle qu'il s'agit, comme essentiellement une armée de logisticiens[19], le regroupement de toutes les activités précédemment destinées à appuyer le combat terrestre, en une doctrine opérationnelle que le déploiement de la force armée et l'engagement viendront éventuellement soutenir, paraît tout à fait cohérente. Elle justifie de plus la conservation d'une armée d'un certain format à une époque où, disparition du Pacte de Varsovie et réduction de budget obligent, une U.S.Navy puissante dotée d'un corps expéditionnaire conséquent pourrait sembler suffisant.

Enfin, n'oublions pas que le budget de Défense est l'un des moteurs de la recherche aux U.S.A et représente un énorme potentiel de subventions qui n'en portent pas le nom. Les développements associés au concept des I.O contribueront à assurer aux U.S.A une avance technologique vitale pour leur garantir le leadership économique à l'aube du XXI^{eme} siècle.

Il reste que si l'on pousse un peu plus loin le concept, les mêmes technologies pourraient offrir les capacités de " fliquer " la planète, en commençant par son propre état. Si ce n'est pas l'objectif d'une mandature de 4 ans, cela pourrait être le fait d'institution - ou d'agences - dont les dirigeants sont plus stables dans leurs fonctions.

[19] Choix des premiers à la sortie de West Point