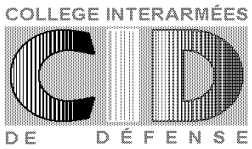
REPUBLIQUE FRANCAISE
MINISTERE DE LA DEFENSE



LA FRANCE PEUT-ELLE ADOPTER UNE STRATEGIE INFORMATIONNELLE OFFENSIVE ?

Mémoire de géopolitique

du capitaine de corvette Yann BIED-CHARRETON

dans le cadre du séminaire « Géopolitique et économie»

Directeur : Monsieur Christian Harbulot

12 Mars 2007

FICHE DOCUMENTAIRE

1. La France peut-elle adopter une stratégie informationnelle offensive ?
2. 2007_memoire_geop_stratinfoffensive_Bied_Charreton
3. Capitaine de corvette, marine, Bied-Charreton Yann , France
4. 12 mars 2007
5. Division A – groupe A3
6. Mémoire de géopolitique
7. Dans le domaine de la guerre de l'information une stratégie défensive est un pis aller, l'avantage est clairement à celui qui adopte une posture offensive. Dans ce champ de conflit, il est nécessaire d'être présent et de pouvoir se battre à armes comparables, sous peine de voir ses intérêts et son influence disparaître. Si elle a pris en compte progressivement la menace, la France, de par son histoire et ses traditions, demeure très réticente voire opposée à toute stratégie informationnelle offensive. On peut pourtant imaginer en France une stratégie globale d'information où l'offensive prendrait toute sa part, au même titre que la défensive.
8. Intelligence économique, Guerre de l'information, stratégie.

La France peut-elle adopter une stratégie informationnelle offensive ?

SOMMAIRE

INTRODUCTION

En 2005, la saga du Clémenceau occuppe le terrain médiatique et devient rapidement ce qu'il convient d'appeler une affaire d'Etat. Il s'agit pourtant à l'origine du simple démantèlement d'une unité militaire. Cette opération avait été préparée en amont et beaucoup d'experts, et même d'associations écologiques, la considéraient comme un cas d'école. L'organisation écologique Greenpeace, animée d'un esprit de revanche envers l'Etat français, décide pourtant de perturber les plans établis en menant une campagne d'information particulièrement efficace. L'Etat français sera en final obligé de renoncer à ses projets. Greenpeace apparaitra comme le grand vainqueur de cettte confrontation pourtant apparamment très déséquilibrée. Cette attaque par l'information contre des intérêts français est loin d'être un cas unique ; on peut ainsi citer la campagne de désinformation orchestrée contre les militaires français de l'opération « Turquoise » au Rwanda. Dans un même ordre d'idée, les entreprises françaises se trouvent confrontées à une concurrence mondiale redoutable où tous les coups sont permis.

La guerre de l'information est aujourd'hui une réalité et les intérêts français se trouvent menacés comme ceux des plus grands pays. La France est-elle prête à mener une stratégie informationnelle offensive ? En d'autres termes, est-elle condamnée à subir des attaques informationnelles, prendre coup après coup et à conduire une riposte désorganisée et tardive ? Ou est-elle au contraire en mesure, en se montrant offensive, de préserver son initiative et de s'autoriser à attaquer et riposter là où l'adversaire à décidé de mener son attaque, sur le même terrain et avec des armes comparables?

Dans le domaine de la guerre de l'information une stratégie défensive est un pis aller, l'avantage est clairement à celui qui adopte une posture offensive. Dans ce champ de conflit, il est nécessaire d'être présent et de pouvoir se battre à armes comparables, sous peine de voir ses intérêts et son influence disparaitre. Si elle a pris en compte progressivement la menace, la France, de par son histoire et ses traditions, demeure très réticente voire opposée à toute stratégie informationnelle offensive. On peut pourtant imaginer en France une stratégie globale d'information où l'offensive prendrait toute sa part, au même titre que la défensive.

Après avoir montré que la guerre de l'information était avant tout une guerre offensive, nous étudierons les nombreux freins qui existent en France, et qui sont de nature à inhiber toute tentative d'adoption d'une stratégie informationnelle offensive. Une telle stratégie reste néanmoins possible, et les pistes de réflexions sur une possible stratégie globale d'information pour la France seront examinées dans une troisième temps.

PREMIÈRE PARTIE

LA GUERRE DE L'INFORMATION : UNE GUERRE OFFENSIVE

Dans le domaine de la guerre de l'information une stratégie défensive ne peut être suffisante. L'avantage est clairement à celui qui adopte une posture offensive. Dans ce champ de conflit qu'est la guerre de l'information, il faut y être présent et se donner les moyens de se battre à armes comparables.

1. LA GUERRE DE L'INFORMATION

1.1. Réalité de la guerre de l'information

Si l'on s'accorde aujourd'hui à identifier les Etats-Unis comme l'unique super puissance mondiale, de nombreux pays se placent néanmoins dans des domaines réduits au même niveau que la puissance américaine. Si l'on examine un à un les facteurs traditionnels de puissance, la Russie peut apparaitre ainsi comme une grande puissance militaire ou économique en regard de l'étendue de ses ressources. Dans un même ordre d'idée, la puissance économique de l'Union Européenne est équivalente à celle des Etats-Unis. Les facteurs de puissances sont multiples, ils possèdent cependant tous une ressource stratégique commune : l'information.

L'information est aujourd'hui source de pouvoir et source de puissance. Ce phénomène n'est pas vraiment nouveau. Pendant l'entre-deux-guerres le Japon avait acquis toute sa puissance militaire en espionnant les puissances militaires alliées. Dès la fin de la seconde guerre mondiale, les Américains et les Russes sont entrés dans une véritable guerre froide culturelle. Le livre *Qui mène la Danse* de Frances Stonor Saunders décrit les mécanismes par lesquels la CIA s'est livrée à des opérations d'influence en Europe pour contrecarrer la propagande communiste. Cette guerre culturelle reposait là aussi déjà sur l'information. La stratégie américaine était fondée sur la création et la mise en place de cercles culturels dont l'unique objectif était de promouvoir les intérêts supérieurs des Etats-Unis en Europe.

L'information est donc depuis bien longtemps au cœur des affrontements entre les puissances. La supériorité informationnelle est d'ailleurs souvent un des facteurs clés des stratégies indirectes car elle doit permettre de remporter des victoires sans entrainer la plupart du temps d'implication directe.

Il serait naïf de croire que l'information est aujourd'hui devenue gratuite et accessible à tous. L'information est en effet impalpable et fragile. Elle peut être utilisée, amplifiée, minimisée ou manipulée. Elle est pourtant bien un instrument de puissance et se trouve au cœur des conflits. Toute volonté de puissance doit donc s'accompagner de l'adoption d'une stratégie informationnelle. Cette stratégie est au bénéfice de la nation qui la met en oeuvre. Elle permet de renforcer son pouvoir d'influence, l'information venant appuyer une politique diplomatique, militaire, culturelle ou économique. Dans ce dernier domaine, celui de l'économie, la guerre de l'information est la clef du concept d'intelligence économique.

Aujourd'hui, la guerre de l'information est en effet souvent mise en rapport avec l'intelligence économique. Cette dernière fait largement appel aux techniques informationnelles. Monsieur Alain Juillet, Haut Responsable Chargé de l'intelligence économique en France, définit l'intelligence économique comme étant « la maitrise et la protection de l'information stratégique utile pour tous les décideurs »[1]. L'économie, en tant qu'atout fondamental de la puissance, est actuellement un des terrains de jeu le plus favorable à la guerre de l'information. C'est pourquoi dans ce mémoire la partie économique sera la plus développée. Mais la guerre de l'information est livrée dans bien d'autres domaines et en particulier dans des domaines militaires, culturels ou diplomatiques. Celui qui maîtrise l'information aura un avantage décisif sur son adversaire. L'information c'est le pouvoir. Elle permet en particulier de bouleverser les rapports de forces existants. Les Etats se doivent donc de renforcer leur politique dans un domaine aussi stratégique qu'est celui de l'information. Ils ne peuvent pas se permettre d'abandonner ce nouveau champ de conflit.

Nous sommes rentrés de plein pied dans l'ère de l'information. Cette information est partout et surabondante. Elle façonne les perceptions, et donc les opinions publiques et individuelles. L'information influe sur les comportements et sur les décisions prises.

---

[1] Discours de Monsieur Alain Juillet, colloque « intelligence économique et pôle de compétitivité », Avignon, le 11 mai 2006.

L'information est une ressource maîtresse dans tous les domaines, sa maîtrise est donc indispensable et sa possession l'objet de rudes combats. Les Etats ou organisations dans le monde sont ainsi placés dans une logique de guerre, une guerre pour et par l'information.

1.2. Les facteurs facilitant le développement de ce champs de conflit

Plusieurs facteurs sont à l'origine du développement de la guerre de l'information aujourd'hui.

Le premier est la prédominance écrasante des puissances qui rend difficile aujourd'hui pour le faible d'exister. Il existe une dissymétrie évidente entre les différents Etats en termes militaires, financiers, économique ou d'influence culturelles. Les pays les plus puissants ont organisé le monde ancien tel que nous le connaissons encore. Les institutions internationales créées à la fin de la seconde guerre mondiale sont en particulier l'héritage d'un monde occidental. Il y a là indiscutablement un terrain très favorable à la contestation, où le faible cherche à se faire une place et à remettre en cause un ordre établi. La contestation se fait grandissante de la part des acteurs étatiques ou non étatiques. Le monde économique est à ce titre assez révélateur ; comme le soulignait récemment Monsieur Alain Juillet : « nous entrons dans un monde concurrentiel comme nous l'avons jamais connu. »[2] Depuis plusieurs centaines d'années quinze à vingt pays monopolisaient le marché mondial en ayant mis en place un système certes concurrentiel, mais finalement relativement consensuel répondant à des références et des normes de commerce convenues. Ces pays se partageaient les fruits de la croissance. Ce système est aujourd'hui remis en cause par de très nombreux pays entrés en lutte pour obtenir des parts de marchés et donc de la croissance. Toutes les barrières mises en place, y compris l'Organisation Mondiale du Commerce, sont ou sont en passe d'être remises en cause. La compétition économique s'est considérablement intensifiée, et nous sommes passés selon l'expression de Monsieur Alain Juillet, d'un « combat au fleuret moucheté à un combat au sabre »[3]. Or les acteurs étatiques ou non étatiques doivent, s'il veulent exister, trouver un terrain favorable dans lequel ils peuvent lutter dans un rapport du faible au fort.

---

[23] Monsieur Alain Juillet, intervention à l'Ecole militaire, le 21 février 2007.

Depuis maintenant un peu plus de vingt ans on assiste parallèlement à une véritable révolution des moyens de communication. Les médias sont ainsi aujourd'hui très présents et peuvent toucher l'ensemble de la planète instantanément. Ils peuvent exerçer une influence importante sur les spectateurs selon la façon dont ils choisissent de traiter toute information. Or bien des médias, poussés par des impératifs commerciaux, donnent souvent la place au sensationnel au détriment de la recherche de la vérité. Internet s'est également considérablement développé, et donne dans la majeure partie des pays du monde un libre accès à une masse infinie d'informations. Ces moyens de communication modernes et ce pouvoir des médias s'exercent en particulier dans les pays ou la liberté de la presse, la liberté d'opinion ou encore celle de circulation sont érigés en dogme. Il devient alors d'autant plus facile d'exploiter ces « faiblesses » des démocraties libérales.

Il existe aujourd'hui une contestation grandissante de la part d'acteurs étatiques ou non étatiques vis-à-vis des puissances dominantes. Les prodigieux outils de communications dont ils disposent sont des armes idéales. Ils peuvent ainsi se placer dans un champ d'action qui leur est beaucoup moins défavorable que les champs de conflits traditionnels.

2. LA MAITRISE DE L'INFORMATION

La guerre de l'information doit reposer sur une véritable stratégie informationnelle. L'information est au cœur de tous les conflits ; c'est elle qui permettra de les gagner ou de les empêcher. Cette information devient un atout stratégique dans les mains de la puissance apte en acquérir la maîtrise. Cela est vrai quelque soit la nature des conflits, qu'ils soient militaires, économiques, culturels, religieux…

Maîtriser l'information consiste à disposer en temps opportun de la bonne information et d'en priver l'adversaire afin de maintenir l'initiative et d'obtenir une supériorité décisionnelle. Cette maîtrise de l'information comprend cinq volets distincts qui sont à mettre en parallèle avec le cycle classique du renseignement :

- La prospective
- L'acquisition de l'information.
- Le traitement de l'information.
- La distribution et l'exploitation de l'information.
- La protection de l'information.

2.1. La prospective

Le travail de prospective doit permettre d'imaginer ce que l'on doit aller chercher comme information à partir de projections sur le futur. Ce travail d'anticipation en amont est indispensable compte tenu des difficultés et de la lourdeur des étapes d'acquisition ou de traitement de l'information qui en découleront.

2.2. L'acquisition de l'information

Cette démarche clairement volontariste consiste à se placer dans les meilleures conditions pour acquérir de l'information, c'est-à-dire du savoir et de la connaissance. Les procédés sont multiples qu'ils soient légaux ou illégaux. D'un coté de l'éventail se trouve le recueil classique d'information à partir de sources ouvertes[4], de l'autre les procédés qui relèvent de la guerre hors limite à laquelle se livrent les services de renseignements. Cette recherche de renseignements est en constante évolution. Le marché des logiciels, dont les moteurs de recherche, et des cabinets spécialisés dans ce domaine en témoignent. Toutes les informations peuvent présenter un intérêt, et on peut estimer que dans quelques années la barrière des langues sera levée avec la mise se le marché de logiciels de traduction automatique aboutis. L'acquisition de l'information ne se limite pas, loin s'en faut, à la recherche de données. La promotion active de la recherche et de la production de la connaissance en est également une composante majeure. Dans le domaine économique, et dans la lutte contre la concurrence mondiale, la meilleure défense reste sans nul doute le développement de sa propre recherche et de son innovation.

2.3. Le traitement de l'information

La quantité d'information disponible par les sources ouvertes s'est accrue de manière explosive durant les deux dernières décennies. Toute personne sachant manipuler un ordinateur est capable d'accéder par le web à des dizaines de milliards de données, et ce nombre est en constante augmentation. Le traitement et l'analyse de cette information est un véritable défi. Cela repose en grande partie sur des outils informatiques fiables et

---

[4] Selon Monsieur Alain Juillet « 95% des informations seraient disponibles sur les sites internet visibles ou invisibles », intervention à l'Ecole militaire, le 21 février 2007.

protégés. Ils doivent inclure des dispositifs d'alerte et des algorithmes poussés permettant d'extraire les données et de faire ressortir de l'information pertinente. Il convient également de fiabiliser et recouper toute cette information. Selon Monsieur Alain Juillet, 20% de l'information économique qui circule aujourd'hui serait fausse. Quant au reste, elle n'est bien souvent que partiellement vraie. Les systèmes informatiques ne sont donc pas suffisants et la place des analystes est ici prépondérante.

2.4. La distribution et l'exploitation de l'information

Cet aspect consiste à chercher la délivrance de la bonne information au bon moment et au bon destinataire. C'est à ce stade que sont également mises en œuvre les techniques de désinformation, de subversion et d'influence. Le champ de bataille médiatique est exploité au maximum. C'est aussi probablement à ce niveau qu'il y aura le plus grand écart entre l'adoption de procédés uniquement défensifs ou la volonté de mener une stratégie offensive. Les méthodes pourraient être là tant légales qu'illégales.

L'exploitation de l'information doit conduire, après un travail d'analyse et de synthèse, à dégager les options stratégiques et de manœuvre possible pour le décideur. La présentation de l'information aux décideurs est une ultime étape qu'il ne faut surtout pas négliger.

2.5. La protection de l'information

L'information ne serait pas maîtrisée si elle ne pouvait être correctement protégée. La protection de l'information stratégique utile est bien un défi d'une brûlante actualité. Pour de multiples raisons, des personnes tentent de s'infiltrer dans les banques de données ou les ordinateurs afin d'en connaître l'activité, ou pire pour y introduire des fausses données. Les données comme les systèmes doivent donc être protégées par de couteux systèmes de sécurité de l'information. La protection des systèmes est particulièrement importante quand on sait que les logiciels couramment utilisés sont loin d'être indépendants. Un moteur de recherche comme « Google » permet à ses concepteurs et à une communauté « d'ayants droit » de connaître l'historique et la nature des demandes des utilisateurs. De même les « firewalls » du commerce ne sont pas étanches à toutes les attaques. Le savoir et le fruit de la recherche doivent également être protégés. Le dépôt de brevets doit permettre d'éviter les risques de pillage.

3. PRIMAUTE DE L'OFFENSIF SUR LE DEFENSIF

En matière de guerre de l'information plusieurs stratégies peuvent se concevoir. Un groupe ou un état peut se contenter de mettre en place une stratégie défensive. Elle reposera alors essentiellement sur la protection de ses informations, mais n'empêche pas la mise en place de veilles stratégiques et l'anticipation des attaques dont il pourrait faire l'objet. D'autres doubleront cette stratégie purement défensive d'une stratégie offensive. L'information est alors exploitée dans un but d'influence et de domination.

Le conflit est en effet aujourd'hui beaucoup plus facile à mener. La guerre de l'information se déroule sur des champs de bataille où les rapports de forces sont bouleversés. Il ne s'agit pas ici de l'affrontement entre armées, puissances financières ou multinationales. Tout à chacun peut attaquer n'importe qui sur n'importe quel sujet avec peu de moyens et peu de risques. Les technologies de l'information sont exploitables par tous, et peuvent permettre de relayer et d'amplifier de l'information comme de la désinformation dans un but d'influence. Les rapports de force classiques s'en trouvent totalement bouleversés.

Les exemples de telles attaques sont très nombreux. On peut citer des groupes de pressions comme Greenpeace, Sortir du Nucléaire ou des groupes politiques comme le Hezbollah qui sont devenus experts en manipulation de l'information. Les Etats ou multinationales visées se trouvent alors contraints de réagir en position défensive et obligés de contre-attaquer alors que le mal est déjà fait. Dans *Guerre économique et information – les stratégies de subversion* les auteurs Didier Lucas et Alain Tiffreau analysent en profondeur ces tactiques subversives. L'exemple développé de la stratégie de Greenpeace face à la société Shell United Kingdom est particulièrement révélateur des mécanismes mis en œuvre.

Le 16 février 1995, le gouvernement britannique accorde l'autorisation à la société Shell UK de couler au large de l'Ecosse une plateforme pétrolière inexploitable, la Brent Spar. Des scientifiques de renom se sont montrés favorables au projet et ont notamment démontré que cette action ne pouvait en rien nuire à l'environnement. Pourtant Greenpeace va lancer une véritable offensive médiatique contre cette opération. Ils contesteront notamment la quantité de produits pétroliers restant à bord, et procèderont au dénigrement systématique des scientifiques appuyant la décision de Shell. Greenpeace appellera

également au boycott de la société, qui s'avèrera particulièrement efficace en Allemagne. Shell renoncera officiellement à son projet le 20 juin 1995, et déboursera en final 35 millions d'euros pour la déconstruction de la plateforme. Le 18 octobre de la même année, un rapport de spécialiste arrive définitivement à la conclusion que cette opération était pourtant sans danger pour l'environnement. Greenpeace reconnaitra a posteriori son erreur d'appréciation, mais ce mea culpa tardif est oublié depuis longtemps. Cette action est caractéristique de ce que peut être une attaque par l'information. Greenpeace aura adopté dès le début une attitude offensive en choisissant la manipulation médiatique.

S'étant laissé surprendre dès le début, la société Shell UK s'est cantonnée dans une posture défensive en s'appuyant sur une démonstration objective et scientifique justifiant son bon droit. La défaite médiatique du groupe Shell provient bien à l'origine d'une sous-estimation de la menace Greenpeace : « Shell a cherché à mener le combat sur l'échiquier qui lui semblait naturellement favorable. Or en demeurant dans un rapport du fort au faible sans en détenir l'initiative, la firme anglaise s'est condamnée à développer une stratégie défensive. L'erreur de Shell fut de croire en sa supériorité et ainsi de mésestimer la pertinence de l'assaut de Greenpeace.»[5]

Cet exemple donne à réfléchir, en particulier lorsque dix ans plus tard Greenpeace appliquera des mécanismes quasi-identiques pour faire plier le gouvernement français dans ce qu'il convient d'appeler l'affaire « Q790 - Clémenceau ». Le droit et la légitimité ne pèsent donc pas lourd face à des stratégies subversives bien rodées, en particulier lorsque les techniques utilisées sont précisément illégales. Si l'espionnage économique ou industriel, strictement illégal, fait l'objet d'une forte répression dans la majeure partie des pays, il est indéniable qu'il est toujours une réalité. Les affaires récentes concernant des stagiaires chinois opérant en France sont loin de constituer un épiphénomène.

Le succès de la Marine française contre Greenpeace en 1995 dans le Pacifique, montre que l'on peut parfois remporter des succès tactiques en se plaçant dans une logique plutôt défensive. Le droit peut également permettre de contrer des attaques informationnelles. Ces succès ne seront toujours que des exceptions.

Faces aux stratégies subversives, où le faible attaque le fort sur le seul terrain où il puisse avoir l'avantage, le combat doit prendre le pas sur la « gesticulation ». Etre offensif

---

[5] LUCAS Didier et TIFFREAU Alain , *Guerre économique et information – les stratégies de subversion ;* Ellipses, 2001, p. 70.

c’est préserver son initiative et s’autoriser à attaquer et riposter là où l’adversaire à décidé de prononcer son attaque.

Les grandes puissances du monde occidental souffrent aujourd’hui du syndrome de Goliath. Fort de leurs suprématies technologiques, culturelles ou financières, elles ont tendance à s’enfermer dans leur mode de pensée et à ignorer les menaces provenant des plus faibles. Dans un rapport du faible au fort ces derniers ont pourtant plus d’un atout. Se plaçant dans une logique d’accroissement de puissance, ils exploitent les faiblesses des pays qui ne cherchent qu’à préserver leur statut de puissance. Ces David ont tous adopté des stratégies informationnelles résolument offensives. La France tient à préserver sont statut de puissance, et à travers cela maintenir à un haut niveau les conditions de vie de ses citoyens. Elle doit donc se donner les moyens de pouvoir lutter à armes égales contre ses concurrents, et ainsi envisager d’adopter une stratégie informationnelle offensive.

DEUXIEME PARTIE

LES FREINS A LA GUERRE DE L'INFORMATION EN FRANCE

La fin de la guerre froide s'est suivie d'une courte période d'euphorie, laissant croire à l'entrée dans un monde sans menace. En France, seule une poignée d'experts ont immédiatement perçu l'avènement d'un monde instable et plus dangereux. Ce sont les acteurs économiques qui ont amorcé une prise de conscience de la réalité de la guerre de l'information. Ainsi, la France a pris progressivement en compte la menace qui pesait sur son économie et donc sur son statut de puissance. Les deux principaux temps forts furent le rapport Martre en 1994 puis le rapport Carayon en 2003. Cette démarche lente, si l'on tient compte des stratégies mises en place depuis fort longtemps dans beaucoup de pays concurrents, est particulièrement révélatrice des freins qui ont existé et qui existent d'ailleurs pour la plupart toujours en France. Si aujourd'hui l'intelligence économique est un concept largement répandu, les structures et les mécanismes nécessaires à l'adoption d'une véritable stratégie informationnelle offensive tardent à se mettre en place.

1. LA PRISE EN COMPTE PROGRESSIVE DE LA MENACE

La France a fait le choix d'une société libérale même si l'Etat reste très présent dans l'économie du pays. Les grandes entreprises françaises se sont dotées des intruments nécessaires pour répondre aux défis de la maîtrise de l'information posé par leurs concurrents multinationaux. C'est en particulier le cas pour des entrepises comme Michelin ou Total qui ont pris conscience depuis longtemps des menaces et qui ont mis en place des réseaux performants d'intelligence économique. Le défi est tout autre pour les petites et moyennes entreprises françaises qui sont loin de disposer des même moyens.

Le rapport Martre de 1994 insistait déjà sur le fait que l'intelligence économique nécessitait l'interaction de tous les acteurs économiques et qu'elle devait être le fruit d'une intention stratégique.

Le rapport Carayon intitulé *Intelligence économique, compétitivité et cohésion sociale*, mettait en avant la nécessité d'une mobilisation mêlant intérêts public et privé. Outre la promotion du « patriotisme économique », ce rapport préconise la mise en place d'une véritable stratégie publique en matière d'intelligence économique. Il met en valeur le rôle prédominant de l'Etat, alors que paradoxalement la mondialisation semblait l'avoir fait disparaître en tant qu'acteur dans l'économie du monde. Monsieur Bernard Carayon montre dans son rapport la réalité des affrontements que se livrent les états et les entreprises sur le terrain économique. L'économie mondiale est selon lui aujourd'hui le principal théâtre sur lequel s'affrontent les pays cherchant à préserver ou à accroitre leur statut de puissance. Ce discours, assez nouveau en France, avait en 2003 le mérite de faire prendre conscience de cette réalité aux pouvoirs publics français peu enclins à entendre ce type d'arguments. Cette réticence repose sur plusieurs éléments caractéristiques de l'état d'esprit de nos élites françaises. Cela est en partie dû à la difficulté de conceptualiser la menace. Pour convaincre les politiques d'agir, il faut au préalable bien comprendre la menace et comprendre comment la guerre d'information se mène.

Le rapport Carayon décrit les objectifs d'une politique d'intelligence économique à mener par l'Etat. Il doit, dans un premier temps, identifier clairement les intérêts qu'il a à promouvoir et à défendre. Cela passe par la définition des secteurs d'activités stratégiques et d'une étude des menaces à prendre en compte. Une réflexion prospective est nécessaire et une veille stratégique dans chacun de ses secteurs doit être mise en place. Il convient par la suite de mettre en place les conditions favorables au développement de l'intelligence économique en France. Les principaux axes d'efforts identifiés étaient en particulier les suivants :

- établir une synergie entre les différentes administrations concernées par les domaines de l'intelligence économique ;
- mettre en place les conditions d'une action coordonnée des initiatives du secteur public et du secteur privé ;
- optimiser le recueil, le traitement et la diffusion de l'information, en prenant en compte les sources ouvertes mais aussi celles plus officieuses collectées par les organismes de renseignement français.

Monsieur Bernard Carayon constate également que cette démarche doit s'accompagner d'un changement des mentalités. Il faut selon lui procéder à « l'enterrement » d'une

certaine naïveté française, qui voit la guerre économique comme un mythe. Les acteurs économiques doivent se donner les moyens de se battre à armes égales en utilisant tous les moyens à leur disposition pour acquérir un avantage compétitif décisif. Les pouvoirs-publics doivent également former les élites administratives en matière d'intelligence économique. Ces derniers perçoivent encore mal la réalité d'un monde « globalisé ». Monsieur Bernard Carayon parle ainsi d'un « État-aveugle ». A cet égard, il est frappant de constater que certaines grandes administrations de l'État font encore régulièrement appel à des cabinets d'audit ou à des banques d'affaires anglo-saxons ou américains.

De nombreux pays ont pris de l'avance sur la France en matière d'intelligence économique. La France doit, comme le préconise Monsieur Alain Juillet, éviter « le double écueil de la naïveté et la paranoïa ». En tant que haut responsable pour l'intelligence économique il se fixe comme objectif de « les rattraper en mobilisant nos capacités pour apprendre à maîtriser les outils, les procédures et ces méthodes d'avant garde »[6]. La mise en place d'une stratégie informationnelle est dans ce domaine déterminant.

2. LES FREINS AU DEVELOPPEMENT D'UNE STRATEGIE OFFENSIVE

Si elle a progressivement pris en compte la menace, la France, de par son histoire et ses traditions, demeure très réticente voire opposée à l'adoption de stratégies offensives. Cette réticence est liée aux nombreux freins qui subsistent encore aujourd'hui en France.

2.1. Freins historiques

La France a su développer au cours du vingtième siècle une véritable compétence en matière d'opérations d'influence. Les militaires français ont en particulier utilisé à de nombreuses reprises des techniques offensives pendant les guerres coloniales. La France a par ailleurs subi pendant la seconde guerre mondiale les actions de propagande allemandes, puis après la guerre des actions d'influence exercées par les deux grandes puissances de la guerre froide. Ainsi, les années 1960 marquent un tournant dans la perception qu'ont les politiques et la société française des opérations d'influence. Le traumatisme de la guerre

[6] Discours de Monsieur Alain Juillet, colloque « intelligence économique et pôle de compétitivité », Avignon, le 11 mai 2006.

d'Algérie, engendré en particulier par les actions psychologiques menées par le contingent français, a inhibé pour très longtemps dans l'idée des politiques toute éventualité de recours à des opérations d'influence militaires ou non. L'image très négative des effets de la propagande au vingtième siècle a également créé un rejet complet de tout processus visant à exercer de l'influence sur les populations.

2.2. Freins déontologiques

La France met toujours en avant ses idéaux démocratiques. Elle ne peut donc n'avoir qu'une vision négative de l'influence ou de la subversion. Les Français préfèrent au contraire user de la raison pour convaincre. Il y a d'autre part un grand risque pour un Etat à vouloir être présent sur le terrain de la guerre de l'information. Les acteurs non étatiques peuvent facilement s'autoriser à utiliser des techniques de manipulation de l'information voire de complète désinformation. Le Hamas ou Greenpeace a dans ce domaine beaucoup moins à perdre que l'Etat français. Un Etat démocratique peut difficilement prendre le risque d'être décrédibilisé si une action d'influence ou de subversion est mise à jour. Certains pays comme les Etats-Unis ou Israël mènent pourtant ce type d'opérations d'influence et de subversion qui sont très difficilement imaginables en France compte tenu de l'existence de nombreux freins culturels.

2.3. Freins culturels

Le tout premier des freins culturels qu'il convient de mentionner est l'absence de sérieux qu'il y en France à la protection du secret. Les journalistes spécialisés trouvent toujours assez aisément des personnes bien informées pour mettre en jour des opérations d'intérêt national. Il existe aux Etats-Unis un système beaucoup plus répressif. Les agissement contre l'intérêt national sont poursuivis et régulièrement condamnés. En France la déposition d'un ministre de la Défense devant la justice ou une note des renseignements généraux peuvent se retrouver en première page des journaux sans qu'il y ait de réelles sanctions. Des fuites sur des opérations d'informations nationales ont une nouvelle fois été mises en ligne sur un site internet[7], cela témoigne d'un manque directe de culture du secret.

---

[7] Article « Contre-influence au service de MBDA », consulté sur le site intelligenceonline.fr le 1er mars 2007.

Les services français de renseignement évoluent de façon assez lente. La culture spécifique des services secrets les rend peu adaptés à mener la lutte sur un nouveau front et avec de nouvelles techniques informationnelles. L'exploitation de l'Open source et l'analyse des attaques informationnelles est quelque chose de nouveau. Ce frein est néanmoins en passe de s'estomper aujourd'hui. Par contre ils restent toujours très cloisonnés, limités chacun dans leur champ d'action ou leur ministère d'appartenance. Les passerelles entre le monde du renseignement et le monde ouvert sont également assez rares. Cela est beaucoup moins vrai aux Etats-Unis où il n'est pas rare de voir des hauts responsables de services de renseignements partir dans le privé. De plus, encore aujourd'hui, de nombreuses élites sorties des grandes écoles américaines choisissent de faire carrière dans ces services. Il existe enfin en France une réticence envers ce monde de l'influence et du renseignement. Il est ainsi assez symptomatique que l'on n'ait pas souhaité employer le terme de renseignement économique alors qu'il s'agissait d'une traduction logique du terme anglais « Intelligence ». Le terme plus politiquement correct et acceptable d'intelligence économique lui a été finalement préféré.

A l'inverse de pays comme les Etats-Unis et la Grande-Bretagne, il y a en France peu de connivence entre les acteurs de la sphère publique et privée. Les élites proviennent de formations distinctes et les transferts entre les deux mondes sont rares et souvent considérés à tort comme suspects. En caricaturant un peu, on retrouve d'un côté les grands commis de l'Etat et de l'autre les acteurs du monde privé. Ces derniers sont dans une logique libérale et souvent peu sensibilisés aux intérêts nationaux. Les premiers ignorent parfois les réalités du monde des entreprises privées.

D'autre part, comme nous l'avons évoqué précédemment, l'information c'est le pouvoir. Il est alors souvent tentant dans le monde de l'entreprise mais aussi au sein des ministères de préserver l'information à son niveau afin de garder ses prérogatives et son influence. La difficulté du partage de l'information ne se limite pas à des contraintes techniques ou aux problèmes liés à la sécurité des systèmes d'informations. La réelle difficulté est plutôt de l'ordre des mentalités. Lorsqu'il y a entente entre les chefs, les problèmes techniques se résolvent bien souvent alors « comme par enchantement ».

Le fonctionnement de l'interministériel est également largement perfectible en France car il n'échappe pas à cette tendance au cloisonnement des administrations. Cela rend difficile le travail de coordination au niveau du Secrétariat Général pour la Défense Nationale. Là encore il s'agit souvent d'une question de mentalités qui doivent encore progressivement évoluer.

Il existe en résumé, de nombreux frein culturels que l'on peut récapituler comme étant l'absence de sérieux sur le protection du secret, l'absence de connivence entre les acteurs du public et du privé, une réticence au partage de l'information source de pouvoir, un évolution trop lente des services de renseignement et un fonctionnement perfectible de l'interministériel.

2.4. Freins juridiques

Les freins juridiques sont justifiés mais aussi conséquents dans toute démocratie, qui par nature sépare les pouvoirs exécutifs et judiciaires. La lutte contre les attaques informationnelles nécessite pourtant des outils et des techniques qui sont à la limite de la légalité. En France, peut-être plus que dans d'autres pays démocratiques, les exigences de la justice prennent le pas sur l'intérêt national. Le Premier Ministre britannique Tony Blair est intervenu récemment pour enterrer tout risque de poursuite contre l'entreprise BAE Systems malgré des suspicions de corruption sur un marché avec l'Arabie Saoudite. Ce type d'intervention est très difficilement imaginable en France. Dans un même ordre d'idée, la Commission Nationale Informatique et Libertés (CNIL) surveille de façon très attentive tous les systèmes d'informations. Cela présente le grand mérite de garantir la vie privée des individus, mais ne facilite par le travail des services de police, de renseignement ou d'intelligence économique publics et privés. Un juste compromis doit exister dans ce domaine si l'on veut pouvoir lutter efficacement contre des acteurs qui utilisent précisément ces faiblesses inhérentes aux systèmes démocratiques.

Tous ces nombreux freins se retrouvent directement dans la façon dont la France tente de mettre en œuvre une stratégie informationnelle crédible.

TROISIEME PARTIE

PISTES DE REFLEXION POUR UNE STRATEGIE INFORMATIONNELLE OFFENSIVE

Après avoir mis en évidence la primauté de l'offensif en guerre de l'information et montré les freins qui existent en France à sa mise en place, cette troisième partie donne des pistes de réflexion sur la possibilité d'adopter en France une stratégie informationnelle offensive. Pour ce faire nous étudierons dans un premier temps le modèle américain, qui montre comment une démocratie libérale s'est donnée les moyens d'adopter une telle stratégie dans le domaine économique. Puis nous verrons l'exemple militaire avec notamment les opérations d'informations mises en place tant d'un point de vue stratégique que tactique par les nations de l'OTAN. Fort de ses exemples et des limitations françaises, nous verrons que la France peut adopter une stratégie globale d'information faisant place à l'offensive.

1. L'EXEMPLE ECONOMIQUE AMERICAIN

Quand on demande au député Bernard Carayon quel est le pays le plus à craindre en matière d'intelligence économique, il répond : « Sans nul doute les Etats-Unis. Contrairement à ce qu'on pourrait croire, et alors qu'il est présenté comme un modèle d'économie libérale, c'est le pays le plus interventionniste lorsqu'il s'agit de protéger les intérêts de ses entreprises et quand il faut les accompagner sur les marchés mondiaux. »[8]

Le concept d'intelligence économique a été introduit par l'économiste américain Michaël Porter il y a environ trente ans. Il a été en particulier un des premiers à développer l'idée que l'information tenait une place centrale dans la compétition économique. Dès les années 1990, les Américains en ont tiré la conclusion qu'ils devaient désormais réorganiser leurs services de renseignement au service de leurs intérêts économiques. Cela a été fait en

[8] Interview paru dans le *journal du management* du 30 novembre 2005.

particulier par la CIA sous l'impulsion de son directeur de l'époque, Monsieur Robert Gates. Le concept d'intelligence économique a bénéficié de l'explosion des nouvelles technologies de traitement de l'information mais aussi d'une impulsion politique forte ; le président Bill Clinton ayant déclaré qu'une des priorités de son second mandat était de faire des entreprises américaines des leaders mondiaux.

Les Etats-Unis ont ainsi depuis la fin de la guerre froide mis leurs services de renseignement au profit de leurs entreprises. On peut souligner le rôle particulièrement actif de la CIA en matière de collecte d'informations dans le domaine économique. A titre d'exemple, en 1994, les services d'écoutes américains permettaient à Boeing de remporter un marché contre Airbus en Arabie Saoudite, de même Raytheon remporta un marché au Brésil au dépend de Thomson CSF. Les Américains ayant décelé à chaque fois des indices de possible corruption, ces éléments communiqués aux entreprises américaines avaient permis d'anéantir définitivement les chances des entreprises françaises pour ces marchés.

Il n'y pas ici de problème d'éthique particulier. Les services de renseignements agissent classiquement dans la recherche d'informations. Les mesures de protection mises en place après le 11 septembre, ont d'ailleurs permis aux autorités américaines de pouvoir surveiller de façon encore plus précise les mouvements liés à des activités commerciales. Pour Monsieur Ali Laïdi, « le dispositif américain, qui allie force militaire et puissance économique, est bien rodé. L'information circule rapidement et avec un minimum de déperdition de l'administartion aux entreprises privées et vice versa »[9].

Aux Etats-Unis une structure interministérielle assure la combinaison de l'ensemble des moyens gouvernementaux d'information et de renseignement, d'influence et d'activisme. Cette responsabilité est assurée par le « Trade Promotion Coordination Commitee » sous la houlette de l' « Advocacy Center ». Ce comité fixe, suit et évalue les politiques de développement des exportations et implantations américaines dans le monde. L' « Advocacy center » étudie le dossier de chaque entreprise américaine et estime s'il est d'intérêt national. Dans l'affirmative, tous les services de l'Etat américain se mobilisent pour les entreprises sélectionnées, avec comme objectif de leur faire gagner leur contrat. Les Etats-Unis se placent ainsi dans une véritable logique de guerre.

---

[9] LAIDI Ali, *Quelques exemples d'affrontements France-Etats-Unis*, Politique internationales Nr 102, 8 décembre 2004

Une large panoplie de moyens est mise en œuvre par les différents acteurs agissant en réseau. Sont ainsi conjugués les moyens financiers (crédits, garantie et dons), l'assistance militaire, technique ou sanitaire, et l'aide alimentaire ; le tout autour de programmes et projets proposés par chacun des différents acteurs et sélectionnés de façon concertée en raison de leurs aspects stratégiques. Il n'y a à ce sujet aucun critère financier minimum retenu, tous les projets susceptibles d'avoir des implications à long terme sont soutenus. Les dossiers sont tous pris en charge et suivis par une cellule de veille. Si le TPCC dépend du ministère du Commerce, son action économique est bien un des volets de la politique étrangère américaine. Il y a bien un souci de cohérence en amont géré par le biais du National Security Council et du National Economic Council. Ces deux organismes sont les points de passage obligés de toutes les décisions de politique économique internationale à caractère stratégique.

En marge du dispositif central de l'administration, la force des Américains est d'avoir mis en place un puissant partenariat public-privé, fondé sur la connivence des dirigeants, formés dans les mêmes institutions et partageant les mêmes valeurs. Les mouvements des dirigeants entre les services du gouvernement et l'administration des entreprises privés sont très fréquents. Les fameux « thinks-thanks » sont également utilisés dans la stratégie d'influence américaine en utilisant leurs nombreuses antennes et connexions internationales.

Les Etats-Unis possèdent également comme atout une véritable communauté du renseignement. Le National Intelligence Council et la CIA ont sur leur contrôle les agences de renseignement de la sphère publique mais cultivent également un lien étroit avec les agences privées de renseignement ou les cabinets spécialisés des grandes entreprises.

La force américaine, qui se traduit par l'ampleur et l'intensité de leurs actions d'influence, repose aussi sur la formation universitaire et l'échange d'idées. Comme le décrit Monsieur Jean-Daniel Gardère, chef des services économiques pour la Belgique, les Pays-Bas et le Luxembourg : « Au-delà des effets d'attraction de « l'hyperpuissance » militaire, du dynamisme économique, de l'omniprésence de certains médias et de l'hégémonie de leur industrie audiovisuelle, au-delà de l'ampleur de l'aide bilatérale et des moyens de développement USAID, les Etats-Unis assoient principalement leur rayonnement et leur capacité d'entraînement sur le capital humain. » [10]

[10] Revue Problèmes économiques – dossier n°2.864 : L'arme de l'intelligence économique, 8 décembre 2004

Les Etats-Unis organisent un accueil extrêmement large d'étudiants, de professeurs et de chercheurs. L'octroi des visas est orienté vers les pays à potentiel économique majeur comme la Chine et l'Inde. L'accueil est très organisé tant d'un point de vue matériel que par les possibilités professionnelles offertes. Celles-ci sont en généralement sans commune mesure avec ce qu'ils auraient pu espérer dans leurs pays d'origine. Les fondations de recherche américaines privilégient des solutions américaines ou « adaptent » les conceptions les plus pertinentes. Le financement des ces opérations est largement assuré par l'échelon fédéral américain et les Etats concernés, mais par des opérations de mécénat grandement facilitées par le prestige et l'intérêt que peut retirer le monde privé de ce type d'opérations.

L'organisation américaine de soutien à son industrie est une référence mondiale. Elle témoigne d'une perception commune de l'intérêt national qui se manifeste à tous les niveaux tant des administrations publiques que privées. Le dispositif américain est offensif par nature tout en respectant les lois des Etats-Unis et « officiellement » celles du commerce mondial. Il peut ainsi servir de référence, même s'il faut bien convenir que les atouts américains sont bien souvent le négatif des freins français étudiés précédemment.

2. LA GUERRE DE L'INFORMATION DANS LES OPERATIONS MILITAIRES

2.1. La révolution dans les affaires militaires

L'essor technologique de la fin du vingtième siècle a conduit les Etats-Unis à développer à partir de 1994 le concept de révolution dans les affaires militaires (« Revolution in Military Affairs). La RMA repose sur un double constat : le retour à une guerre non conventionnelle de type asymétrique face à des acteurs la plupart du temps non étatiques et l'accroissement considérable des moyens d'informations. Les Américains en tirent plusieurs principes dont celui de la dominance informationnelle (« Information dominance »). Ce principe fondamental de la RMA doit permettre d'être capable à tous les niveaux d'altérer ou de neutraliser la capacité d'information de l'adversaire. Il s'agit également d'augmenter les capacités d'échange d'informations amies afin de raccourcir la boucle « OODA » (orientation, observation, décision et action) sur le champs de bataille. La finalité est bien ici de maintenir l'initiative en étant capable de prendre ses décisions

plus rapidement que l'adversaire. On retrouve une nouvelle fois le concept d'une défense globale, où il s'agit de dépasser les aspects strictement militaires pour faire face à de nouveaux types de menace. La gestion de cette information stratégique doit être réalisé selon le concept de « Network centric warfare ». L'information se retrouve partagée en réseau, ce qui permet de mettre en place un processus collaboratif optimisé permettant de décentraliser les actions et donc d'augmenter la rapidité de prise de décision.

Là encore, avec ce concept de dominance informationnelle, les Etats-Unis montrent leur résolution à mener stratégie informationnelle offensive.

2.2. Les opérations d'informations

Les opérations d'informations font partie depuis longtemps des doctrines militaires. Utilisées par les Forces armées elles visent à utiliser ou à défendre l'information, les systèmes d'information et les processus décisionnels pour appuyer une stratégie d'influence et contribuer à l'atteinte de l'état final recherché. D'un point de vue tactique elles comprennent de multiples volets comme la lutte informatique, les opérations psychologiques, la protection des informations sensibles, les tactiques de déception ou encore la guerre électronique dans son double aspect d'exploitation des indiscrétions mais aussi d'actions de neutralisation des moyens d'informations adverses… Ces techniques viennent en support des nouvelles options stratégiques développées par l'Alliance Atlantique. L'OTAN développe en particulier le nouveau concept d' « Effect Base Approach Operations » qui vise à élargir les options stratégiques possibles sur un théatre d'opérations. L'action militaire et l'usage de la force n'est plus la seule option envisageable. Il s'agit au contraire d'envisager la situation du théatre dans sa globalité, en prenant en compte les facteurs religieux, culturels, économiques ou sociologiques qui entrent en ligne de compte dans la résolution du conflit. Dans ce domaine la stratégie d'influence joue un rôle déterminant. Elle permet d'agir dans tous les domaines évoqués précédemment.

En France, ces opérations sont désormais reconnues et font l'objet d'un concept interarmées[11]. Cette reconnaissance est venue assez tardivement avec, comme nous l'avons vu précédemment, la grande réticence de la part des politiques de mentionner le terme d'actions psychologiques fréquemment utilisé par les militaires anglo-saxons. Ce terme

[11] Concept interarmées des opérations d'informations – PIA n°03.152, N° 294/DEF/EMA/EMP.1/NP du 11 mars 2005 (document joint en annexe).

n'est d'ailleurs pas utilisé dans le document, mais il fait bien mention de la volonté d'exercer une influence sur les populations et de chercher à légitimiser l'action des forces.

Ce concept limité aux opérations sur un théatre de crise est néanmoins assez unique dans la mesure où il évoque le terme de « stratégie d'information » dans le cadre de la défense globale de l'Etat. Il reconnait l'existence d'un domaine fonctionnel propre à l'information, en distinguant trois catégories de fonctions :

- des fonctions « dédiées à la production et à la diffusion de l'information : communication médias, communication interne et communication locale » ;

- des fonctions techniques permettant « d'exploiter ou de protéger les systèmes d'informations : lutte informatique, guerre électronique » ;

- la fonction technique permanente de « sécurité des opérations » correspondant à la protection des informations ;

A ce titre, les opérations d'informations développées par les militaires sont d'un point de vue stratégique comme d'un point de vue tactique un bon exemple de stratégie informationnelle offensive. Ce concept reconnait en effet l'utilisation de l'offensive lorsqu'il s'agira notamment d'influencer les acteurs sur le théatre d'une crise et de s'assurer de la superiorité décisionnelle en agissant contre les systèmes d'informations de l'adversaire.

3. PERSPECTIVES FRANÇAISES

L'exemple économique américain et l'exemple militaire français donnent de réelles pistes de reflexions sur ce que pourrait être la nature d'une stratégie globale d'information pour la France.

3.1. Vers une « sécurité économique active »

Fort de son analyse du modèle américain, Monsieur Alain Juillet préconise, dans un article paru dans la revue de la Défense nationale[12] , d'adopter en France une démarche de

[12] Revue de la défense nationale – *du renseignement à l'intelligence économique* – Décembre 2004

« sécurité économique active ». Il s'agit de prendre en compte les particularités culturelles françaises en dépassant le modèle de la défense économique traditionnelle. L'objectif déclaré est de donner aux entreprises « les moyens complémentaires nécessaires pour qu'elles se battent à armes égales dans cette confrontation économique mondiale sur la base de règles claires connues de tous ». L'Etat est ainsi amené à sélectionner des secteurs stratégiques et des sociétés qui en font partie afin de les intégrer dans un dispositif de veille et d'alerte. Il s'agit également pour l'Etat de soutenir les entreprises dans leurs démarches d'adaptation aux lois communautaires.

L'Etat et les collectivités territoriales sont appelées à se mobiliser afin de répondre aux besoins en veille des PME-PMI. Cette veille qui se fait de plus en plus par des moyens techniques et de moins en moins par moyens humains, comprend des facettes technologiques, concurrentielles, commerciales, réglementaires, financières ou encore stratégiques. Seuls les grands groupes français sont donc en mesure d'y consacrer des moyens financiers importants en créant des directions adaptées ou en recourant à des cabinets privés spécialisés.

Au niveau de l'analyse, Mr Alain Juillet préconise le partenariat public-privé qui a montré toute son efficacité aux Etats-Unis avec l' « Advocacy Center ». L'Etat vient compléter les dispositifs privés des entreprises en les renforçant par ses moyens puissants de collecte et d'analyse de l'information. L'horizon temporel est ici très différent, l'Etat travaillant sur le long terme il n'est pas soumis aux contraintes pressantes des marchés. Il peut ainsi intervenir sur des dossiers où son influence peut prendre toute sa dimension comme l'évolution des normes et des règles locales et internationales. De tels mécanismes sont possibles en France sous réserve d'une évolution des mentalités et la mise en place d'une « formation technique qualifiante » pour les plus concernés.

La France doit également se doter d'organismes de « bouillonnement » d'idées sur le modèle performant des « thinks-thanks » américains. Prenant en compte nos spécificités nationales, ils seraient à même d'être une formidable force de propositions pour éclairer les choix gouvernementaux.

L'importance des services des renseignements est également réaffirmée, avec comme principal axe d'effort la nécessité d'améliorer leur façon de collaborer entre-eux, avec les administrations et avec les entreprises.

Monsieur Alain Juillet évoque également la place de la « sécurité économique active » dans le contexte européen. Au stade actuel de la construction européenne, cette stratégie ne

peut-être que nationale. Elle doit néanmoins s'inscrire dans un cadre plus général qui est celui de l'Europe. Seule une politique affichée d'Europe de puissance pourrait, à terme, aboutir à l'adoption d'une stratégie informationnelle européenne. Une coopération européenne est néanmoins nécessaire et possible aujourd'hui. Une fois que l'on dispose des informations, il faut être prêt à les échanger. Au niveau européen des coopérations ciblées sont possibles dès lors que les intérêts des entreprises convergent. Force est aujourd'hui de constater qu'aucun Etat européen ne pourra à l'avenir assurer seul sa sécurité économique. Le partage des ressources est à terme nécessaire. Il pourra se faire dans un premier temps par une coopération accrue de certains Etats partageant les mêmes vision et ambitions dans des domaines stratégiques sur lequel se placent leurs entreprises.

3.2. Vers une stratégie globale d'information pour la France

En étendant ce concept de sécurité économique active hors du champ restreint de l'économie, il est possible de songer à une stratégie globale d'information pour la France. Cette stratégie avec sa part défensive mais aussi offensive pourrait reposer sur quatre piliers :

- l'alerte
- la coordination
- la protection
- l'attaque.

3.2.1. L'alerte

Il est nécessaire d'acquérir les moyens de mise en alerte contre tout risque d'attaque informationnelle. Cela doit permettre d'anticiper afin de ne pas subir et ainsi de pouvoir maintenir ou choisir à tout moment l'initiative. Il ne s'agit pas seulement de comprendre les tentatives de désinformation en cours mais surtout de prévoir celles à venir.

Cette capacité nécessite de disposer d'une veille stratégique adaptée aux menaces. Elle doit être organisée et doit comprendre plusieurs aspects que sont l'observation exhaustive des organisations sensibles, la mise en évidence des mécanismes en jeux et au final de convaincre les décideurs de la nécessité d'agir.

L'observation des pratiques exercées par les nations ou les groupes de pressions les plus offensifs est donc la première des étapes. Sur le terrain économique, ces nations sont en particulier les Etats-Unis, la Chine, le Japon et la Russie. Sur un terrain politique, tous

les groupes politiques non étatiques ou les Etats sont des entités à surveiller particulièrement. Les groupes altermondialistes, ou les associations environnementales telles que Greenpeace, doivent également être surveillés. Parfois autonomes, ils sont aussi autant de caisses de résonances utilisables par les organisations décidées à mener des attaques informationnelles. Il s'agit ainsi d'examiner toute la concurrence et les menaces qui peuvent peser sur les intérêts de l'Etat français et des entreprises françaises. L'observation doit se faire avec un état d'esprit ouvert et non dominateur. Comme le précisent très bien les auteurs Didier Lucas et Alain Tiffreau : « Dans une rencontre, l'important n'est pas tant de connaître l'autre que de s'identifier dans les yeux de l'autre »[13].

Un travail de synthèse très important est à opérer par la suite. Il s'agit alors dans un premier temps de parvenir à conceptualiser la menace, c'est-à-dire de comprendre la menace et comprendre comment la guerre d'information se mène. Une fois les mécanismes décryptés et les jeux mis en évidence, il sera alors beaucoup plus aisé de convaincre les décideurs de la nécessité d'agir.

Pour pouvoir correctement mener ce dispositif d'alerte il est nécessaire de disposer d'un organisme dédié sorte d' « observatoire des risques informationnels ». La gestion des risques informationnels ne peut en effet se concevoir dans l'improvisation. Il est nécessaire de dépasser le cadre mis en place dans le dispositif d'intelligence économique, en disposant d'un observatoire prenant en compte l'ensemble des menaces.

La place de l'offensive est particulièrement importante dans ce dispositif. Au-delà de la sécurité économique active entrevue précédemment, nous avons vu jusqu'à présent que la part de l'offensif restait très limité. Il y a pourtant de nombreux exemples où l'Etat s'autorise à agir de façon offensive. Outre l'exemple des militaires sur les théâtres d'opérations extérieures, on peut citer l'exemple des techniques mises en œuvre dans la lutte contre la criminalité ou la menace terroriste. Dans ces opérations un cadre légal est défini afin de réaliser des écoutes téléphoniques ou pour infiltrer des organisations. Les services de renseignement doivent donc être mobilisés en ces sens ; d'autant plus qu'aujourd'hui la lutte contre le terrorisme et la lutte contre les attaques informationnelles sont parfois étroitement liés.

---

[13] LUCAS Didier et TIFFREAU Alain , *Guerre économique et information – les stratégies de subversion* ; Ellipses, 2001, p. 114.

3.2.2. La coordination

La capacité à pouvoir se coordonner et d'agir en réseau est essentielle tant pour l'alerte, la protection et l'attaque. Il s'agit d'acquérir une véritable capacité à travailler en réseau et d'être capable de se partager l'information utile sans restrictions infondées.

Tous les acteurs français concernés doivent travailler en synergie. Ils sont particulièrement nombreux car l'on recense en effet :

- Les représentants de l'Etat français jouant un rôle en matière d'information. Ces sont les ministères, les ambassades, les collectivités territoriales, les Armées, la Police ou la Délégation Générale pour l'Armement. Le Secrétariat Général pour la Défense nationale joue un rôle tout particulier dans la mesure où il par excellence un organisme de coordination de l'action interministérielle dans le domaine de la défense. Cela est particulièrement vrai en matière d'intelligence économique, puisqu'il s'agit de l'organisme d'emploi de Monsieur Alain Juillet.

- Les acteurs du renseignement étatiques que sont en particulier la Direction Générale de la Sécurité Extérieure, la Direction de la Surveillance du Territoire, les Renseignements Généraux et la Direction du Renseignement Militaire. Il faut également y rajouter tous les acteurs privés spécialisés dans le renseignement d'intérêt économique.

- Les acteurs économiques : entreprises, organismes financiers, conseils économiques et sociaux régionaux, fédérations professionnelles, chambre de commerce et d'industrie, syndicats de salariés, groupes d'intérêts, français de l'étranger, consultants, intermédiaires en information, journalistes…

3.2.3. La protection

La capacité à se protéger des attaques informationnelles est également essentielle. C'est surtout le terrain de la stratégie défensive. La protection se conçoit dans un dispositif permanent, qui met en place des organisations et des techniques valables dans la durée. Elle doit également se concevoir en fonction des alertes. Le dispositif décrit précédemment doit permettre de connaitre les risques d'attaques potentiels et d'adapter son dispositif de protection en conséquence.

3.2.4. L'attaque

La possibilité d'attaquer, d'être offensif, doit permettre de lutter efficacement contre les attaques informationnelles recherchant le bouleversement des rapports de force. Ainsi, face au « faible » le fort ne doit pas manœuvrer ni « gesticuler » mais a au contraire parfois l'obligation de combattre. Si ce mode d'action est retenu, il convient alors dans un premier temps de construire un argumentaire et donc une stratégie d'attaque. Cela nécessite également de pouvoir disposer de différents moyens d'attaque et d'avoir la liberté de les utiliser.

En fonction de l'analyse de la situation, un argumentaire d'attaque doit être construit. Il doit particulièrement veiller à s'appuyer sur une information exacte et vérifiable ou du moins sur des faits d'une évidence telle qu'ils ne pourront être contestés.

Une fois le risque d'attaque et la stratégie établie, il est alors très efficace d'employer des techniques de désinformations en leurrant son adversaire. Si la désinformation directe peut être répréhensible, le brouillage des cartes en créant de l'information parasite ne pose pas de problème de déontologie. Cette technique peut-être employée pour faire croire à de faux sujets d'intérêts à des fins de déception. Il s'agit ainsi de développer une réelle stratégie de contre-information à l'encontre des agresseurs potentiels.

Un dispositif de dissuasion peut être utilement mis en place. L'attaquant possède forcément des points de faiblesse et pourra renoncer à mener une attaque par l'information s'il existe une forte probabilité d'une riposte. L'analyse des failles adverses pour pouvoir s'y engouffrer et la préparation du terrain sont donc essentiels lors du travail d'analyse destiné à la mise en alerte. La crédibilité de l'Etat français ne pourra exister que s'il est en mesure de produire lui-même des attaques informationnelles.

La capacité à jouer sur l'auditoire et véhiculer son argumentaire via les caisses de résonance adéquates est le point de difficulté essentiel. La France doit être capable se doter d'une « agence interministérielle de lutte informationnelle ». Elle doit avoir un rôle de coordination entre ministères et les services clés ; avec possibilité de s'affranchir du circuit hiérarchique. Là encore il ne s'agit pas de créer une agence de désinformation de l'Etat, mais une structure capable de faire passer les bons argumentaires aux bons moments. Il

faut pour cela disposer de l'arsenal législatif adéquat et d'un réseau de caisses de résonances savamment organisé.

Les structures nécessaires à la mise en place d'une telle stratégie existent, elles doivent cependant encore s'adapter. Il ne s'agit pas d'un problème financier, les investissements nécessaires à l'adaptation de ces structures étant loin d'être considérables. Il s'agit avant tout d'acquérir la volonté et la capacité de travailler en réseau. Un organisme de coordination central doit cependant être crée. Le mandat de Monsieur Alain Juillet ne couvre en effet que le domaine de l'intelligence économique. Les attaques informationnelles potentielles contre les intérêts de la France couvrent bien d'autres domaines. Un organisme de coordination central devrait ainsi voir le jour, dont l'intelligence économique serait une partie seulement de ses attributions. Il aurait pour tâche de remplir les fonctions d'alerte et de coordination, ainsi que de superviser la protection et l'attaque. Un « observatoire des risques informationnels » lui serait subordonné et chargé d'alerter les différents services de l'Etat et du privé sur les menaces. Une « agence de lutte informationnelle » serait quant à elle chargée de mener l'attaque.

CONCLUSION

Il ne s'agit pas aujourd'hui de se limiter à l'intelligence économique en matière de guerre de l'information. La France peut se donner les moyens d'adopter une stratégie globale d'information faisant une large part à l'offensive. Cela nécessite une évolution des mentalités qui devrait s'opérer au fur et à mesure de la perception par les politiques et les citoyens de la réalité et des dangers de la guerre de l'information moderne. Il est possible et nécessaire d'aller plus loin en s'inspirant du modèle de stratégie informationnelle américain et en l'adaptant aux spécificités françaises.

Avec une véritable stratégie informationnelle offensive, l'affaire du Clémenceau aurait put avoir une toute autre issue. Le scénario aurait put ainsi se dérouler de la façon suivante :

Une veille stratégique adaptée permet d'identifier la menace Greenpeace très en amont. Les services de l'Etat affectés à cette surveillance alertent le ministère de la Défense sur la réalité de la menace Greenpeace.

Alerté, le ministère de la Défense diffère sont projet et analyse les stratégies possibles de Greenpeace. Par des relais d'influence et caisses de résonance adaptées, il crée un environnement favorable à l'annonce de son projet avec deux axes d'efforts :

- La crédibilisation du projet de démantèlement, par exemple par des films promotionnels montrant la compétence des chantiers indiens et en restaurant ainsi leur image.
- La décrédibilisation systématique de la stratégie de Greenpeace, en montrant le lourd passé de Greenpeace en matière de manipulation d'information. L'affaire de la Brent Spar aurait à titre d'exemple put être exploitée au bon moment.

Le succès n'aurait pas été garanti, mais au moins l'effet de surprise aurait été limité et une action offensive entreprise.

ANNEXE 1

CONCEPT INTERARMEES DES OPERATIONS D'INFORMATIONS

1. Le besoin

1.1. Globalité des crises

L'information rend aujourd'hui le monde plus proche et apparemment plus transparent. L'événement est diffusé immédiatement et dans le monde entier par les différents médias, voire par des individus.
L'information a ainsi globalisé les crises et les conflits. Sur les théâtres d'opération, les militaires **interagissent** avec des protagonistes toujours plus nombreux et plus influents. Ils sont **observés** et jugés à distance.

1.2. Vers l'état final recherché

La **globalité des crises** impose désormais de mettre en œuvre une **stratégie globale**, coordonnant les outils diplomatiques, économiques, financiers, culturels et militaires pour atteindre **l'état final recherché**. Le politique et l'opinion n'attendent pas de la force engagée la seule défaite de l'ennemi, mais l'obtention des **effets** qui conduiront à la **sortie de crise**.

1.3. L'ère de l'information

L'information est partout et surabondante. L'information façonne les **perceptions**, et donc les opinions publiques ou individuelles. Elle influe ainsi sur les comportements et sur les **décisions** prises.
Mais l'information est impalpable et **fragile**. Elle peut être utilisée, amplifiée, minimisée ou manipulée. L'enjeu de ce début de siècle n'est plus d'y accéder, mais de la **valoriser** et de la faire parvenir à l'endroit voulu. Acteurs, spectateurs ou victimes, les militaires ne peuvent s'en extraire.
Il convient donc de s'organiser pour :

- s'**assurer** de la vérité de l'information ;
- être en mesure de **contrer** les effets d'une information fausse ou manipulée ;
- utiliser l'information pour **contribuer** à l'atteinte de l'état final recherché dans une crise,

en respectant toujours les **valeurs** de liberté, de vérité et de démocratie qui fondent notre société.

1.4. Le défi de l'information

A l'instar des forces armées des grands pays occidentaux, les forces armées françaises se doivent désormais de répondre à ce défi en développant avant tout une véritable **vision stratégique** de l'information et une **synergie opératoire** entre les **différents instruments** s'y rapportant afin de renforcer l'**anticipation** et la **cohérence**, les deux clés de voûte d'une politique de l'information efficace. Elles doivent également s'investir encore plus dans la prise en compte **des nouvelles technologies de l'information** pour rivaliser avec l'usage qu'en font désormais systématiquement leurs adversaires potentiels mais également leurs principaux alliés.

2. Domaine et définition

2.1. Les dimensions de l'opération

Toutes les actions que conduisent les forces constituent une information. Cette action doit être interprétée positivement par ceux que nous cherchons à défendre. Elle doit parfois constituer un message fort pour l'adversaire ou les perturbateurs.
Cette dimension de l'information a toujours été prise en compte de façon intuitive dans les opérations.
A l'ère de l'information, cela n'est plus suffisant et les armées doivent désormais **occuper** et **défendre l'espace de l'information** comme elles occupent et défendent l'espace physique. Sur le terrain de l'information, l'action des forces doit pouvoir être planifiée, coordonnée et décrite comme elle l'est sur le terrain physique.

L'information est **dans** la manœuvre, au même titre que l'usage de la force. Information et usage de la force se combinent et s'appuient mutuellement dans les voies choisies pour atteindre l'état final recherché.

2.2. Stratégie d'information

La stratégie d'information de l'Etat est globale. Elle est conduite **avant, pendant et après la crise**.
Elle utilise différents instruments à sa disposition.
S'il ne constitue qu'une partie d'un plan global, l'instrument militaire est cependant exceptionnel car il permet de mettre en œuvre une grande variété de moyens au service de cette stratégie.
Son succès repose sur la multiplicité et sur la cohérence des actions menées. **Tous les militaires** engagés dans l'opération y participent au quotidien, par leur attitude, leur comportement et les contacts qu'ils établissent ; en particulier la **coopération civilo-militaire**, la **diplomatie** de défense, et toutes les fonctions non-spécialisées en information, mettant en **relation** les forces avec l'extérieur.
Il existe cependant un domaine fonctionnel propre à l'information[1] :

- certaines fonctions sont **dédiées** à la **production** et à la **diffusion** de l'information : **communication médias, communication interne** et **communication**[2] **locale** ;
- d'autres **fonctions techniques** permettent d'exploiter ou de protéger les systèmes d'information : **lutte informatique, guerre électronique** ;
- permanente, la **sécurité des opérations** est une fonction technique de protection de l'information qui est élaborée par des experts mais qui doit être mise en œuvre **par tous**, spécialistes et non-spécialistes.

L'emploi de moyens militaires classiques participe à la **dissuasion et à la persuasion**, et peut **agir** (destruction) sur les systèmes d'information. Il peut se **combiner** très directement aux opérations d'information, comme dans le cas de la déception.

2.3. Définition

Les opérations d'information sont constituées par l'ensemble des actions menées par les forces armées, dirigé et coordonné au plus haut niveau, visant à utiliser ou à défendre l'information, les systèmes d'information et les processus décisionnels, pour appuyer une stratégie d'influence et contribuer, dans le cadre des opérations, à l'atteinte de l'état final recherché, en respectant les valeurs défendues.

2.4. Entités visées

De l'ennemi formel à l'individu trublion doté d'un pouvoir de nuisance, tous les **acteurs** du théâtre de l'information peuvent être concernés, y compris nos troupes. Pour **faire coïncider** les objectifs de ces différents acteurs avec l'état final recherché, ou en **minimiser** les divergences, les opérations d'information ciblent leur **connaissance**, leur **capacité** et in fine leur **volonté**. L'action porte ainsi sur des individus, des populations ou des communautés, des organisations ou des installations. Pour chaque opération il faut identifier les info-cibles et répartir leur traitement au niveau adéquat, avec les moyens appropriés, en gardant la cohérence du message délivré.

3. Objectifs

L'usage de l'information permet de préparer des opérations décisives, de créer des opportunités. Il peut parfois se substituer à l'usage de la force, épargner des vies humaines, réduire le niveau de violence, gagner les esprits et les cœurs. C'est tantôt un outil d'influence, d'aide à la diplomatie préventive, et parfois un outil de soutien aux opérations de combat. Les opérations d'information servent trois objectifs majeurs.

---

[1] Ces fonctions spécialisées et techniques contribuent aussi au **recueil** d'une grande partie de la **connaissance** nécessaire aux opérations d'information.
[2] cette fonction appelée à évoluer correspond dans les grandes lignes à la notion de « Psyops » de l'OTAN telle que décrite dans l'*Allied Joint Publication* 3.7.

3.1. Garantir la liberté d'action

La liberté d'action dépend de l'aptitude à conserver la **supériorité décisionnelle** et la **capacité à informer**. La première impose de protéger et de **défendre** ses systèmes d'information et ses processus décisionnels tout en **agissant** contre ceux de l'adversaire ; la seconde impose d'occuper le terrain de l'information, pour garantir la **crédibilité** de la force, et pour **convaincre**.

3.2. Exercer une influence

À l'inverse de la contrainte physique, la **persuasion** vise l'adhésion volontaire, le consentement ; elle a des effets bien plus durables et mieux tolérés.
L'information est le **levier des mécanismes de sortie de crise** car elle conduit dans la durée à la **prise de conscience** des opinions et des acteurs. Elle est le vecteur principal d'une **stratégie d'influence** visant à promouvoir les valeurs prônées par la France.

3.3. Légitimer l'action des forces

Lorsqu'une crise éclate, **l'opinion publique** est désormais systématiquement prise à partie. Les opposants potentiels à l'action des forces armées sont nombreux et variés. L'amplification de leur position par la puissance des médias fait peser des risques importants sur la conduite des opérations. Dans la **course à la légitimité** et à l'influence, il convient de prendre en compte ces opposants potentiels et de tenter d'en faire des alliés, tout en persuadant les opinions du **bien-fondé** de l'opération.

4. Principes d'emploi

4.1. Cohérence

De l'extérieur, les forces sont perçues comme un **tout indissociable**, au service de l'Etat ou de la coalition qui les mandate. L'efficacité des opérations d'information repose sur la **cohérence** des actions menées du niveau stratégique à l'échelon tactique. Le fond des messages doit être unique, ce qui nécessite une direction centralisée.

4.2. Crédibilité

L'image de la force et les messages délivrés doivent rester crédibles. Il faut avancer avec la plus grande **précaution** dans l'utilisation et le dosage de procédés sensibles comme la déception ou la ruse. Le mensonge est un risque considérable car il conduit à la perte de confiance et de crédibilité. Toute perte de crédibilité est une victoire relative de l'opposant. Elle compromet pour longtemps les efforts entrepris par ailleurs.

4.3. Pertinence

Persuader implique un niveau de **pertinence** qui ne peut être atteint que grâce à une connaissance intime de l'environnement, de la culture et de la pensée de l'entité visée.
Pour obtenir un **effet recherché**, l'information doit parvenir à un moment précis, après une mise en condition préalable créée par des évènements naturels ou provoqués.

4.4. Pluridisciplinarité

La pleine efficacité des opérations d'information s'obtient en choisissant le moyen le mieux adapté, au cas par cas, et en **combinant harmonieusement** un ensemble d'actions dans le temps. Toutes les forces doivent être en mesure de participer à cette **synergie**.

4.5. Subsidiarité

Le choix d'actions multiples et décentralisées impose l'adoption du principe de subsidiarité vers les échelons subordonnés. Une part de **confiance** est accordée aux forces concernant l'usage des armes, régi par le droit, des conventions et des règles d'engagement. Une même part de confiance doit être accordée dans l'usage de l'information, régi par une **éthique**, une **déontologie**, des **règles de comportement** et des **éléments de langage**.

4.6. Déontologie

Quelles que soient les circonstances, les modes d'action retenus dans les opérations d'information doivent correspondre aux **valeurs** défendues. La fin ne peut justifier des moyens qui ne respectent pas des règles éthiques. Le recours à des propos dégradants, à la calomnie et au chantage est donc formellement exclu. Cette ligne déontologique est incontournable, même si elle constitue une vulnérabilité que l'adversaire ne manquera pas d'exploiter.

4.7. Evaluation

La conduite des opérations d'information nécessite une prévision des **effets** et leur **mesure** a posteriori.
Or le **délai** entre une cause et un effet est variable et peut être très long. Le **cycle action-évaluation** des opérations d'information ne peut être calqué sur celui des opérations dans le domaine physique.
La mesure d'effets dépendants de **facteurs humains** est particulièrement délicate, elle nécessite des méthodes adaptées.

*
* *

BIBLIOGRAPHIE

Ouvrages en français

- BARBA Morjane, *Guérilla Kit. Ruses et techniques des nouvelles luttes anticapitalistes. Nouveau guide militant* ; La Découverte, Paris, 2003.
- BESSON Bernard et POSSIN Jean-Claude, *Du renseignement à l'intelligence économique* ; Dunod, 1996.
- BOURNOIS Frank et ROMANI Pierre-Jacquelin Romani, *L'intelligence économique et stratégique dans les entreprises françaises* ; Institut des Hautes Etudes de la Défense Nationale. Economica, 2000.
- CARAYON Bernard, *Intelligence économique, compétitivité et cohésion sociale*; La documentation française, 2003.
- DRAY Joss et SIEFFERT Denis, *La guerre israélienne de l'information* ; La Découverte, 2002.
- Dirigé par HARBULOT Christian et LUCAS Didier, *La France a-t-elle une stratégie de puissance économique ?*, Ouvrage collectif ; Editions Lavauzelle (collection renseignement et guerre secrète), 2003.
- Sous la direction de FRANCOIS Ludovic, *Business sous influence. Marché financiers, ONG, marketers, Etat… Qui manipule qui ?* ; Editions d'Organisation, 2004.
- HUYGHE François Bernard, *L'information c'est la guerre*; Editions Charles Corlet, 2001.
- LOINTIER Pascal et ROSE Philippe, *Le Web de crise*, 2004.
- LIANG Qiao et XIANGSUI Wang, *La guerre hors limites*, Payot et Rivages, 2003.
- LUCAS Didier et TIFFREAU Alain, *Guerre économique et information – Les stratégies de subversion,* Editions Ellipses, 2001.
- Rapport présidé par MARTRE Henri, *Intelligence économique et stratégie des entreprises*, La documentation française, 1994.
- MYARD Jacques, *La France dans la guerre de l'information. Information, désinformation et géostratégie*, Editions L'Harmattan, 2006.

Ouvrages en anglais

- ARMISTEAD Leigh E., *Information Warfare : Separating Hype from Reality*, 2007.
- GREENBERG Lawrence T, GOODMAN Seymour E., SOO HOO Kevin J., *Information Warfare and International Law*, DoD Command and Control Research Program, National Defense University, 1998
- LORD Carnes, BARNETT Franck R., *Political Warfare and Psychological Operations : rethinking the US Approach*, National Defense University and National Strategy Information Center, 1989.
- WALZ Edward, *Information Warfare Principles and Operations*, Artech House, 1998.

ARTICLES DE REVUES EN FRANÇAIS

- Interview de CARAYON Bernard, paru dans le *journal du management* du 30 novembre 2005.
- GARDERE Jean-noël, « Intelligence stratégique et stratégie d'influence : les leçons de l'étranger », revue Accomex, Novembre-décembre 2003.
- MANCEAU Jean-Jacques, « La France pillée », l'Expansion, novembre 2006, numéro 713.

ARTICLES SUR INTERNET

- Discours de JUILLET Alain – 11 mai 2006 Avignon. Blog OlivierPommeret.com consulté le 11 janvier 2007.
- Auteur inconnu, « Contre-influence au service de MBDA », consulté sur le site intelligenceonline.fr le 1er mars 2007.

TABLE DES MATIÈRES