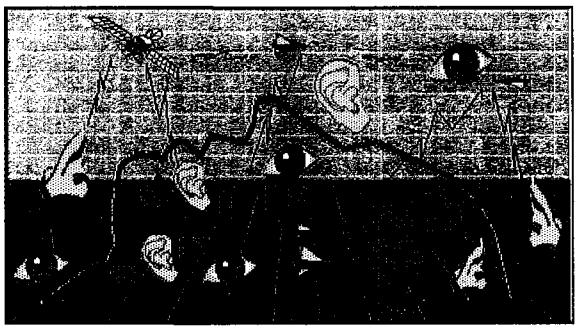
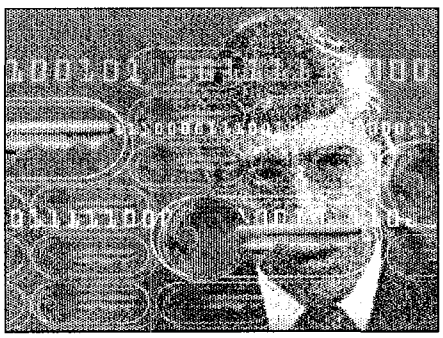
1998 D3.

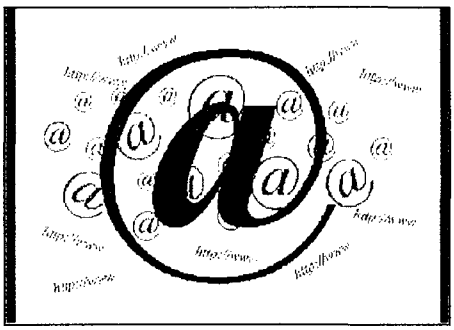
COLLEGE INTERARMEES DE DEFENSE

ETUDE PARTICULIERE A OPTION :

La guerre de l'information D 15







Avril 1998

Stagiaires	Responsable
LCL COURBOIS D1	
LCL ARNAUT D3	
ICA COMBRISSON D4	COL BERLAUD SGDN
CDT NORDH D1	
CDT TINE D4	

SOMMAIRE

INTRODUCTION GENERALE

Notre société est entrée de plain-pied dans la troisième vague[1] post-industrielle de l'ère de l'information. L'information circule aujourd'hui en temps réel d'un bout à l'autre de la planète grâce aux extraordinaires progrès technologiques accomplis dans le domaine des technologies de l'information.

Le développement des moyens de communication aidant, un nombre croissant d'individus auront désormais accès à l'information. Les risques de manipulation seront d'autant plus grands que l'information pourra être analysée, traitée et diffusée selon le message que l'on souhaite faire passer. D'où la nécessité de la maîtriser. La maîtrise de l'information et de la communication est ainsi devenue un enjeu stratégique: car qui possède l'information, détient le pouvoir.

De nombreux acteurs ont pris conscience depuis peu de cet enjeu: on peut citer les états, les forces armées, les décideurs économiques et les organisations non gouvernementales. La « guerre de l'information » est devenue pour eux une réalité quotidienne face à laquelle ils doivent mettent en oeuvre une stratégie adaptée.

Pour les états, et leurs forces armées en particulier, la guerre de l'information comporte un aspect essentiel qu'aujourd'hui aucun belligérant ne pourra désormais négliger s'il veut garder quelque chance de remporter la victoire. Il s'agit de la **guerre psychologique** que nous appellerons également manoeuvre psychologique, objet de la première partie de cette étude. Comme le disait François Géré, « ...dans les décennies à venir, il ne sera pas possible de faire la guerre victorieusement dans n'importe quel conflit sans disposer des moyens d'une action psychologique cohérente[2] »

Les Etats-Unis ont développé, dans un cadre plus large appelé « révolution dans les affaires militaires », un concept doctrinal spécifique de la guerre de l'information. Ce concept de « information warfare »[3] n'est toutefois pas exactement le même selon que l'on considère la vision du Département de la Défense américain ou celle de chacune des armées. La deuxième partie de cette étude examinera plus en détail les différents aspects de cette **conception opérationnelle de la guerre de l'information.**

---

[1] Terme employé par Alvin et Heidi Toffler dans leur ouvrage « Guerre et contre-guerre: comment survivre à l'aube du XXI° siècle ».
[2] - François Géré : La guerre psychologique, p.5
[3] IW - Information Warfare

La guerre de l'information concerne aussi le domaine économique. Dans un monde économiquement globalisé, l'information est devenue une matière première essentielle, au même titre que l'énergie et les matériaux : elle est en effet produite, stockée, extraite puis retravaillée et constitue désormais une des richesses de l'entreprise. Sa maîtrise devient essentielle dans tous les secteurs économiques. C'est pourquoi **l'intelligence économique**, qui a pour objet de collecter, trier et analyser ces informations stratégiques, est devenue une priorité pour tous les décideurs économiques. La troisième partie de cette étude y sera consacrée.

Les réseaux globaux d'information transforment notre société et facilitent la communication planétaire; grâce à Internet, les échanges de textes, photographies, sons et images vidéo sont possibles pour quiconque dispose d'un accès téléphonique. Le caractère transnational de ces réseaux pose dès lors le problème de la sécurité comme une des questions clés pour un développement viable de la société de l'information. Face à une criminalité informatique croissante et de plus en plus efficace, nous montrerons dans une quatrième partie pourquoi la **cryptologie** est aujourd'hui le seul moyen qui permette d'assurer une protection efficace des réseaux ouverts.

Aujourd'hui les **organisations non-gouvernementales** et intergouvernementales sont devenues des acteurs qui ont une influence importante sur les décisions prises par les gouvernements. Ces organisations utilisent aujourd'hui tous les moyens de communication possibles, tels Internet. Pratiquent-ils une guerre de l'information sur Internet? Quelle est leur stratégie d'utilisation de ce nouveau media? La dernière partie de cette étude apportera une réponse à ces questions.

PREMIERE PARTIE

«L'aspect psychologique dans la guerre de l'information»

INTRODUCTION

La décennie qui s'achève a été le témoin du développement fulgurant des moyens de communication. Le monde est devenu « un village planétaire » grâce à la multiplication des satellites de télécommunication, la numérisation et le développement des capacités de stockage de données et leur mise à disposition. Les relations inter-humaines en sont modifiées au point que ce qui se produit à des milliers de kilomètres de soi est ressenti aujourd'hui comme intéressant directement tout le monde. Le rôle joué par les médias dans la révélation et la dénonciation du génocide rwandais et de la purification ethnique en Bosnie-Herzégovine montre à quel point les moyens de communication et d'information sont devenus incontournables dans ce qu'il est convenu d'appeler la guerre psychologique. Au seuil du 21° siècle qui verra incontestablement les moyens audiovisuels se développer d'une manière vertigineuse, la maîtrise de cette nouvelle arme est devenue un enjeu capital.

Cette révolution qui s'opère sous nos yeux ne laisse personne indifférent, pas même les pays exclus de la course technologique tant celle-ci est globale. Elle touche bien évidemment le domaine de la défense. En effet, la multiplication des satellites de communications et d'observation implique une dimension militaire fondamentale qu'il convient de prendre en compte dans la conception et la conduite des opérations. Dans le domaine du renseignement, les implications sont énormes. Désormais, les stratèges militaires n'auront plus besoin d'envoyer systématiquement des unités spécialisées derrière les lignes ennemies pour savoir ce qui s'y passe. Les mouvements de l'ennemi, le nombre de divisions, de régiments, de bataillons et de compagnies pourront être connus, observés et communiqués en temps réel, ce qui était quasiment impossible quelques décennies auparavant. Les avions de reconnaissance, les drones et maintenant le satellite auront largement entamé, sinon totalement accompli le travail à la place du commando quand bien même celui-ci demeurera encore indispensable. De même, un nombre de personnes de plus en plus important aura désormais accès à l'information, ce qui pourrait à terme augmenter les risques de manipulation. Ainsi, il est devenu impératif pour tous les décideurs, politiques comme militaires de se doter de moyens capables de conduire une manoeuvre psychologique, composante essentielle dans le nouvel environnement médiatique. Et, comme le disait François Géré, « ...dans les décennies à venir, il ne sera pas possible de faire la guerre victorieusement dans n'importe quel conflit sans disposer des moyens d'une action psychologique cohérente[4] ». Dans une première partie nous tenterons de définir la guerre psychologique et d'en faire un bref historique, dans une seconde partie nous parlerons de son importance dans la conduite des opérations militaires et enfin dans une troisième et dernière partie nous tenterons de faire la corrélation entre la guerre psychologique et les médias.

[4] - François Géré : La guerre psychologique, p.5

1 -TENTATIVE DE DEFINITION

Il semble quelque peu difficile de donner une définition satisfaisante de ce qu'est la guerre psychologique. Nous retiendrons simplement « qu'elle vise à réduire le potentiel de l'adversaire, les capacités de lutte et la volonté psychologique[5] ».Toutefois, elle peut être subdivisée en deux parties essentielles : l'action psychologique et la guerre psychologique.

-l'action psychologique vise à « exercer une influence sur son propre camp, ses alliés, pour la communication ouverte d'une information officielle, libre et vérifiable mais aussi bien organisée et dirigée que possible[6]».

-la guerre psychologique est « un ensemble de manoeuvres hostiles à l'égard de l'ennemi particulier. Il convient également de protéger son propre camp contre les attaques psychologiques venant de l'adversaire[7] ».

Ainsi, la guerre psychologique a une double action. Elle s'exerce autant sur l'ennemi que sur les amis et en particulier sur sa propre opinion publique. En effet, le fait est qu'on peut perdre une guerre du fait de l'un ou de l'autre de ces deux concepts. La guerre psychologique n'est pas un concept nouveau dans la conduite des opérations militaires. Un court aperçu de l'histoire de la guerre montre que la manoeuvre psychologique a été de tout le temps une de ses composantes essentielles même si sa pratique n'a pas toujours été à la hauteur des enjeux stratégiques qu'elle recèle. Les Romains, Les Mongols, Napoléon, les régimes fasciste et nazi de Mussolini et de Hitler, tous y eurent recours très largement « pour conforter le moral de leur camp et propager le doute et, si possible, le désarroi chez l'adversaire[8] ».

La guerre du Golfe, de par la diversité et les performances des moyens médiatiques mis en oeuvre, donne également un aperçu de l'importance de la manoeuvre psychologique dans la conception et la conduite des opérations militaires sur le champ de bataille. De ce point de vue, la liberté de manoeuvre est bien évidemment tributaire de l'existence d'une doctrine d'emploi et de moyens d'action psychologique, ce que très peu de nations possèdent en ce moment.

Les transformations observées sur la scène médiatique ces dernières années et la place prise par les opinions publiques dans la gestion des crises pèsent de plus en plus lourdement sur les décisions gouvernementales appelées à plus de prudence quant à la nature et à la conduite des engagements militaires. Une action militaire, quelle qu'elle soit, nécessite désormais une véritable manoeuvre psychologique pour lui donner toutes les chances de réussir.

Quant aux militaires, le nouvel environnement médiatique leur impose d'inscrire toutes leurs opérations dans un cadre psycho-médiatique visant à la fois l'adversaire, s'il est clairement identifié, les belligérants et les opinions publiques. Les considérations purement opérationnelles ou militaires ne déterminent plus à elles seules les décisions des autorités car il leur sera de plus en plus demandé des comptes à rendre sur la manière dont ils auront conduit ces opérations. La comparution d'officiers devant les tribunaux internationaux pour la Bosnie et le Rwanda a été rendu possible grâce à l'action des médias, et dans certains cas on pourrait même parler d'acharnement médiatique.

---

[5] - François Géré, La guerre psychologique, p. 19
[6] - idem, p.15
[7] - idem, p. 16
[8] -Gérard Chaliand La persuasion de masse

2-DE L'IMPORTANCE DE LA GUERRE PSYCHOLOGIQUE DANS LA CONDUITE DES OPERATIONS

L'évolution observée dans la conception des nouvelles armes et dans la prise de conscience de l'opinion publique a conduit les belligérants à modifier les objectifs stratégiques et tactiques face à un adversaire donné. Par exemple, l'anéantissement total de l'ennemi n'est plus forcément l'objectif recherché. Dans certains cas, l'objectif sera de le faire capituler ou renoncer à son action sans avoir à utiliser les armes. Il s'agit alors de conduire toute une action psychologique qui peut aller de la propagande à la dissuasion.

La propagande fut largement utilisée par les régimes communistes du temps de la guerre froide ainsi que par les mouvements révolutionnaires. Elle peut prendre diverses formes allant du tract, au message radio et à l'émission télévisuelle. L'usage que les régimes communistes en firent lui ôta tout intérêt dans le monde dit libre au point que son utilisation y fut plus ou moins bannie. Il convient néanmoins de dire que «la propagande dès lors qu'elle ne cherche pas à tromper, à se faire ruse, mensonge, traquenard constitue une information qui cherche à produire un effet d'influence sur le récepteur [9]».

Quant à la dissuasion, elle se caractérise par la possession d'une capacité de violence, de la démonstration de cette capacité et de la détermination à l'exercer en cas de besoin. Pour qu'elle fonctionne, « il faut que la menace soit de dimension suffisamment impressionnante et que l'intention de la mettre en exécution en cas de besoin paraisse aussi indubitable que possible[10] ». Le tout est d'amener l'adversaire à renoncer à ses objectifs.

Ceci nous amène à aborder un point fondamental dans la conception et la conduite de la manoeuvre psychologique. Il s'agit du rôle du pouvoir. C'est lui qui détermine la politique de défense du pays, donne aux forces armées les moyens de l'appliquer. Son rôle est donc déterminant dans la conduite et le succès des opérations militaires y compris de la guerre psychologique. La manoeuvre psychologique n'aura de chance de réussite que dans la mesure où elle traduit véritablement la détermination du pouvoir politique. Le blocus de Cuba par l'armée américaine amena les Soviétiques à retirer leurs missiles parce qu'il exprimait la détermination du gouvernement américain à recourir à la force pour empêcher leur installation à proximité de ses frontières.

La guerre psychologique, nous l'avons vu dans les définitions, n'est pas seulement dirigée contre un adversaire. Elle doit être également conçue d'une part pour soutenir nos forces et d'autre part pour mobiliser derrière l'action gouvernementale l'opinion publique nationale et internationale tout en les protégeant contre les actes de guerre psychologique menés par l'ennemi. Si on admet que l'action psychologique, autant que les actes de guerre psychologique, est partie intégrante de la planification et de la conduite des opérations de guerre, il convient également de reconnaître que le soutien de son opinion publique est tout aussi déterminant et qu'il est loin d'être acquis dans certaines situations. Il importe donc de rechercher par tous les moyens ce soutien et comme le dit Gérard Chaliand, « ...les réactions de l'opinion publique ne résultent pas d'une évaluation rationnelle de la menace, mais de l'image que l'on a su en donner par les procédés de la lutte psychologique[11]».

---

[9] -François Géré, La guerre psychologique, p.28
[10] -idem, p.35
[11] -Gérard Chaliand, La persuasion de masse, p.43

Les forces engagées dans des opérations de guerre ont besoin de se sentir soutenues par la population. Celle-ci doit d'abord être pénétrée de la justesse de la cause défendue et de la nécessité pour ses soldats de la défendre, au besoin en y laissant la vie. Cela ne doit pas être une action de propagande mais la vérité. La cause doit donc être vraie ou en tout cas présentée comme telle et comme le dit François Géré « la lutte psychologique peut rarement créer de toutes pièces des situations entièrement factices[12]». L'engagement américain dans le golfe contre l'Irak n'était pas seulement motivé par la libération du Koweït mais également par la préservation des intérêts stratégiques des Etats-Unis dans une région où ils tirent l'essentiel de leurs approvisionnements en pétrole. Cela le soldat et le peuple américains peuvent le concevoir et l'accepter au nom des intérêts de leur pays. La défense du Koweït en tant que telle n'aurait peut-être pas suscité pareille mobilisation de l'opinion publique américaine si également elle ne soulevait certaines valeurs chères à l'Amérique telles que la démocratie, même si le régime koweïtien n'était pas un modèle du genre, et la liberté reconnue à chaque peuple de disposer de lui-même.

Pour ce qui est de la France, la guerre qu'elle mena en Indochine fut un échec. En effet, ni les soldats engagés, pour la plupart des légionnaires et des Africains du sud et du nord ressortissant des colonies, ni la population française elle-même n'avaient soutenu réellement un tel engagement, tout au moins vers la fin du conflit. Contrairement aux troupes françaises, qui entendaient d'abord contrôler le terrain, le Viêt-minh s'engagea en priorité dans une action psychologique destinée à amener dans son camp les populations et du Nord et du Sud du Vietnam. Et tandis que l'engagement de la France au Vietnam manquait de cohésion et de consensus au niveau national, « le Viêt-minh gardera constamment le même objectif : l'indépendance, et la même direction politique et stratégique d'une grande fermeté[13] ».

De même, l'échec de l'armée soviétique en Afghanistan peut être, en partie, imputable au manque de soutien psychologique de la population soviétique au moment où la résistance afghane portait de sérieux coups à la « force d'occupation soviétique ». Cela est vrai en partie, car c'est bien la contre-propagande des forces de résistance afghanes menée avec beaucoup d'efficacité qui a fait plier le moral des troupes soviétiques, ce qui provoqua leur défaite. Le sentiment de mener une guerre sainte, une djihad, contre les ennemis de Dieu (car tel était le socle sur lequel reposait la propagande afghane) ne donnait aux combattants afghans qu'une seule alternative : vaincre ou mourir au nom d'Allah. Ainsi que le note Maurice Torrelli, « ...toute transcendance peut être capturée pour servir des causes nationales ou sociales. La capture permettra alors de nourrir la légitimité de la cause et de mobiliser des combattants dans la guerre internationale comme dans la guerre civile[14]». C'est bien ce que firent les principaux dirigeants afghans durant toute la guerre contre l'occupant soviétique. Ce fut également l'arme secrète par laquelle la révolution iranienne triompha, en 1979, du régime du Shah qui disposait alors de la cinquième armée au monde.

---

[12] - idem 8

[13] -Gérard Chaliand La persuasion de masse

[14] -Institut du droit de la paix et du développement « Religions et Guerre », p.11

Les exemples ne manquent pas qui soulignent le rôle déterminant que peut jouer une manoeuvre psychologique pour amener les masses à épouser ses vues et à rejeter celles de l'ennemi. C'est ainsi que le régime laïc de Saddam Husseïn, conscient de la réprobation internationale qu'avait suscité l'envahissement puis l'occupation du Koweït, y compris dans le monde arabe, n'hésita pas à faire appel à la religion en présentant l'intervention de la coalition comme une nouvelle croisade du monde judéo-chrétien contre l'Islam. Cette opération que l'on peut qualifier de propagande ne fut pas sans conséquence sur l'opinion et sur certains dirigeants arabes. Des voix s'élevèrent alors pour dénoncer cette intervention et pour exiger le retrait de toutes les forces onusiennes de la région oubliant même que l'Irak avait envahi et occupé un autre pays arabe, geste non moins acceptable. Dans le camp de la coalition, on ne manqua pas d'user également de cette tactique pour mobiliser les diverses opinions publiques derrière l'ONU.

Les autorités américaines, par l'intermédiaire de la chaîne CNN notamment, menèrent une bataille psychologique visant à discréditer le régime de Bagdad d'une part et à légitimer l'intervention militaire en préparation contre les forces d'occupation irakiennes d'autre part. L'importance des grandes chaînes de télévision est une nouvelle donne dans la gestion des crises et les autorités, civiles ou militaires, en sont bien conscientes. En renvoyant tous les journalistes d'Irak à la veille du déclenchement de la guerre à l'exception de CNN, le s autorités irakiennes avaient bien perçu l'intérêt qu'elles pouvaient tirer de cette décision. En montrant le bombardement meurtrier de sites abritant des civils utilisés comme boucliers, Saddam Husseïn voulait pousser l'opinion publique internationale et occidentale en particulier à reconsidérer son soutien à l'action de la coalition dès lors que celle-ci violerait les règles élémentaires des droits de l'homme, ce qui est inadmissible en démocratie.

Le fait est qu'aujourd'hui la guerre n'est plus seulement une affaire de soldats; elle concerne toute la population et celle-ci exige de plus en plus des explications à son gouvernement dans la conduite et la gestion de la vie de la nation. La marge de manoeuvre des autorités est devenue trop étroite pour qu'elles puissent agir sans tenir compte de l'avis de la population. De même, le développement des moyens de communication tend de plus en plus à exposer l'opinion publique à une manipulation, à une propagande de l'adversaire pour priver telle autorité gouvernementale du soutien de sa population et même de celui de l'opinion internationale. Toutes ces menaces qui pèsent sur les opérations militaires témoignent de l'importance prise par la dimension psychologique dans la préparation et la conduite de la guerre et ce, au moment même où nous assistons, depuis la guerre du Golfe, à une hypermédiatisation des conflits armés.

3-GUERRE PSYCHOLOGIQUE ET MEDIAS

Comme nous l'avons déjà évoqué, depuis la guerre du Golfe les conflits se déroulent et continueront de se dérouler dans un environnement hypermédiatisé où la caméra observera et le départ du coup et son impact sur l'objectif. Les correspondants de guerre ne vont plus se contenter des points de presse organisés à leur intention par le haut commandement militaire. Ils seront en première ligne pour voir de leurs propres yeux ce qu'ils vont raconter aux auditeurs et téléspectateurs. La guerre va désormais se dérouler simultanément, sur le champ de bataille et dans les foyers.

Une telle implication des médias dans le déroulement d'un conflit n'est pas sans conséquence. La médiatisation des conflits remonte à peu près à la fin de la guerre du Vietnam. C'est également la période où commencent les progrès fulgurants observés depuis dans le développement des moyens audiovisuels. Après avoir longtemps mené une guerre « sans témoin », les autorités américaines ont regardé déferler sur les champs de bataille et en nombre croissant, sans trop y prendre garde, des journalistes de la radio et surtout de la télévision.

Les opérations militaires sont retransmises presque instantanément aux Etats-Unis par les grandes chaînes de radio et de télévision en pleine croissance et le peuple américain commence à vivre la guerre en direct avec toutes ses horreurs. De plus en plus de voix s'élèveront pour dénoncer la barbarie des opérations militaires et le carnage engendrés par cette guerre. Les raisons avancées tout au début pour justifier l'intervention américaine ne suffisaient plus pour mobiliser l'opinion publique.

Celle-ci commença alors à douter de la nécessité d'un tel engagement et finit par demander au gouvernement de rapatrier les forces du Vietnam. Un tel revirement ne fut possible que grâce au rôle joué par les médias dans la retransmission des événements tels qu'ils se déroulaient sur le terrain mais aussi grâce à la manipulation psychologique dont ils usèrent largement pour faire réagir l'opinion. En montrant des images de villages vietnamiens rasés sous les bombardements de l'aviation américaine, des petits enfants brûlés au napalm et tentant de fuir les bombardements et de jeunes soldats américains torturés à mort par les communistes vietnamiens, les médias américains pesèrent lourd dans la décision du gouvernement de se retirer du Vietnam. Il faut signaler que beaucoup d'images retransmises par la télévision étaient tout simplement falsifiées pour mieux agir sur l'opinion publique américaine Ainsi, c'est toute une action psychologique qui fut montée par la plupart des médias qui étaient en réalité contre cette guerre. De son côté, surpris par cette nouvelle arme qu'il avait négligée, le gouvernement américain ne sut réagir pour en limiter les conséquences.

En revanche, les communistes vietnamiens surent tirer profit de cette nouvelle situation (médiatique) dans la guerre que constituaient les médias. Par des opérations spectaculaires, telles que l'attaque de Saigon et l'occupation de l'ambassade américaine qui leur causèrent de lourdes pertes, ils montraient au peuple américain leur bravoure et leur détermination à obtenir l'indépendance de tout le Vietnam.

Cette implication des médias américains fut, selon certains, à l'origine de la défaite américaine au Vietnam. Plus que par les armes, celle-ci fut d'abord la conjonction de plusieurs facteurs, à savoir l'action psychologique jouée par la presse dans la seconde moitié du conflit, la non-prise en compte suffisante de la dimension psychologique dans toutes les phases du conflit par le commandement américain et enfin l'exploitation outrancière qu'en fit le Viêt-cong dès le début du conflit.

La guerre du Golfe fut à l'opposé de celle du Vietnam sur de nombreux plans, particulièrement dans sa médiatisation. Il est vrai qu'entre temps les moyens de l'audiovisuel s'étaient considérablement développés. Traumatisées par le fiasco médiatique vietnamien, les autorités américaines, civiles et militaires, entendaient faire effort dans la maîtrise de l'information dans toute sa globalité. Et pour cela, il fallait d'abord disposer de suffisamment de moyens d'information et ensuite trouver une stratégie pour traiter les médias en tant que partenaires et non plus comme adversaires comme ce fut trop souvent le cas par le passé. Cette opération fut à vrai dire couronnée de succès car non seulement les médias couvrirent cette guerre mais elles le firent de la façon dont les autorités militaires l'avaient souhaité et voulu.

L'opinion publique américaine et mondiale, grâce à une campagne médiatique remarquablement conduite par les Etats-Unis, fut plutôt bien préparée à cette guerre. Le régime irakien était systématiquement diabolisé pour son invasion du Koweït inacceptable pour la communauté internationale ;les Etats-Unis avaient le devoir moral d'intervenir pour rétablir la souveraineté de ce pays et la légalité constitutionnelle.

La catastrophe écologique que l'Irak faisait courir à la région et la guerre « propre » que les Etats-Unis allaient mener, avec peu de pertes avaient fini de convaincre l'opinion publique américaine.

Par-delà ce succès indéniable, il convient de s'interroger sur les possibilités de concilier les contraintes opérationnelles des militaires et les exigences d'information des médias dans les pays démocratiques. Il est bien évident que le coup de la guerre du Golfe ne risque pas de se renouveler à l'avenir et que par conséquent il est d'une impérieuse nécessité de trouver un compromis entre ces deux exigences.

CONCLUSION

La prise de conscience des opinions publiques est devenue une nouvelle donne dans la conduite des opérations militaires. La guerre n'est plus une affaire exclusivement réservée aux seuls militaires et gouvernants, la nation exige de plus en plus d'être consultée avant tout engagement de ses soldats et demande des comptes à ceux qui sont chargés de cet engagement. L'opinion publique est devenue de ce fait un enjeu majeur de la guerre et les protagonistes , conscients de cette réalité, se battent pour en assurer le contrôle. Il ne suffit plus pour une armée de posséder les systèmes d'armes les plus performants pour gagner la guerre, encore faudra-t-il gagner d'abord et avant tout la bataille de la guerre psychologique.

BIBLIOGRAPHIE

-CHALIAND Gérard, *La persuasion de masse,* Robert Laffont - Paris

-GERE François, *La guerre psychologique* ECONOMICA

-Institut du droit de la paix et du développement, *Religions et guerre* MAME, Editions universitaires

DEUXIEME PARTIE

LE NIVEAU OPERATIONNEL DE LA GUERRE DE L'INFORMATION

- L'EXEMPLE AMERICAIN -

INTRODUCTION

La révolution des affaires militaires qui se développe aux Etats-Unis n'est pas seulement la conséquence de la maîtrise des nouvelles technologies d'information par la nation américaine. Cette révolution est plus profonde; elle est poussée par toute une nouvelle mentalité de discussion publique et ouverte des sujets portant sur les différents domaines de la politique de défense. Ainsi, l'investissement sur les matériels est accompagné par un investissement sur le développement de nouveaux concepts, par la suggestion d'améliorations de la doctrine d'emploi actuelle et par la recherche des orientations à suivre dans un futur à 10 - 20 ans. Ce processus continu est loin d'être limité au cercle strictement militaire. Des études sont commandées à différentes organisations non gouvernementales, notamment les universités, et la quantité de documents produits est énorme. Une fois établie la supériorité technologique, les Etats-Unis distancent maintenant les autres pays par la réflexion conceptuelle.

1. CONCEPTS

1.1 Environnement d'Information Global

La doctrine opérationnelle américaine part du principe que toute intervention militaire se fera dans un nouveau cadre appelé Environnement d'Information Global[15]. Les médias[16], les organisations, les agences internationales et même les individus constituent quelques-uns des acteurs du GIE. Grâce à la technologie, les différents aspects d'une opération militaire peuvent être connus partout et presque en temps réel, sans être filtrés. On reconnaît que la suppression ou la censure de l'information ne sera ni possible, ni désirable. En outre le GIE contient les processus et les systèmes d'information qui ne dépendent pas des militaires ou même de la Défense, mais qui peuvent avoir un rôle décisif dans le succès ou l'échec des opérations militaires. La partie du GIE constituée de systèmes d'information et d'organisations amies et adversaires, militaires et non-militaires qui permettent, appuient ou influencent de manière décisive une opération militaire spécifique, est appelée Environnement d'Information Militaire (MIE)[17].

---

[15] GIE : Global Information Environment

[16] 147 journalistes ont été présentes pendant l'opération Overlord, 800 ont suivi Just Cause au Panama et 1300 ont été sur le théâtre d'opérations du Koweït pendant Desert Storm.

[17] MIE : Military Information Environment

1.2 Guerre de l'Information

Information Warfare est la terminologie adoptée par le Département de la Défense (DOD)[18] et par l'Etat-major Interarmées (JCS)[19] pour désigner l'éventail d'actions prises pendant un conflit pour obtenir une supériorité dans le domaine de l'information. Le document CJCSI 3210.01 la définit comme *les actions prises pour obtenir la supériorité dans le domaine de l'information, agir sur l'information, le processus de traitement de l'information, les systèmes d'information et les réseaux informatiques de l'adversaire, tout en protégeant les nôtres.*

L'Armée de Terre, par exemple, pense que le concept énoncé par le DOD et le JCS est beaucoup trop ciblé sur la phase du conflit. Elle a adopté une vision plus large du sujet reconnaissant que les problèmes de l'information sont présents dans tout l'éventail des opérations militaires, depuis le temps de paix jusqu'à la guerre totale. Elle propose un concept plus élargi qu'elle appelle Opérations de l'Information (IO)[20] et qui constitue l'application de la IW pour le commandant de la composante terrestre. Le FM 100-6, Information Operations, publié par le TRADOC[21] en août 1996 constitue la doctrine de base pour ces opérations.

Les activités qui supportent les IO peuvent être regroupées dans trois domaines: les opérations, l'information et le renseignement, et les systèmes d'information. Le domaine le plus intéressant est celui des opérations et constituera l'objet d'une analyse plus profonde.

Les trois opérations que L'Armée américaine utilise pour gagner et maintenir la suprématie dans le domaine de l'information et du commandement et de contrôle (C2)[22] sont la Guerre de Commandement et de Contrôle (C2W)[23], les Affaires Civilo-Militaires (CA)[24] et les Affaires Publiques (PA)[25].

2. LA GUERRE DE C2

L'efficacité d'une force militaire dépend de plus en plus de l'exactitude et de l'opportunité de l'information qu'elle reçoit, qu'elle traite et qu'elle diffuse. Il est donc naturel que le système de Commandement et de Contrôle (C2), clé de voûte du flux de cette information, soit un système fondamental pour la conduite des opérations. Un système C2, outil capable de transformer les capacités militaires en puissance militaire effective, est constitué d'opérateurs, de senseurs, de processeurs, de décideurs et de bases de données, s'appuyant sur un système de communications. Chaque élément du système C2 est vulnérable à différents degrés aux opérations militaires. Les actions qui dégradent des composants du système, provoquent une réaction en chaîne de tout le système.

---

[18] DOD : Department of Defense
[19] JCS : Joint Chiefs of Staff
[20] IO : Information Operations
[21] TRADOC : US Army Training and Doctrine Command
[22] C2 : Command and Control
[23] C2W : Command and Control Warfare
[24] CA : Civil Affairs
[25] PA : Public Affairs

En premier lieu la perte ou la distorsion de l'information réduit l'efficacité de l'estimation de la situation par les décideurs. Or l'augmentation de l'incertitude détériore le processus de décision. Par la suite, décisions erronées ou tardives diminuent la crédibilité du commandement, ce qui renforce l'incertitude. Le développement de ce processus en chaîne, stimulé par des attaques constantes au système, peut contribuer à la capitulation de l'adversaire.

L'obtention et le maintien d'une supériorité de C2 face à l'adversaire constituent un avantage significatif. Cet avantage permet au commandant l'application complète de son potentiel de combat. Une supériorité en C2 peut donc contribuer, rapidement et à moindre risque, à assurer l'obtention de la victoire pendant un conflit ou à obtenir le succès au cours d'une opération de non-guerre.

La guerre de commandement et de contrôle (C2W) est l'intégration de toutes les capacités militaires, incluant la Sécurité des Opérations, la Déception, les Opérations Psychologiques, la Guerre Electronique et la Destruction Physique, mutuellement supportées par le Renseignement. Sa finalité est d'ôter l'information à l'ennemi, influencer et détériorer ses capacités C2, tout en protégeant nos capacités de C2 contre des actions similaires.

Les deux volets qui constituent la guerre de commandement et contrôle sont les contre-mesures de commandement et de contrôle et les mesures de protection de commandement et contrôle, ou, pour faire simple, l'attaque de C2 et la protection de C2.

2.1 L'attaque de C2

L'attaque de C2 est l'exécution coordonnée des actions contre des objectifs établis qui empêchent l'adversaire de commander et de contrôler ses forces. Ce but est obtenu en ôtant de l'information et par la dégradation, l'influence ou la destruction du système de C2 de l'adversaire.

Les principes de l'attaque de C2 sont les suivants:

- Programmation orientée par la mission de l'unité, l'intention et le concept d'opérations du Commandant;
- Synchronisation avec le Plan d'Opérations;

Conquête et maintien de l'initiative par la dégradation du système d'information de l'adversaire, l'obligeant a être réactif.

En général, les effets provoqués par l'attaque de C2 peuvent être les suivants:

- Dégradation de la capacité adverse à formuler des orientations et à prendre des décisions;
- Influencer le commandant adverse pour lui faire prendre des décisions erronées.
- Neutralisation du système d'informations de l'adversaire par la destruction physique de ses noeuds de communication.

2.2 La protection de C2

La protection du Commandement et du Contrôle assure le maintien de la capacité de C2 en nos forces et empêche à l'adversaire d'obtenir l'information à partir de nos systèmes ou de déclencher des actions visant à influencer, dégrader ou détruire nos systèmes de C2. On peut trouver, dans le cadre de la protection de C2, des mesures de nature offensive (utilisation des cinq composantes de la C2W pour réduire la capacité de l'ennemi de conduire des actions contre notre système C2) et de nature défensive (comme les mesures prises par nos forces pour se protéger physiquement ou électroniquement, par exemple).

Les principes de protection de C2 sont les suivants:

- Gagner la supériorité en Commandement et Contrôle;
- Réduire la capacité de l'adversaire à conduire des actions d'attaque de C2W;
- Réduire les vulnérabilités de notre système C2;
- Réduire les interférences mutuelles de nos systèmes de C2.

Le respect de ces principes peut causer les effets suivants:

- L'adversaire n'aura pas d'information de qualité pour ses prises de décision;
- L'adversaire prendra des actions qui lui seront préjudiciables, ou les prendra trop tard, ou restera inactif;
- Les actions de C2W adverses sur nos systèmes seront inefficaces.

2.3 ETUDE DE CAS: La Guerre de C2 pendant DESERT STORM

Pendant les opérations DESERT SHIELD et DESERT STORM, la guerre de commandement et contrôle a joué un rôle primordial. Pendant la phase de programmation des opérations, les échelons de décision les plus élevés ont reconnu la faiblesse du système C2 irakien et ont conclu que la destruction de ce système permettrait d'obtenir une victoire avec un minimum de pertes humaines. Cet aspect est présenté dans la directive du Secrétaire d'état américain portant sur les objectifs militaires de l'opération DESERT STORM:

- Neutraliser la capacité du commandement national irakien à diriger des opérations militaires;
- Expulser du Koweït les forces armées irakiennes;
- Détruire les capacités balistiques, nucléaires, biologiques et chimiques de l'Irak;

Collaborer à la restauration du gouvernement légitime du Koweït.

Pendant les opérations aériennes de Desert Storm, le commandement irakien a été sélectivement aveuglé par la guerre électronique et la destruction physique, actions qui ont permis d'occulter les mouvements et les opérations des Alliés. La déception militaire a renforcé en plus la perception erronée de l'Irak à l'égard des intentions réelles de ses adversaires. L'utilisation de la guerre électronique et des bombardements aériens de précision dirigés contre les cibles C2 irakiens, ont permis la désorganisation et l'isolement des forces irakiennes.

Quand les opérations terrestres ont démarré, les forces irakiennes étaient proches de la désintégration, avec plusieurs unités incapables de coordonner leurs efforts. L'incapacité de l'Irak en matière de protection et d'attaque de C2 a réduit, non seulement le nombre de pertes des deux cotés, mais a aussi réduit le temps nécessaire pour l'obtention de la victoire des Alliés.

3. LES OPERATIONS CIVILO-MILITAIRES

Le rôle des affaires civilo-militaires est fondamental parce qu'elles constituent l'interface entre les opérations et quelques uns des acteurs essentiels du GIE. Que se soit en temps de paix, de crise ou de guerre, les opérations civilo-militaires permettent d'établir, maintenir, influencer ou explorer les relations entre les forces militaires, les autorités civiles et la population de la zone d'opérations.

Pendant l'intervention *Restore Hope* en Haïti, les activités d'affaires civilo-militaires ont informé les populations en utilisant différents médias et en suscitant le débat public. Elles ont conduit une campagne d'opérations psychologiques bien ciblée. Parce qu'elle illustre bien l'utilisation de l'information comme arme (et pas seulement comme cible), on étudiera les opérations psychologiques pendant *Restore Hope* comme deuxième cas de figure.

ETUDE DE CAS: opérations psychologiques pendant RESTORE HOPE

Restore Hope constitue un des cas les plus intéressants d'opérations psychologiques utilisant les moyens de production, de traitement et de diffusion de l'information les plus modernes.

En juin 1994 le Groupe d'Appui d'Information Militaire (MIST) a été constitué à Washington pour soutenir la politique américaine vers l'instauration de la démocratie en Haïti, combattre l'information diffusée par le gouvernement militaire en Haïti, et pour diffuser des messages de l'ancien président Aristide vers les Haïtiens.

En juillet il avait mis en route la Radio Democracy, utilisant une bande AM et trois bandes FM, la Radio AM 940[26] et, à partir d'août, la chaîne de télévision *Television Democracy*. Musique populaire d'Haïti alternait avec des messages d'Aristide, des messages de Clinton et d'autres personnalités américaines ou haïtiennes en exil. Le but était de discréditer les militaires au pouvoir, de montrer les avantages de la démocratie, d'établir un lien entre le retour d'Aristide et l'arrivée de l'aide humanitaire Pour garantir que les émissions soient de bonne qualité, le *193d Special Operations Group (US Army Reserve, Pennsylvania)* effectuait des vols près du territoire haïtien en diffusant les émissions.

Le 14 septembre un avion américain a dispersé des milliers d'affiches sur trois villes d'Haïti pour mettre sous pression le gouvernement militaire. La campagne ne s'est pas arrêtée après la capitulation de la *Junte* le 18 septembre. Le lendemain, des hélicoptères appuyant le *4th PSYOP Group (Airborne)* ont survolé Port-au-Prince en diffusant des messages par des enceintes acoustiques annonçant l'arrivée pacifique des troupes américaines pour rétablir la démocratie. Les soldats annonçaient que les troupes avaient été invitées et que les Haïtiens ne devaient pas interférer avec les opérations.

---

[26] Cette radio soeur visait à éviter l'émigration des haitiens vers les Etats-Unis.

Un très grand effet a été obtenu avec la diffusion de la chanson *Viv la Pe*, commandé à un compositeur haïtien par le groupe conjoint des opérations psychologiques. La chanson appelant à la réconciliation, a été produite en différentes versions (musique, ou musique mélangée avec des messages d'Aristide). Elle a été diffusée sans cesse par des haut-parleurs installés sur des véhicules qui circulaient dans les villes haïtiennes.

Le bon accueil des forces américaines en Haïti, avec toutes ses conséquences bénéfiques liées à la protection de la force et à la simplification de la mission est, en grande partie, dû à l'ampleur des moyens psychologiques utilisés et intégrés pendant toutes les phases de la campagne.

4. LES OPERATIONS DES AFFAIRES PUBLIQUES

Les opérations militaires sont aujourd'hui conduites devant l'opinion mondiale. La couverture médiatique des interventions contribue ainsi à influencer l'opinion publique.

En outre les médias servent aussi à l'expression des préoccupations individuelles ou collectives concernant les opérations elles-mêmes. Les objectifs, l'opportunité, les moyens et les techniques employés, la maîtrise de la violence, constituent des domaines souvent abordés par l'opinion publique et par les médias. Son impact sur l'activité de programmation et de conduite des opérations militaires est énorme et ne cessera de s'amplifier. Une intervention peut être condamnée à l'échec, d'un point de vue de l'opinion publique, même avant le déclenchement des actions militaires.

Les officiers de PA sont généralement responsables :

- d'assister le commandant dans les tâches d'obtention de la confiance et de l'appui du public à l'opération;
- de faciliter l'accès des médias indépendants aux unités et aux soldats de la force;

de présenter une information juste et crédible qui raconte les événements d'une façon complète, précise et rapide.

La mission des Affaires Publiques ne doit pas se limiter à la communication extérieure. Parfois des gros ennuis résultent d'un manque d'information interne: un soldat participant à des opérations à l'extérieur qui affirme , devant les cameras « je ne sais pas ce que je fais ici » affecte sérieusement la crédibilité d'une opération militaire. Le programme d'information interne du commandement de la force, arrêté en collaboration avec les Affaires Publiques constitue le bon ciment pour le bâtiment des opérations d'information. En plus ce mécanisme permet de faire face aux campagnes de désinformation mises en place par l'adversaire.

CONCLUSION

La révolution des affaires militaires conduite par les Etats-Unis visant la dominance de l'information, est la conséquence d'un énorme effort d'investissement dans le domaine des nouvelles technologies, mais surtout de l'investissement dans la réflexion portant sur les niveaux stratégique, opérationnel et tactique de la défense. Cette surabondance de réflexion comporte aussi des risques: on peut trouver des petites nuances dans les concepts de guerre de l'information des différents organismes de la défense américaine.

La médiatisation croissante des opérations militaires implique que leur succès dépend, aujourd'hui, des acteurs qui interagissent dans un environnement d'information plus global. La doctrine opérationnelle américaine valorise donc les opérations des affaires civilo-militaires et des affaires publiques, opérations destinées à influencer favorablement ces acteurs.

Pour maîtriser l'information dans les théâtres d'opérations du futur, les forces américaines exploiteront les aspects doctrinaires offensifs et défensifs de la Guerre de Commandement et de Contrôle. Les cas qui ont été étudiés, montrent l'efficacité des moyens d'attaque de C2 employés par les américains en Irak et en Haïti. Toutefois, la faiblesse des moyens d'attaque de C2 de ses adversaires, ne permet pas de conclure sur la capacité actuelle américaine en protection de C2.

La cohérence entre les moyens disponibles et la doctrine de son emploi constitue le grand objectif de la puissance militaire américaine en cette fin de siècle. Les Etats-Unis ont pris conscience que la supériorité acquise dans le domaine de l'information garantira une grande liberté d'action à son instrument militaire.

BIBLIOGRAPHIE

BARTLETT, Henry C., *Force Planning, Military Revolutions and the Tyranny of Technology*, Strategic Review, Fall 1996

BROWN, Stephen D., *PSYOP in Operation Uphold Democracy*, Military Review, September-October 1996

CENTNER, Christopher M., *Precision-Guided Propaganda: Exploiting the US Information Advantage in Peacetime*, Strategic Review, Spring 1997

FM 100-6, *Information Operations*, TRADOC US ARMY, August 1996

GRAY, Chris Hables, *Postmodern War, the new politics of conflicts*, The Guilford Press, New York 1997

JCS - Joint Chiefs of Staff, *Joint Vision 2010*, JCS Publication, 1997
MURPHY, LCL Dennis M., *Information Operations on the Nontraditional Field*, Military Review, November-December 1996

STARRY, Colonel Michael D., *Information Operations*, Military Review, November-December 1996

STEIN, Professor George J., *Information Attack: Information Warfare in 2025,* Research Paper presented to Air Force 2025, Air War College, August 1996

Troisième partie

L'INTELLIGENCE ECONOMIQUE OU LA REVOLUTION DANS LES AFFAIRES ECONOMIQUES

"Se faire battre est excusable; se faire surprendre est impardonnable" NAPOLEON

INTRODUCTION

Le théâtre de la guerre de l'information, comme celui de la guerre elle-même, se déplace de plus en plus sur le terrain économique. De tout temps l'activité humaine destinée à produire de la valeur ajoutée a nécessité une connaissance de l'environnement dans lequel les biens et services sont produits, vendus, utilisés. Néanmoins l'accélération récente du progrès a suscité une démarche nouvelle dans la plupart des pays industrialisés, véritable révolution dans les affaires économiques: il s'agit de l'intelligence économique.

Nous examinerons d'abord en quoi l'intelligence économique est une façon radicalement nouvelle d'élaborer une stratégie économique et quels en sont les principaux outils, avant d'aborder le point de vue des entreprises qui sont les premières concernées. En partant du cas américain, nous montrerons ensuite comment l'Etat français a donné une impulsion à ce concept, à la fois pour sa propre administration et pour les entreprises. A travers ses différents éclairages, nous espérons montrer comment les spécificités culturelles françaises sont souvent un obstacle au développement de l'intelligence économique en France.

1. L'EMERGENCE RECENTE DE L'INTELLIGENCE ECONOMIQUE

De multiples définitions de l'intelligence économique existent. Certains contestent même le vocable "d'intelligence" qu'ils assimilent au terme anglo-saxon signifiant renseignement. La plupart des experts sont d'accord sur le fait que l'intelligence économique est une discipline qui a pour objet de collecter, de trier et d'analyser des informations utiles à l'entreprise pour prendre des décisions stratégiques. Ces informations de nature économiques, concurrentielles, technologiques, juridiques, permettent à l'entreprise de "sentir" son environnement économique et ses évolutions afin d'anticiper les bonnes décisions. La plupart des Etats industrialisés (notamment Etats-Unis, Japon, Allemagne, Suède, et la France plus récemment) se sont également emparés de cette méthodologie, à la fois pour accompagner les entreprises, mais également pour leur usage propre.

L'intelligence économique n'est pas un concept inventé par quelques cabinets de conseil à la recherche de nouveaux débouchés. En fait, les récentes évolutions des technologies de traitement de l'information ont révolutionné la façon d'aborder la connaissance des marchés pour les entreprises et comme souvent, la technologie a fait évoluer la doctrine.

Quatre facteurs sont à retenir :

1. Tout d'abord **l'accélération du temps** qui rend les échanges économiques d'autant plus rapides que les flux financiers s'échangent aux quatre coins de la planète à la vitesse de la lumière. Le cycle de vie des produits s'est par ailleurs considérablement raccourci et l'on a coutume de dire que la moitié des produits et services qui existeront dans dix ans restent à inventer. La rapidité de réaction est désormais un avantage majeur pour toute entreprise qui peut être condamnée à l'obsolescence de ses activités en quelques années faute d'avoir anticipé l'évolution du marché.

2. **La concurrence désormais mondiale** sur presque tous les marchés de biens et de services nécessite des connaissances étendues sur des concurrents parfois lointains géographiquement, dont on connaît mal la langue et la culture. Ces transformations résultent en particulier de la recomposition du monde en nouvelles communautés économiques régionales après l'éclatement du bloc communiste.

3. L'information est devenue **une matière première essentielle**, au même titre que l'énergie et les matériaux : elle est en effet produite, stockée, extraite puis retravaillée et constitue désormais une des richesses de l'entreprise. Sa maîtrise devient essentielle dans tous les secteurs économiques.

4. Enfin **l'essor des technologies de l'information**, qui grâce aux algorithmes de numérisation et aux progrès de la micro-électronique a permis de produire, de stocker et de transmettre tout type d'informations : texte, sons, images, données.

1.1 Un art pourtant difficile

Un industriel déclarait lors d'un récent colloque sur l'intelligence économique que "**l'intelligence économique est l'art de mesurer les signaux faibles**". En effet tout le monde reconnaît que le problème n'est pas aujourd'hui l'accès à l'information mais la sélection de l'information utile qui doit arriver au bon moment sur le bureau du décideur qui en a réellement besoin. Bien des ouvrages récents sur l'intelligence économique ne sont cependant que des plaidoyers destinés à des décideurs d'entreprise pourtant fort bien payés pour montrer la voie. On peut également regretter que les nombreux séminaires, toujours confortables, tâtonnent entre des discours de Café du Commerce, avec ou sans bon sens, et des élucubrations informatico-linguistiques illustrant la magie des techniciens.

Les professionnels eux-mêmes manquent de crédibilité : après tout ni Michael Gorbatchev, ex-patron du KGB ni George Bush, ex-patron de la CIA, n'ont prévu l'implosion du communisme et la fin d'une guerre froide qui, durant quarante ans, a mobilisé tant de ressources. "La situation de l'intelligence économique est désespérée mais peut-être pas sérieuse" pourrait-on dire. L'intelligence économique servant à éclairer les décisions stratégiques doit ainsi ramener à la modestie tous les experts de l'art de la prévision.

1.2 L'information, un atout stratégique

La période contemporaine a pu être qualifiée de "mondialisation conflictuelle propice à l'usage de toutes les formes de renseignement". Le développement sans précédent des systèmes d'information, conjugué avec les bouleversements politiques et culturels des économies désormais interdépendantes, a placé l'information au rang de matière première stratégique. L'information, c'est le savoir. Le savoir, c'est le pouvoir. De sa maîtrise dépend à terme la préservation de notre identité nationale, à travers notamment celle des savoir-faire scientifique et technologique de nos entreprises et de nos collectivités. L'enjeu de la cohésion sociale lui-même est aussi à ce prix.

L'information doit apporter aux décideurs des entreprises un meilleur contrôle des paramètres de l'efficacité. S'engager sur un marché suppose de le connaître sous tous ses aspects : politiques, culturels, technologiques et concurrentiels, afin d'anticiper les difficultés et d'exploiter les opportunités. C'est peut être la grande leçon de l'intelligence économique, **la compréhension globale du marché**. L'une des fonctions de la veille technologique et concurrentielle est de **créer de la clarté**, de faire apparaître des enjeux, des stratégies sous-tendues par la réalité du marché, et d'amener ainsi les dirigeants à prendre leurs décisions avec un maximum de certitudes, en confrontant leur expérience à des données externes fiables et contrôlées. On ne saurait trop rappeler que l'information est **un puissant réducteur de risque**, un moyen d'éclairer l'avenir; elle s'affirme donc comme **une matière première de la stratégie**.

La principale limite de cette ressource est la difficulté de saisir de façon simple, compréhensible et utilisable un volume d'informations rendu très important par l'extrême complexité des marchés. A quoi sert de stocker une information sur support papier ou informatisé sans en tirer profit ? Comment l'utiliser quand le simple temps de consultation et d'analyse dépasse celui disponible pour définir la stratégie et contrer une action concurrente ? Ainsi les nouveaux réseaux de communication (Internet, base de données professionnelles en ligne), rendus accessibles par tous, ont soulevé plus de problèmes qu'ils n'en ont résolus, et rendu désuètes les stratégies reposant sur les méthodes du renseignement "classique".
La réponse se trouve dans les buts et la clarté de la stratégie qui permettent seuls de qualifier l'information, de la trier et de la rendre utilisable en fonction de son degré de cohérence et de proximité avec les impératifs définis, par la stratégie. Comme toujours "il n'est pas de vent favorable à qui ne sait où aller". Ainsi la réflexion sur la veille concurrentielle et technologique, dont la question de base est toujours : "que voulons-nous savoir ?", se heurte-t-elle souvent au manque de réponse à la question préalable : "que voulons-nous atteindre ?". Sans réponse à cette dernière, le champ d'investigation sur les nouveaux systèmes d'information est tel qu'on s'y perd.

En conséquence, le décideur français fait généralement face au dilemme suivant : décider vite sur la base de son expérience (c'est-à-dire d'un modèle qui peut être obsolète) ou consacrer le temps nécessaire à une information suffisante et arrêter ensuite sa stratégie. Dans bien des cas, on le sait, la première solution prend le pas sur une réflexion stratégique structurée. Par ailleurs, on observe fréquemment une confusion entre la connaissance académique (que rejettent les opérationnels) et les informations nécessaires à l'action.

La primauté du savoir pour le savoir est un mal français très fortement ancré dans les mentalités. Il importe de passer du "savoir pour savoir" au "savoir pour agir".

Le premier volet de l'intelligence économique est celui de l'information stratégique, c'est-à-dire de l'information dont les dirigeants, privés et publics, ont besoin pour prendre à temps les meilleures décisions en matière de recherche et de développement, d'investissements, de partenariats, de contrats... Si l'importance de l'information est une donnée permanente de l'histoire, son rôle est aujourd'hui modifié. Dans une économie qui vit à l'échelle planétaire, où la qualité et la rapidité des transmissions et des transports effacent l'espace et le temps, aiguisent la concurrence et assurent une circulation sans entrave des technologies et des capitaux, l'information évolue et s'échange sans cesse. L'Etat et les entreprises sont conduits à regarder au-delà de l'hexagone et à déployer en permanence leurs capteurs dans tous les domaines et dans le monde entier. Le développement d'Internet, du multimédia et bientôt des autoroutes de l'information, fondés sur la numérisation de la compression des données, ouvre la voie à la mondialisation de l'information, forme la plus accomplie de la mondialisation des échanges.

Pour avoir pris conscience les premiers de cette nouvelle exigence, des pays aussi différents que le Japon, la Suède, la Corée et Israël ont atteint le degré de développement qu'on leur connaît. Aujourd'hui l'Allemagne, le Royaume-Uni, les Etats-Unis s'appuient eux aussi sur une stratégie de conquête par l'information.

2. LES OUTILS TECHNIQUES

S'il est difficile d'évaluer le marché de l'intelligence économique, on observe toutefois une éclosion de sociétés de conseil dans ce domaine. Et des outils qui permettent de s'y retrouver dans des centaines de millions d'informations. *"La difficulté est de trier l'utile de l'inutile pour provoquer les décisions",* précise Bruno Martinet, directeur de l'intelligence économique du groupe Ciments Français. Il existe sur le marché pas moins de 50 moteurs puissants utilisables dans le cadre de l'intelligence économique[27].

"La sélection des sources est compliquée par la multiplication des serveurs, même si la part des banques de données dans les sources ouvertes diminue au profit des publications généralistes", constate Laurent Le Foll, directeur général de Verity France.

L'avantage essentiel des outils est de renverser le processus d'acquisition et de traitement de l'information : *"Avec Internet, on passe 70% du temps à chercher, 30% à parcourir les documents trouvés et seulement 10% à lire les bons documents,* estime Laurent Le Foll, *avec des info-agents, on passe 30% du temps à chercher et 70% à lire les bons documents qui ont été filtrés au préalable".*

Comme le signale l'ADIT, l'avenir appartient aux robots de recherche, qui exploiteront 24h/24h les réseaux mondiaux à la recherche de l'information, réaliseront une analyse sémantique de l'information, et par différents recoupements en déduiront l'information utile pour l'entreprise.

---

[27] Les moteurs les plus connus sur Internet s'appellent Yahoo, Altavista, Metacrawler, Lycos. Malgré une indexation automatique des nouveaux serveurs qui apparaissent, on estime aujourd'hui que le meilleur des moteurs de recherche sur Internet ne couvre que 30% de l'information présente sur le Web. On trouve également sur le marché professionnel des outils d'analyse sémantique des documents, qui à l'origine ont souvent été développés pour les services spéciaux.

A ce sujet, il convient de signaler le caractère inquiétant de la fuite vers les Etats-Unis des petites sociétés françaises de logiciel spécialisé de recherche documentaire.

3. UN OUTIL AU SERVICE DES ENTREPRISES

L'intelligence économique est d'abord, rappelons-le, un outil au service des entreprises, même si, on le verra, l'Etat peut utiliser cette méthode de travail soit à son profit, soit à celui des entreprises elles-mêmes. Rappelons les principaux domaines de veille qui sont à couvrir par l'entreprise, et qui sont désormais très étendues :

- Veille technologique : brevets, équipements, produits sensibles
- Veille commerciale : clients, concurrents, fournisseurs, capacités et comportements, projets.
- Veille économique : facteurs offre-demande, croissance, équilibres et déséquilibres, études sectorielles, études pays

Veille socio-politique : comportements des acteurs politiques, valeurs et règles, institutions, conflits, risques, insécurité, coopération

Les étapes principales du processus de veille sont :

- S'informer : via les médias, les banques de données, les réseaux, les enquêtes
- Comprendre, expliquer, prévoir : par l'analyse, l'évaluation, la prévision, la prospective
- Décider : en fonction des opportunités, des risques et des modalités
- Agir : éviter, prévenir, se protéger, s'assurer, exploiter

En résumé, la nécessité pour l'entreprise de réagir vite face à des concurrents mondiaux qu'elle doit connaître, de maîtriser son patrimoine immatériel que constitue son savoir-faire, ses processus, ses brevets, lui impose de mettre en place une cellule d'intelligence économique chargée de jouer les "vigies" au profit du capitaine d'entreprise. L'intelligence économique est plus simplement un outil d'aide à la décision, mais qui repose sur des hommes formés, une méthodologie, et des technologies de plus en plus sophistiquées.

En cela la décision du manager ne s'éloigne pas tellement du chef militaire, qui avant d'engager les opérations, se doit de mener le recueil et l'exploitation du renseignement. Mais la comparaison s'arrête là : en économie il n'y a pas de morts, même si certains ont assimilé les chômeurs aux victimes de la guerre économique, les médias aimant les métaphores guerrières qui frappent l'imagination du grand public. Il ne faut pas non plus confondre l'intelligence économique avec le renseignement, qui est l'art de collecter et d'exploiter des informations fermées, protégées, par des moyens qui peuvent ne pas être légaux. Il faut dire encore une fois que le vocable "intelligence" a semé le doute car son équivalent anglais signifie précisément renseignement. Mais la différence fondamentale est que l'intelligence économique s'inscrit dans un strict cadre déontologique, où seule l'information ouverte doit être recherchée. Bien sûr seuls les naïfs croiront que l'ère de l'espionnage industriel a laissé la place à celle de l'intelligence économique. En fait ces deux activités sont menées en parallèle, mais les maîtres à penser de l'intelligence économique reconnaissent tous que la recherche de l'information ouverte ne répond pas du tout aux mêmes méthodes de recueil et de traitement que celles de l'espionnage industriel, même si l'information fermée peut évidemment participer à une prise de décision.

Après tout, les rapports entre l'intelligence économique et le renseignement militaire sont parfois assez étroits (industries de défense, matières premières et technologies d'intérêt stratégique, psychologie des décideurs). Et ces rapports se sont nettement accrus depuis la démobilisation de la Guerre Froide et la présidence de Bill Clinton, comme on le verra plus loin.

Pour l'entreprise, l'information stratégique porte pour l'essentiel sur deux domaines : d'un côté les marchés, les produits et la concurrence, de l'autre les techniques et les savoir-faire. Elle constitue une matière première essentielle, bien qu'elle ne soit ni considérée comme un facteur de production, ni prise en compte dans le bilan de l'entreprise. Et l'offre d'information stratégique est plus importante que la demande : notre pays, troisième producteur mondial d'informations, en est seulement le seizième consommateur. Cette information peut être acquise au moindre coût, dès que possible et par des moyens légaux partout où elle est disponible. Elle permet de répondre à plus de 90 % des questions que se posent les entreprises. Aujourd'hui les nouvelles techniques offrent des outils de conservation, de collecte ou de traitement de l'information qui confèrent un avantage déterminant à ceux qui les maîtrisent.

3.1 La nécessité d'un management adapté

Par ailleurs les spécificités culturelles du management français ne sont pas un atout de ce point de vue : **la culture des entreprises françaises reste dominée par celle de l'ingénieur et de l'excellence technologique** (l'élégance de la solution, la beauté du prototype). Elle se révèle peu propice à la mise en place spontanée de moyens de surveillance des marchés et de leur environnement. "Pourquoi aller chercher ailleurs ce qu'on peut inventer nous-mêmes" reste la devise de l'ingénieur français, à l'opposé de celle de son collègue japonais. Celle de l'américain restant toujours "Fabriquons ce qui se vendra".

En France, l'élaboration d'une planification concernant le renseignement et la prévision est considérée comme un luxe, alors qu'une politique de couverture coûteuse est développée par ailleurs (assurances, entente avec le pays hôte...), assortie parfois de demandes de renseignements officieux auprès de telle ou telle administration.

En France, les entreprises les plus avancées en intelligence économique relèvent des secteurs confrontés à une forte concurrence dans des marchés de masse (agro-alimentaire, cosmétiques...). On les rencontre aussi (et paradoxalement) dans le secteur de l'armement où les mécanismes de décision ont toujours dépassé la prise en compte des seules fonctions d'un produit et où la logique de marché a longtemps été secondaire par rapport à la signification politique des contrats. Dans ce secteur, les entreprises ont multiplié leurs liens avec les réseaux diplomatiques et les services spécialisés. Protégées ou dispensées du jeu du marché, elles ont en contrepartie développé une culture dominée par l'excellence du produit technologique où la logique financière, sans être négligée, demeurait secondaire. Certains industriels se considèrent même dégagés des impératifs de rentabilité et de compétitivité, les risques demeurant couverts par des structures d'Etat (banques, offices, assurances). En conséquence, nos entreprises de défense se révèlent aujourd'hui moins performantes commercialement que certains de leurs concurrents internationaux, ce qui est grave car les règles du marché s'appliquent de plus en plus au secteur de l'armement.

L'intelligence économique ne correspond pas seulement à la constitution d'un système de veille informative, certes nécessaire, mais qui n'est qu'un moyen. Elle combine information et action, grâce à sa capacité à détecter des occasions et à développer des stratégies offensives. Elle a pour but de préparer le marché à l'action de l'entreprise (compréhension des mécanismes de décision locaux et des spécificités culturelles, pénétration des milieux d'affaires, opérations d'influence) et cherche à utiliser à son avantage les règles du jeu. Elle va au-delà d'une simple logique commerciale pour influer sur les multiples ressorts des choix, car il ne suffit plus d'être le plus compétitif sur ses domaines pour gagner. Il faut désormais être le plus innovant en stratégie globale, savoir maîtriser la complexité et développer des actions d'influence précises.

Dans certaines industries, la résistance à l'intégration systématique de l'information dans la décision relève de plusieurs facteurs :

- une culture "maison" marquée par le secret, ce qui a une incidence réelle sur les mentalités et les processus d'accès à l'information : "je ne veux pas dévoiler mon ignorance"
- l'idée que la formation et l'expérience professionnelles de nombreux cadres les exemptent de toute recherche préalable d'information : "je n'en ai pas besoin"
- la méfiance réelle vis-à-vis de l'intelligence économique assimilée à de l'espionnage industriel : "je ne veux pas me compromettre"
- la prérogative liée au rang ou à la fonction dans l'accès à l'information, reflet du pouvoir : "je n'en suis pas responsable"

La performance d'une entreprise est aujourd'hui fondée sur la clarté de ses buts et sur la connaissance de l'environnement concurrentiel qu'elle aura à combattre, faute de quoi toute stratégie (mobilisation des moyens et ressources dans le temps et l'espace au service des buts arrêtés) sera vaine. Certes, seul un travail soutenu d'intelligence économique peut apporter à l'entreprise la matière première de sa réflexion stratégique, puis en cours d'action les éléments indispensables d'évaluation et de réalignement face aux évolutions du marché. Cependant, sans stratégie définie au plus haut niveau de l'entreprise, l'information ne saurait avoir de signification.

Comparées à leurs grands concurrents, les entreprises françaises paraissent manquer d'expérience sur la stratégie, non pas sur la définition des buts (exercice conceptuel que nous concevons presque comme une prérogative), mais sur la définition des modalités d'exécution qui permettront d'atteindre ces buts. Tout se passe comme si les décideurs français n'accordaient pas aux notions d'objectifs et de stratégie le crédit que d'autres leur reconnaissent. Sans doute peut-on voir là un double héritage. D'une part, celui d'une culture rurale, agraire, qui prône l'excellence du geste (semer) et se soumet à l'idée que le résultat (la moisson) dépend aussi des cycles naturels, du hasard ou de la nature. "Nous avons fait ce que nous devions faire et si le résultat n'est pas là nul n'est à blâmer..."; une position souvent soutenue en France et que contestent les cultures centrées sur le résultat.

D'autre part, il y a la tradition romaine qui valorise l'efficacité des systèmes au détriment de l'initiative individuelle. Ainsi, "changer de mentalité", en France, se limite-t-il souvent à "repenser l'organisation", et à s'en tenir là, c'est-à-dire au système. Le changement vient en priorité de ce qui échappe à celui-ci : il faut savoir l'admettre.

Pourtant développer l'intelligence économique au sein de l'entreprise est un moyen puissant de donner du sens à des menaces externes souvent jugées trop théoriques. Il importe donc que la fonction soit créée et que son interaction avec le reste de l'organisation soit considérée non seulement comme un moyen de concevoir de bonnes stratégies, mais encore comme un levier de changement des mentalités internes. Elle doit pour cela être reconnue comme indispensable et disposer des ressources nécessaires à son efficacité. Isolée, la fonction perd de son sens et de son efficacité; maillée au reste de l'entreprise, elle capte, organise et dissémine l'information.

Le développement de l'intelligence économique au sein de l'entreprise permet également de favoriser l'ouverture internationale, qui est un formidable moyen de prise de conscience. Une entreprise soudain confrontée à d'autres cultures, d'autres façons de penser et d'agir, améliore ses méthodes et peut s'interroger sur ses propres scléroses, soudain mises en lumière. Il s'agit, en s'ouvrant, de s'enrichir sans se déstabiliser. Les partenariats bilatéraux ou multilatéraux, la participation à des réflexions internationales, le recrutement de cadres non nationaux sont autant de moyens d'ouvrir l'esprit et de laisser les idées extérieures pénétrer l'entreprise. Ces projets eux-mêmes doivent être conçus et présentés dans l'entreprise comme des modes de fonctionnement qui iront en se généralisant. Ils sont en soi des agents de changement efficaces.

L'intelligence économique n'est pas une nouvelle notion qui vient s'ajouter à des pratiques existant dans le domaine de la stratégie : c'est un renouveau de la démarche informative qui nourrit et éclaire en temps réel le processus analyse-décision-action. Quant à la réflexion stratégique, laquelle demeure en France victime d'un désintérêt relatif, il s'agit d'en étendre la pratique et d'en professionnaliser le cadre conceptuel et la mise en oeuvre, aussi bien sur le marché qu'au sein de l'entreprise.

Le recours accru à ces moyens est rendu nécessaire par la généralisation de la compétition économique, par la montée en puissance de la concurrence internationale et par l'extraordinaire occasion que constitue l'entrée de nos sociétés dans l'ère de l'information. Les gagnants seront ceux qui sauront passer d'une simple veille technologique et concurrentielle à un processus complet de formulation stratégique. L'intelligence économique et la réflexion stratégique sont les leviers qui permettront à nos industries de maintenir et de développer, sur la scène internationale, seules et en partenariat, la remarquable base industrielle et technologique de défense constituée jusqu'à ce jour.

Le management de l'information n'est pas encore entré dans les moeurs. Les obstacles se situent à la fois sur le plan du management, de la motivation, des structures peu flexibles des entreprises européennes et de la difficulté d'extraire l'information stratégique. Une évolution des méthodes et des mentalités semble donc indispensable. Un tel changement nécessite de profondes remises en cause et ne pourra avoir lieu sans la création d'une véritable culture stratégique.

4. LE CAS AMERICAIN

Aux Etats-Unis le président Clinton s'investit quotidiennement dans la promotion des intérêts économiques de son pays dans le monde. En 1992, il a créé à cet effet le Conseil économique national (NEC) qui lui est directement rattaché et qui a pris une importance comparable à celle du Conseil national de sécurité. Réuni régulièrement sous son autorité, le NEC conseille en particulier le président sur les orientations de la diplomatie économique dont les entreprises françaises vivent chaque jour la réalité de l'efficacité sur les marchés européens et internationaux.

L'aboutissement de cette volonté politique s'exprime aujourd'hui à travers les offensives de diplomatie mobilisant l'administration américaine au service des entreprises sur les marchés internationaux. C'est également dans cet état d'esprit qu'a été élaborée la stratégie nationale à l'exportation conçue par le Secrétaire américain au Commerce, Ron Brown. Lancée en septembre 1993, cette stratégie a pour axe principal l'établissement d'un réseau de coordination des efforts afin de développer un système efficace en coordination étroite avec le secteur privé dans le cadre de la politique extérieure globale des Etats-Unis. Elle repose à cette fin sur une volonté de coordination accrue entre l'action de l'administration nationale, locale et internationale et les besoins des entreprises.

Cette stratégie repose sur un réseau administratif dense et coordonné dont les principaux acteurs sont : le Centre de promotion (Advocacy Center), les Centres d'assistance à l'exportation, le réseau des experts de l'US and Foreign commercial service et le réseau des fonctionnaires américains dans les organismes internationaux. La "War Room" de l'administration américaine du commerce constitue le cœur stratégique d'un réseau d'appui aux entreprises, aujourd'hui en action. Instrument central de surveillance permanente des grands projets, elle est le réceptacle des demandes et le lieu de préparation des missions ministérielles.

Ce dispositif rapproché permet au président américain de mobiliser l'ensemble de son administration en appui des priorités définies et de l'intérêt national partout dans le monde où cela s'avère nécessaire. L'administration américaine démontre ainsi un soutien déterminé à l'exportation en appui des entreprises nationales et n'hésite pas à évoquer les exemples de réussite de ces interventions qui ont notamment abouti à évincer Thomson CSF du projet brésilien SIVAM.

5. LE CAS JAPONAIS

Le Japon est connu pour un dispositif de recueil de l'information particulièrement performant, grâce à la mobilisation de chaque japonais, véritable "réseau humain international". Mais c'est surtout un dispositif étatique reposant principalement sur le MITI et son organe international le JETRO (Japan External Trade Organization), ainsi que son organisme de recherche l'AIST (Agency of Industrial Science and Technology). Le Japon envoie de plus de jeunes fonctionnaires se former à l'étranger. Mais on ne saurait oublier les données culturelles favorables au développement de l'intelligence économique : la petitesse de l'espace vital sur l'archipel japonais a toujours obligé ceux-ci à coopérer entre eux et à travailler en groupe, et l'isolement du reste du monde pendant tout le XVII et XVIIIème siècle, qui est à l'origine de la curiosité japonaise.

6. UN OUTIL AU SERVICE DE L'ETAT

L'intelligence économique est aussi au service de la cohésion sociale. L'instauration de relations entre l'Etat et les acteurs économiques et sociaux adaptées aux enjeux mondiaux de la compétitivité participent, par le développement économique, au maintien du tissu social.

Elle est également au service de l'Etat. La définition de politiques et de stratégies, la mise en cohérence de modes d'organisation et de travail au sein du gouvernement et de l'administration visent à augmenter la performance économique de la France notamment par une meilleure circulation de l'information et une collaboration interministérielle plus fréquente. En ce sens, l'intelligence économique est un levier de réforme de l'Etat.

Or la France, malgré ses atouts économiques, est en retard sur le plan de l'intelligence économique. Celle-ci s'accommode en effet mal des modes d'organisation hiérarchiques, cloisonnés, où pouvoir rime avec savoir. **L'intelligence économique est avant tout un mode de management impliquant une circulation de l'information descendante et ascendante, mais aussi transverse afin que tout décideur, quel que soit son niveau, puisse avoir accès aux informations**.

Le Président de la République, devant l'IHEDN le 8 juin 1996 en fait un enjeu national :

"Dans ce monde différent, affranchi de la logique des blocs, les ressorts de la puissance deviennent plus variés : au poids du nombre ou des armes s'ajoutent de plus en plus, la capacité économique, le potentiel scientifique et technique, l'aptitude à l'innovation dans tous les domaines...Si nous ne parvenons pas à mesurer pleinement l'ampleur de la mutation engagée, si nous n'avions pas assez de détermination pour en tirer toutes les conséquences, nous serions très rapidement condamnés à subir les événements au lieu de contribuer à les façonner."

Les années récentes ont vu se développer le sentiment que la puissance d'une nation se traduit en termes économiques, industriels, scientifiques et technologiques, plus que militaires. Cette perception nouvelle a trouvé un premier écho dans le développement de l'intelligence économique qui a pour ambition de rassembler et de traiter l'information au service des décideurs, de renforcer la sécurité de notre patrimoine technologique et plus généralement de développer l'influence de notre pays dans le monde. Pour l'Etat, principal acteur économique, le problème de l'information dans les secteurs scientifiques, technologiques, économiques et financiers revêt la même importance et pose les mêmes questions. L'Etat dispose-t-il aujourd'hui des informations dont il a besoin pour prendre les bonnes décisions ? Le niveau politique est-il satisfait de la qualité des informations qui lui sont apportées par les administrations ?

Pour le pays dans son ensemble, "économiquement plus intelligent" suppose que chacun soit davantage sensibilisé à l'importance du recueil de l'information, véritable patriotisme qui doit conduire chaque citoyen à être un veilleur au profit de son entreprise, son laboratoire, son administration. Une culture nationale de l'information serait un atout supplémentaire dans la coopération économique mondiale.

Il ne faut pas non plus négliger le volet "action d'influence" dans la démarche de l'intelligence économique. De quoi s'agit-il ? Concrètement, de convaincre, au niveau européen ou mondial, de la qualité de ses normes de production, d'utiliser l'information pour défendre ses intérêts, de placer des hommes de confiance aux postes stratégiques, de savoir agir efficacement au sein des structures et des organisations où se prennent les décisions commerciales ou technologiques majeures.

7. L'AIDE DES ADMINISTRATIONS AUX ENTREPRISES

Le 4 avril 1995, le *Journal officiel* a publié un décret en Conseil des ministres portant création d'un Comité pour la Compétitivité et la Sécurité Economique (CCSE) et, fait exceptionnel, précédé du rapport du Premier ministre au Président de la République explicitant les enjeux que présente pour la France la décision de se doter d'un dispositif national de gestion collective de l'information.

Pour la première fois, par cet acte fondateur, la France se dote, au plus haut niveau de l'Etat, d'une structure d'orientation stratégique en matière de compétitivité et de sécurité économique. Placé sous la présidence du Premier ministre, puis par délégation sous celle du ministre de l'Economie, des Finances et du Plan, le Comité pour la compétitivité et la sécurité économique est chargé de conseiller le gouvernement dans le domaine de l'intelligence économique. Mais il a aussi pour mission de définir les grandes priorités nationales en cette matière. D'éminentes personnalités, chefs d'entreprise et grands chercheurs ont été nommées membres du Comité pour conduire cette tâche ambitieuse. Le secrétaire du Comité est le Secrétariat Général de la Défense Nationale (SGDN) et le secrétaire exécutif l'Agence pour la Diffusion de l'Information Technologique (ADIT).

Ainsi notre pays a-t-il entrepris de se doter de la capacité lui permettant de se placer au niveau de ses partenaires et concurrents les plus performants au regard de la gestion collective de l'information scientifique, technique et économique au service des entreprises. En effet, la performance industrielle et commerciale des modèles d'organisation allemand, japonais ou américain se fonde sur une telle démarche d'intelligence économique et est probablement à l'origine d'une bonne partie des succès économiques de ces pays.

Cette dynamique repose certes sur de puissants appareils de production de données, mais avant tout sur la maîtrise de l'organisation de réseaux et de leur maillage stratégique. C'est au sein de ces dispositifs savamment maillés que s'échangent la connaissance, l'expertise et la compétence à la fois publiques et privées. Stratégie d'influence et pressions diplomatiques n'en deviennent alors que plus efficaces. Dès lors, de telles pratiques de la part de nos concurrents nous condamnent à l'efficacité et à la synergie des actions.

Le Comité pour la compétitivité et la sécurité économique représente le cœur d'un dispositif collectif plus ambitieux qui se met progressivement en place. En effet, à la demande du Premier ministre, le SGDN a proposé un dispositif national de compétitivité et de sécurité économique simple, évolutif, coordonné. C'est celui qu'il incombe aujourd'hui, à la fois aux administrations et aux entreprises, de bâtir et d'animer à travers une responsabilité collective. Ce dispositif est simple; il ne comporte aucune création de structure administrative nouvelle. L'enjeu repose bien sur la mobilisation des réseaux d'expertise et des foyers de compétence nationaux et locaux qu'il convient de valoriser, d'orienter.

Ce dispositif est coordonné; l'ensemble des actions mises en œuvre à partir des orientations du Comité sera conduit selon un objectif clair. L'administration, en toute circonstance, doit mieux répondre aux besoins en informations utiles, exprimés par l'ensemble des acteurs économiques, et en particulier par les PME-PMI, qui contribuent chaque jour de façon décisive à la création des richesses et de l'emploi de notre pays.

Par ailleurs, l'Agence pour la diffusion de l'information technologique constitue un acteur important du dispositif. Son contact de proximité avec les entreprises représente l'indispensable garantie que leurs besoins en informations seront analysés et satisfaits dans les meilleurs délais et les meilleures conditions.

Enfin, ce dispositif est évolutif. La garantie du succès du caractère opérationnel de ses actions ambitieuses repose en effet sur sa capacité à proposer et suivre un ensemble d'expériences nationales et locales. Ce caractère expérimental est essentiel, car il porte la garantie de tout apprentissage : la maîtrise progressive de la démarche, des objectifs opérationnels précis, une évaluation régulière.

Certains départements ont été désignés comme pilote pour mettre en oeuvre cette démarche d'intelligence économique, afin que celle-ci ne reste pas une pure démarche de cabinet ministériel. L'action d'intelligence économique s'élabore par exemple en Essonne, sous le parrainage du Comité pour la Compétitivité et la Sécurité Economique.

Opérations "pilotes" locales en France

Ainsi, dans le département de l'Essonne, une expérience de sensibilisation et de formation d'un échantillon représentatif d'entreprises à la démarche d'intelligence économique a été lancée. Les partenaires de cette première expérience nationale, la Chambre de Commerce et d'Industrie, le SGDN, la Préfecture, EDF-GDF, l'Agence pour la diffusion de l'information technologique, se sont fixés des objectifs de développement économique et d'emplois très clairs. Cette initiative expérimentale a vocation d'exemplarité nationale et déjà des régions Rhône-Alpes, Midi-Pyrénées sont sur les rangs pour conduire une expérience similaire, à l'initiative des préfets de région.

L'objectif recherché par l'opération pilote menée dans l'Essonne est de donner aux responsables d'entreprises du département la maîtrise de l'intelligence économique afin d'accroître leur compétitivité technologique. Cette opération pilote vise les petites et moyennes entreprises du département, sociétés en nom propre ou filialisées. Les moyens concrets mis en place sont la formation, l'information et une aide directe aux entreprises volontaires pour participer à cette action gratuite, d'environ 12 mois, qui comprend entre autres :

- des séminaires thématiques permettant d'aborder sur le fond les différents aspects de l'intelligence économique et son apport dans le domaine de la décision
- des cycles de formation portant sur la veille technologique, sur les méthodes de recueil, de sélection et d'exploitation de l'information, notamment par une meilleure approche des moyens modernes de l'informatique
- la diffusion sélective et régulière d'informations technologiques
- des audits, réalisés à la demande, conduits par des spécialistes en vue de faciliter la mise en place, au sein des entreprises, d'une cellule dédiée à l'intelligence économique.

Néanmoins la problématique de l'aide de l'Etat aux entreprises se heurte à deux difficultés selon la taille de l'entreprise. Pour ce qui est des grandes sociétés, disposant depuis longtemps de service de documentation, de veille économique, l'Etat n'a à apporter que peu de choses en intelligence économique. Pour ce qui est des petites sociétés, leur vrai besoin en informations est souvent très ciblé et l'Etat n'a pas les moyens de répondre à de multiples petites demandes particulières. Il faut néanmoins noter l'initiative de mise en place de serveurs d'informations générales sur l'administration française : AdmiFrance et Légafrance, véritables points d'entrée Internet des entreprises vers l'Etat.

8. LE ROLE DE L'ETAT A L'AVENIR

De l'acte fondateur du Comité pour la compétitivité et la sécurité économique et de l'organisation du nouveau dispositif, il convient de retenir deux éléments essentiels. Tout d'abord, le rôle de l'Etat, producteur de données d'analyses et de stratégies, ne saurait produire d'efficacité s'il n'est pas en permanence méticuleusement informé des besoins et des demandes des industriels. En second lieu, les nouveaux défis concurrentiels, mais aussi coopératifs, ne pourront être relevés sans une véritable stratégie collective de gestion de l'information associant étroitement la production des réseaux publics et privés dans ce domaine.

Il revient à l'Etat de penser plus encore ses missions de recueil, d'exploitation et de diffusion de l'information, au rythme de la concurrence. Les industriels ont besoin d'un véritable partenariat stratégique en ce domaine. Le dispositif d'appui aux entreprises, en termes d'informations élaborées et d'aide à la décision, existe. Des pôles de compétences et d'expertises constituent un "appareil de données" puissant et organisé.

Toutefois, aujourd'hui, l'efficacité des réponses aux défis de la concurrence ne peut advenir qu'au travers d'une responsabilité collective et partagée entre l'Etat et les entreprises dans le domaine du renseignement ouvert. C'est ainsi qu'il appartient aux industriels de formuler précisément et collectivement leurs besoins d'informations. Il revient aux entreprises de faire remonter vers les centres de compétence de l'Etat et de l'administration l'ensemble des alertes, des menaces, des ouvertures captées sur les marchés. L'optimisation des ressources en informations produites par l'administration en est l'enjeu. Il en est aussi de l'efficacité industrielle et concurrentielle sur les marchés à défendre et à prendre.

Une telle politique a trois fonctions essentielles :

- une fonction de maîtrise du patrimoine scientifique et technologique;
- une fonction d'identification des menaces et des ouvertures sur les marchés;
- une fonction d'élaboration de stratégies communes et stratégies d'influence au service de l'intérêt national, mais aussi des entreprises.

L'industrie automobile ou l'industrie pharmaceutique, par exemple, représentent en ce sens des secteurs stratégiques de notre économie. L'attention portée au développement de leur capacité de recherche et développement, comme la protection de leurs savoir-faire, sont prioritaires, ne serait-ce qu'au regard du nombre d'emplois qu'elles représentent.

Voilà un premier cadre de réflexion vers l'élaboration d'une doctrine nationale de sécurité économique active, mais l'ampleur des questions auxquelles il convient de répondre ne doit pas être méconnue : la nécessité de mieux organiser le recueil et le traitement de l'information ouverte, la définition d'un cadre juridique de protection des informations économiques et technologiques non classifiées et, enfin, l'indispensable prise en compte des contraintes juridiques du droit économique contemporain et notamment communautaire.

Ainsi, il revient à l'Etat et aux entreprises de dynamiser le cycle de l'information pour atteindre à l'élaboration de stratégies communes : il s'agit là de l'une des fonctions majeures de l'intelligence économique. Il reste à accomplir toutefois une tâche immense de mobilisation collective sur ce grand enjeu national que représente l'intelligence économique. Etat et entreprises doivent s'attacher sans défaillance à la nourrir chaque jour d'innovations partagées.

BIBLIOGRAPHIE

Philippe CLERC : Intelligence économique : enjeux et perspectives, (Rapport mondial sur l'information, UNESCO), avril 97

Jean-Louis LEVET : Sortir la France de l'impasse, Editions Economica, 1996

Henri MARTRE : Intelligence économique et stratégie des entreprises, Commissariat général du plan, mars 97

ALLAIN-DUPRE et DUHARD : Les armes secrètes de la décision, Editions GUALINO, 1997

QUATRIEME PARTIE

LA CRYPTOGRAPHIE: UN MOYEN DE PROTECTION EFFICACE POUR LES RESEAUX D'INFORMATION

INTRODUCTION

Les réseaux globaux d'information transforment notre société et facilitent la communication planétaire; grâce à Internet, les échanges de textes, photographies, sons et images vidéo sont possibles pour quiconque dispose d'un accès téléphonique. Le caractère transnational de ces réseaux pose dès lors le problème de la sécurité comme une des questions clés pour un développement viable de la société de l'information.

Face à une criminalité informatique croissante et de plus en plus efficace, la cryptologie est aujourd'hui le seul moyen qui permette d'assurer une protection efficace des réseaux ouverts.

La France dispose dans ce domaine d'une législation complète et originale en comparaison des autres pays.

Mais dans un contexte de guerre de l'information de plus en plus actif, notamment dans le domaine de la guerre économique, il nous faut examiner si certains Etats ne sont pas en train de développer une stratégie qui vise en fait à disposer de la maîtrise totale des nouvelles technologies de l'information.

1. LES MENACES

La criminalité informatique est un risque sous-estimé, et pourtant le « cyber-terrorisme »[28] est devenue une réalité face à laquelle les Etats se doivent d'apporter une réponse efficace.

Dans un contexte de mondialisation de l'économie et d'internationalisation des échanges, l'information devient un enjeu stratégique. Comme le souligne le célèbre futurologue Alvin Toffler « Qui détient le savoir détient le pouvoir »[29]. Le « village planétaire » est un lieu extraordinaire de dialogue et d'échanges d'informations de toute nature. Mais il présente une importante faiblesse: notre société est devenue totalement dépendante de ses technologies de l'information, et cette dépendance la rend de plus en plus vulnérable au terrorisme informatique.

[28] Lire à ce sujet l'article de Daniel Martin « Cyber-terrorisme: le nouveau péril », politique internationale, 9/97.

[29] « Guerre et contre-guerre: comment survivre à l'aube du XXI° siècle », Alvin et Heidi Toffler,1993.

1.1 Le terrorisme informatique: une réalité quotidienne.

Le terrorisme informatique est devenu une réalité quotidienne. Et le danger est suffisamment sérieux pour que les ministres du G8[30]décident d'adopter un plan d'action contre la criminalité informatique.[31].Comme le souligne le communiqué final, « à l'heure où les Etats deviennent de plus en plus dépendants de ces technologies, leur exploitation par des criminels maîtrisant les technologies de pointe constitue une menace encore plus importante pour la sécurité publique ».[32]

Régulièrement, la presse fait Etat d'intrusions au sein des ordinateurs du Pentagone pourtant réputés comme les mieux protégés de la planète. Ainsi, le Pentagone a reconnu qu'en 1996 ses ordinateurs ont fait l'objet de plus de 100 000 tentatives d'effraction, et le FBI estime qu'au moins sept pays étrangers forment des pirates informatiques contre les Etats-Unis, dans un but militaire ou commercial.[33] Les pertes dues aux attaques électroniques dans le monde ont, selon le FBI, atteint 7,5 milliards de dollars en 1996.[34] En fait, comme le souligne un juge fédéral américain spécialiste de la criminalité informatique, « Aujourd'hui, rien n'est impossible pour un *hacker*. C'est juste une question d'imagination ». Les criminels informatiques disposent en effet d'une vaste palette de méthodes et d'outils logiciels ou électroniques.

1.2. Les différentes méthodes de piratage informatique.

Avec la banalisation des outils de piratage et de destruction, n'importe qui peut aujourd'hui se transformer en *hacker*. Le Pentagone a évalué l'incidence de ces attaques sur les sites militaires américains: le taux de réussite serait de 88 %! De plus, seuls 4 % des sites attaqués ont repéré ces attaques, et moins de 0,5 % d'entre elles ont donné lieu à un rapport. Face à de telles agressions, il n'existe que deux parades: l'**attaque** et la **défense**.

S'agissant de la première, elle est du ressort des services de police compétents; la Gendarmerie Nationale a développé à cet égard une unité efficace pour débusquer les pirates informatiques. Concernant la solution défensive, les solutions classiques de protection physique de l'information sont devenues caduques en raison de l'interconnexion croissante et inéluctable, à l'échelle planétaire, des systèmes informatiques.

La croissance du réseau Internet est devenue une réalité en France aussi. Ainsi, selon la dernière enquête annuelle menée par UFB Locabail auprès des 250 000 entreprises de 6 à 200 salariés, 24% d'entre elles déclarent posséder au moins un accès à Internet, soit deux fois plus que l'année précédente. « Une telle progression n'a jamais été enregistrée, même lors des débuts de la micro ».[35]

---

[30] G8: groupe des 7 pays les plus industrialisés de la planète, auquel est venue s'ajouter la Russie.
[31] Réunion des ministres de l'intérieur et de la justice des pays membres du G8 à Washington les 9 et 10 décembre.1997
[32] Lire la revue « Documents d'actualité internationale », numéro 3, 1° février 1998.
[33] Voir Laurent Zecchini dans « Le Monde » du 12 décembre 1997
[34] Informatiques magazine, 1er novembre 1997.
[35] Echos du 5 mars 1998.

2. LES MOYENS DE PROTECTION POSSIBLES

Les moyens de protection sont divers et variés. Une de ces méthodes part du constat que tout matériel informatique, ainsi que les câbles et les fils électriques qui lui sont raccordés, rayonne des ondes électromagnétiques parasites susceptibles d'être interceptées en temps réel par toute personne malintentionnée. **L'anti-compromission électromagnétique** permet alors d'éviter cette interception d'informations classifiées à condition que les équipements soient soumis à une norme internationale, d'origine américaine, appelée Tempest. Une autre méthode, beaucoup moins coûteuse, consiste à appliquer les règles élémentaires de **sécurité informatique.**

Au temps où les informations étaient confinées dans un ordinateur central, la sécurité informatique était facile à assurer. Mais la réalité a changé. L'informatique est aujourd'hui distribuée sur des réseaux interconnectés à l'échelle mondiale. Le développement d'Internet est en train de modifier complètement les règles.

2.1 Internet: une ascension fulgurante.

Créé en 1969 à la demande du Pentagone, sous le nom d'ARPANET[36], ce réseau est réservé pendant une quinzaine d'années à un cercle restreint d'utilisateurs. Il faut attendre 1989, pour qu'un ingénieur du C.E.R.N.[37], Timothy Berners-lee, conçoive une interface d'utilisation simple et conviviale: le World Wide Web (WWW). Devenu entre temps Internet, il faut attendre l'apparition en 1993 du premier navigateur[38] pour qu'Internet connaisse son ascension fulgurante. On compte approximativement 30 millions de personnes connectées de par le monde, et les prévisions font Etat de 200 millions d'internautes en l'an 2000. La croissance du nombre de serveurs Internet de par le monde est d'ailleurs significative de cet extraordinaire essor.[39] Cette croissance concerne les sites Web, la messagerie électronique, les forums de discussion, mais aussi et surtout le commerce électronique.

2.2 L'essor du commerce électronique.

Pouvant être défini comme « l'ensemble des échanges numérisés, liés à des activités commerciales, entre entreprises, entre entreprises et particuliers ou entreprises et administrations »[40], le commerce électronique est appelé à connaître dans les années à venir un essor considérable.

Celui-ci représentait en France, en 1997, 45 millions de dollars d'échanges, devrait atteindre 4500 millions de dollars en 2001[41], soit une croissance de 1000 % d'ici 4 ans à peine! L'ampleur de ce phénomène est identique pour l'ensemble des pays de la l'union européenne.

---

[36] Advanced Research Project Agency
[37] Centre Européen de Recherche Nucléaire
[38] Logiciel permettant au néophyte en informatique de se promener en toute simplicité sur Internet.
[39] Voir figures en annexe 3
[40] Rapport du groupe de travail présidé par M. Francis LORENTZ sur le commerce électronique
[41] Ibid.

Le développement de telles transactions sur un réseau de plus en plus ouvert pose divers problèmes de sécurité relatifs notamment à l'authentification des parties qui communiquent, à l'intégrité des données communiquées, à la confidentialité des renseignements et à l'assurance que les transactions ont été autorisées par les utilisateurs légitimes. Ces conditions sont un préalable indispensable pour pouvoir « créer un environnement favorable à la compétitivité des entreprises françaises et générateur de confiance pour celles-ci et pour leurs clients »[42].

La **cryptographie** est alors le seul moyen existant aujourd'hui qui puisse répondre à ces besoins de sécurité. C'est pourquoi la cryptographie est au coeur des grands débats actuels, car elle conditionne en particulier les développements du commerce électronique.

2.3. La cryptographie

La **cryptographie** peut se définir comme l'art de dissimuler une information dont on désire assurer la confidentialité. Les méthodes cryptographiques modernes permettent le **chiffrement,** le **déchiffrement** et la **signature numérique.** Le **chiffrement** garantit la confidentialité. Autrement dit, il protège l'information contre toute divulgation non autorisée.

Les **signatures numériques**, analogues aux signatures manuscrites, remplissent trois autres fonctions:

- l'*authentification*: preuve que l'utilisateur est bien qui il prétend être,
- la *non répudiation*: preuve que la transaction a eu lieu ou que le message a bien été envoyé ou reçu; ni l'émetteur ni le destinataire ne peuvent donc nier l'échange,
- l'*intégrité*: les données ne peuvent être modifiées sans que ce soit décelable.

Lorsque le chiffrement est utilisé pour protéger les données au cours d'une communication, les entités communicantes doivent au préalable convenir d'une procédure de chiffrement, ce qui revient en fait à choisir une **clé de chiffrement** qui pourra être employée pour chiffrer, déchiffrer et vérifier les données numériques transmises. Or, avant d'envoyer les données chiffrées sur la ligne de transmission, la valeur de la clé doit suivre le même chemin. C'est pourquoi la gestion des clés de chiffrement est une tâche particulièrement cruciale puisque la sécurité globale du système repose sur ces clés.

Il existe principalement deux méthodes cryptographiques:

- la **cryptographie à clé secrète**,
- la **cryptographie à clé publique.**

[42] Ibid.

2.3.1. La cryptographie à clé secrète

Dans le cas de la cryptographie à **clé secrète**, les deux parties doivent au préalable se communiquer la clé unique qui sera utilisée aux fins de chiffrement et de déchiffrement. Cette méthode ne convient donc pas aux réseaux d'information ouverts de type Internet car si l'on a recours au chiffrement en raison de l'insécurité du canal de transmission, il parait évident qu'il ne faut pas transmettre la clé secrète par la même voie; n'importe qui pourrait en effet copier cette clé et déchiffrer toutes les informations.

2.3.2. La cryptographie à clé publique

La cryptographie à **clé publique** offre une solution à ce problème puisqu'elle prévoit l'utilisation d'une paire de clés différentes, quoique liées entre elles. Chaque utilisateur détient une clé secrète (ou privée) et une clé publique. La clé secrète demeure confidentielle et n'est connue que de l'utilisateur; l'autre clé peut être rendue publique et être transmise à chaque correspondant par l'intermédiaire du réseau, voire même publiée. La clé secrète permet au destinataire de déchiffrer les messages qui lui sont envoyés, mais l'expéditeur chiffre avec une clé différente qu'il est possible de rendre publique sans risque de compromission pour le système. Ce système est dit « asymétrique » car il fournit une communication sécurisée dans une direction seulement. l'établissement d'une communication sûre dans l'autre direction nécessite une seconde paire de clés.

L'avantage d'un système cryptographique à clés publiques est qu'il présente l'intérêt de ne pas nécessiter le transport d'une clé secrète entre l'expéditeur et le destinataire pour établir une communication chiffrée. Le système de cryptographie à clé publique présente cependant le défaut de ne pas assurer l'authentification: un intrus pourrait en effet utiliser la clé publique pour forger de faux messages. Il s'agit là d'une différence importante avec le système de cryptographie à clé secrète dans lequel l'expéditeur et le destinataire partagent une clé secrète qui les « unit ». L'absence d'authentification dans le chiffrement à clé publique peut être surmontée grâce à l'utilisation de la **signature numérique**.

2.3.3 La signature numérique

L'authentification des messages garantit au destinataire l'authenticité du message reçu par le fait que l'identité véritable de l'expéditeur d'une part est connue, et par le fait qu'une altération du message intervenue après son expédition peut être détectée. Les deux parties sont sûres qu'une tierce partie n'a pas pu s'immiscer dans la communication en insérant un message, ni travestir l'origine du message sans être détectée. Techniquement, les signatures numériques sont créées et vérifiées par des techniques cryptographiques similaires à celles utilisées pour le chiffrement. Deux clés complémentaires sont générées et assignées à un utilisateur. L'une d'elles - la clé de signature - reste secrète ("*clé privée*"), alors que l'autre - la clé de vérification de signature - est rendue publique. Il est évidemment essentiel que la clé privée ne puisse être calculée à partir de la clé publique.

Contrairement à la cryptographie utilisée à des fins de confidentialité, les signatures numériques sont annexées aux données et laissent le contenu intact. La vérification de l'authenticité et de l'intégrité des données ne prouve pas nécessairement l'identité du propriétaire de la clé publique. N'importe qui peut publier une clé publique sous un autre nom. C'est pourquoi le destinataire peut souhaiter obtenir des informations plus sûres concernant l'identité du propriétaire de la clé. Une telle information peut être fournie par le propriétaire de la clé en personne en fournissant au destinataire une preuve satisfaisante.

Dans le contexte des signatures numériques, ces tierces parties sont communément appelées *Autorités de certification*. Souvent, ces autorités sont confondues avec ce que l'on appelle les *Tiers de confiance* qui désignent en fait des autorités de certification auxquelles quelqu'un d'autre que le propriétaire de données fait appel.

2.3.4. L'efficacité de protection des systèmes cryptographiques

La grande majorité des systèmes de cryptographie utilisés aujourd'hui répond à une norme internationalement reconnue: la norme DES[43] C'est pourquoi on peut estimer que la solidité d'un tel produit est directement liée à la longueur de la clé de chiffrement associée. Il est usuellement admis que la limite se situe au niveau des clés à 56 bits: cette longueur de clé est certainement « cassable » dans des délais raisonnables par des organismes tels que la N.S.A.[44] puisque les Etats-Unis ne semblent pas vouloir imposer de restrictions à l'exportation pour les systèmes utilisant des longueurs de clés inférieures.

De même, une déclaration récente du gouvernement français semble conforter ce point de vue.[45] De plus, le directeur du FBI a signalé qu'un nombre croissant d'organisations criminelles utilisaient des clés à 56 bits. Au-delà, il semble admis qu'un code à 256 bits soit incassable dans la mesure où un tel algorithme générerait plus de solutions possibles qu'il n'existe de particules dans l'univers connu[46].

3. LA POLITIQUE DES DIFFERENTS ETATS EN MATIERE DE CHIFFREMENT

3.1 La politique française

3.1.1 La libéralisation de la réglementation

La totalité des moyens de cryptologie, que ceux-ci assurent des fonctions d'intégrité, de signature, d'authentification ou de confidentialité, a été, jusqu'en 1990, soumise à contrôle en ce qui concerne son *exportation*, sa fourniture ou son *usage*.

---

[43] DES: Data Encryption Standard
[44] National Security Agency
[45] Déclaration de M. Pierret, ministre de l'industrie, en date du 16 janvier.
[46] « Sécurité dans les réseaux informatiques », Davies D.W. et Price, éditions AFNOR, 1993.

L'utilisation détournée de ces techniques, considérées comme des matériels de guerre, représentait en effet un risque important pour la sécurité extérieure de l'Etat. La loi de 1990[47] est venue apporter un premier assouplissement en distinguant les moyens de cryptologie à usage militaire de ceux qui sont à usage civil, et en soumettant à un simple régime de déclaration les seuls moyens d'authentification et d'intégrité. Les autres moyens cryptographiques étaient soumis à un régime d'autorisation.

Avec le développement d'Internet, et la volonté clairement affichée par le gouvernement français de « Préparer l'entrée de la France dans la société de l'information », la France a décidé d'assouplir cette législation, notamment pour favoriser l'expansion du commerce électronique.[48] C'est pourquoi une nouvelle loi a été adoptée en 1996[49] dans le but de faciliter l'*usage* des moyens de cryptologie[50]. Cette loi libéralise complètement l'utilisation de moyens de cryptologie assurant l'*authentification*, la *garantie d'intégrité* et la *non répudiation* des messages (signature électronique). L'utilisation de la signature électronique est soumise à une déclaration simplifiée. Mais la véritable nouveauté de cette loi réside dans la création d'un système dit de tiers de confiance, car la France est le premier pays au monde à se doter d'un tel système (et le seul jusqu'à présent).

3.1.2 Le système des tiers de confiance

Ce système offre en effet une liberté d'utilisation totale de tout moyen de cryptologie, quelle que soit sa force, si la convention secrète est gérée par un tiers de confiance. Le tiers de confiance est un organisme qui gère les clés privées de chiffrement utilisées pour garantir la confidentialité d'une information, qui les transmet à l'utilisateur, et qui doit remettre lesdites clés à l'autorité judiciaire ou aux services chargés des écoutes administratives dans les cadres prévus par la loi. L'organisme devra être agréé par le premier ministre, dans les conditions fixées par le décret 98-102 du 24 février 1998.

L'intérêt de ce régime est qu'il constitue une solution intermédiaire entre le dépôt des moyens de cryptologie auprès du SCSSI, et l'absence de dépôt qui interdit l'interception des messages dans le cadre de procédures pénales. Ce régime permet donc de concilier le besoin de protéger les intérêts fondamentaux du respect de la vie privée et les intérêts tout aussi fondamentaux de la sécurité publique.

---

[47] loi 90-1170 du 29 décembre 1990
[48] Titre du rapport gouvernemental du premier ministre
[49] article 17 de la loi de réglementation des télécommunications du 26 juillet 1996
[50] voir annexe 2.

3.2 La politique des autres Etats

3.2.1. Directives supranationales

Ces dernières années, la plupart des pays ont oeuvré pour essayer d'harmoniser leurs politiques à l'égard de la cryptographie; l'objectif est de supprimer toute législation nationale qui serait de nature à freiner le développement des réseaux d'information, notamment en ce qui concerne le commerce électronique.

C'est dans cet esprit que les pays membres de l'O.C.D.E. ont établi huit principes directeurs concernant la politique de cryptographie [51] et que la commission au Parlement européen a souligné le besoin « d'assurer la sécurité et la confiance dans la communication électronique ».[52]Ces directives visent essentiellement à libéraliser l'*usage* des matériels de cryptographie.

Cependant, pour ce qui concerne l'*exportation* des produits de chiffrement, la presque totalité des pays pratique une politique de contrôle rigoureuse pour interdire l'accès d'opposants étrangers aux techniques de chiffrement, et prévenir ainsi la prolifération au niveau international de ces technologies. C'est ainsi que les produits de chiffrement, qui étaient inclus dans la liste du COCOM[53], font désormais partie intégrante d'un accord[54]dit de Wassenaar élargi à 28 pays.

Au niveau européen, un règlement[55] institue des normes communes pour ce qui concerne le contrôle à l'exportation des biens à double usage[56] dont font partie les produits de chiffrement; ce règlement laisse cependant une grande liberté dans la mise en oeuvre des contrôles nationaux.

3.2.2. Politiques nationales

Certains pays ont décidé cependant d'appliquer des politiques nationales beaucoup plus contraignantes. Ainsi, la Biélorussie, la Chine, Israël, le Pakistan, l'Iran, la Russie et Singapour font partie des pays dans lesquels l'utilisation ou l'importation de moyens de cryptographie est sévèrement contrôlée. D'autres pays ont décidé d'appliquer une politique plus libérale vis-à-vis de l'utilisation de moyens cryptographiques: on peut citer par exemple le Brésil, le Danemark, l'Estonie, la Finlande, l'Allemagne, la Grèce, la Norvège, la Suède et la Suisse[57]. Mais il est intéressant d'examiner la stratégie des Etats-Unis, considérée a priori comme libérale mais qui, dans les faits, semble développer une stratégie que l'on peut qualifier de « guerre de l'information ».

---

[51] Rapport sur les lignes directrices régissant la politique de cryptographie de l'O.C.D.E. (27 mars 1997)

[52] Communication de la Commision au Parlement européen, au Comité économique et social et au comité des régions, COM(97) 503 du 8 octobre 1997.

[53] COCOM: comité de coordination pour le contrôle multilatéral des exportations, créé en 1949 et dissous en 1994. Regroupait les 17 pays membres de l'OTAN (sauf l'Islande) ainsi que le Japon et l'Australie.

[54] Arrangement de Wassenaar sur les contrôles à l'exportation pour les armes conventionnelles et les biens et technologies à double usage, signé le 19/12/1995

[55] Réglement CE n° 3381/94 du 19 décembre 1994.

[56] Biens susceptibles d'application civile et militaire.

[57] Selon l'étude effectuée par le G.I.L.C. (Global Internet Liberty Campaign), organisme américain qui défend la libéralisation de la cryptographie.

3.2.3 La politique des Etats-Unis

Les moyens de cryptologie représentent pour les Etats-Unis un enjeu commercial très important qui est à replacer dans le contexte plus général des technologies de l'information qui a représenté l'année dernière près de 40% de la croissance annuelle de son PNB[58].

Les Etats-Unis estiment que le chiffrement est indispensable au développement du commerce électronique, et qu'une sur-règlementation en matière de cryptographie doit être évitée. Le secteur du commerce électronique est jugé suffisamment stratégique pour que le président Clinton édicte neuf recommandations très précises; la sixième de ces recommandations stipule toutefois que, tout en favorisant l'utilisation des techniques de chiffrement, les U.S.A. doivent garantir la sécurité nationale. Les autres recommandations précisent aussi que, s'il faut oeuvrer pour standardiser les règlements au niveau mondial, c'est le marché qui doit déterminer les standards au niveau technique. Clairement, les Etats-Unis veulent tirer profit de leur position de domination dans l'industrie cryptographique pour imposer, à travers leur industrie, des standards reconnus au niveau international.

Cela explique pourquoi les Etats-Unis conservent une politique très restrictive d'*exportation* de leurs produits cryptographiques. C'est pourquoi ils ont établi une loi spécifique sur ce problème[59]. Cet « executive order » semble a priori libéraliser l'exportation de ces produits puisqu'il transfère au département du commerce le droit de délivrance des licences d'exportation pour ce qui concerne les produits de chiffrement à usage civil.

Toutefois, les départements de la Justice, des Affaires étrangères, de la Défense, de l'Energie et les agences du contrôle des armes et du désarmement conservent un droit de regard sur les licences accordées. La politique américaine n'a donc pas été assouplie du fait de ce transfert de compétences.

De plus, après avoir pratiqué une politique très libérale pour ce qui concerne l'*utilisation* de la cryptographie, les Etats-Unis ont essayé d'implanter en 1993 un « clipper chip »[60]. Devant le tollé provoqué par ce projet, le gouvernement américain a renoncé et essaie actuellement de mettre en place un système de « key escrow »[61] (ou de « key recovery »[62]), qui imposerait que des copies des clés (ou des informations concernant ces clés) soient transmises à un tiers. Cette affaire est prise très au sérieux par des membres du congrès américain[63] qui, avec l'appui des industriels, essaient d'assouplir les contrôles à l'exportation imposés sur les matériels de cryptographie.

---

[58] Discours du Secretary Daley, secrétaire d'Etat au commerce des U.S.A., prononcé le 8 juillet 1997 à l'occasion de la conférence ministérielle européenne de Bonn sur les réseaux globaux d'information.

[59] Executive Order du 15 novembre 1996 concernant l'exportation de produits de cryptographie.

[60] Sorte de puce électronique qui, implantée dans un système de cryptographie, permet une interception en temps réel des communications chiffrées.

[61] Système de clé sous seing privé

[62] Système de recouvrement de clé

[63] Bob Goodlate, membre du congrès, essaie de faire adopter le SAFE act (Security and Freedom Through Encryption) qui s'oppose aux contrôles à l'export des matériels de cryptographie américains.

CONCLUSION

La cryptographie est aujourd'hui le seul moyen efficace de protéger la confidentialité, l'intégrité et l'authenticité des informations appelées de plus en plus, avec le développement d'Internet, à circuler sur des réseaux ouverts à couverture mondiale.

La France dispose dans ce domaine d'une législation très complète qui lui permet, tout en protégeant les libertés de chacun et en respectant les impératifs de sécurité nationale, de favoriser le développement d'une société française de l'information.

Mais dans un contexte de guerre de l'information, et plus particulièrement de guerre économique, que nous connaissons aujourd'hui, certains pays développent une stratégie qui vise à maintenir leur domination dans le secteur des technologies de l'information.

Ainsi, les Etats-Unis, profitant de leur position dominante dans le secteur des produits de cryptographie, appliquent une politique de resserrement des contrôles à l'exportation dans le but de faire acheter par des pays tiers des produits de chiffrement dont les autorités américaines détiennent la clé. Il ne faut pas oublier ce qu'affirmait le président Clinton[64]: « les capacités de renseignement des Etats-Unis sont décisives pour notre puissance nationale et font partie intégrante de la mise en oeuvre de notre stratégie de sécurité nationale ».

[64] Lu sur le site internet officiel de la NSA: http://www.nsa.org/mission

ANNEXE 1

DIFFERENTES METHODES DE PIRATAGE INFORMATIQUE

- la **bombe logique**: programme dissimulé par un pirate sur un réseau informatique. A la date et à l'heure voulues, il déclenche une action malveillante (destruction de fichiers,...),

- la ***brute force attack***: harcèlement de mots de passe d'un ordinateur ou d'un réseau informatique,

- le **cheval de Troie**: fonction apparemment inoffensive qui contient une fonction illicite cachée, généralement utilisée pour pénétrer par effraction l'ordinateur et consulter, modifier ou détruire des informations,

- la **trap door**: mécanisme qui permet de prendre à distance le pouvoir d'une machine ou d'un système en contournant le contrôle d'accès,

- l'**interception électromagnétique**: grâce à un kit de radiations de type Van Eck, il est possible d'intercepter et de reconstituer les radiations électromagnétiques d'un écran d'ordinateur. le pirate, situé à une centaine de mètres, peut ainsi lire un document affiché à l'écran,

- le ***phreaking***: détournement de centraux téléphoniques permettant de téléphoner gratuitement. Les pirates utilisent des logiciels spécifiques,

- le ***sniffer***: programme chargé d'enregistrer le trafic sur un réseau. Il mémorise notamment les premiers bits d'un paquet d'informations, où sont inscrits les mots de passe de l 'utilisateur,

- le ***spoofing***: envoyer un courrier électronique contenant des messages faux ou nuisibles en se faisant passer pour un expéditeur connu du destinataire.

ANNEXE 2

PRINCIPALES DISPOSITIONS DE LA LOI DE 1996

	UTILISATION	FOURNITURE	EXPORTATION
Cartes à puce, distributeurs de billets, terminaux point de vente	LIBRE	LIBRE	LIBRE
Signature électronique	LIBRE	DECLARATION SIMPLIFIEE	DECLARATION SIMPLIFIEE
Confidentialité utilisant un algorithme de moins de 40 bits	LIBRE	DECLARATION	LICENCE
Confidentialité avec tiers de séquestre	LIBRE	AUTORISATION	AUTORISATION
Autres cas de confidentialité	AUTORISATION	AUTORISATION	AUTORISATION

BIBLIOGRAPHIE

« Sécurité dans les réseaux informatiques », Davies D.W. et Price, éditions AFNOR, 1993.

« La politique de cryptographie: les lignes directrices et les questions actuelles », rapport de l'O.C.D.E., mars 1997, disponible à http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm

« Cryptography and Liberty: an international survey of encryption policy », document du G.I.L.C. (Global Internet liberty Campaign), 9 février 1998, disponible à http://www.gilc.org/crypto/crypto-survey.html

« La sécurité au travers de la législation sur la cryptologie », Maître Frédérique DUPOUIS-TOUBOL, Enjeux atlantiques, février 1997

« Le droit de la cryptologie », Contrôleur Général des Armées Claude Sornat, revue « L'armement », n° 60, décembre 1997/janvier 1998.

« Commerce électronique, sécurité et législation », Général Jean-Louis DESVIGNES, Enjeux atlantiques, février 1997

Conférence ministérielle européenne (UE, AELE, PECO) sur les réseaux globaux de l'information, Bonn, 6/8 juillet 1997, disponible à http://www2.echo.lu/bonn/conference.html

Déclaration du secrétaire d'Etat au commerce des Etats-Unis Daley lors de la conférence ministérielle européenne sur les réseaux globaux de l'information, Bonn, 8 juillet 1998

Communication de la commission au parlement européen, au comité économique et social et au comité des régions relative à « Assurer la sécurité et la confiance dans la communication électronique: vers un cadre européen pour les signatures numériques et le chiffrement »

Rapport de F. Lorentz sur le commerce électronique, 7 janvier 1998, disponible à http://www.telecom.gouv.fr

Communiqué de presse de M. Pierret, secrétaire d'Etat à l'industrie, relatif à la libéralisation prochaine de la cryptologie jusqu'au niveau de clé de 56 bits, 16 janvier 1998, disponible à http://www.telecom.gouv.fr

Arrangement de Wassenaar relatif au contrôle multilatéral des exportations pour les armes conventionnelles et les marchandises et technologies à double usage, 11 et 12 juillet 1996

« Cyber-terrorisme: le nouveau péril », Daniel Martin, Politique internationale no 77, septembre 1997.

Communiqué final de la réunion ministérielle « justice intérieure » du G7/P8 relatif à la criminalité informatique, tenue à Washington les 9 et 10 décembre 1997, documents d'actualité internationale no 3, 1° février 1998

Audition de Louis J. Freeh, directeur du FBI, devant le sénat américain et relative à la cryptographie et à la criminalité informatique, 3 mars 1998, disponible à http://www.jya.com/fbi-dvstate.htm

Executive Order du gouvernement américain concernant l'exportation des produits de cryptographie, 15 novembre 1996, disponible à http://www.bxa.doc.gov/eo13026.htm

« Clinton continue à broncher sur le terme « encryptage », John Markoff, New York Times, 27 février 1998, disponible à http://www.nytimes.com

Rapport du membre du congrès américain Zoe Lofgren concernant l'encryptage et la proposition de loi connue sous le terme « S.A.F.E. Act », 4 mars 1998, disponible à http://www.jya.com/acp-pols.htm

Discours du président William Clinton sur le commerce électronique (Washington, 1° juillet 1997), documents d'actualité internationale n°17, 1° septembre 1997

LOIS ET DECRETS

Décret no 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'Etat

Règlement (CE) 3381/94 du Conseil modifié en date du 19 décembre 1994 instituant un régime communautaire de contrôle des exportations de biens à double usage

Loi no 91-646 du 10 juillet 1991 modifiée relative au secret des correspondances émises par la voie des télécommunications

Arrêté du 28 décembre 1992 définissant les conditions particulières auxquelles sont soumises les prestations de cryptologie

Décret no 95-613 du 5 mai 1995 relatif au contrôle à l'exportation des biens à double usage

Décret no 95-589 du 6 mai 1995 modifié relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions

Article 28 de la loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications modifiée par la loi no 96-648 du 11 juillet 1991 et par l'article 17 de la loi no 96-659 du 26 juillet 1996 de réglementation des télécommunications

Décret no 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie

Décret no 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications

CINQUIEME PARTIE

LES ORGANISATIONS NON GOUVERNEMENTALES ET INTERGOUVERNEMENTALES ET INTERNET

INTRODUCTION

Aujourd'hui les organisations non-gouvernementales et intergouvernementales sont des acteurs mondiaux et font partie des puissances politiques. Ils ont une influence sur les décisions prises par des gouvernements et des organismes autour du monde. Ces organisations utilisent aujourd'hui tous les chaînes de communication possibles, l'Internet inclus. Est-ce qu'ils pratiquent une guerre d'information sur l'Internet? Quelle est leur stratégie pour l'utilisation de ce nouveau média? Pour répondre a ces questions il faut d'abord brièvement définir la notion de la guerre d'information et à quoi consiste-t-il l'Internet. Ensuite on regardera comment les organisations utilisent les différentes possibilités de l'Internet. Dans une conclusion on répondra à la question de la stratégie des organisations mondiales concernant l'Internet.

Une stratégie peut être ouverte ou secrète. Certains éléments sont communiqués, d'autres restent au sein de l'organisation, qu'elle soit militaire ou civile. Dans le domaine de stratégie envisagée pour la communication sur l'Internet par les organisations non-gouvernementales ou intergouvernementales, l'information est difficile à trouver et le domaine reste inexploré. En regardant les différents sites d'Internet une partie de cette information peut être obtenue. Ensuite, la technique d'interview a permis d'obtenir d'autres informations. Enfin, en analysant des articles, des livres et des rapports, une dernière partie de cette information peut être capturée. Pour regarder comment les organisations traitent un sujet actuel, on utilisera la campagne contre les mines antipersonnel.

1. LA GUERRE D'INFORMATION ET L'INTERNET

1.1 La guerre d'information

Il est nécessaire de donner une définition de la notion de guerre de l'information. On peut dire que cette guerre est l'utilisation offensive et défensive de l'information ou des systèmes d'information, dans le but d'exploiter, d'influencer ou de détruire l'information et les systèmes d'information de l'adversaire. La protection de l'information et les systèmes d'information amis sont aussi un élément de cette notion. Le but ultime est évidemment de gagner un avantage sur l'adversaire, d'acquérir une supériorité dans le domaine de la connaissance.

On peut aussi dire que la guerre de l'information a pour objectif de maîtriser le processus de décision pour atteindre des objectifs stratégiques.[65] Concernant la finalité de cette guerre, on peut rajouter la thèse de Clausewitz, en disant que le but est d'imposer sa volonté à l'ennemi.

Pour illustrer la notion de la guerre de l'information on peut étudier la bataille entre l'organisation Greenpeace et le Service d'information et de relations publiques des armées - SIRPA, qui a eu lieu pendant la reprise des essais nucléaires français en 1995. La mobilisation des ressources médiatiques à côté des armées a été faible pendant le début de l'action. Greenpeace a eu l'avantage initialement. L'organisation a dès le début montré une activité médiatique intense, dirigée par un commandement central, et une stratégie bien élaborée. Les ressources mises en place ont donné une possibilité pour Greenpeace d'être la source primaire pour les médias mondiaux. Cette position a donné une possibilité de montrer des images favorables à la cause antinucléaire. Le service médiatique aux côtés des autorités françaises, le gouvernement, l'armée et le Commissariat à l'énergie atomique, dont l'action est coordonnée sur le plan logistique par le SIRPA, ont été pris par surprise au début de l'action. L'impact créé par Greenpeace a été important et les autorités françaises ont dû changer leur stratégie et augmenter les ressources pour reprendre l'initiative.

Dans la deuxième phase du combat entre Greenpeace et le SIRPA, ce dernier a pris la décision d'augmenter les ressources médiatiques sur place, d'offrir un service médiatique très important, de changer d'attitude en évoluant d'un silence vers une plus grande ouverture et une plus grande transparence. Par la mobilisation de ces moyens et par une stratégie d'action plus active, le SIRPA a gagné le deuxième phase de cette guerre de l'information.[66] Cette lutte entre une organisation d'un côté et l'autorité d'une nation de l'autre côté montre l'importance de la connaissance et de la maîtrise de la guerre de l'information et des moyens de communication. Pendant cet épisode, ni Greenpeace, ni le SIRPA n'ont utilisé l'Internet.[67]

Les organisations non-gouvernementales et intergouvernementales sont des acteurs qui parfois sont à côté des forces armées, et parfois parmi les adversaires. Ces organisations sont montées en puissance ces dernières années et elles sont beaucoup plus présentes sur la scène internationale. Selon certains chercheurs, les organisations non-gouvernementales vont avoir une importance plus grande dans l'avenir. Des milliers d'organisations grandissent et la plupart ont un intérêt plus vaste que les frontières d'un état. Elles ont un programme global, qui leur est propre. L'importance du renseignement et de l'information s'accroissent.[68] L'utilisation de l'information et des réseaux autorise des distances presque illimitées entre l'émetteur et le récepteur, et permet un impact instantanée.

---

[65] Chauvancy, François, *Stratégie et communication*, défense nationale, Août-Septembre 1995, p.86.
[66] Derville, Grégory, *Le combat singulier de Greenpeace - SIRPA*, p.589-629.
[67] Lebrun, Pascal, Capitaine, Chef du bureau Internet, SIRPA.
[68] Toffler, Alvin & Heidi, *War and Anti-War*, p.291.

1.2 Le rôle d'Internet

Avec l'émergence d'Internet, la question est posée de savoir comment utiliser ce nouveau média, et définir son utilité pour prévenir, traiter et même résoudre les conflits. Selon certains penseurs, l'accroissement de l'information et de la communication internationales que permet l'Internet peut mener vers des routes plus paisibles pour résoudre les conflits.[69] Cela suppose que l'information librement accessible peut contribuer à un dialogue ou même une résolution de ces conflits. Avec une information beaucoup plus accessible, les acteurs peuvent mieux comprendre les problèmes et les différents points de vues. Cette conversation globale met une pression sur les gouvernements, influençant progressivement le procès politique. Parmi les acteurs globaux on trouve les organisations non-gouvernementales et intergouvernementales.

Pour ces organisations, les nouveaux médias sont encore une nouvelle possibilité de diffuser l'information. Mais ce nouveau média ne reste pas un domaine exclusif des organisations. Les forces armées à travers le monde sont également présentes sur le réseau. Depuis la fin du mois de janvier 1998, les forces armées françaises et le ministère de la défense sont présents sur l'Internet avec un site très riche en informations. Les objectifs de ce site sont multiples mais le but est de diffuser l'information. Ce média est traité comme un média parmi d'autres. Toutes les informations concernant les actualités sont rédigées et mises en place par le bureau Internet du SIRPA.[70]

Mais la défense a aussi un intérêt à collecter du renseignement sur l'Internet. Selon certains chercheurs, l'Internet est une source de plus en plus intéressante à cet égard. Dans ce média on peut trouver les compte rendus des événements actuels, des analyses faites par des observateurs proches de la source, souvent avec un aperçu unique. Il est aussi possible de trouver la planification concernant des opérations et des actions à venir. On peut donc envisager une utilisation d'Internet comme une source de renseignement. Il est clair qu'une surveillance des sites sera indispensable pour obtenir des éléments de renseignement importants.

2. LES ORGANISATIONS NON-GOUVERNEMENTALES ET INTERGOUVERNEMENTALES

Quand il s'agit du domaine des organisations internationales il est nécessaire de marquer une différence entre les organisations intergouvernementales, comme par exemple les Nations Unies et ses différentes organismes, et les organisations non-gouvernementales. Parmi elles on peut citer la Croix Rouge et Handicap International. Chaque organisation a ses propres règles et sa propre doctrine. Cette différence est très claire en examinant leurs sites sur Internet. Les organisations intergouvernementales ont des sites de caractère informatif, or les ONG ont des sites beaucoup plus politiques.

---

[69] Report of the First International Conference on the FUTURE OF INTERNET SERVICES ON CONFLICT AND ETHNICITY, Held at INCORE headquarters, Aberfoyle House, Derry, Northern Ireland, 7 - 9 November, 1996. http://www.incore.ulst.ac.uk/events/fisce1/report.html.

[70] Lebrun, Pascal, Capitaine, Chef du bureau Internet, SIRPA.

Elles ont la liberté de mener des campagnes et de publier de l'information que l'on peut qualifier de propagande. Cette différence s'étend aussi au domaine du courrier électronique.

2.1 Les organisations et l'Internet

L'information aujourd'hui se moque des frontières et traverse sans grand difficulté le monde entier. Déjà, l'Internet joue un rôle de plus en plus important dans le monde de l'information et dans la vie de la sécurité internationale.[71] L'estimation de certains acteurs est que l'Internet est déjà aujourd'hui le média le plus important pour la communication mondiale.[72] Aujourd'hui, la quasi totalité des organisations non-gouvernementales et intergouvernementales sont présentes sur l'Internet. Elles ont leur sites, utilisent le courrier électronique et certaines sont actives dans les forums de discussion. En regardant comment elles utilisent l'Internet, il faut faire une distinction entre ces trois domaines.

Même si les grandes organisations ont leur sites propres et s'occupent de la mise en fonction elles mêmes, un grand nombre d'organisations plus petites ont besoin d'un soutien dans ce domaine. Un problème qu'on ne peut pas négliger est le problème technique. Il n'est pas évident que la compétence existe dans tous les endroits où sont représentées les organisations. Le plus grand et le plus actif des acteurs qui utilise l'Internet, et qui incite d'autres organisations à le faire, semble être *Institute for Global Communications* et le *Association for Progressive Communications*.[73] Ces organisations peuvent aider des associations à créer un site et une stratégie de communication. Ils fournissent leurs services à plus de 25000 organisations différentes à travers le monde. Le réseau de communication de l'IGC et de leurs partenaires est aujourd'hui le seul totalement dédié au travail pour l'environnement, la paix et les droits de l'homme. Les nouvelles technologies aident les organisations à coopérer beaucoup plus efficacement. Il est facile d'arranger des conférences pour faciliter un processus de décision commun et de diviser le travail pour une campagne. APC est aujourd'hui le plus grand réseau pour les ONG et les citoyens activistes.

2.2 Le courrier électronique

L'utilisation du courrier électronique est devenu un moyen de diffusion de l'information très important pour les organisations mondiales. Dans la coordination d'une campagne cet outil est indispensable. Mais ce n'est pas seulement l'étendue qui est importante, c'est aussi la possibilité d'agir et de réagir instantanément. Dans La Campagne Internationale pour Interdire les Mines, cette utilisation du courrier électronique a été importante. Le mouvement a été fondé en 1992 par six organisations non-gouvernementales et regroupe aujourd'hui plus d'un millier d'organismes. L'action de cette campagne a été coordonnée par un comité de pilotage qui se compose des représentants de dix différentes organisations.

---

[71] Swett, Charles. *Strategic Assessment: The Internet.* Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), the Pentagon. 17 July 1995

[72] Mme Laje, UNESCO.

[73] http://www.igc.apc.org

Pour la coordination le courrier électronique a été indispensable. Un autre aspect du courrier électronique est la possibilité de mener une campagne au moyen de messages directement adressés aux hommes politiques. Cette manière d'utiliser cet outil a aussi été utilisée. Il faut donc prendre en compte le fait que dans certains pays la télécopie est encore un moyen beaucoup plus répandu. La diffusion par courrier électronique est aujourd'hui largement développée aux Etats Unis et au Japon, et reste encore dans une phase d'évolution dans les autres pays. Mais l'information concernant l'utilisation du courrier électronique n'est pas nette: selon les recherches faites aux Etats-Unis les partis politiques ne reçoivent pas beaucoup de messages en provenance d'organisations représentant un intérêt particulier.[74] Le fax reste donc le moyen le plus utilisé, mais les connexions sur Internet augmentent et la situation va changer.

2.4. Les sites sur le Web

Le site d'une organisation sur l'Internet est une fenêtre vers la société publique. Dans le site on présente la structure l'activité de l'organisation. Aujourd'hui la communication à travers l'Internet est considérée comme un moyen supplémentaire et n'a pas encore remplacé les autres moyens.[75] Le nombre de visiteurs dans un site Internet varie considérablement. Les estimations sont très diverses: Handicap International déclare entre 800 et 3000 visites par mois, et l'UNESCO déclare environ 50000 visiteurs par mois. Les organisations sont très attentives sur le profil du visiteur et le site peut être ciblé pour un ou plusieurs groupes différents. Les sites sont ainsi structurés d'une certaine manière pour l'information générale, et d'une autre pour les visiteurs qui recherchent une information particulière. Ce type de visiteur peut être un journaliste, un étudiant, un chercheur, etc. Notamment les journalistes et les étudiants forment un groupe qui de plus en plus cherche l'information sur les sites des organisations non-gouvernementales d'Internet.[76]

En examinant dix différents sites[77] sur le thème des mines antipersonnel, on peut constater que la plupart ont une ressemblance dans leur construction. La langue principale est l'anglais, il y a des liens vers d'autres sites, ils contiennent une base de données historiques sur le thème des mines antipersonnel et présentent la situation actuelle. L'information donnée est crédible, mais pas toujours complète. La quasi totalité des sites possède une adresse pour une réponse par courrier électronique. La plupart des sites prennent position sur ce sujet. Une moindre partie est disposée à engager un dialogue interactif avec le visiteur du site, ou offre la possibilité d'effectuer des recherches dans leurs archives. Les archives couvrent normalement une période limitée dans le temps. La moitié des sites permet une communication dans une deuxième langue. Une minorité de sites offre des lettres de pétition prêtes à remplir, destinées aux autorités politiques. Aucun site ne présente de statistiques concernant par exemple le nombre de visiteurs.

---

[74] Courrier International N°379, p.10.
[75] Pelissier, D, UNESCO et Brigot, S, Handicap International.
[76] Brigot, S, Handicap International.
[77] Les sites choisis sont marqués par un * dans la partie Sources.

En conclusion on peut dire que les sites semblent avoir pour mission principale d'éclairer le grand public. Ces sites sont facilement accessibles et donnent une information compréhensible, mais parfois peu élaborée. L'étendue d'un site reflète souvent les ressources financières de l'organisation. L'information est toujours présentée dans un sens qui correspond à la stratégie de l'organisation, mais la grande sélection de sites existant sur Internet permet cependant de se forger une opinion sur le sujet.

2.5 Les forums de discussion

Une troisième dimension concernant l'Internet est constituée par les forums de discussion. Cet endroit est une place de libre échange des idées et des opinions. D'avoir une vue d'ensemble des différentes domaines dans lequel les discussion ayant lieu est très difficile. Il est aussi difficile de clarifier si les organisations mondiales sont présentes ou non dans ces forums de discussion. Il est possible de participer sans avouer son identité, et il n'est peut donc pas être exclu que certaines organisations expriment leurs points de vue sous l'anonymat.

CONCLUSION

Les exemples dans le passé montrent l'importance d'une maîtrise de l'information. L'impact des médias ne cesse d'augmenter et l'émergence de nouveaux médias offre continuellement de nouveaux champs de bataille. La transmission lointaine et instantanée d'informations est un avantage incontestable d'Internet. Le but d'une campagne de la guerre de l'information au niveau stratégique est d'influencer les choix, et de diriger l'adversaire sans qu'il puisse se rendre compte qu'il est influencé.[78] Dans ce contexte les organisations non-gouvernementales et intergouvernementales ont une possibilité de mener une guerre de l'information contre les Etats. Actuellement leur utilisation de l'Internet est menée sur deux axes. Le premier est les sites. Les sites sont principalement un moyen de communiquer avec le grand public, avant tout pour présenter son organisation et son activité. De plus en plus, les sites sont accompagnés d'une possibilité de faire une recherche pour trouver l'information souhaitée. Cette possibilité d'interagir augmente avec le nombre de journalistes et d'étudiants qui visitent les sites. Le deuxième axe est le courrier électronique. Par ce moyen les organisations peuvent coordonner une grande masse d'information sur une échelle mondiale, et en plus presque instantanément. Cette possibilité peut donner un avantage considérable vis-à-vis d'un adversaire plus lent.

Pour la défense il s'agit de suivre cette évolution le plus en avant possible. Dans l'utilisation offensive il est donc nécessaire d'avoir un site pour avoir la possibilité de donner l'information souhaitée. Il est aussi nécessaire d'utiliser le courrier électronique pour avoir la possibilité de communiquer directement et réagir rapidement. Dans le rôle plus défensif il s'agit de surveiller ce qui se passe dans tous les domaines de l'Internet pour ne pas donner un avantage informationnel aux organisations, qu'elles soient non-gouvernementale ou intergouvernementales.

---

[78] Szafranski, Richard, A Theory of Information Warfare, p.4.

SOURCES

Sources imprimées

Guisnel, Jean, *Guerre dans le cyberespace.*
La Découverte/Poche, ISBN 2-7071-2716-7, Paris, 1997.

Toffler, Alvin & Heidi, *War and Anti-War.*
Warner Books, ISBN 0-446-60259-0, New York, 1995.

Sources périodiques

Bougnoux, Daniel (red), *Crise de l'information,*
Problèmes politiques et sociaux, N°737, 21/10 1994. ISSN 0015-9743. Paris, 1994.

Chauvancy, François, *Stratégie et communication.*
défense nationale, Août-Septembre 1995. ISSN 0336-1489. Paris, 1995.

Derville, Grégory, *Le combat singulier Greenpeace-SIRPA.*
Revue Française de Science Politique, Volume 47, Numéro 5, 1997, ISSN 0035-2950, Presses de Sciences Po, Paris, 1997.

Géré, François, *Guerre de l'information: la nature de l'animal.*
Perspectives Stratégiques, N°32, Novembre 1997. ISSN 1254-2148. Paris, 1997.

Internet

Szafranski, Richard, *A Theory of Information Warfare - Preparing for 2020.*
http://www.cdsar.af.mil/apj/szfran.html.

Association for Progressive Communications - *http://www.igc.apc.org/*

ADME - *http://www.adme.asso.fr/*

CARE - *http://www.care.org/* *

CICR - Comité International de la Croix-Rouge - *http://www.icrc.org/* *

GlobeNet - *http://www.globenet.org/*

Handicap International - *http://www.handicap-international.org/* *

Human Rights Watch - *http://www.hrw.org/* *

Humanweb - *http://www.humanweb.org/*

Institute for Global Communications - *http://www.igc.apc.org/*

Organisation des Nations Unies - *http://www.un.org/* *

Défense Nationale du Canada - *http://www.cfcsc.dnd.ca/* *

NETpop - *http://netpop.cam.org/*

netprogressiste - *http://www.internatif.org/internatif/netprogres/*

OneWorld - *http://www.oneworld.org/* *

OXFAM - *http://www.oxfam.org.uk/* *

Paix et Sécurité Internationales PSI - *http://www.toile.org/psi/*

Stockholm International Peace Research Institute - SIPRI - *http://www.sipri.se/* *

UNHCR - *http://www.unhcr.ch/*

Vietnam Veterans of America Foundation - *http://www.vvaf.org/* *

CONCLUSION GENERALE

Avec le développement des réseaux d'information numériques, et d'Internet en particulier, l'information est devenue un enjeu stratégique pour de nombreux acteurs. Les Etats, les entreprises et les organisations non gouvernementales ont ainsi compris l'intérêt d'une maîtrise de l'information; qui aujourd'hui détient le savoir détient le pouvoir: tel est l'objectif de la guerre de l'information devenue une réalité quotidienne.

La guerre psychologique est devenue une arme indispensable pour triompher des conflits à venir; certains Etats, les Etats-Unis en particulier, ont développé une doctrine opérationnelle de guerre de l'information visant à leur procurer une maîtrise de l'information dans les théâtres d'opérations du futur.

Les grandes entreprises, aidées en cela par les Etats, ont compris que dans un monde où la guerre économique fait rage, l'information constitue un atout stratégique; l'intelligence économique est devenue aujourd'hui une priorité de survie.

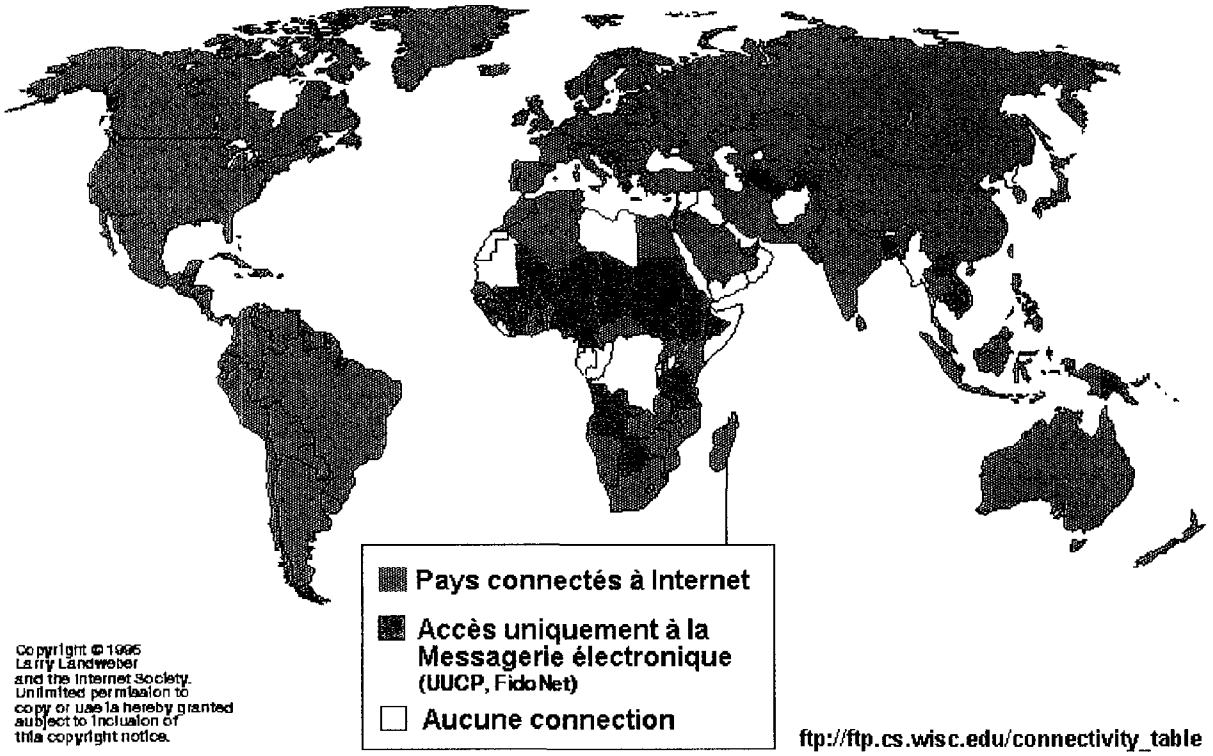
La protection des informations, qui circuleront de plus en plus sur des réseaux ouverts de type Internet, nécessitera la mise en oeuvre de moyens de cryptographie. Certains pays, à l'instar des Etats-Unis, développent à cet égard une stratégie qui vise en fait à maintenir leur domination dans le secteur des technologies de l'information.

Les Etats-Unis développent un effort important en matière de guerre de l'information. Le concept de l'*Information dominance*, qui s 'applique aux domaines politique, économique, social et militaire, considère qu'il est possible de maîtriser son environnement en maîtrisant l'information. La guerre de l'information est ainsi devenue une priorité nationale.

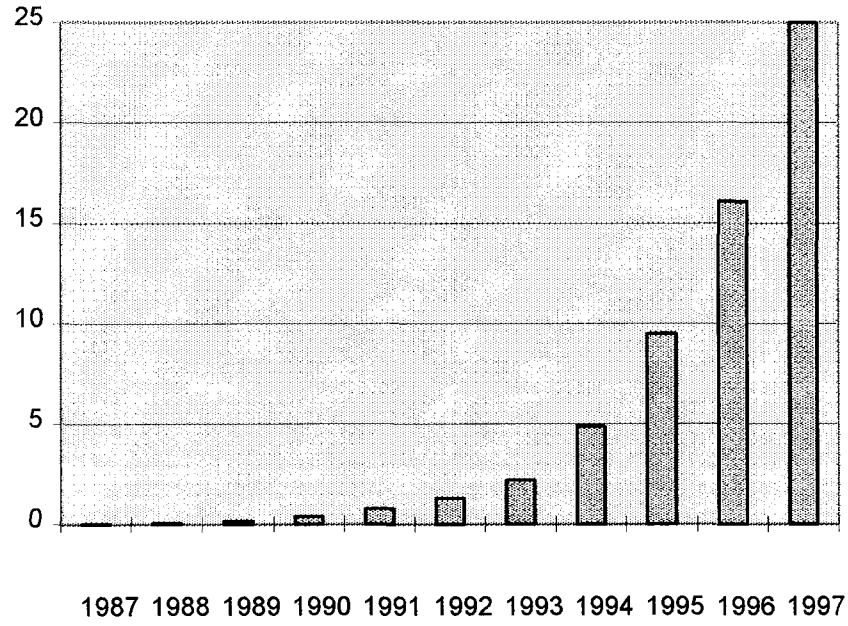
Face à cette stratégie américaine, les autres Etats, la France en particulier, mettent en oeuvre des dispositifs qui devraient lui permettre de conserver une certaine autonomie stratégique dans le secteur clé des technologies de l'information.

ANNEXE 3

Internet dans le monde (1995)



Croissance du nombre de serveurs Internet (en millions) de 1987 à 1997[38]



[38] Source statistique: Network Wizards (http://www.nw.com)

ENTRETIENS

- GBA PORCHIER (SGDN: adjoint au directeur des affaires internationales et stratégiques)

- ICA LE PIVAIN (SGDN: directeur du pôle « économie et défense »)

- COL FRANCESCONI (SGDN / TTS / SSI)

- COL DICKES (SIRPA)

- IPA DEJEAN (SCSSI: chef de la division chiffre)

- CNE BERNARD (SGDN / TTS / SSI)

- CNE LEBRUN P. (SIRPA, chef du bureau Internet)

- M. GOUJON (Agence pour la Diffusion de l'Information technologique)

- H. FONTANA (DGA / Direction des relations internationales)

- MME BRIGOT S (Handicap International, Rue Oberkampf, Paris)

- MME LAJE C. (UNESCO, Bureau de presse, Paris)

- MME PELISIER D. (UNESCO, chef de la division documentation et information)