

NOTE D'ANALYSE

1^{ER} FÉVRIER 2002

INFODOMINANCE

LES LEÇONS DU 11 SEPTEMBRE 2001

Michel Wautelet



GRIP
GROUPE DE RECHERCHE
ET D'INFORMATION
SUR LA PAIX ET LA SÉCURITÉ

•
Rue Van Hoorde 33
B-1030 Bruxelles
Tél. : (32-2) 241.84.20
Fax : (32-2) 245.19.33
E-mail : admi@grip.org
Site Web: <http://www.grip.org>

(page blanche)

INFODOMINANCE : LES LEÇONS DU 11 SEPTEMBRE 2001

MICHEL WAUTELET

Université de Mons-Hainaut

GRIP (Groupe de Recherche et d'Information sur la Paix et la Sécurité)

Le 11 septembre 2001, les Etats-Unis ont perdu, tragiquement, une importante bataille. Cette défaite aura, dans les années à venir, des conséquences qu'il n'est pas encore possible de prévoir. Néanmoins, le seul fait qu'une hyperpuissance économique et militaire ait pu être attaquée, sur son propre sol, par des individus fanatisés, mais issus de pays défavorisés, aura des répercussions sur la manière dont les Etats-Unis seront désormais considérés dans le monde entier. Cette défaite importante n'est pas seulement due à l'attitude des Etats-Unis vis-à-vis du reste du monde. Elle résulte aussi d'une conception des méthodes de domination du monde, dont les aspects positifs et négatifs n'ont pas été correctement évalués. Dans un monde qui évolue – du moins vu de l'Occident – très vite, l'action et la précipitation priment sur la réflexion. Si nous ne voulons pas que d'autres batailles soient perdues, il est temps de regarder, froidement, les événements qui ont conduit à la situation actuelle.

On le sait, on en discute dans les médias, les causes sont, notamment, géopolitiques. C'est sur celles-là qu'il faudra travailler dans le moyen et long terme. Mais, à court et moyen terme, il est aussi nécessaire de comprendre les erreurs qui ont conduit à la tragédie du 11 septembre 2001. Car il y eu des failles dans notre système sûr de lui-même. Si nous n'évaluons pas correctement ces failles, c'est vers de nouvelles défaites que nous, Occidentaux – car dans ce domaine, nos problèmes sont communs à ceux des Etats-Unis –, allons nous trouver confrontés, tôt ou tard.

Notre société occidentale repose, depuis un demi-siècle, sur un développement technoscientifique imposant. Lequel conduit à des changements de niveau de vie, mais aussi à des effets d'optique trompeurs. Nous avons l'impression que le monde entier raisonne comme nous le voudrions. C'est cet effet d'optique qui nous a aveuglé et a, notamment, permis les événements du 11 septembre 2001.

C'est surtout après la Seconde Guerre Mondiale que notre société occidentale a découvert la véritable puissance de la science. S'en est suivie une époque d'euphorie scientifique dans les années 1960-1970 : les *Golden sixties*. Tout le monde était alors persuadé que les sciences représentaient le sommet du génie humain. Les sciences allaient permettre de résoudre tous les problèmes. La conquête de l'espace, l'avènement de l'électroménager, l'automobile pour tous, la télévision, le confort domestique, l'abondance de biens étaient des facteurs qui ne pouvaient que développer notre croyance dans la toute puissance des sciences et des techniques.

Puis, retour de manivelle, dans les années 1970-1980, les hommes découvrent la fragilité de ce nouveau monde. La crise pétrolière de 1973, les accidents de pétroliers, la chute de quelques avions porteurs de bombes nucléaires, la pollution de rivières et des villes, le réchauffement de l'atmosphère, la course effrénée aux armements entraînent un insidieux sentiment de catastrophisme. Tout cela est-il aussi sûr qu'on a voulu nous le faire croire ?

Au catastrophisme des années 1980 succède la mise en perspective des problèmes dans la décennie 1990 avec, en prime, la fin de la Guerre froide et l'éloignement – mais pas la disparition – du spectre de la guerre nucléaire. La fin de la Guerre froide semble aussi

représenter la fin d'un monde bipolaire et le début d'une ère multipolaire, plus difficile à prévoir. Simultanément, le concept de société de l'information commence à s'imposer dans les esprits. Les discours sont résolument optimistes. La société de l'information sera celle de la liberté, de la démocratie universelle, de la tolérance, des échanges, du commerce libre, etc. Bref, il ne pourra en sortir que du bien. Mais les actes sont moins rassurants. Car, avec la société de l'information arrivent aussi de nouvelles manières de concevoir, de mener des conflits [0]. La séparation entre conflits militaires et civils est floue.

Pour les stratèges occidentaux, l'information joue même un rôle central dans de nouveaux types de conflits, qu'ils soient militaires, civils ou terroristes [1]. La guerre au XXI^e siècle, telle que conçue par les occidentaux, sera peut-être une guerre technologique [2], mais elle sera aussi, notamment selon la doctrine militaire américaine, basée sur « *l'Information Dominance* » [3], ou « *Infodominance* ». C'est cette notion qui a guidé et guide encore quantité de stratèges au niveau mondial, mais dont les diverses implications ne semblent pas avoir été suffisamment pesées avant le 11 septembre 2001. Quant au futur, il semble que, malheureusement, la fuite en avant technologique prévale sur la critique constructive.

Infodominance : gain d'un avantage opérationnel par l'acquisition, l'altération ou le traitement de données ou connaissances.[4].

Suite à la conduite de la Guerre du Golfe et du conflit bosniaque, le rôle majeur de l'information dans les conflits a été mis en évidence. Ces succès ont convaincu beaucoup de monde que dominer les flux d'information au niveau mondial, les contrôler, les surveiller, les utiliser – bref, développer « l'Infodominance » – sont la voie à suivre pour un monde sûr. Cette notion ne recouvre pas que des buts militaires, mais s'applique aussi à l'économie, surtout mondialisée, pour laquelle toute information sur le concurrent ou le client représente un avantage. Afin de mieux appréhender les difficultés de ce concept, il n'est pas inutile d'examiner les hypothèses de base.

1. Hypothèses de base de l'Infodominance

Le concept d'Infodominance résulte de plusieurs hypothèses de base, de dogmes non remis en cause, bien ancrés dans l'esprit des stratèges et dirigeants occidentaux. Ces dogmes ne sont pas discutables, car allant de soi. Pourtant, les événements du 11 septembre 2001 en ont démontré certaines limites.

1.1. Hypothèse 1 : notre civilisation occidentale est « bonne ».

« Nous sommes bons » : cette phrase, prononcée par le président George W. Bush peu après les tragédies du 11 septembre 2001, résume bien le sentiment général des Américains, mais aussi de la quasi-totalité des Occidentaux. Notre civilisation occidentale est « bonne ». Notre fonctionnement démocratique est le seul bon ; nous devons donc l'imposer pour que tous les hommes soient heureux. Le progrès scientifique et technologique nous a aidé à installer définitivement notre démocratie chez nous. Grâce à ces progrès, nous sommes heureux. Notre économie est puissante. Tout prouve que c'est la bonne solution pour l'humanité. Il nous faut donc imposer notre mode de civilisation, à tous les niveaux. Ce qui, incidemment, implique que nous nous considérons comme étant constamment en conflit : économique, idéologique, culturel, militaire, etc.

Nous devons vaincre ceux qui ne pensent pas comme nous, nous devons nous méfier des autres, nous devons savoir qui sont nos ennemis et nos alliés. Et le monde étant nécessairement dangereux pour les gentils, il faut bien que nous nous protéjions contre les méchants. Il faut aussi que nous dominions les autres.

1.2. Hypothèse 2: la maîtrise de l'information est nécessaire pour pouvoir dominer le monde.

Dans ce contexte, l'information est alors vue comme une arme, défensive et offensive. Si nous savons tout ce qui se dit et s'échange, nous pouvons tout contrôler, tout prévoir. C'est essentiel, car l'information dicte la décision. Pour bien comprendre l'importance de l'information, il est intéressant de savoir comment elle est perçue par ceux dont le métier est de préparer et de faire la guerre: les militaires. Pour les militaires, le premier but de l'information est la prise de décisions et, donc, l'action [5]. Meilleure est l'information (et donc le système de renseignement), meilleure est la décision. En guerre, deux groupes de décisions sont importants: les nôtres et les leurs. La guerre offensive de l'information a pour but d'affecter l'information circulant de l'autre côté ou vers l'autre côté, de telle sorte que « leurs » décisions soient à « notre » avantage. La guerre défensive de l'information consiste à « les » empêcher de faire la même chose contre « nous ».

Etant donné que le phénomène de l'information est très large et est inclus dans toutes les activités humaines, une large gamme d'actions peut être comprise dans une telle définition. Du point de vue militaire, dans le passé, cela consistait essentiellement à détruire le commandement ennemi, ou à manipuler son organisation politique. Avec les développements technologiques des dernières décennies, les choses ont changé. Dans la guerre actuelle avec des engins guidés ou intelligents [6], capables d'atteindre des cibles avec grande précision, l'information prend une part de plus en plus prépondérante. Il faut savoir à tout moment où les cibles se trouvent et se trouveront dans les heures ou minutes qui suivent. Il faut donc des moyens puissants de surveillance, de transmission et de traitement de l'information, afin de prendre la bonne décision au bon moment. Avec les autoroutes de l'information, leur rôle est encore plus prépondérant, car les informations recueillies peuvent concerner quelqu'un à l'autre bout de la planète.

La maîtrise de l'information est complexe. Elle demande une connaissance de l'autre qui est bien plus profonde et complète que celle requise pour un combat physique. On doit savoir :

- quelle information sert à la décision de l'autre;
- comment l'information circule dans l'espace, le temps;
- dans quelle bande spectrale l'information est transmise ;
- quelles règles régissent la transmission et la réception de l'information;
- quelles informations sont superflues;
- qui décide de la pertinence de l'information pour la décision;
- combien de décisions sont liées à d'autres facteurs.

Si on ne connaît pas ces paramètres, les opérations sont lancées dans le noir. Si l'information est évidemment essentielle en cas de conflit militaire, elle le devient de plus en plus dans une société technologiquement développée comme la nôtre.

Tout ce qui vient d'être dit s'applique aussi aux secteurs industriels et publics, à l'information économique, à l'idéologie, aux médias. Néanmoins, la maîtrise de l'information est rendue complexe par le fait que l'information est un concept à plusieurs entrées, interdépendantes.

Celles-ci concernent, dans le désordre, les acteurs, les destinataires, les moyens de communication, les buts, le moment.

Concernant les acteurs et destinataires, plusieurs entrées sont à considérer :

1. Eux (nos concurrents, nos ennemis, les mauvais) ; nous (les bons) ; leurs et nos alliés (toujours suspects de changer de camp) ; les autres (qui pourraient nous gêner). Pour « eux », la maîtrise de l'information requiert de savoir ce qu'ils savent et échanger, mais aussi de leur distiller l'information « adéquate » sur « nous ». A « nous », il convient de nous rassurer sur nos capacités, sur notre bonne volonté, et de nous protéger.
2. Les décideurs, les « ouvriers » et « soldats », l'opinion publique. L'information concernée est de « qualité » différente. « Leurs » décideurs sont évidemment très importants. Leurs motivations, leur mode de pensée, leur poids, l'information dont ils disposent et celle qu'ils échanger ont une valeur inestimable pour « nous ». « Leurs » ouvriers ont aussi une importance à ne pas sous-estimer, car ils peuvent échanger des choses qui devraient être cachées. A nous de bien les repérer. « Leur » opinion publique est essentielle pour nous, car elle nous fournit les informations sur le milieu dans lequel agir. « Nos » décideurs doivent avoir l'information adéquate au moment adéquat. « Nos » ouvriers doivent être convaincus que nous sommes forts et sûrs de nous, et nous suivre au bon moment. Il faut donc maîtriser l'information que nous distillons.
3. Les forts et les faibles. Selon que l'on soit soi-même fort ou faible, et que l'autre soit fort ou faible, le message peut être différent. Le fort est sûr de son fait et, généralement, possède des moyens importants. Le faible doit pouvoir « ruser » vis-à-vis du fort, le diaboliser.
4. Les attaquants et les attaqués. Que ce soit « nous » ou « eux », on peut être (ou se sentir) attaquant ou attaqué, selon le moment du conflit ou selon celui à qui l'on parle. L'attaque peut être physique (militaire), idéologique, économique, culturelle.
5. La civilisation, la culture, l'idéologie. Le monde est divisé en peuples, tribus, groupes qui ont chacun leur identité propre, leur mode de fonctionnement. Les informations qui intéressent un peuple d'Afrique centrale ne sont pas celles qui intéressent un pays du Moyen-Orient. Ce qui, combiné au fait que leur degré de développement et d'implantation des moyens de communication et d'information est différent du nôtre, rend la question opérationnelle difficile.

Comme on le voit, la maîtrise de l'information est essentielle pour dominer le monde, mais cette maîtrise n'est pas simple.

1.3. Hypothèse 3 : la technologie est l'outil essentiel de la maîtrise de l'information

Etant donné la complexité de l'information, il faut des outils pour pouvoir la maîtriser. Seule « la technologie » en est capable. Le développement des systèmes électroniques résulte de certaines hypothèses bien ancrées dans l'esprit des décideurs et des citoyens.

1.3.1. Hypothèse 3a : l'électronique est l'outil le plus efficace pour la maîtrise de l'information.

Tous les messages envoyés par les citoyens du monde passant (ou en voie de passer) par des systèmes « numérisés », donc traités par ordinateur, des engins électroniques placés aux endroits stratégiques devraient permettre de tout voir passer. Vu la quantité énorme

d'information transitant par ces endroits stratégiques, seule l'électronique intelligente peut donner accès à cette information et de la contrôler.

1.3.2. Hypothèse 3b : grâce à l'électronique, les risques liés aux erreurs humaines sont supprimés.

Les hommes sont des êtres faillibles. Ils peuvent se tromper, mal évaluer une situation, être fatigués ou distraits, etc... Ce n'est pas le cas des machines qui font exactement ce qu'on leur demande, sans erreur possible. Il « suffit » de leur injecter les critères de choix, de tris.

1.3.3. Hypothèse 3c : avec l'électronique, les hommes ne sont plus aussi nécessaires.

Pour obtenir l'information nécessaire sur le concurrent, l'ennemi, l'allié, il n'est plus nécessaire d'envoyer des hommes sur le terrain, chez l'autre. Cela peut se faire à distance, devant un clavier d'ordinateur. De plus, la situation est psychologiquement confortable. L'adversaire n'est pas un homme. Il s'agit d'un jeu sur ordinateur, sans victime, sans destruction.

Il n'est plus nécessaire d'envoyer des compagnies d'hommes sur le terrain. Cela se fait à distance, par quelques hommes bien entraînés au traitement de l'information, devant un ordinateur. Pour lutter contre un ennemi, il ne faut plus qu'un nombre minime de personnel. On pourrait donc passer d'hommes sur le terrain.

Les progrès ultra-rapides dans le domaine de l'informatique, le développement du réseau *Internet*, le fait qu'il n'y ait eu, jusqu'à aujourd'hui, que des incidents relativement mineurs sur *Internet*, les discours rassurants des responsables de la sécurité informatique, sont des éléments qui ont conforté les responsables politiques et autres, de l'utilité de développer la surveillance informatique.

Cette vision de l'efficacité de l'électronique est encore répandue dans le public via quantité de films, souvent américains, impliquant ordinateurs, *Internet* et satellites de surveillance. Ne voit-on pas, dans plusieurs films, des policiers suivre un suspect à la trace grâce à des satellites espions. Techniquement, on n'est pas près d'y arriver, mais qui, dans les milieux non spécialistes, le sait ? Dans une société démocratique, où l'avis de la population est essentielle, l'éducation du public fait aussi partie de la préparation aux conflits.

2. Un modèle adéquat du monde pour appliquer l'infodominance.

Pour dominer le monde grâce à l'infodominance, l'idéal serait d'arriver à une division du monde en catégories adéquates, bien déterminées et faciles à classer. L'idéal, du point de vue de l'infodominance, serait une division en deux catégories : les bons et les mauvais. Pour y arriver, il faut que les bons soient les forts, et les mauvais soient les faibles.

Puisque le développement de cette infodominance prend racine dans le développement d'*Internet* et du cyberspace, il est utile de retourner à leurs sources. La volonté politique qui a porté leur développement prend racine dans les idées de futurologues américains des années 1970, notamment les Toffler. Selon eux, il s'agit, au départ, d'une idée pour redynamiser la société américaine. Depuis la publication de leur premier best-seller, *Le Choc du Futur*, en 1970, les idées des Toffler ont pénétré les esprits de bien des dirigeants et économistes, pas seulement américains. Selon eux, nous sommes en train de passer d'un

monde dual (Nord -Sud, riche et pauvre, industrialisé et agricole) à une société "triséquée". Selon un ordre historique, le monde est divisé en trois secteurs ou sociétés :

- les sociétés de la Première Vague, *offrent les ressources agricoles et minérales* ;
- les sociétés de la Deuxième Vague, *fournissent une main-d'œuvre bon marché et s'acquittent de la production en série* ;
- les sociétés de la Troisième Vague *vendent au monde de l'information et de l'innovation, du management, de la haute culture et de la culture pop, de la technologie avancée, des logiciels, de l'éducation, de la formation, des soins médicaux, et des services financiers ou autres.*

Les nations sont classées selon ces trois « vagues ». Bien entendu, les pays développés doivent être de la troisième vague, pour garder la domination du monde. Cette vague, basée sur l'information et le savoir, ne peut se réaliser sans des outils spécifiques. C'est ici qu'entre en scène *Internet*, les autoroutes de l'information, les multimédias, le cyberspace, etc. On le voit, développer les autoroutes de l'information est nécessaire pour ne pas rater la transition vers la Troisième Vague, pour garder la domination économique, mais surtout intellectuelle du monde.

Le classement actuel du monde selon la puissance du cyberspace est donc important pour appréhender l'état d'avancement de ce monde idéal du point de vue de l'infodominance. Cette nouvelle division du monde, de la cyberplanète, se reflète dans les nouveaux rapports de force, qui consolident les rôles des puissants et des serviteurs. Mais il permet aussi l'arrivée de nouveaux acteurs non désirés, qui risquent de menacer l'ordre en cours d'établissement. Dans le contexte actuel, on peut classer les pays et groupes en sept catégories.

1. A tout seigneur, tout honneur ; dans la première catégorie, on ne trouve aujourd'hui que les Etats-Unis. La prééminence américaine dans le cyberspace est évidente. Faut-il rappeler la place de *Microsoft* dans le secteur des logiciels informatiques, d'*Intel* dans les processeurs. Les premières constellations de satellites dédiés aux télécommunications personnelles en cours de déploiement sont américaines. Les cybernautes américains représentent environ les deux tiers des utilisateurs d'*Internet*. Cette prééminence américaine s'étend ailleurs que dans le civil. Ils sont aussi les plus avancés dans le domaine militaire, ainsi que dans celui de l'espionnage ou, si l'on préfère, de la surveillance. Ils n'hésitent pas à visiter les ordinateurs de leurs concurrents, voire de prôner de nouvelles formes de conflits pour garder le contrôle de l'économie mondiale. Les Etats-Unis dépassent tous les autres pays dans le domaine des hautes technologies pour les secteurs militaires et de surveillance. Les Etats-Unis génèrent plus de mots et d'images dans le domaine militaire et la guerre de l'information, que le reste du monde rassemblé. Quant à leur cyberspace civil, il est aussi extrêmement développé. Aucun secteur stratégique n'est indépendant du cyberspace : télécommunications, énergie, transports, banques, médias, etc. sont tous interconnectés via *Internet*.
2. La deuxième catégorie inclut des pays déjà branchés sur *Internet*, mais qui, bien que puissants économiquement, sont derrière les Etats-Unis en ce qui concerne le développement actuel du cyberspace. Ce sont essentiellement les pays de l'Union européenne, le Japon, la Suisse. Ces pays pourraient rivaliser avec les Etats-Unis, surtout dans le domaine civil, s'il y avait une véritable volonté politique. Malheureusement, la place prise, de fait, par des sociétés, comme *Microsoft* et *Intel*, dans le marché de l'informatique risque de rendre la prééminence américaine incontournable pour longtemps.

3. Dans la troisième catégorie, on rencontre des pays peu branchés sur *Internet*, mais en cours de branchement, comme l'Afrique du Sud. Ces pays ont l'ambition et, sans doute les moyens, de rester ou de devenir une puissance régionale.
4. La quatrième catégorie comprend des pays qui sont des puissances régionales, mais ne sont guère ou pas branchés sur *Internet*. Ce sont des pays comme l'Irak, l'Iran. Déjà relégués du commerce mondial, ils se verront encore plus marginalisés par le non branchement au cyberspace.
5. Il y a ensuite tous les autres pays, non développés et qui, à cause de diverses particularités (géographiques, politiques, humaines) ont peu d'espoir d'être bientôt branchés de manière satisfaisante sur le cyberspace. Ce sont notamment la plupart des pays d'Afrique.
6. Outre ces cinq catégories apparaissent de nouveaux acteurs, qui ne sont plus définis à partir de pays d'origine. La sixième catégorie inclut des organisations cohérentes, structurées au niveau mondial ou transnational, avec des moyens financiers et des lieux d'accueil importants. Certaines organisations, comme l'ONU ou l'OTAN, ne disposent pas de forces propres, mais recourent à celles d'autres pays. Elles utilisent de manière importante des systèmes sophistiqués, parfois fournis par les Etats-Unis ou d'autres pays développés. Même si, à proprement parler, ces organisations ne font pas de commerce, elles jouent un rôle de suivi, de législation important et essentiel pour un développement harmonieux du cyberspace et, surtout, de l'ordre mondial associé. D'autres exemples concernent des associations du crime organisé ou de terrorisme, éventuellement soutenues par certaines nations. Leur adaptabilité aux nouvelles technologies de l'information en fait des composants perturbateurs à ne pas négliger. Leur puissance a été dramatiquement révélée par l'attentat du 11 septembre.
7. Enfin, la septième catégorie comprend des groupes fragmentés, décentralisés ou des individus. Leurs disponibilités sont généralement faibles, mais leur capacité à faire des dégâts ou des bénéfices est considérablement accrue par la technologie et la possibilité d'utiliser l'infrastructure de leurs ennemis. Ce sont notamment quantité de pirates informatiques, qui se sont révélés lors de plusieurs attaques de sites Web, mais aussi que certains ont menacé d'employer lors de conflits locaux, comme ceux du Timor oriental.
8. Comme on le voit, avec le cyberspace, l'environnement mondial, les interlocuteurs changent. Ils s'échelonnent de la superpuissance mondiale (actuellement les Etats-Unis) à l'individu mal intentionné.

A ce stade, il n'est sans doute pas inutile de remarquer que cette nouvelle division du monde est compatible avec celle des trois vagues de Toffler. Aux catégories 1 à 3, l'accès à la Troisième Vague, avec la catégorie 6 pour régulateur ou gendarme. Aux autres, le maintien dans les première et deuxième vague. Quant à certains de la catégorie 6 et de la septième catégorie, il s'agit des empêcheurs de dominer en rond. Les idéologies marquent aussi la géographie économique.

Il n'est pas non plus inutile de remarquer que, aujourd'hui, avec le cyberspace, le groupe des trois grandes puissances économiques (Etats-Unis, Europe, Japon) est divisée. Et ce, au profit du premier, les Etats-Unis. Ainsi donc, le cyberspace établit de nouveaux rapports de force ou consolide les rôles des puissants et des serviteurs. Mais il permet aussi l'arrivée de nouveaux acteurs non désirés, qui risquent de menacer l'ordre en cours d'établissement. Quant au futur, les cartes des grands programmes de déploiement des fibres optiques confirment ce qui a été dit précédemment.. L'Afrique sera contournée, avec quelques branchements, dont un vers l'Afrique du Sud. Quant au détroit de Gibraltar et au canal de Suez, ils sont des lieux de passage obligés des fibres optiques et, donc, redeviennent des endroits stratégiquement importants.

3. Les leçons du 11 septembre 2001.

Jusqu'au 11 septembre 2001, tout semblait conforter cette vision de la domination du monde par le cyberspace. Mais, ce jour-là, tragiquement, la démonstration fut faite qu'il faut revoir certains concepts. Car qu'est-il arrivé ce jour-là ?

Nous avons tous en tête les images souvent diffusées des collisions des avions sur les tours jumelles du World Trade Center à New York. Nous revoyons l'effondrement des tours, la fuite des gens dans les rues envahies par un nuage de poussières. Nous revoyons, moins distinctement, l'incendie du Pentagone à Washington, ainsi que la vue lointaine des débris du quatrième avion. Nous nous souvenons du premier discours du président Bush, de sa disparition pendant quelques heures, de ses autres discours s'étonnant que l'on puisse faire du mal à l'Amérique, si « bonne », de son ton guerrier lorsqu'il parle de poursuivre les commanditaires des attentats, et de les prendre, morts ou vifs, comme dans les plus célèbres westerns.

Mais si on connaît les événements et les suites, a-t-on réfléchi à ce que le fait que les attentats aient pu se produire signifie ? A-t-on pris conscience que le 11 septembre 2001 représente une sanglante et cinglante défaite pour les Etats-Unis ? Qu'il ne s'agit pas seulement de terrorisme, mais de la première bataille perdue d'un nouveau type de conflit, pourtant prévu : un cyberconflit. Il s'agit bien d'un cyberconflit, car les terroristes ont utilisé le cyberspace, en déjouant les énormes moyens déployés pour les empêcher de nuire. Si les terroristes ont réussi leurs actions, c'est que quelque chose a raté en Occident. Ou, en tout cas, que des hypothèses de départ se sont révélées fausses. Quoi ? Pour s'en rendre compte, une lecture des événements ayant eu lieu avant et après le 11 septembre 2001 est utile.

Avant le 11 septembre 2001

Dans les jours qui ont suivi les attentats, plusieurs commentateurs les ont comparé à l'attaque de Pearl Harbor, le 7 décembre 1941. Les Etats-Unis ne s'attendaient pas certes ni à l'attaque de Pearl Harbor ni aux attentats du World Trade Center ; mais la comparaison s'arrête là. Car ils connaissaient Ben Laden, et ils n'ont pas réussi à le surveiller. Depuis le premier attentat à l'explosif contre le WTC, le 26 février 1993 ; après les destructions aux ambassades américaines à Nairobi (Kenya) et à Dar Es-salaam (Tanzanie) le 7 août 1998, après la destruction du destroyer USS Cole à Aden (Yémen) le 12 octobre 2000, tout le monde connaît le nom du commanditaire : Oussama Ben Laden. Dans une interview bien connue, il a décrété la guerre sainte contre les Etats-Unis et l'Occident. On sait qu'il dirige le réseau terroriste Al-Qaida. Il est considéré comme l'ennemi public numéro 1 des Etats-Unis [7] et, donc, est très surveillé. L'histoire nous dira pourquoi les attaques ne furent pas prévues.

Maintenant que les médias ont révélé le parcours des terroristes, la coordination de leurs entraînements au niveau mondial, mais aussi l'incroyable non infiltration des réseaux terroristes par les services secrets occidentaux, on peut au moins affirmer que plusieurs hypothèses de base de la domination du monde par la maîtrise de l'information sont remises en cause :

- *Hypothèse 3c : avec l'électronique, les hommes ne sont plus aussi nécessaires.* C'est évidemment faux. Si les services secrets avaient réussi à infiltrer le réseau Al-Qaida, certaines choses auraient **peut-être** pu être prévues. Cette hypothèse repose sur l'oubli que l'information est, à la base, une affaire d'hommes. Ce sont eux

qui communiquent. Pas les machines, qui ne sont que des outils aux mains des hommes.

- *Hypothèse 3b : grâce à l'électronique, les risques liés aux erreurs humaines sont supprimés.* C'est faux, car, au départ, ce sont des hommes qui dictent aux machines ce qu'elles doivent faire. Ce sont des hommes qui programment les logiciels d'analyse de données, qui disent l'importance à accorder à certains mots-clés. Plus pervers encore, ce sont les hommes qui dictent le poids mathématique à accorder à un terme. Si, par exemple, le seuil pour retenir un mot est à un poids déterminé par l'homme de 50%, et que l'ordinateur lui calcule dans un message un poids de 49,99%, il ne sera pas retenu. Ce sont les aléas des statistiques appliquées au contrôle de l'information.
- *Hypothèse 3a : l'électronique est l'outil le plus efficace pour la maîtrise de l'information.* C'est partiellement vrai, si on considère que la quantité d'informations à traiter est telle qu'aucun homme ou groupe d'hommes n'est capable de tout lire. C'est partiellement faux, car l'électronique ne fait que ce que les hommes lui disent de faire. Et la quantité d'informations échangées étant énorme, on ne peut tout contrôler. Sauf hasard, il faut savoir qui contrôler au départ. Après coup, on peut, peut-être, savoir qui a envoyé quoi à qui. Pendant, cela relève de la loterie. Le système d'écoute planétaire *Echelon* a échoué pour trois raisons :
 - 1) l'impossibilité de tout traiter ;
 - 2) parce que les Etats-Unis ont eu tendance à dévoyer ces écoutes pour récolter des informations économiques au détriment du renseignement militaire ;
 - 3) parce que le réseau est connu du grand public et donc, évidemment, des terroristes, qui se méfient des communications classiques.

A ces éléments, il faut ajouter que, dans la préparation du 11 septembre 2001, les terroristes ont utilisé les ressources d'*Internet* à bon escient. En effet, parmi les risques liés au cyberspace [2], le premier est son utilisation pour ce qu'il est prévu : échanger des messages, des e-mails. Ce que les terroristes ont certainement fait. Qui plus est, cela a pu se faire discrètement par l'utilisation de logiciels de cryptage, disponibles librement sur le réseau.

Mais ils ont aussi pu contourner nombre d'obstacles présents sur le réseau en... n'utilisant pas *Internet* et d'autres voies classiques. Car il s'agit là aussi de quelque chose que les spécialistes de l'électronique et de l'informatique semblent avoir oubliée : il y a d'autres moyens de communiquer que les voies informatiques. Après tout, cela n'a rien d'étonnant, car les premiers logiciels permettant de surfer, d'envoyer des e-mails, à savoir *Mosaic* puis *Netscape*, ne furent diffusés qu'en 1993. Croire que cela est entré dans les mœurs de chacun sur Terre est une aberration, une illusion d'optique de notre société occidentale hyper-rapide et développée. Ceux qui sont isolés dans les contrées désertiques d'Afghanistan et autres Somalie n'ont pas nos réflexes. Ils raisonnent encore « à l'ancienne », et, malheureusement, avec une grande efficacité meurtrière.

Ceci implique que si :

- *Hypothèse 2: la maîtrise de l'information est nécessaire pour pouvoir dominer le monde,* on peut aussi affirmer aussi péremptoirement que :
- *Contre-hypothèse 2: la maîtrise totale de l'information est un leurre.* En effet, pour cela, il faudrait qu'elle soit contrôlable. Or, elle ne l'est ni pour des raisons techniques, ni parce que tout le monde n'utilise pas les canaux adéquats, ni parce que tous les

habitants du monde n'y ont pas accès. Combien d'êtres humains n'ont-ils jamais vu de téléphone ?

Tout au plus pourrait-on affirmer que :

- *Hypothèse 2 modifiée : la maîtrise de l'information est nécessaire pour pouvoir dominer ceux qui possèdent et utilisent les canaux d'information adéquats. Ce qui est certes important, mais pas suffisant pour contrôler certaines menaces non sophistiquées, comme les menaces terroristes.*

Après le 11 septembre 2001

L'infodominance ne signifie pas uniquement la surveillance, l'espionnage. Il faut encore pouvoir contrôler l'information diffusée. De ce point de vue, l'après 11 septembre est instructif.

La diffusion de l'information par les médias est mondiale. Elle n'est plus seulement du ressort de l'Occident. La chaîne Qatari Al-Jazira en est la preuve. Inconnue chez nous avant le 11 septembre 2001, elle est devenue la chaîne de référence des pays arabes et musulmans. Elle a diffusé les cassettes de Ben Laden, contournant ainsi la censure des milieux occidentaux. Lesquels, par ailleurs, n'étaient pas tous d'accord de s'auto-censurer sur toutes les informations disponibles. Ainsi, à côté de l'Occident, s'est développée une infrastructure d'information indépendante de l'Occident, crédible, mais non contrôlable par les puissants occidentaux. La pilule a dû être dure à avaler pour certains. Cela conforte la contre-hypothèse 2 ci-dessus.

Quant aux Etats-Unis, trois épisodes valent la peine d'être mentionnés : la couverture du conflit en Afghanistan, l'Anthrax, la cassette des aveux de Ben Laden.

En ce qui concerne la couverture du conflit en Afghanistan, l'armée américaine semble avoir compris les leçons du Vietnam et de la guerre du Golfe. Lors de la guerre du Vietnam, les militaires américains ont laissé faire les médias. Ceux-ci ont montré nombre de scènes de guerre qui ont eu pour effet de rendre la guerre impopulaire aux Etats-Unis et ailleurs. Les militaires ont compris la leçon. Pendant la guerre du Golfe, les militaires ont parfaitement maîtrisé les informations par rapport aux opérations militaires menées sur le terrain. Résultat : lorsque, après le conflit, les détails sur les circonstances de la guerre du Golfe ont été révélés, les médias et le public se sont sentis trompés. On nous avait dit que les missiles Patriot avaient détruits les missiles Scud, alors que ceux-ci se sont simplement désintégrés avant d'atteindre le sol ; on nous a dit que la victoire avait été acquise grâce aux frappes chirurgicales des missiles intelligents, alors que l'on a caché les tonnes de bombes lancées en tapis sur l'Irak dans les derniers jours des conflits ; etc. La désinformation a marché sur le moment, mais les réactions des médias et du public ne se sont pas faites attendre. On n'a plus confiance dans les informations fournies par les militaires. On l'a bien vu lors de la guerre du Kosovo, quelques années plus tard. Nous montrait-on bien la vérité ou étaient-ce des documents truqués ? Et le doute portait sur les informations provenant des deux camps. Pendant le conflit en Afghanistan, le contrôle militaire de l'information a été particulièrement strict. On ne révélait presque rien. A part les occasions de montrer que l'Amérique est « bonne », lors du largage de vivres. La meilleure information militaire médiatique est celle qui n'existe pas.

Avec les épisodes des lettres à l'anthrax, il semble que la même tactique ait été utilisée. Mais, ici, à cause du fait que les événements aient eu lieu sur place et que la population soit peu informée des questions scientifiques et médicales, cela a donné lieu à une panique

généralisée. Quant à la possible confirmation de l'origine américaine de l'anthrax, l'avenir nous dira l'effet que cela aura sur la confiance des citoyens américains dans leurs autorités.

Et puis, il y eut le rapide épisode de la cassette trouvée par hasard en Afghanistan, et dans laquelle Ben Laden en personne raconte ce que nous voulions qu'il dise : il est bien le commanditaire des attentats du 11 septembre et, même, l'organisateur. Cette cassette en a convaincu certains, mais en a laissé beaucoup dans le doute, même aux Etats-Unis. Ce doute de certains vaut la peine d'être mentionné : tout le monde n'a plus confiance dans l'information officielle. C'est un effet pervers, dangereux pour la démocratie, de l'usage inconsidéré de la fausse information.

Ces trois épisodes démontrent que la maîtrise de l'information n'est pas quelque chose d'évident quant à ses retombées. Cela accrédite même une nouvelle contre-hypothèse :

- *Contre-Hypothèse 2 modifiée : la maîtrise de l'information n'est pas suffisante pour pouvoir dominer ceux qui possèdent et utilisent les canaux d'information adéquats.*

C'est qu'il ne faut pas négliger l'esprit critique des citoyens. Et ils n'aiment pas être trompés. Si, sur l'instant, cela marche la première fois, rien n'indique que cela marchera la deuxième fois. Et il ne faut surtout pas croire que les critiques se tairont. A l'opposé, le manque de culture, notamment scientifique, de beaucoup de citoyens est un élément amplificateur d'effets de paniques. Dominer, cela implique agir sur des êtres humains, qui ne sont pas des robots.

Maîtriser l'information, c'est aussi maîtriser les médias. Il peut être facile de diffuser de la fausse information sur *Internet*, mais qui la lit. La plupart des internautes n'utilisent pas le réseau pour s'informer sur la politique ou le militaire (sauf dans quelques cas très particuliers). Ce sont les journaux, les radios et les télévisions qui ont ce rôle de diffusion et d'analyse de l'information. Or, les journalistes ont pour règle de trier et de vérifier l'information. Certes, il est toujours possible de mettre une fausse information sur un nombre suffisant de sites pour que la véracité soit impossible à vérifier. Mais l'opération est dangereuse.

4. Et maintenant ?

Dominer le monde en maîtrisant l'information est un concept séduisant. Malheureusement, il s'agit d'une illusion dangereuse.

C'est une illusion, comme une réflexion critique sur les événements autour des attentats du 11 septembre 2001 le démontre.

C'est une illusion dangereuse, car, en se braquant sur l'infodominance, on néglige d'autres problèmes importants pour notre planète, on distrait l'attention des gens. En évitant de regarder les problèmes en face, en poursuivant une fuite en avant, on fonce dans un mur, les yeux fermés. Le réveil sera dur. Car les événements du 11 septembre 2001 ont montré que l'Occident est vulnérable. Il est malheureusement probable que cela donnera des idées à certains.

Si on ne veut pas que ces événements tragiques se reproduisent, il est temps de reconnaître les problèmes liés à l'infodominance. Mais quel sera le futur. Deux voies principales s'offrent à nous.

La première est de se dire que le concept d'infodominance reste valable. Mais on n'a pas mis l'accent sur ce qu'il fallait. Il convient d'aller plus loin, de renforcer la surveillance, les

renseignements. Donc de mettre sur pied de nouveaux systèmes plus sophistiqués. C'est la fuite en avant, notamment technologique.

La deuxième est de réfléchir de manière critique sur les concepts de base de l'infodominance et d'oser reconnaître que l'Occident a perdu une bataille majeure. Il faudrait alors réfléchir à de nouvelles manières de conduire les affaires du monde.

Aujourd'hui, il semble que, du moins aux Etats-Unis, ce soit la première voie qui soit choisie par l'administration Bush. Il est vrai que les intérêts de divers secteurs industriels (militaro-industriel, informatique, espace,...), d'organismes de renseignements (NSA, CIA, FBI, etc.) sont tels qu'il n'est guère possible de renverser le courant. Les Etats-Unis sont probablement arrivés à un point de non retour. L'avenir de la sécurité s'y annonce difficile.

Quant aux Européens, si les secteurs du renseignement et industriels sont actuellement moins développés, le mode de pensée des responsables est très semblable à celui des Etats-Unis. Devrons-nous attendre un 11 septembre en Europe pour réagir ?

Notes :

0. F.-B. Huyghe, *L'ennemi à l'ère numérique* (PUF, Paris, 2001).
1. M. Wautelet, *Les cyberconflits* (GRIP-Complexe, Bruxelles, 1998).
2. L. Murawiec, *La guerre au XXI^e siècle* (Odile Jacob, Paris, 2000).
3. A. Mattelart, *Histoire de la société de l'information* (La Découverte, Paris, 2001).
4. F.-B. Huyghe, in : *L'information, c'est la guerre* (Panoramiques, Paris, 2001).
5. M.C. Libicki, « Information Warfare: A Brief Guide to Defense Preparedness », *Phys. Today* (Sept. 1997), pp. 40-45.
6. Michel Wautelet, *Les missiles intelligents*, Labor, Bruxelles, 1992.
7. Denis Jeambar (sous la direction de), *La première guerre du XXI^e siècle*, L'Express Editions, Paris, 2001.