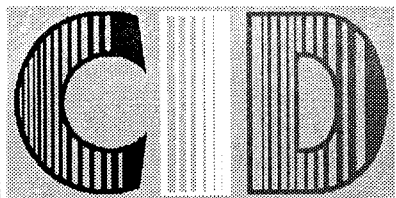


1998 . 263

COLLEGE INTERARMEES



DE DEFENSE

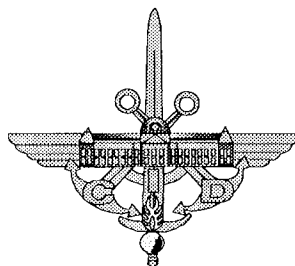
D 11

EPO FED N°3.

## Etude particulière à option

# Nouveaux médias et actions psychologiques en temps de crise

Sous la direction de M. François Géré, directeur d'étude



Commandant (T) Mohamed BERRID (Maroc)  
Commandant (A) Bruno MIGNOT  
Lieutenant-colonel (A) Sultan MUNZER (Liban)  
Chef de bataillon (T) Thierry PRUNIERE  
Lieutenant-colonel (T) André VIDALIS (Grèce)

5° PROMOTION 1997-1998



## INTRODUCTION

### I/ REMARQUES PRELIMINAIRES

#### 11. Les acteurs et la crise.

1.1.1. définir la crise.

1.1.2. définir les acteurs et les liens qui les unissent.

#### 12. L'action psychologique.

1.2.1. Définition.

1.2.2. Le but.

1.2.3. Comment.

#### 13. Les nouveaux médias.

Conclusion partielle.

### II/ LES NOUVEAUX PHENOMENES MEDIATIQUES

#### 21. Evolutions décisives.

2.1.1 Le perfectionnement de la technique.

2.1.2 L'évolution des mentalités.

#### 22. Le seul nouveau médium : INTERNET.

2.2.1 Historique de la création d'Internet.

2.2.2 Fonctionnement du réseau.

2.2.3 Etat actuel.

2.2.4 Les enjeux.

#### 23. La télévision numérique.

2.3.1. Numérisation et chaînes de télévision.

2.3.2. Technologie numérique et reportages.

2.3.3. Technique numérique et manipulation de l'image.

#### 24. Analyse des conséquences de ces changements.

2.4.1. Le poids de la Télévision dans les médias actuels .

2.4.2. Modification du support principal.

2.4.3. Un public plus critique.

2.4.4. Un nouveau rapport de force.

2.4.5. Conclusion partielle.

## **III / MESURES ET CONTREMESURES**

### 31. Actions psychologiques sur le réseau Internet.

- 3.1.1. Comment agir sur Internet en temps de crise ?
- 3.1.2. Comment se prémunir des actions psychologiques ?

### 32. Techniques numériques et actions psychologiques.

- 3.2.1. Apport du numériques et actions psychologiques.
- 3.2.2. Dispositions et précautions à adopter.

### 33. Un concept d'actions psychologiques.

- 3.3.1. Un concept nécessaire.
- 3.3.2. Recenser les moyens nécessaires.
- 3.3.3. les modes d'actions.

### 34. Les méthodes.

- 3.4.1. Méthodes pour aujourd'hui.
- 3.4.2. Méthodes pour demain.
- 3.4.3. La nouvelle stratégie américaine du savoir.
- 3.4.4. L'utilisation des faiblesses des médias.

## **CONCLUSION.**

## **BIBLIOGRAPHIE.**

## **CONTACTS.**

## **ANNEXE A.**

## **ANNEXE B.**





## INTRODUCTION

Au cours du XXe siècle, la propagation des idées, la formation intellectuelle et l'instruction des populations ont conduit les sociétés évoluées à diffuser une masse toujours plus importante d'informations. Concomitamment, le progrès technique a donné aux hommes les instruments nécessaires à la circulation de l'information.

Devant une telle expansion, les moyens de communication ont pris eux aussi un essor fantastique. La puissance des médias s'en est ainsi renforcée, certains affirmant qu'ils sont désormais devenus un "quatrième pouvoir". Tout gouvernement démocratique ne peut dorénavant inscrire sa politique hors des aspirations de son opinion publique. La tâche des responsables politiques et militaires est d'autant plus délicate que leur liberté d'action se trouve aujourd'hui limitée par le rôle croissant que jouent les médias dans le traitement des crises. Les opinions publiques sont devenues accessibles par des acteurs non-étatiques et vulnérables face à des actions médiatiques pouvant, du fait de la désinformation et de l'explosion des nouveaux systèmes, aller à l'encontre de la vocation des choix, ou des intérêts du pays.

Cependant, l'information n'est pas l'apanage des médias. En effet, elle affecte l'ensemble de la société contemporaine. Aujourd'hui, son influence se mesure à la multiplication des services de "communication", et à celle des postes de travail informatique - ces derniers sont attractifs parce qu'ils offrent des vitesses de travail et de traitement, ainsi que des capacités de stockage immenses, mais également parce que les ordinateurs sont devenus les vecteurs essentiels à la communication ouverte sur l'entreprise (Intranet) et sur le monde (Internet).

Or, le mensonge ne date pas d'hier. L'information est destinée à l'homme qui, jusqu'à présent, demeure encore celui qui décide en dernier ressort. Donc, par nature, elle est le lieu idéal d'actions psychologiques. Nous assistons actuellement à l'émergence de moyens de communication nouveaux - il s'agit d'Internet et, dans une moindre mesure, des réseaux internes Intranet - et à une évolution de moyens plus anciens, suffisamment significative pour affirmer qu'il s'agit là d'une véritable révolution - c'est l'arrivée du traitement numérique de l'information. Ce qui est réellement nouveau, c'est la possibilité de manipuler le contenu des systèmes d'information - l'information elle-même - et le contenant - les outils nécessaires pour mettre en forme et acheminer cette information. C'est également la possibilité de contrôler, grâce à l'offre dans le domaine des réseaux, des machines et des logiciels applicatifs, le support de l'information et l'information elle-même<sup>1</sup>.

Déjà, les analystes observent les conséquences de ces deux phénomènes. Mais elles sont caractéristiques du temps de paix au cours duquel elles sont nées. En ce qui concerne le milieu de la défense, il y a lieu de s'interroger sur les nouveaux médias et l'action psychologique dès lors qu'une crise apparaît.

Le XXIe siècle sera, dit-on, le siècle de la communication. Par ailleurs, nous assistons aujourd'hui à la conjonction de plusieurs faits : la fin de la guerre froide, la suprématie des Etats-Unis d'Amérique, le renforcement de l'Organisation des Nations unies. Des idées autrefois en sommeil émergent désormais pleinement : la paix entre les peuples et le respect de la vie humaine.

<sup>1</sup> Voir l'article du Colonel Molinier, revue *L'Armement*, n°60 de décembre 1997-janvier 1998, p13.

Des concepts apparaissent, ceux de "zéro mort", d'ingérence humanitaire... En outre, le progrès technologique permet de penser à de futurs "autoroutes de l'information", ouverts à tout le monde. Un tel rétrécissement des distances s'accompagne d'une demande d'information toujours plus grande, donc de méthodes de travail différentes.

Les nouveaux médias que sont Internet et les télévisions numériques offrent des champs d'action psychologique gigantesques, surtout en temps de crise car, à ce moment-là, le temps réel prime. Il convient donc de bien cerner les possibilités de ces actions, de savoir comment s'en prémunir et d'apprendre éventuellement à s'en servir.

Volontairement limité aux nouveaux médias et au temps de crise, ce travail propose de mener l'étude du sujet suivant un plan choisissant de bien définir, au préalable, les acteurs du temps de crise et le champ d'application de l'action psychologique en général.

Puis, il s'agira de présenter les nouveaux phénomènes médiatiques avant de développer une analyse concernant les conséquences des changements en cours. C'est alors qu'on pourra aborder le cœur même du sujet : les actions psychologiques possibles en temps de crise grâce aux nouveaux médias, et les contre-mesures à adopter afin de les détecter et de s'y opposer.

## I- REMARQUES PRELIMINAIRES

Un tel sujet impose de reprendre les termes du titre afin d'en définir les contours. C'est ce que nous ferons dans ce premier chapitre en gardant à l'esprit l'angle très particulier qui nous intéresse pour insister sur les interactions que nous considérons significatives. Dans un premier temps, nous tenterons de cerner ce qu'est une crise dans un pays démocratique. Puis, nous verrons pourquoi l'action psychologique (re)devient une arme moderne, bien que difficilement maniable pour des raisons éthiques et pratiques. Enfin, l'expression "nouveaux médias" mérite bien une introduction avant un développement plus long dans le deuxième chapitre.

### 11. Les acteurs et la crise

Après avoir constaté la variété des situations que recouvre le mot crise, nous présenterons les différents acteurs et les liens qui relient les différents protagonistes dans une société démocratique où les médias sont omniprésents.

#### 111. Définir la crise

Le mot crise vient du grec *krisis* qui signifie décision. Il en résulte que la crise doit correspondre à un état essentiellement transitoire, à un brusque changement, une période courte de manifestation aiguë d'un phénomène ou d'une rupture d'équilibre, qui amène un responsable à prendre une décision<sup>2</sup>.

Etymologiquement, la crise impose donc au responsable de prendre position, de réagir à une situation mouvante. Elle peut être nationale (manifestation des chômeurs français durant l'hiver 1997), nationale mais avec des répercussions internationales (grèves des routiers français) ou internationale (ultimatum américain contre l'Irak en février 1998). La liberté d'action d'un gouvernement est d'autant plus réduite que les répercussions de ses actions auront un retentissement international.

Les crises entraînent une brusque et volumineuse demande d'informations dont dépendront les retombées en termes d'images. Elles ne sont ni grandes ni petites ; il n'y a que des effets plus ou moins bien contrôlés de gestion de crise. Il faut différencier trois périodes dans cette gestion des images :

- "l'avant" ou, plus exactement, les prémices : les tensions existent mais le problème reste encore relativement confidentiel ;
- le "pendant" : la crise bat son plein ;
- la "sortie" où une défaite politique peut être encore transformée en victoire médiatique.

Notons que les crises ne sont pas un phénomène nouveau, mais, dans nos sociétés, le niveau politique impliqué dans le traitement du problème est souvent très élevé. Les décisions sont prises à un haut niveau, la gestion est centralisée et les initiatives des exécutants sur le terrain sont limitées. Cet état de fait facilite la nécessaire coordination des différents acteurs gouvernementaux et doit permettre, dans le cadre de l'action psychologique, l'indispensable définition d'un but unique.

Il n'existe pas de définition juridique du mot crise. Quant une démocratie est en guerre, le gouvernement dispose de pouvoirs particuliers sur l'information, ce que l'opinion publique et la presse acceptent globalement. En temps de paix, l'opinion publique exige une très grande transparence. Or il n'y a pas de situation intermédiaire qui permettrait à un gouvernement, lors d'une crise grave, d'intervenir dans la boucle de l'information en s'appuyant sur un cadre juridique. Cette

<sup>2</sup> D'après le dictionnaire *Petit Robert*.

absence est à comparer au véritable travail sémantique effectué dans le cadre des actions de l'ONU, qui distingue entre les deux états paix/guerre, le *peacemaking*, le *peace enforcement*, le *peace consolidation*, le *peace implementation*, le *peace keeping* et le *peace building*<sup>3</sup>. A chaque palier, une stratégie de communication différente peut être mise en place.

### 112. Définir les acteurs et les liens qui les unissent

Les décideurs doivent "gérer" la crise quasiment en temps réel. Ils ont perdu le privilège d'être informé avant l'opinion publique. Or, cette dernière exige la transparence des débats, de l'action. Le silence est interprété comme un aveu de la faute<sup>4</sup>. Dans nos sociétés, il y a nécessairement communication quand il y a crise. C'est tellement important que, parfois et malheureusement, l'annonce d'une décision vaut acte.

Les liens entre les médias et le décideur sont très ambigus. Ce dernier est à la fois débiteur - il veut faire passer son message, et créateur puisque il constitue une source de renseignements privilégiée pour les médias. Enfin, il est aussi consommateur, puisque lecteur ou téléspectateur assidu pour savoir comment son message est rendu.

Les médias, parfois qualifiés de quatrième pouvoir, ont un rôle central mais complexe à quantifier dans une crise. Toutes les chaînes revendiquent l'indépendance face au pouvoir politique<sup>5</sup> et l'objectivité de la présentation de l'information.

Les médias sont divers ; leur vocation est locale, régionale, nationale ou internationale. La presse traditionnelle se divise en presse écrite, parlée ou télévisée et doit répondre à des attentes différentes de la part des clients. En simplifiant, on peut écrire que la télévision rend compte dans l'immédiateté, la radio fournit les explications et la presse écrite commente. Les besoins, les buts, les centres d'intérêts et les méthodes de travail ne sont donc pas semblables. Néanmoins, tous recherchent la crédibilité qui fidélisera la clientèle indispensable à leur survie.

Cependant, le pouvoir réel des médias demeure un mystère pour les chercheurs : "La recherche récente en communication de masse paraît être marquée par une certaine incertitude. Non seulement les chercheurs travaillent dans des directions de plus en plus divergentes, mais rares sont ceux qui estiment pouvoir aboutir à des diagnostics assurés quant aux effets des médias"<sup>6</sup>. Cette phrase de la conclusion de G. Derville montre bien le désarroi des scientifiques pour prouver ce que nous croyons savoir instinctivement sur le pouvoir des médias.

L'opinion publique, l'enjeu en quelque sorte de la bataille moderne que livre un gouvernement démocratique remettant sans cesse en cause sa légitimité, est moins faible et désarmée qu'on veut souvent le dire. Le citoyen est fort de son droit de vote : c'est son pouvoir sur l'homme politique. Il achète ou non l'information : c'est son pouvoir sur les médias. Mais également, "la presse forme moins l'opinion du lecteur qu'elle ne la subit"<sup>7</sup>. L'opinion publique n'est donc pas uniquement un récepteur passif. Ce modèle, émetteur (médias)/récepteur (spectateur) dépassé depuis longtemps, ne peut que se désagréger encore un peu plus avec le développement des nouveaux médias.

Les protagonistes d'une crise vont désormais tenter d'éveiller la curiosité de l'opinion publique, puis de la mettre en mouvement de façon à ce qu'elle s'implique dans la crise. Ce n'est pas tout à fait la même chose, ainsi les Américains se sont passionnés pour les supposées frasques sexuelles de M.

<sup>3</sup> Rétablissement de la paix, imposition de la paix, consolidation de la paix, mise en application de la paix, maintien de la paix, reconstruction de la paix.

<sup>4</sup> Le groupe anglo-néerlandais Shell l'a encore constaté lors de l'affaire de la plateforme pétrolière l'ayant opposé à Greenpeace, en 1996.

<sup>5</sup> L'indépendance face au pouvoir économique est une question autrement sensible.

<sup>6</sup> Voir le livre *Le pouvoir des médias* de G. Derville, PUG, 1997, p 158.

<sup>7</sup> Voir *Le journal, miroir des lecteurs ?* de M. Goissaudeau, in *Comment va la presse*, 1984.

Clinton, sans pour autant que la cote de popularité du président des Etats-Unis ne soit entamée. Ils ont ainsi déjoué tous les pronostiques politiques<sup>8</sup>.

Les forces en présence, manifestants, forces armées, forces de l'ordre..., qu'elles soient constitutionnelles ou non, sont conscientes de l'importance des images et de la communication. Chaque camp fait donc de gros efforts pour séduire le journaliste dans l'espoir qu'il fera (consciemment ou non) mieux passer le message auprès de l'opinion publique.

Même si, désormais, toutes les institutions communiquent, les forces "de l'ordre" en général pâtissent d'un manque d'exploitation de l'arme médiatique durant l'action. Elles conservent une certaine frilosité devant les caméras, tandis que leurs adversaires ciblent de plus en plus leurs actions. Greenpeace s'en était fait une spécialité, mais les coups d'éclat récents<sup>9</sup> des chômeurs prouvent que l'organisation a fait des émules. Les armées françaises ont su, durant l'hiver 1995/1996 gagner la bataille médiatique<sup>10</sup> dans le Pacifique sud. Il n'est pas certain que la police et la gendarmerie exploitent réellement la force de l'image.

Enfin, n'oublions pas que les forces de l'ordre sont composées d'hommes qui, comme leurs concitoyens, ont besoin d'être convaincus du bien fondé de leurs actions et sont sensibles aux actions de guerre psychologique. Dans les conflits armés de haute intensité, plus de 50 % des évacuations sanitaires sont dus non pas à des atteintes physiques mais à des troubles psychologiques. Le moral des hommes et des femmes travaillant pour la Défense est donc primordial. Le grand nombre de suicides chez les policiers - affaire qui défraya la chronique en 1997 - vient sans doute en partie du peu de considération que leur témoignent l'opinion publique et les hommes politiques.

Pour résumer, le mot crise décrit une réalité très vague. C'est le moment rarement prévisible où les différends se durcissent brutalement. Leur gestion est faite à un très haut niveau de l'Etat et toute action est appuyée au plus vite par un plan de communication. Les médias, très variés, présentent, si possible en direct, les événements suivant une déontologie qui leur est propre à une opinion publique très volatile dans son intérêt.

## 12. L'action psychologique

Après avoir expliqué ce qu'il faut entendre par "action psychologique", nous exposerons le but recherché, mais également l'ambiguïté de cette notion.

En préambule, pour comprendre à quelle difficulté particulière la réflexion se heurte en France, il faut rappeler que cette expression nous ramène à la guerre d'Algérie et au "5e bureau". Une partie de l'intelligentsia française a depuis banni ce mot de son vocabulaire. Derrière le concept d'action psychologique, le déni de démocratie ne semble jamais loin. Cela inhibe certainement nos autorités politiques, militaires et universitaires et explique en partie le retard que la France a sur le sujet par rapport à ses alliés anglo-saxons.

### 121. Définition

L'arme psychologique pose fondamentalement un problème de limites et, par la suite, de définition<sup>11</sup>. Pour fixer les idées rappelons que :

- la guerre psychologique vise à dissuader ou à affaiblir l'adversaire et, si possible, à le subvertir, à le désagréger. Elle s'adresse uniquement au camp adverse.

- l'action psychologique se limite, quant à elle, à son propre camp. Le but recherché est de faire serrer les rangs afin que toute la nation soutienne l'action entreprise.

<sup>8</sup> Voir *Comment agir sur l'opinion publique pour que celle-ci influe sur la décision politique ?* de P. Boniface, in *Les manipulations de l'image et du son*, FED, Hachette, p 334. On peut y lire, p 269, "qu'il est beaucoup plus compliqué qu'on ne le pense de manipuler l'opinion publique".

<sup>9</sup> Il est fait référence aux occupations de locaux symboliques, par de très petits groupes. Les médias en parlent alors que l'événement est en lui-même non représentatif.

<sup>10</sup> Au prix d'un effort important en hommes et en matériel.

<sup>11</sup> L'expression est du professeur Dabezies.

Aux yeux de Raymond Aron, la guerre psychologique n'est pas une arme offensive. Il en limite donc le pouvoir. Toutefois, il considère que cinq facteurs doivent être analysés pour la gestion de crise : facteurs politique, géographique, économique et militaire, et la volonté nationale. L'action psychologique permet bien évidemment de modifier très sensiblement le dernier facteur.

Surannée durant la guerre froide, où l'information (et non la propagande) renforçait la démocratie, l'action psychologique redevient très moderne dans un monde où l'on ne cherche plus à anéantir l'adversaire, mais à le "convaincre". Elle devient l'arme par excellence, qui permet à un Etat<sup>12</sup>, en protégeant la légitimité de son action, d'imposer ses vues à une opinion publique plus exigeante en matière d'information. Elle cadre parfaitement à la notion de zéro mort, importante aux yeux de l'opinion publique.

Enfin, ce n'est pas un sujet tabou. C'est une arme complexe, que certains utilisent déjà et il serait très dangereux que la France ne réfléchisse pas à son exploitation ou au moins aux façons de s'en prémunir.

### 122. Le but

Pour les Américains<sup>13</sup>, le but des opérations psychologiques est de produire ou de renforcer des attitudes et des comportements étrangers favorables aux objectifs de leur auteur.

En France, le but est de modeler l'environnement pour favoriser l'action et la résolution d'une crise à son avantage. Il est intéressant de relever<sup>14</sup> que lorsque Koffi Anam négociait avec Saddam Hussein, la presse anglaise regorgeait d'informations sur les "armes" destructrices que ce dernier soustrayait aux inspecteurs de l'armement. Dans le même temps, en France, où le gouvernement soutenait activement les accords de paix, il était plutôt question des souffrances que le peuple irakien endurait à cause de l'embargo. Coïncidence ou preuve que l'action psychologique est déjà une réalité bien présente dans les démocraties ?

Ce qui est certain, c'est que les actions psychologiques ne sont pas une arme absolue. Elles participent avec d'autres à la réussite d'une action. Elles doivent accompagner de façon cohérente les actions entreprises par les autorités. Ce besoin de cohérence impose que la décision de leur mise en œuvre soit prise à un très haut niveau.

En outre, les buts doivent être fixés par une instance politique et non pas par une instance militaire. D'une part, l'action psychologique<sup>15</sup> ne peut être cantonnée au niveau local ou tactique dans le monde actuel : il faut donc une vision globale ; d'autre part, le souci de contrôle démocratique doit être permanent.

### 123. Les moyens

Comment arriver aujourd'hui à mener cette action ? Pour convaincre son opinion publique, il faut lui expliquer la situation, l'informer, donc communiquer. M. Halimi<sup>16</sup>, citant M. Lake<sup>17</sup>, rappelle "qu'avec la rapidité et le pouvoir des images, si nous n'avons pas expliqué au Congrès et au peuple américain en quoi consistent nos intérêts et notre mission, nous ne pouvons plus reprendre les choses en main".

Il faut donc mettre sur pied une structure qui essaie de détecter les crises, afin que l'action psychologique puisse jouer son rôle en amont et dès le début des événements.

<sup>12</sup> Ceci est valable aussi bien pour les crises nationales que pour les actions de l'ONU, par principe internationales.

<sup>13</sup> Dans le *Field Manual 100-6*, paragraphe concernant l'information et les opérations, août 1996.

<sup>14</sup> Ceci est une impression du groupe, non pas un fait statistique.

<sup>15</sup> Il ne faut pas confondre l'action qui est locale, et le but qui doit prendre en compte le problème globalement.

<sup>16</sup> Voir l'article *Les médias nombrilistes, Médias et contrôle des esprits*, dans *Le Monde diplomatique* du 27 août 1995, p 71.

<sup>17</sup> M. Lake est l'assistant du président américain Bill Clinton pour les questions de sécurité nationale.

L'information devient "un moyen au service de toutes les forces", mais aussi un "milieu", un "environnement" (on parle d'infosphère), et un "enjeu" (on parle d'*infowar*). Demain, les opposants s'affronteront donc :

- *grâce à l'information* : la dictature du visible, une action n'a de l'importance que si elle est connue ;
- *dans l'information* : pour convaincre, imposer ses normes ;
- *pour l'information* : savoir, c'est déjà avoir la possibilité de commencer une campagne médiatique.

L'information est une nécessité. Le silence et l'étouffement ne sont plus possibles. D'abord par éthique, comme le note le capitaine Caude<sup>18</sup> : "La propagande démocratique peut difficilement faire admettre à l'opinion publique que, pour des raisons impérieuses de défense nationale, elle n'a pas à lui rendre compte de certains faits". Ensuite, par simple bon sens, comment empêcher les médias d'avoir accès aux événements dès lors qu'ils se passent ? La guerre du Golfe est un cas très particulier, mais une grève nationale et le cas de l'ex-Yougoslavie prouvent l'impossibilité d'une telle solution.

Mais où s'arrête l'information et où commence l'influence ? D'après Nicole Dubois<sup>19</sup>, "on entend par influence - chaque chercheur insistant selon son domaine d'étude sur tel ou tel aspect du phénomène, la façon dont une personne ou des personnes sont amenées à changer de croyance, d'attitude ou de comportement, suite à l'intervention délibérée de ce que nous appellerons une source ou un agent de changement".

Il semble que le *lobbying*<sup>20</sup> - un groupe prépare un dossier complet avec argumentaire pour prouver que son option est la meilleure - réponde parfaitement à cette définition. Or cette pratique est parfaitement admise et avouable aux Etats-Unis ou à Bruxelles ; pourtant, les opposants dénoncent une démocratie sous influence.

La construction d'image est aussi un élément de notre vie démocratique car un homme politique se vend comme un produit. Dans nos sociétés, en réalité, toujours d'après Nicole Dubois, de nombreux corps de métier sont des agents d'influence : les publicistes, les professionnels du *marketing*, les avocats, les éducateurs, etc. Toutefois, il ne semble pas que la démocratie soit mise en danger par ces professionnels de l'action psychologique.

La mésinformation, qui consiste à donner une information fautive en partie ou tronquée, est naturellement moralement condamnable. Pourtant, les Etats-Unis n'ont pas hésité à la pratiquer en ne fournissant qu'une partie de l'enregistrement de la conversation entre le pilote de chasse soviétique et celui du vol 007 de la Korean airlines<sup>21</sup>. Ceci dans le but d'accréditer la thèse que l'avion a été abattu sans sommations. Or, il est désormais établi qu'il y a bien eu mésinformation, mais sans conséquence pour le gouvernement américain qui, dénonçant la sauvagerie de l'action n'a pas répondu aux accusations d'espionnage de Moscou. Le procédé est donc utilisable, utilisé et efficace.

La désinformation demande un montage plus complexe et s'adresse *a priori* à l'adversaire. Le sujet ne sera donc pas développé. Toutefois, il semble difficile, dans le "village planétaire", de monter une opération de désinformation sans que sa propre population soit touchée.

Les armées, qui, depuis plusieurs années, interviennent dans des opérations d'imposition de la paix, ont pris en compte l'action psychologique. En effet, elles connaissent l'importance de la légitimité d'une action auprès de l'opinion publique, des populations secourues et de leurs propres soldats. La dernière instruction générale sur l'emploi des forces terrestres (IGEFT) définit ainsi une sous-fonction "information" et une sous-fonction "gestion des médias", ayant pour objet de mobiliser

<sup>18</sup> Voir l'article *Propagande et guerre psychologique*, revue *Défense nationale*, 2e semestre 1995.

<sup>19</sup> Madame Dubois est professeur de psychologie à l'université de Nancy.

<sup>20</sup> "Groupe de pression", en français.

<sup>21</sup> Voir l'article *Les médias nombrilistes, Médias et contrôle des esprits*, dans *Le Monde diplomatique* du 27 août 1995, p 76.

les énergies, de lutter contre la désinformation et les rumeurs, de justifier l'action auprès de l'opinion, de rassurer les familles et la population, de valoriser les forces et de participer à la désinformation de l'adversaire. Ce type de structure pourrait être coiffée par un organisme gouvernemental plus vaste incluant le ministère de l'Intérieur pour des actions visant l'opinion publique française.

Enfin, l'action psychologique ne concerne pas seulement les faits, mais aussi les normes. De nos jours, les oppositions entre les normes anglo-saxonnes dominantes et les normes françaises, par exemple, sont de plus en plus nombreuses. Il est primordial de défendre son mode de raisonnement, sinon le combat est déjà à moitié perdu. Le même argument n'a pas du tout la même importance si l'on raisonne dans une logique de *copyright* ou de droit d'auteur.

M. Vianson-Ponte assure que "le quatrième pouvoir n'est pas la presse mais l'information. (...) Il ne suffit plus de la contenir par la censure ou la loi, de l'asphyxier par le secret ou de l'envahir par l'intoxication. Il faut désormais utiliser cette arme, s'assurer à tout prix sa disposition exclusive, du moins son usage. Toutefois, un Etat démocratique ne peut, sans se renier, mentir à son opinion publique. Il perdrait rapidement la légitimité constituant le socle de son autorité. L'action psychologique, comme nous l'avons définie, doit être pensée au niveau politique le plus haut, de façon à garantir sa légitimité et son efficacité.

### 13. Les nouveaux médias

Selon le dictionnaire, est un média "tout support de diffusion de l'information (radio, télévision, presse imprimée, livre, ordinateur, vidéogramme, satellite de télécommunications) constituant à la fois un moyen d'expression et un intermédiaire un message à l'intention d'un groupe".

Internet est de toute évidence une nouvelle possibilité d'échanger des messages. Il est incontestablement un nouveau média, mais, plus profondément, il modifie les rapports entre l'individu et la société. Facilitant les échanges d'information, modifiant les possibilités d'accès à la connaissance, Internet modifie naturellement le travail des journalistes, quels qu'ils soient. Par ce biais, il influence nécessairement tous les types de médias.

Les termes de "nouveaux médias", au pluriel, sont donc peut être exagérés au sens strict, mais parfaitement justifiés dans une acceptation globale. Ils soulignent surtout les possibilités nouvelles et encore mal cernées qu'offre un réseau mondial.

Ce réseau se caractérise par la grande liberté qui y règne, que certains<sup>22</sup> voudraient totale. Sans dirigeant, sans hiérarchie, sans début ni fin, ce réseau abolit la territorialité, les frontières. Les Etats, souvent pris de court, faute de spécialistes, peinent et hésitent à adapter les lois (commerciale, pénale...) s'appuyant sur ces notions de plus en plus floues. Comme nous le verrons plus loin, Internet devient surtout attrayant grâce à l'alliance de différentes technologies.

### Conclusion partielle

Dans un monde où l'individu demande toujours plus de compte à l'Etat, où la peur fédératrice et oppressante du communisme s'est estompée, le gouvernement doit plus que jamais expliquer, convaincre son opinion publique de la légitimité des actions menées. Il faut relever la convergence entre les nouvelles disponibilités techniques et les exigences plus pressantes des opinions publiques. L'action psychologique, même avec ses limites et ses dangers, devient donc un moyen privilégié d'action pour les démocraties.

Après une description des possibilités offertes par Internet et des conséquences des phénomènes médiatiques, nous tenterons de montrer comment un gouvernement peut les utiliser dans le cadre d'une action psychologique.

<sup>22</sup> On assiste là encore au combat des normes anglo-saxonnes contre les "autres", Anglais et Américains défendant généralement l'exigence de liberté totale sur le réseau.

## II- LES NOUVEAUX PHENOMENES MEDIATIQUES

Avant d'aborder le cœur du sujet qui nous préoccupe, il convenait de bien rappeler le champ d'application de cette étude *Nouveaux médias et action psychologique en temps de crise*. Nous l'avons fait dans le chapitre précédent.

Le *Larousse* définit les "nouveaux médias", comme "découlant des technologies récentes (informatique, bureautique, etc.), envisagés en particulier du point de vue des débouchés, des marchés qu'ils sont susceptibles de faire naître". Il s'agit maintenant de déterminer quelles sont ces technologies dites récentes ayant une influence sur les médias que nous connaissons, de montrer leur sensibilité aux actions psychologiques, dans un cadre volontairement limité au temps de crise.

Toutefois, il n'est pas possible de mettre délibérément de côté l'évolution de la mentalité humaine - d'ailleurs souvent consécutive au progrès technique, puisque tout média s'adresse *in fine* à l'homme, à sa conscience, à son discernement, à son jugement. Car c'est bien à la conjonction de plusieurs facteurs, matériel et immatériel, que nous devons les transformations actuelles subies par le monde moderne.

### 21. Evolutions décisives

#### 211. Le perfectionnement de la technique

Pendant la deuxième moitié du XXe siècle, deux phénomènes techniques majeurs sont apparus : la miniaturisation des équipements électroniques et la numérisation de l'information.

##### 211-1 La miniaturisation

L'invention du transistor puis celle de la puce ont révolutionné l'électronique, augmentant dans des proportions considérables la vitesse et la capacité de traitement de l'information, tout en diminuant dans le même temps l'encombrement du matériel. La miniaturisation des composants a permis d'accéder à la mobilité. Désormais, l'électronique est présente partout, du réveil à la voiture et naturellement au cœur de l'ordinateur.

Connaît-on l'impact du téléphone portable sur le comportement de l'individu qui pourra bientôt, à partir de n'importe quel point de la Terre, discuter avec un interlocuteur situé aux antipodes ou alerter n'importe quel média ?

La miniaturisation du *hardware*<sup>23</sup> offre également la possibilité de stocker un nombre quasi-illimité de données, de les trier, de les organiser ou de les gérer. Ainsi, l'homme peut multiplier les sources d'informations, les senseurs, les récepteurs. Il doit choisir ; il n'a plus à chercher, il doit commander.

##### 211-2 L'arrivée du numérique

La numérisation est une méthode de traitement qui réduit toute information à une suite de 0 et de 1. Transformées en langage informatique ou immédiatement utilisables en l'état par l'ordinateur, ces suites sont maniables à volonté. On peut les modifier, les convertir, les étiqueter ou les adresser de manière quasi-instantanée. Au début, les informations arrivaient sous la forme analogique, étaient numérisées, traitées ou classées, puis étaient retransformées en signal analogique. Aujourd'hui, de plus en plus de machines travaillent directement en mode numérique, ce qui réduit d'autant le temps de traitement de l'information.

##### 211-3 Un cocktail explosif

<sup>23</sup> *Hardware*, ou matériel, est à opposer à *software*, logiciel.

Chacune des deux évolutions que sont la numérisation et la miniaturisation participe au développement de l'autre. La première contribue à la seconde car les informations numérisées prennent beaucoup moins de place que les analogiques ; à l'inverse, il n'y aurait pas autant de canaux offerts par les satellites si le poids des plates-formes n'avait été considérablement allégé.

Ainsi, la conjonction des deux multiplie les possibilités offertes :

- tout est transformable, même les informations les plus "gourmandes" en octets, comme une photographie ou une image vidéo par exemple. Cela induit des effets fantastiques en ce qui concerne la technique, mais effrayants quant à l'utilisation qui peut en être faite. Nous verrons plus loin ce qu'il en est.

- tout est concevable ; ainsi, les images de synthèse sont-elles élaborées à partir de millions de données récupérées par des capteurs disséminés sur le corps d'un cobaye. Il est même déjà possible de confier à un seul logiciel la conception de telles images sans passer au préalable par le recueil de ces données. Demain, on parviendra à copier parfaitement l'allure d'un humain, sans pouvoir discerner le virtuel du réel.

- tout est réalisable : des progrès immenses en terme de transmission de données ont été faits. Avec la technique récente de compression de données et en utilisant la télécommunication par satellite, les possibilités techniques sont multipliées par un facteur de l'ordre d'un million. L'évolution récente des technologies liées à l'électronique a engendré une véritable révolution en matière d'encombrement, de traitement et de vitesse de l'information.

## **212. L'évolution des mentalités**

Cinquante ans de "paix froide" ont permis au progrès scientifique de poursuivre un essor quelque peu entravé - ou mal orienté - par la Seconde Guerre mondiale. Aujourd'hui, tout est fait pour le bien-être ou le confort de l'homme. Une télévision ne se conçoit plus sans télécommande ou une voiture sans direction assistée. Le confort n'est pas que matériel ; il est tout aussi mental. L'homme considère que tout lui est dû - grâce à l'Etat-providence - et que tout doit lui parvenir sans effort. Le pouvoir des médias, qui récoltent pour lui, mâchent pour lui et digèrent pour lui l'information, s'en trouve *de facto* agrandi. L'appréhension du côté médiatique du comportement humain fait assurément partie intégrante, si ce n'est la plus importante, de toute étude sur l'évolution des mentalités. C'est en jouant sur la perception qu'a l'homme de ce qui se déroule quelque part dans le monde, à travers ce qui lui est présenté, que les nouveaux médias exercent ou non une action psychologique susceptible de modifier la réalité.

### **212-1 La primauté de l'image**

L'arrivée de la télévision, dans les années 50, a radicalement changé l'équilibre qui existait entre les médias : l'image a alors détrôné l'écrit. Au cinéma, on venait chercher le rêve et l'évasion, sachant pertinemment qu'un film n'était qu'une fiction. La télévision brouilla cela. Elle entérina le fait que les hommes étaient désormais enclins à plus de confort, apportant avec elle :

- la facilité car l'unique effort demandé est d'ouvrir les yeux et de "gober" l'image ;
- la synthèse car on appréhende d'un seul coup d'œil la situation des personnes et de leur environnement sans qu'il y ait besoin d'explications interminables ;
- la paresse car l'information ainsi diffusée légitime la passivité devant le petit écran.

### **212-2 La puissance du direct**

La diffusion de l'information pendant la guerre du Golfe a révélé l'impact du direct et l'avènement des réseaux mondiaux de transmission des images.

En France, "trois millions de téléspectateurs étaient face à leur poste le matin du 16 janvier, à l'expiration de l'ultimatum, et ils étaient cinq millions, le 17, à l'ouverture des hostilités, soit 7,8 fois

plus que l'année précédente à la même époque"<sup>24</sup>. Le besoin d'images a même contraint les télévisions à utiliser des images d'archives, sans les nommer, pour faire du remplissage. C'est pourquoi on a vu de vieilles images de manifestations au Liban illustrer celles d'Alger. Quelquefois, la primauté de l'image peut donc conduire au mensonge, voire à la manipulation.

Par ailleurs, le suspens de la crise irakienne, le suivi en temps réel puis l'intervention armée ont conduit à une demande toujours plus grande d'images en direct. Ainsi, on a assisté au couronnement de la chaîne américaine CNN<sup>25</sup>, "la technique (le direct) prenant le pas sur le contenu (l'information). La prééminence de l'image en direct a fait de l'information un spectacle, qui doit se poursuivre quoi qu'il advienne ; dramatisation et besoin d'images en sont les deux principes"<sup>26</sup>.

### 212-3 "L'effet CNN"

Le triomphe de CNN procède de deux phénomènes : d'une part, la possibilité nouvelle de transmettre des images à l'échelle de la planète et, d'autre part, la présence partout dans le monde de récepteurs de télévision, dans les foyers, les hôtels, les administrations.

Aujourd'hui, une information diffusée sur CNN est vérité vraie, de par l'impact qu'elle a sur l'opinion publique mondiale. Ainsi, quand un chef d'Etat désire alerter, convaincre, ou expliquer son point de vue, il passe sur CNN, si possible au *Larry's show*<sup>27</sup>. Il est indéniable que posséder un instrument tel que CNN, c'est posséder une véritable arme de puissance. Depuis la guerre du Golfe, "tous les pays essaient de conserver une parcelle de cette puissance, en adaptant les réseaux régionaux déjà en activité à la peinture mondiale : NHK, Skynews, TF1, Euronews... La mondialisation de la communication a ouvert la voie à la mondialisation de la manipulation"<sup>28</sup>.

CNN n'est pas à proprement parler un "nouveau média" ; elle est une chaîne d'information utilisant à plein le progrès technique. "L'effet CNN" serait en effet bien moindre s'il n'y avait pas l'appoint décisif de la miniaturisation, de la technologie numérique et du progrès des transmissions.

A l'Organisation des Nations unies, on n'hésite pas à dire que "CNN est devenue le sixième membre permanent du Conseil de sécurité". Cette boutade n'est pas dénuée de fondement car elle symbolise la perte du pouvoir régalien des Etats souverains du temps de gestion et de réaction face à l'information.

## 22 Le seul nouveau média : Internet

### 221. Historique de la création d'Internet

Le réseau Internet, qu'on appelle aussi le "réseau des réseaux", a été créé par le département de la Défense américain pendant la guerre froide. Mis en service en 1975, il avait initialement pour nom "Arpanet", du nom de sa créatrice, l'agence américaine DARPA (*Defense advance research projects agency*). Son objectif était de "réaliser un réseau de transmission de données grande distance entre différents centres, capable de résister à une destruction partielle"<sup>29</sup>. Il s'agit alors d'un maillage de transmissions et de protocoles de commutation entre les centres de recherche militaire et universitaire. Puis, plus tard, se sont joints des représentants de sociétés commerciales, à des fins d'expansion et d'intelligence économique. Plus récemment, en 1983, le département de la Défense

<sup>24</sup> *La persuasion de masse, guerre psychologique/guerre médiatique*, sous la direction de Gérard Chaliand, éditions Robert Laffont, p 122.

<sup>25</sup> *Cable news network*, chaîne américaine d'information continue, créée en 1980.

<sup>26</sup> Cf. op. cit., p 124.

<sup>27</sup> Lors de son dernier voyage aux Etats-Unis, le président Chirac est intervenu lors de cette émission afin de légitimer l'ultime campagne d'essais nucléaires qu'il avait décidée quelques temps auparavant.

<sup>28</sup> Cf. op. cit., p 127.

<sup>29</sup> Voir l'article *Internet, un vrai défi pour les armées françaises* du commandant Philippe Danieau, dans la *Tribune* du Collège interarmées de défense de janvier 1998, p 119.

américain a isolé le volet strictement militaire (Milnet), tandis que le volet civil (Arpanet) s'associait à d'autres réseaux existants<sup>30</sup> :

- réseaux continentaux (Ebone, Europanet, MCIInet, Sprintlink, etc.) ;
- réseaux de desserte (Renater, Olean, etc.) ;
- fournisseurs d'accès régionaux reliés aux réseaux téléphoniques ;
- réseaux internes aux entreprises (Intranet).

Réseau mondial d'ordinateurs aux finalités scientifiques, commerciales et communicationnelles "temps réel" remarquables, Internet n'existe dans sa forme actuelle que depuis huit ans environ. Mais plus de 60 millions d'ordinateurs y sont aujourd'hui reliés à travers le monde. M. Vittet-Philippe, expert technique à la Commission européenne<sup>31</sup>, estime qu'Internet "s'est imposé au cours des dernières années comme un des principaux éléments de l'infrastructure de l'information et comme un enjeu essentiel de la société de l'information en Europe".

## 222. Fonctionnement du réseau

On ne peut pas comprendre les possibilités, les limitations et les dangers d'Internet si l'on ne connaît pas son mode de fonctionnement.

### 222-1 Fonctionnement technique

Internet interconnecte des réseaux locaux (*Local area network*), répartis dans des secteurs limités ("Intranet" d'entreprises, centres d'études...), et des réseaux plus étendus (*Wide area network*) qui relient plusieurs réseaux locaux entre eux (par exemple, le réseau national français Renater<sup>32</sup>). Il utilise plusieurs protocoles<sup>33</sup> :

- *TCP IP* : ligne à haut débit acheminant 1,5 millions de bits par seconde, acceptant tout langage informatique, reposant sur des lignes spécialisées, reliées par des commutateurs (la plupart des grands centres et des grandes entreprises se sert de ce protocole pour se connecter sur Internet) ;
- *ATM* (technique temporelle asynchrone) : nouveau protocole capable de transporter des données à très haut débit (des milliards de bits par seconde) donc de transférer de la vidéo.

Chaque adresse sur le réseau est précédée du préfixe "www", signifiant *World wide web* ou "Web", et est composée d'un ou de plusieurs mots se rapportant au site, puis d'un suffixe correspondant à un "domaine"<sup>34</sup> ou d'un bigramme se rapportant au pays d'origine<sup>35</sup>. Les domaines étaient régis jusqu'à très récemment par un centre américain détenant le monopole des dépôts d'adresses, InterNIC. Début 1998, la société NSI, gérant les domaines *com*, *org* ou *net* pour InterNIC, s'est trouvé confrontée à plus d'une centaine de concurrents habilités à commercialiser d'autres domaines<sup>36</sup>. La gestion de ces nouvelles "plaques d'immatriculation" s'est alors décentralisée.

Quelque soit le pays où l'on se trouve, pour accéder à Internet, il faut s'adresser au préalable à un fournisseur d'accès - *Provider*, spécialisé pour les entreprises (en France, ce sont Imaginet, Transpac, Olean, etc.), ou pour le grand public (AOL, Wanadoo, HOL, etc.). La France en compte aujourd'hui 210<sup>37</sup>. Tous les fournisseurs offrent également à leurs clients un mini-site<sup>38</sup> leur permettant, à travers une vingtaine de pages de texte, de présenter des informations personnelles.

<sup>30</sup> Voir article op. cit.

<sup>31</sup> Voir l'étude *Infosphère, espace stratégique ?*, synthèse des travaux du groupe intercomités n° 3, IHEDN, 49e session nationale, mai 1997, séance n°2.

<sup>32</sup> Mis en œuvre par France Télécom, sous la tutelle du ministère de l'Education nationale, le réseau Renater connecte les universités entre elles, ainsi que certains établissements publics comme le CEA, le CNES, le CNRS, l'INRIA, EDF, ou privés, comme l'Institut Pasteur.

<sup>33</sup> Voir l'étude de l'IHEDN, op. cit., séance n°2.

<sup>34</sup> *Com* pour les sociétés commerciales, *org* pour les organisations, *net* pour le réseau, *mil* pour les sites militaires...

<sup>35</sup> *Fr* pour la France, *us* pour les Etats-Unis, *uk* pour le Royaume-Uni...

<sup>36</sup> *Arts*, *firm*, *web*, *info*, *nom* (pour les individus), *rec* (pour les loisirs), *store* (pour les magasins), etc.

<sup>37</sup> D'après le récapitulatif effectué par le mensuel *Planète Internet* dans son n°25 de décembre 1997.

<sup>38</sup> D'environ 5 mégaoctets. C'est le service appelé *Homepage*.

Si l'on possède un logiciel particulier, on peut accéder aux forums de discussion thématique, aussi appelés *Newsgroups*<sup>39</sup>. Ces forums sont créés par cooptation "démocratique", après aval d'une "cyberassociation"<sup>40</sup> implantée aux Etats-Unis mais composée de membres disséminés à travers le monde. Ses membres ne se voient toutefois jamais.

Actuellement, il existe environ 18 000 *Newsgroups*, véhiculant en tout 200 000 messages nouveaux par jour. Pour le confort de l'utilisateur, les fournisseurs d'accès se chargent de rapatrier les *Newsgroups* mais "suppriment de manière totalement arbitraire la facilité d'accès de certains émetteurs"<sup>41</sup> : par exemple, ceux ayant une activité considérée comme pédophile ou néonazie. Cette censure artificielle correspond à des critères qui leur sont propres. N'ayant pas (encore) d'image de gauche, de droite, écologiste, réactionnaire ou autre, les *providers* ne laissent donc qu'un choix limité à leurs abonnés. Toutefois, puisqu'il est presque impossible de tous les vérifier, ces mêmes fournisseurs avouent que le nom du *Newsgroup* est souvent leur seul critère de sélection, ce qui signifie que beaucoup passent à travers les mailles du filet. Néanmoins, ces forums n'étant qu'un regroupement de serveurs, il est possible de retrouver les "interdits" par la voie normale, sans disposer du logiciel supplémentaire, mais cela nécessite un temps de recherche plus long.

Pour se connecter eux-mêmes à Internet, les fournisseurs d'accès s'adressent directement aux grandes entreprises de télécommunications. Les liaisons passent par les lignes téléphoniques, la fibre optique, les faisceaux hertziens ou satellites. Internet n'a pas besoin de point central, si bien que l'information circule par la première voie utilisable.

Pour un utilisateur standard, le coût d'un abonnement varie de 50 à 200 francs par mois, prix auquel il faut ajouter celui de la communication téléphonique, qui n'est pas chère. Toutefois, si l'on s'adresse à un serveur situé aux Etats-Unis, il faut éviter de se connecter pendant les heures de travail américaines car les lignes sont souvent encombrées : le téléchargement est donc plus long<sup>42</sup>.

### 222-2 Matériel nécessaire

Pour se connecter à Internet, il suffit d'un ordinateur, d'une ligne téléphonique et d'un modem. Ce dernier permet la connexion au site et la lecture des fichiers, voire leur transit entre l'installation téléphonique et l'ordinateur. Quand un internaute, où qu'il se trouve, s'adresse à un site, le logiciel de navigation envoie une requête pour obtenir l'adresse numérique correspondante<sup>43</sup>. Cette dernière est fournie par l'un des douze ordinateurs serveurs d'adresses, répartis dans le monde et gérés par l'*Internet assigned numbers authority* (IANA)<sup>44</sup>. Un ordinateur central, sous la tutelle du gouvernement américain, situé à Herndon, en Virginie, est quant à lui chargé du trafic des demandes d'adresses.

Afin de faciliter la recherche de l'information de la part de l'utilisateur, et devant la multiplication des serveurs, des aides ont été mises en place. Véritables carnets d'adresses, des "moteurs de recherche" sélectionnent les sites répertoriés en fonction d'un thème, d'un titre, d'un mot-clé.... Ils permettent d'aiguiller le "surfeur" vers le site le plus approprié à sa recherche et dans le délai le plus court possible. En France, les plus couramment utilisés sont Yahoo, Alta Vista, Lycos ou Nomade, chacun proposant son propre carnet d'adresses. Dès qu'un serveur correspond à la recherche demandée, le moteur connecte automatiquement l'utilisateur sur le site en question. Si les

<sup>39</sup> Selon Christian Harbulot, directeur des études de l'Ecole de guerre économique, "les forums de discussion constituent un lien privilégié pour l'art de la polémique. (...) A côté des pirates informatiques, nous verrons bientôt apparaître des francs-tireurs que l'on pourrait appeler des « guerriers de la connaissance », des personnes intellectuellement bien outillées, capables d'alimenter des débats et de faire passer de l'information pour déstabiliser l'adversaire en visant son talon d'Achille".

<sup>40</sup> Il s'agit de "l'association historique de l'Internet".

<sup>41</sup> Ce sont les propres termes de M. Patrick Robin, directeur de la société Imaginet.

<sup>42</sup> Voir l'article *Fenêtre sur le monde* de Jean-Philippe Gunet, dans *Armées d'aujourd'hui*, de février 1998, p 64.

<sup>43</sup> Par exemple, à l'adresse "www.lemonde.fr", du quotidien du soir *Le Monde*, correspond le code 194 2 31 156.

<sup>44</sup> L'IANA travaille sous contrat avec le secrétariat d'Etat américain à la Défense, à travers la DARPA.

informations sont intéressantes, elles peuvent être "téléchargées", c'est-à-dire copiées sur le disque dur de l'ordinateur receveur.

La simplicité de l'action montre que tout ordinateur est susceptible de recevoir un virus susceptible de détruire toutes ses données stockées en mémoire.

## 223- Etat actuel

### 223-1 Services rendus par Internet

Internet regroupe à lui seul de nombreux services, faisant ainsi concurrence à la poste, au téléphone, à la télécopie, à la presse écrite... Il assure les fonctions suivantes :

- recherche documentaire et transfert de fichiers (texte, audio, vidéo),
- messagerie électronique (boîtes aux lettres électroniques @<sup>45</sup> mail),
- journaux électroniques,
- forums de discussion autour d'un thème (*Newsgroups*),
- multimédias interactifs, télévision et son numériques<sup>46</sup>,
- tractations financières et publicités commerciales.

### 223-2 Multiplication des sites et des abonnés

Grâce à Internet, tout connecté peut recevoir et diffuser<sup>47</sup> librement ce qu'il désire : du texte, du son ou des images. L'intérêt porté par le public à Internet se mesure à la formidable explosion des demandes d'abonnement. De manière concomitante, les serveurs se multiplient également car les entreprises savent qu'elles atteindront de plus en plus de gens par cette voie. En 1994 :

- en France, 72 000 ordinateurs étaient connectés,
- en Allemagne, 150 000,
- aux Etats-Unis, 3,2 millions.

Certains analystes estiment qu'Internet touche aujourd'hui 80 millions d'individus, d'autres vont jusqu'à 140 millions. Quels que soient les chiffres, une constante apparaît néanmoins :

- 60 % d'entre eux résident en Amérique du Nord,
- 25 % résident en Europe,
- 13 % résident en Asie,
- 1 % résident en Amérique du Sud,
- moins de 1 % résident en Afrique (dont 90 % en Afrique du Sud).

A ce rythme, on peut raisonnablement penser qu'il y aura environ 400 millions d'utilisateurs en 2000, et un milliard en 2002.

Parallèlement à l'augmentation du nombre des internautes, on assiste à l'explosion du marché mondial de l'informatique. En cinq ans, le monde a vu les ventes d'ordinateur tripler. En 1996, le taux d'équipement des ménages était de 14,4 % en France, de 20 % au Royaume-Uni, de 30 % en Allemagne et de 35 % aux Etats-Unis<sup>48</sup>. Au Japon, le nombre de branchements sur Internet a été multiplié par cinq en deux ans, passant de 1,5 millions en 1995 à 8,5 millions en 1997<sup>49</sup>.

### 223-3 La pénétration d'Internet en France

En France, on estime qu'en 1998, le réseau mondial est reçu par 300 000 ordinateurs, soit une augmentation de 300 % en quatre ans. La "culture Minitel" entraîne cependant un sous-équipement

<sup>45</sup> @ est l'arobase signifiant "chez" (*at* en anglais) dans une adresse électronique.

<sup>46</sup> C'est ce qu'on appelle le "Web".

<sup>47</sup> Dans la limite des 5 mégaoctets pour l'utilisateur standard.

<sup>48</sup> Voir l'article *Internet, un vrai défi pour la France* du chef d'escadron Patrick Barillon dans la *Tribune* du Collège interarmées de défense de janvier 1998, p 182.

<sup>49</sup> C'est le tremblement de terre de Kobe qui a décidé du succès d'Internet au Japon car, le 17 janvier 1995 au matin, toute communication intérieure étant presque impossible, seuls les internautes ont pu transmettre les premières informations relatives à la situation sur place.

chronique des foyers français en récepteurs Internet, bien que le Minitel ait permis à des millions de Français de se familiariser avec l'information télématique. Depuis 1997, l'essor d'Internet en France est considérable : le cabinet Médiangles, qui publie chaque année depuis 1995 une étude sur les internautes français, recensait 1 120 000 utilisateurs en mai 1997 contre 420 000 un an plus tôt, soit une progression de 160 %. Il estime que le nombre a atteint les 2 millions au début de l'année 1998.

De leur côté, les autorités françaises ont multiplié les ouvertures de sites : aujourd'hui, l'Elysée, Matignon et de nombreux ministères disposent d'un serveur. Le ministère de l'Education nationale a décidé fin 1997 de consacrer 15 milliards de francs sur trois ans à l'initiation aux nouvelles technologies de l'information : Internet est l'axe central des mesures décidées et devrait en être le principal bénéficiaire. En effet, il est d'ores et déjà prévu de créer un réseau - baptisé "Educnnet" - où seraient connectés tous les établissements scolaires. Quant aux armées, début 1998, le SIRPA mettait en œuvre le site du ministère de la Défense<sup>50</sup> : le menu proposé est cependant assez succinct. Ce site a mis un temps assez long à se mettre en place, essentiellement pour des raisons de sécurité.

## 224. Les enjeux

### 224-1 Internet et les "autoroutes de l'information"

Par les services offerts, Internet préfigure les autoroutes de l'information. Il efface les distances donc les délais d'acheminement de l'information et permet d'accéder en temps réel, ou presque, à une masse de données en augmentation constante et dont personne ne sait aujourd'hui quelles en seront les limites. Sa conception lui permet d'intégrer tout type de projet technologique. C'est en particulier le cas des réseaux Intranet qui se multiplient actuellement ou des nouveaux moyens de communication dits "multimédias" (CD-Roms surtout).

Internet est un instrument de communication extraordinaire. Sans aucun doute, une bataille pour la maîtrise du réseau est en cours. D'après Paul Virilio<sup>51</sup>, "tout le travail mené actuellement consiste à développer cette puissance de l'information pour en faire une véritable arme de dissuasion mondiale". La défense militaire, économique ou civile, est donc concernée. Le Pentagone ne s'y trompe pas puisqu'il organise, chaque année depuis 1995, une douzaine d'exercices de "cyberguerre" associant civils et militaires, afin de faire constater aux sceptiques que les réseaux des armées dépendent dorénavant des réseaux civils.

Par ailleurs, contrairement à ce qui se passait à l'origine, les Américains n'exercent plus une complète domination sur le Net. En effet, les agressions informatiques dont sont victimes le Pentagone et la CIA (plusieurs centaines quotidiennement) sont autant d'exemples montrant qu'Internet échappe à son promoteur. La théorie selon laquelle Internet serait un outil d'hégémonisme américain n'est donc pas totalement valable, même s'il faut garder à l'esprit qu'en 1994, 95 % des messages transitant sur le *Web* étaient en anglais...

### 224-2 Les enjeux commerciaux

Selon Claude Esmein, de la mission Innovation du ministère de la Défense, "le Net est un formidable outil au sens « publicitaire » du terme et non à celui de « transmission », dans la mesure où n'importe quelle personne physique ou morale peut l'employer afin de faire connaître ses idées et ses produits pour des sommes ridiculement basses en regard de l'étendue du public susceptible d'être touché". Effectivement, une campagne de publicité sur Internet coûte infiniment moins cher qu'une campagne télévisée. Par conséquent, Internet engage la planète entière dans une révolution culturelle et commerciale qui bouleversera à terme toutes les sphères d'activité en général.

<sup>50</sup> L'adresse du site est "www.defense.gouv.fr" et son @-mail est "defense@defense.gouv.fr".

<sup>51</sup> Voir son livre *Cybermonde, la politique du pire*, éditions Textuel, au Seuil.

Les enjeux commerciaux sont colossaux et les sommes d'argent brassées déjà phénoménales, sans qu'il y ait pourtant de contrôle *a priori* ou *a posteriori*. L'étude de l'IHEDN, déjà citée, rapporte les statistiques que Joel de Rosnay<sup>52</sup> a établies :

	En 1996	En 2000
Nombre de serveurs reliés à Internet	16 millions	100 millions
Nombre d'internautes	50 millions (30 aux USA)	400 millions
Chiffre d'affaires du commerce électronique	600 millions de \$	200 milliards \$
Chiffre d'affaires de la publicité	300 millions de \$	2,5 milliards \$

### 224-3 Les enjeux technologiques

Le développement d'Internet est dopé par celui des réseaux internes d'entreprise, les Intranets. Il bénéficie en retour des investissements effectués par les entreprises en réseaux privés. On estime qu'aujourd'hui 64 % des mille plus grandes sociétés mondiales offrent à leurs employés un tel réseau, et que les 36 % qui restent en auront un dans deux ans. Le développement des Intranets est même devenu plus rapide que celui d'Internet. Un Intranet possède en effet quatre avantages :

- il utilise la plupart du temps des équipements informatiques existants ;
- il utilise souvent des réseaux existants ;
- il bénéficie de l'expérience acquise par Internet ;
- il indexe lui aussi automatiquement l'information par des moteurs de recherche.

Devant l'engouement face à Internet, nombreux sont les centres qui cherchent comment atteindre encore plus de monde. C'est ainsi que, dans les années à venir, il est possible que l'accès à Internet se fasse par une voie différente de celle du téléphone. En effet, fin 1997, l'opérateur canadien Nortel et la société britannique United Utilities ont annoncé qu'ils étaient technologiquement capables de permettre l'accès *via* le réseau électrique. Ce dernier relie la quasi-totalité des foyers et son maillage est précis et redondant.

En France, EDF conduit depuis 1987 des études à ce sujet. Il s'agit d'étendre au réseau national la technique des courants porteurs déjà utilisée par les interphones de chambres d'enfant qui utilisent le réseau électrique de la maison. Si cette technique se révélait vraiment efficace, la pénétration d'Internet serait considérablement accrue.

### 23. La télévision numérique

Certes, la télévision n'est pas un nouveau média. Mais ce que la télévision connaît aujourd'hui, grâce à l'apport de la technologie numérique, est une véritable révolution<sup>53</sup>. C'est pourquoi cette étude se penche sur les conséquences de la numérisation des systèmes de télévision.

### 231. Numérisation et chaînes de télévision

#### 231-1 La numérisation de l'image

Une image est un ensemble de points et d'éléments de teinte homogène, appelés pixels<sup>54</sup>, éclairés par une source de lumière. Dès lors qu'elle est en couleurs, sa mise en mémoire et son traitement par une machine sont complexes. Le numérique apporte à la télévision - à la photographie également - une méthode de décomposition de l'image bien plus fine que l'analogique. La netteté et les couleurs sont bien supérieures en qualité. En outre, si l'on associe numérisation à compression et miniaturisation, on révolutionne toute la chaîne suivie par une image avant de parvenir au récepteur. Ainsi, les émetteurs sont moins encombrants, avec des capacités de mémoire bien plus étendues,

<sup>52</sup> M. de Rosnay est directeur de la stratégie à la Cité des sciences et de l'industrie de Paris.

<sup>53</sup> De l'aveu même d'un spécialiste : Jean Pierre Quittard, de TF 1.

<sup>54</sup> Pixel est la contraction des mots anglais *picture element*.

permettant de transmettre beaucoup plus d'images dans un temps nettement plus court. La numérisation ne répond donc pas à l'incessante demande d'images, elle la dépasse considérablement !

### 231-2 Les bouquets numériques

Devant les capacités offertes par les satellites et la baisse du prix du lancement, les télécommunications ont pris un essor formidable. Les nouvelles puissances de transmission offrent aux ingénieurs des champs nouveaux d'expansion du média "télévision". C'est ainsi que l'on assiste de plus en plus à des duplex en direct, avec un correspondant pouvant se situer à l'autre bout de la Terre. Dans le même temps les chaînes câblées ou transmises par satellite se multiplient.

En France, ce dernier phénomène se retrouve à travers les deux "bouquets numériques" proposés aux téléspectateurs : TPS, regroupant TF 1 et France télévision, et Canal satellite, chaîne à péage. Le terme de "bouquet" est bien choisi car le choix offert est varié ; chacun peut en effet trouver, sur une des nombreuses chaînes à thème, le programme correspondant à ses préoccupations. Le nombre de chaînes proposées peut être décuplé si l'on décide l'accès aux chaînes étrangères.

## 232. Technologie numérique et reportages

### 232-1 Conséquences pour les équipes de reporters

Seuls sont ici abordés les reportages d'actualité, susceptibles d'être diffusés aux journaux télévisés du jour, les autres n'ayant pas les mêmes contraintes de temps.

Une équipe de télévision en reportage à l'extérieur est confrontée au problème de la transmission de ses images. Celles-ci peuvent transiter à travers plusieurs types de support : par satellite, faisceau hertzien, fibre optique, câble, ou de manière mixte. Dans la plupart des cas, une équipe ne sait pas par quel moyen ses images vont transiter, puisque c'est la société chargée de la transmission qui choisit le moyen, en fonction du coût, de l'encombrement des faisceaux, des délais, etc. Deux cas se présentent alors :

- *déplacement en France métropolitaine ou sur un territoire pourvu d'équipements équivalents aux moyens français* : l'équipe s'adresse à une station émettrice spécialisée pour ce type de transmission ; dans la plupart des cas, il s'agit de la station FR 3 régionale ou d'une chaîne étrangère locale. Si l'actualité ou les délais l'imposent, les chaînes de télévision peuvent utiliser des moyens mobiles, sous la forme de camionnettes ou de véhicules monospaces<sup>55</sup>. Cependant, ces moyens sont très peu nombreux, TF 1 ne dispose que par exemple d'un seul exemplaire!

- *déplacement dans un pays non équipé de moyens modernes de transmission* : en fonction des délais demandés par Paris, l'équipe s'adresse à la chaîne nationale ou bien utilise des moyens de transmission par satellite autonomes. L'apport de la technologie numérique est alors décisif. En effet, il existe désormais des appareils de la taille d'un magnétoscope, capables de monter des images numériques et de les transmettre compressées directement à la rédaction nationale, *via un réseau satellite*. C'est le cas du *Toko*<sup>56</sup>. Hier, la transmission d'images nécessitait de disposer d'un émetteur référencé et d'un créneau satellite à réserver auprès d'un prestataire de service<sup>57</sup>. Pour transmettre une minute d'images, il fallait trouver des installations aptes à transmettre pendant environ une heure,

<sup>55</sup> Entre mai et juillet 1997, la société française AMP-C3C a vendu six véhicules *Volkswagen Transporter* équipés d'une antenne parabolique de 1,30 m, d'un récepteur GPS, de codeurs, décodeurs, modulateurs, amplificateurs et transmetteurs satellite (vers Telecom 2, Eutelsat ou Intelsat), aptes à transmettre des données audio et vidéo, analogiques ou numériques.. Le coût de ce système est d'environ 2 millions de francs.

<sup>56</sup> Cet ensemble, d'un poids de 35 kg, est un moyen de transmission très rapide, avant ou après montage, d'images vidéo compressées (et cryptées si cela est demandé), par l'intermédiaire d'une station *Inmarsat B* à haut débit. D'une mise en service simple et rapide, il nécessite un ensemble à chaque extrémité de la liaison en duplex (émission et réception) et est actuellement utilisé par de nombreuses chaînes de télévision françaises et étrangères (TF 1, FR 2, BBC, etc.). La société française IN-SNEC, filiale d'Intertechnique, le vend à environ 250 000 francs l'unité.

<sup>57</sup> Le réseau Serte de France Télécom permet tout type de transmission.

tout en s'astreignant aux créneaux alloués : le coût dépassait les mille francs. Aujourd'hui, le système *Toko* a besoin de trente minutes pour un coût de trois mille francs, mais il est entièrement autonome et n'est astreint à aucun créneau.

### 232-2 Conséquences pour les rédactions

Avant l'arrivée de la technologie numérique, et suivant les délais demandés, soit les équipes de télévision disposaient d'assez de temps pour mixer leurs images - grâce à un banc de montage très encombrant, soit elles les transmettaient pêle-mêle à la rédaction nationale qui procédait alors au montage, sans connaître toutefois le sujet. Dorénavant, la numérisation de l'image permet le montage sur place et la transmission quasi-simultanée du produit fini, l'équipe n'emportant que des appareils d'un poids et d'un volume très restreints (effet de la miniaturisation).

Or, les rédactions étaient organisées en fonction des délais d'acheminement des images en provenance des théâtres de crise. Les liaisons en direct étaient très rares et nécessitaient une préparation du plateau particulière. Aujourd'hui, il y a de moins en moins de différences entre le direct et le très léger différé : les images arrivant très rapidement, souvent simultanément avec l'événement, les rédactions sont confrontées à une véritable révolution. C'est un bouleversement des habitudes rédactionnelles car deux niveaux doivent cohabiter :

- celui qui distille l'information dès que l'événement se produit : il intéresse le petit nombre d'individus dont le métier est de "coller" à l'actualité, pour la traiter immédiatement ;

- celui qui traite, conserve, sélectionne puis diffuse l'information - en fonction de critères quelquefois ahurissants<sup>58</sup> : tout est réalisé pour le journal de 20 h 00, émission suivie par les téléspectateurs habitués au "rite du 20 h 00".

Puisqu'on ne peut évidemment pas intervenir à chaque instant pendant les programmes des chaînes traditionnelles, il faut songer à une autre solution. D'où la création des chaînes d'information continue, comme CNN, LCI ou Euronews.

### 233. Technique numérique et manipulation de l'image

Un téléspectateur peut être manipulé de quatre façons différentes :

- *par imposture d'image* : ce qui est montré ne correspond pas à la réalité. Par exemple, dès que des images d'archives sont projetées, on omet de l'inscrire sur l'écran. Cela prêle quelquefois à des erreurs grossières qui entament la crédibilité de la chaîne incriminée<sup>59</sup>.

Autre méthode : des "acteurs" sont chargés de transcrire un événement ou un fait qui n'est jamais arrivé<sup>60</sup>. Ce type de manipulation est ancien, il est facilement démontable mais, en général, la puissance de l'image a déjà sévi, les mises au point ultérieures passant totalement inaperçues.

- *par montage mensongé* : des images provenant de reportages différents sont intentionnellement montées dans le but de rapprocher des faits ou des gens. Tout est possible tant que le produit final est plausible, mais il doit nécessairement subsister une unité minimale de temps et de lieu<sup>61</sup>.

- *par insertion d'images subliminales* : ce procédé de piraterie ne sera pas étudié ici, puisqu'étant connu, peu utilisé et non lié à l'arrivée de la technologie numérique.

<sup>58</sup> Il suffit de comparer les retombées médiatiques, au printemps 1994, de l'affaire *Whitewater* aux Etats-Unis face à celles des massacres au Rwanda, ou, à l'été 1997, de la mort de Lady Di face à celle de Mère Theresa... La hiérarchisation de l'information par les médias suit une morale que la raison ignore.

<sup>59</sup> Lors de la dissolution du GLAM par le Premier ministre Edouard Balladur, en juillet 1995, les images diffusées sur les chaînes montraient les avions incriminés, des *Mystere XX* au décollage ou au roulage. Pourtant, le GLAM ne possédait pas ce type d'avions.

<sup>60</sup> A Timisoara, en Roumanie, à l'automne 1989, les mêmes cadavres ont été filmés, puis déplacés pour être filmés à nouveau, donnant ainsi une impression de nombre, donc d'un véritable charnier.

<sup>61</sup> Peu de temps avant la guerre du Golfe, fin 1990, Patrick Poivre d'Arvor a fait croire qu'il avait eu un entretien télévisé avec Saddam Hussein, alors qu'il n'avait pas quitté son bureau parisien.

- *par manipulation technique de l'image elle-même* : c'est ce que nous allons aborder plus précisément.

### 233-1 L'état de l'art avant l'arrivée du numérique

Avant que la technologie numérique change considérablement les méthodes de travail, et surtout sa qualité, plusieurs procédés de manipulation technique de l'image étaient déjà au point, avec plus ou moins de succès.

- *superposition ou "compositing"* : une silhouette en mouvement est filmée sur un fond neutre. Par simple découpe, seule la silhouette est transposée sur n'importe quel autre fond, lui-même filmé ailleurs par un autre caméra. Les chaînes de télévision utilisent cette méthode pour présenter la météorologie. La manipulation est ici innocente. Cependant, il arrive souvent que les contours de la silhouette ne soient pas très précis. Par ailleurs, il s'agit de garder une certaine cohérence entre les conditions du plateau et celles du fond utilisé : si un cinéaste ne tient pas compte de cette obligation, l'effet recherché sera au mieux mal perçu, au pire complètement raté.

- *incrustation point à point* : c'est un procédé d'incrustation beaucoup plus complexe que le précédent car il fait appel à la création d'images en deux ou trois dimensions, pixel par pixel, afin que le produit final soit le plus parfait possible. Les trois effets liés à l'image sont alors traités de manière très élaborée : effet de focale permettant de restituer la juste taille des sujets entre eux, de lumière pour que les ombres correspondent et que les objets éclairés aient la même couleur, et effet de découpe afin que les contours soient les plus fins possibles. Le tout demande environ 10 000 fois plus de temps de travail qu'avec la méthode précédente ! Ces opérations sont donc réservées à des sujets très précis, essentiellement pour le cinéma<sup>62</sup>. Ne pas s'astreindre à un travail aussi rigoureux, rend la manipulation visible<sup>63</sup>.

- *détection de contour* : cette méthode consiste à substituer une partie d'image par une autre, créée en studio. Il est indiqué à l'ordinateur la portion d'image à remplacer : après détection de son contour, appréciation de sa silhouette en fonction des axes de prises de vue, des focales utilisées et de l'environnement lumineux existant, on la substitue par une autre dont les caractéristiques doivent être très proches de l'image "mère". Cette technique n'est pas encore tout à fait au point car des problèmes de flou aux pourtours persistent, mais des essais ont déjà été effectués<sup>64</sup>.

- *adjonction d'images de synthèse* : sur un fond naturel et bien réel, on superpose des images totalement virtuelles, dites de synthèse. On donne ainsi l'impression que le tout est une même réalité. Si ces images sont conçues en trois dimensions, le téléspectateur est parfaitement "dupable"<sup>65</sup>. La technique actuelle est arrivée à un degré de mise au point excellente<sup>66</sup>.

### 233- 2 L'apport du numérique

Les procédés précédemment décrits présentent des résultats souvent limités parce que nécessitant des puissances de traitement informatique de plus en plus élevées.

<sup>62</sup> C'est le cas du film *Forrest Gump*, où le héros est "transporté" dans le bureau de trois présidents américains (Kennedy, Johnson et Nixon).

<sup>63</sup> Sur Canal +, Karl Zéro produit chaque semaine des séquences truquées mettant en scène des hommes politiques. Afin de laisser le téléspectateur s'en rendre compte par lui-même, il fait exprès de ne pas pousser la manipulation à la perfection ; par ailleurs, il est inscrit sur l'écran "séquence réalisée avec trucage".

<sup>64</sup> Par exemple, lors d'un match de football, on substitue les panneaux publicitaires disséminés le long de la pelouse par d'autres, à une heure donnée en fonction des contrats passés avec les annonceurs. Cette méthode a aussi été proposée pour éliminer les publicités de marques de tabac sur les circuits de grand-prix automobiles.

<sup>65</sup> Il existe de nombreux exemples : Renault s'en est servi pour la promotion de la *Twingo* en superposant un prototype sur un paysage routier, James Cameron a largement fait appel à cette technique lors du tournage de *Titanic*, en créant l'illusion sur le nombre de passagers ou la taille du bateau.

<sup>66</sup> Il faut voir le succès du film *Toys story* de Walt Disney, alors que beaucoup prédisaient son échec complet !

La numérisation de l'information et la puissance de traitement des ordinateurs actuellement disponibles<sup>67</sup> permettent de créer des effets virtuels quasiment impossibles à discerner du réel. Avec une image transformée et travaillée point par point, il n'y a plus de problème de découpe, de flou, de lumière, de focale : tout est pris en compte par l'ordinateur et restitué de manière quasi parfaite. Les techniciens truquent les images en un temps beaucoup plus satisfaisant, tous les axes sont respectés et travaillés, les images de synthèse sont introduites dans des scènes même en premier plan.

Toutefois, si on peut abuser le spectateur, le technicien peut encore s'apercevoir que les images qu'il reçoit sont truquées, et cela pour plusieurs raisons :

- très rares sont les cas où les images ne sont pas visionnées avant diffusion ;
- grâce aux techniques actuelles, le monteur ne peut pas laisser passer un trucage qui n'ait pas été parfaitement réalisé ;
- même si ce trucage parfait est désormais possible, il nécessite un temps de traitement<sup>68</sup> incompatible avec des images qu'il est urgent de transmettre.

Ainsi, pour quelques temps encore, la manipulation de l'image ne touchera pas le direct ou le très léger différé. Toutefois, à la vitesse où la technologie évolue, cela ne durera pas. Demain, il sera vraisemblablement possible de truquer une image à la source et ainsi de manipuler une population entière, en profitant des sujétions des chaînes de télévision : la primauté de l'image et la "dictature" du temps réel.

#### 24. Analyse des conséquences de ces changements

Les nouvelles capacités techniques décrites précédemment et l'évolution des mentalités font qu'aujourd'hui, nos rapports avec l'information et les médias ont évolué et continueront à évoluer. Dans la première partie de ce chapitre, il a été rappelé les évolutions des médias avant même l'apparition d'Internet. Les lignes qui suivent recensent les changements majeurs qu'il faut sans doute avoir en tête pour mener des actions psychologiques aujourd'hui.

##### 241. Le poids de la télévision dans les médias actuels

En préambule, en quelque sorte, partons de la primauté de l'image dans notre société. Il est impossible de compter les études ayant trait à l'influence de la télévision sur les enfants, la famille... Les conséquences de l'omniprésence de l'écran dans notre société intéressent naturellement les chercheurs. K. Popper<sup>69</sup> voit dans le pouvoir de la télévision un danger pour la démocratie. Sa dangerosité vient de la conjonction du pouvoir de l'image et du nombre d'heures<sup>70</sup> important passée devant le petit écran. Ce qui est certain, c'est que la télévision, média le plus puissant actuellement, réunit chaque soir une grande proportion de la population qui ne s'informe que par ce biais.

En conséquence, tout événement doit pour pouvoir être "traduit" en images pour devenir une information vendable aux chaînes et aux spectateurs. Ce qui explique que les médias tendent à n'accorder de l'importance qu'à ce qui communique bien par leur intermédiaire. Il faut savoir "vendre" son événement aux médias, sinon il ne sera pas traité et donc inconnu du plus grand nombre.

La dictature du visible, comme l'appellent certains, ne va pas disparaître avec les nouveaux médias ; simplement, ces derniers multiplieront les opportunités de faire accéder "son information" au plus grand nombre. Il faut d'ailleurs remarquer que la télévision utilise de plus en plus régulièrement pour les informations des images d'amateurs afin d'illustrer un événement imprévisible mais spectaculaire (catastrophe aérienne à Madagascar, tueur fou en Australie...).

<sup>67</sup> On estime que la vitesse de travail des logiciels double tous les dix-huit mois, à peu près au même rythme que la capacité de mémoire des ordinateurs.

<sup>68</sup> Aujourd'hui, il faut au moins quatre heures de travail pour truquer parfaitement cinq secondes d'images.

<sup>69</sup> Voir le livre *La télévision : un danger pour la démocratie* de K. Popper, bibliothèque 10/18, 1997.

<sup>70</sup> 95 % des foyers occidentaux possèdent une télévision et 80 % des ménages la regardent au moins trois heures par jour.

Cette multiplication des sources pouvant fournir de l'information rend difficile la vérification de son intégrité et de son sérieux.

### 242. Modification du support principal

On assiste actuellement, pour des raisons diverses, à deux mouvements contradictoires qui complexifient certainement la maîtrise de l'information.

#### 242-1 Eclatement des supports...

D'une part, la conjugaison de la fin des monopoles d'Etat et les progrès technologiques autorisent la multiplication et la diversification des moyens d'émission. Ainsi, le nombre de radios ou de chaînes TV disponibles est sans commune mesure aujourd'hui avec ce que nous connaissions il y a 15 ans seulement. Il y a un réel éclatement de l'offre. Les chaînes thématiques visent un public, plus ou moins large, qui fait le choix de s'intéresser au sujet présenté (musique, cinéma, information, documentaire...). Une évolution naturelle, mais dangereuse, est que ce public s'isole et s'enferme dans une logique perverse (site révisionniste sur Internet).

On peut imaginer que des chaînes régionales<sup>71</sup>, avec des petits budgets de fonctionnement, n'émettant que quelques heures par jour, prennent de l'importance. Elles viseraient un public présélectionné suivant un intérêt régional, basque, breton, corse ou corporatiste. Ces petites unités de diffusion seraient certainement plus faciles à manipuler à leur insu, car leurs moyens seraient limités et la chaîne de vérification de l'information moins fiable que celle des grosses unités. En outre, partisans par essence, elles risqueraient de succomber plus facilement à la tentation (ou le piège) du militantisme<sup>72</sup>.

#### 242-2 ... et concentration

D'autre part, les moyens techniques d'acquisition, de transmission, de traitement de l'information sont toujours plus performants mais aussi plus onéreux. A l'inverse du mouvement décrit précédemment, on assiste également à une course au gigantisme pour amortir les investissements. Les chaînes (radio ou TV) spécialisées dans l'information, par exemple, se font concurrence pour capter le maximum de clients et donc de recettes. Or le produit (l'information) étant forcément très semblable, puisque trois agences<sup>73</sup> principales se partagent le marché, la différenciation se fait sur la manière de présenter le produit. Ce qui pousse les médias vers :

- *le concept de "glocal"* : ce mot américain se compose naturellement de "global" et de "local", mots qui ne nécessitent pas de traduction. Il signifie que les événements ou les informations locales peuvent très rapidement être repris par les médias du monde entier. Cela tient à l'apparition de média à vocation mondiale (CNN) et disposant des moyens financiers nécessaires pour envoyer des équipes dans le monde entier.

Il devient en conséquence difficile, voire impossible dans une démocratie, de faire varier un message suivant son public. L'information est donnée ou trouvée par les médias ; ensuite, elle commence une vie "indépendante" impossible à maîtriser par le pouvoir politique. On constate immédiatement, dans le cadre de notre étude, la difficulté qu'il y a de prévoir les multiples conséquences d'une action psychologique.

Autre conséquence contenue dans le seul mot global, la mondialisation de l'information permet la mondialisation<sup>74</sup> de la manipulation. Perspective effrayante qui mérite que l'on réfléchisse aux moyens de s'en préserver.

- *le concept d'infoternmaint*<sup>75</sup> : cette notion évoque le mélange des genres entre information et distraction. Elle est apparue au grand jour durant la guerre du Golfe. Il n'est pas certain que

<sup>71</sup> Ou bien des chaînes de partis politiques, de religions ou de sectes.

<sup>72</sup> Ainsi le média des "chasseurs" serait, par exemple, certainement prêt à diffuser une nouvelle douteuse sur Mme Voynet.

<sup>73</sup> AP (*Associated Press*), AFP (agence France-press) et Reuter.

<sup>74</sup> Voir le livre *La persuasion de masse, guerre psychologique/guerre médiatique*, déjà cité, p 126 et 127.

l'information y gagne en qualité car elle est traitée de façon toujours plus émotionnelle. La construction de l'image est privilégiée par rapport au fait, et l'on recherche la dramatisation de l'événement ou du problème ("l'horreur ne suffit plus, il faut le cadrage"<sup>76</sup>).

Dans le même temps, la fiction se rapproche de la réalité. On assiste à la multiplication des *reality shows*, des reconstitutions<sup>77</sup>, avec le risque évident qu'à la longue le spectateur ne distingue plus très bien le vrai, le "reconstruit", le faux. Cette tendance est naturellement accentuée par la virtuosité dont font preuve les cinéastes qui, grâce aux images de synthèse, mêlent monde réel et imaginaire, mélangeant toujours plus vérité et fiction.

- *la concurrence entre les chaînes* : elle pousse au direct, à l'immédiateté. Avec CNN, le temps, l'espace sont escamotés. L'information devient un slogan répété des dizaines de fois, au même moment dans le monde. Le temps de la réflexion n'existe plus, l'individu est abandonné seul en tête à tête avec les événements.

Plus grave, cet impératif de vitesse réduit, comme nous l'avons vu, le temps nécessaire à la vérification des *news* par les rédactions. Cela devient un risque pour la qualité et la crédibilité de l'information. Les nouveaux médias ne feront qu'amplifier cette tendance puisque chacun devient potentiellement un "donneur" d'informations, de *scoops* qu'il sera tentant d'exploiter.

### **243. Un public plus critique**

Jusqu'ici, nous avons vu pourquoi il fallait s'inquiéter des nouvelles technologies. Toutefois, il ne faut pas croire que les perspectives d'avenir sont si mauvaises.

Lorsqu'on visionne des émissions vieilles d'un demi-siècle, on réalise combien les moyens de manipulation étaient frustrés. Pourtant, la Seconde Guerre mondiale, sa propagande, avait été un excellent terrain d'entraînement pour les spécialistes. L'opinion publique, aujourd'hui, est moins crédule, plus exigeante sur la transparence et la véracité des messages. De façon instinctive, il semble qu'une protection naturelle se mette en place chez l'individu. Des émissions télévisées<sup>78</sup> (encore) démontent même la magie de l'image et commentent non pas l'actualité, mais la façon dont tel ou tel reportage rend compte d'un événement.

De surcroît, les citoyens s'organisent pour ne pas être seuls face au pouvoir colossal des médias. En 1989, les associations françaises de défense du téléspectateur se sont regroupées en Union fédérale des auditeurs et des téléspectateurs. Des structures indépendantes se sont mises en place, certes doucement, pour essayer de garantir un minimum de droit au public.

Les concepteurs de l'action psychologique ne peuvent donc pas ignorer ce type d'évolution.

### **244. Un nouveau rapport de force**

Grâce aux nouveaux médias, l'individu prend soudainement une autre dimension face aux Etats. Ainsi, on a pu lire des livres pourtant retirés de la vente<sup>79</sup>. Un homme seul peut, quasiment sans frais, faire parvenir son témoignage en temps réel dans le monde entier à des milliers d'interlocuteurs. Il peut même intoxiquer des personnalités et provoquer une affaire d'Etat comme l'a montré l'affaire de la TWA et M. Salinger.

Le pouvoir d'un homme seul, hors de toute organisation devient soudainement extraordinaire.

### **Conclusion partielle**

On parle aujourd'hui beaucoup d'action psychologique car les mœurs politiques ont évolué.

<sup>75</sup> *Informationlenteternmaint.*

<sup>76</sup> Voir *Médias et contrôle des esprits*, par E. Roskis (enseignant les mécanismes de photojournalisme à l'université Paris X), dans *Le Monde diplomatique* du 27 août 1995, p 18.

<sup>77</sup> Sur son site Internet, l'AFP présente des images de synthèse pour illustrer des événements dont elle ne possède pas d'images réelles.

<sup>78</sup> Comme l'émission *Arrêt sur image*.

<sup>79</sup> Comme *Le grand secret* du docteur Gubler.

La légitimation des opérations militaires<sup>80</sup> et la démonstration de l'adaptation de leur style aux objectifs fixés sont désormais les passages obligés du succès. Il en est de même en politique intérieure : la manoeuvre médiatique destinée à créer un environnement favorable pour sortir d'une crise est devenue un souci pour tous les gouvernements.

Les possibilités immenses qu'offrent les nouvelles technologies permettent en matière d'action psychologique les rêves les plus fous. Toutefois, dans une démocratie, se livrer à ce genre d'action pose inmanquablement un problème éthique : qui peut faire quoi et avec quel contrôle ?

Si le sujet semble à la mode, la réalité du moment reste très complexe à cerner car certains propos sont alarmistes et personne n'avoue son implication dans ce type d'activité contre sa propre opinion publique.

Dans le chapitre suivant, nous verrons ce qu'un gouvernement semble pouvoir faire pour défendre et expliquer son action, mais aussi ce qu'il doit faire pour détecter et réagir à des actes hostiles venant d'individus ou d'Etats.

L'action psychologique est sans doute délicate à manier, mais il appartient au gouvernement de l'exploiter car c'est une arme de temps de paix.

---

<sup>80</sup> Voir la directive n°466 du chef d'état-major de l'armée de terre, datée du 7 février 1997.

### III- MESURES ET CONTREMESURES

#### 31. Actions psychologiques sur le réseau Internet

Nous verrons, dans un premier temps, comment utiliser les capacités offertes par Internet et par la technologie numérique, puis comment organiser une action psychologique ou, au contraire, s'en défendre.

#### 311. Comment agir sur Internet en temps de crise ?

##### 311-1 Généralités

Le temps de crise entraîne deux mensonges<sup>81</sup> : on ment à l'ennemi pour lui cacher ses plans, pour le démoraliser ou le désorganiser ; on ment également à ses concitoyens pour ne pas démoraliser les troupes, pour poursuivre l'effort, pour éviter de renseigner l'ennemi<sup>82</sup>. En outre, en temps de crise, tout pouvoir tente de restreindre certaines libertés. La liberté d'expression est en général la première touchée, car il s'agit de ne pas divulguer ses intentions secrètes ; toutefois, paradoxalement, il convient d'utiliser les médias comme une arme à part entière dans le combat qui s'engage, afin de légitimer une décision ou une opération.

Internet fait appel surtout au jugement du quidam avant celui de l'institution. Il est difficilement brouillable : il sort ainsi *de facto* du champ de filtrage effectué par l'Etat et constitue donc pour lui une menace sérieuse<sup>83</sup>.

Internet a le pouvoir de toucher une population assez élitiste, entreprenante, un minimum intellectuelle, voire contestataire. Si, aujourd'hui, le public concerné demeure encore restreint, il n'en sera pas de même dans les années qui viennent. A terme, on retrouvera donc sur Internet les mêmes actions psychologiques que pour les autres médias, chacune étant le résultat d'une opération délibérée, fonction de la population ciblée et du résultat recherché. Internet permet en effet d'agir en écrits (diffusion d'avis, d'opinions, de jugements), en images (photographies, vidéos), et en son, pour qui détient les logiciels adéquates. Tous les champs de la diffusion de l'information sont concernés.

Il semble possible de créer artificiellement un courant d'opinion spontané, en construisant de faux documents à partir de vrais, en créant de faux personnages, objets ou phénomènes, en faisant passer des rumeurs... De surcroît, l'architecture du réseau présente des failles<sup>84</sup> qu'il est facile de mettre à profit. Internet est donc doublement intéressant.

Le temps de crise réduit le champ de l'action psychologique à une course contre la montre : il s'agit de frapper l'opinion publique pour orienter la politique des Etats. C'est la politique du court terme, celle du long terme étant caractéristique du temps de paix et celle du moyen terme n'étant à envisager que si la crise est appelée à durer.

En sasant les actions psychologiques connues à travers le prisme d'Internet, on peut d'ores et déjà dégager deux domaines d'action : l'intervention directe sur le réseau et l'intervention sur son architecture. On parle aujourd'hui de COMINT, d'ELINT, d'HUMINT<sup>85</sup>, on parlera demain

<sup>81</sup> Voir *L'information, la désinformation et la réalité*, op. cit., p 90.

<sup>82</sup> Opération *Desert Storm*.

<sup>83</sup> Internet a montré comment la loi française, interdisant la publication de sondages une semaine avant un vote, pouvait être impunément transgressée : lors des élections législatives françaises de juin 1997, *La Tribune de Genève* a divulgué sur le *web* les résultats de ce type de sondages, ce qui a permis à chaque internaute-électeur français de connaître les estimations des résultats du second tour.

<sup>84</sup> Voir 224 Les enjeux.

<sup>85</sup> *Communication intelligence, Electronic intelligence, Human intelligence*, c'est-à-dire renseignement d'origine électromagnétique discursive, non-discursive ou humaine.

de COMPINT : *Computer intelligence*. En effet, la connaissance et l'utilisation de l'informatique sont des domaines de recueil d'informations maintenant essentiels ; à terme, Internet en sera le premier champ d'application.

### 311-2 L'intervention sur le réseau

Selon Jean Baudrillard<sup>86</sup>, "la virtualité ne se rapproche du bonheur que parce qu'elle retire subrepticement toute référence aux choses. Elle vous donne tout, mais, subtilement, elle vous dérobe tout en même temps. Le sujet y est parfaitement réalisé, mais quand le sujet est parfaitement réalisé, il devient automatiquement objet". C'est la raison pour laquelle l'internaute, citoyen d'un monde virtuel, est une proie facilement manipulable, d'autant plus que l'appartenance à la nouvelle "agora cybernétique" rejette les "have not" ou les "infopauvres", en d'autres termes les non-connectés<sup>87</sup>.

Par ailleurs, si les internautes disposent d'outils leur permettant de travailler en commun et de disséminer l'information plus facilement, ils sont aussi des citoyens présents sur tout le territoire pouvant la diffuser autour d'eux, ce qui fait de chacun d'eux un manipulé manipulateur en puissance. Cet effet de réaction en chaîne est très intéressant pour qui, en temps de crise, désire déstabiliser un gouvernement en semant le doute parmi une population intellectuellement agissante.

Une information comporte deux éléments : le contenu et la source. Spontanément, on s'intéresse toujours au contenu avant de faire attention à la source. M. Esmein<sup>88</sup> estime qu'Internet "correspond tout à fait à la mentalité anglo-saxonne : la liberté d'expression de tous, par tous et pour tous doit amener le système à s'autoréguler et à tendre vers l'honnêteté et la véracité des propos.(...) La bonne foi est présumée".

L'intérêt d'Internet est que la communication est à la demande : celui qui cherche l'information se tourne de lui-même vers celui qui la détient, sans lien physique. Ainsi, puisqu'elle fait l'objet d'une recherche, l'information recueillie présente un caractère de quasi vérité, partant du principe que ce serait celui qui veut manipuler qui ferait l'effort d'atteindre un grand nombre de personnes. Incidemment, on peut donc orienter une opinion ou manipuler une catégorie de personnes dont on sait qu'elle viendra puiser l'information dans un site bien particulier.

Le temps de crise change quelque peu cette mentalité car toute information émanant d'une source non amie, ou répertoriée comme telle, a des chances d'être classée douteuse : ainsi, l'action du manipulateur sur la source devient un objectif tout aussi important. Mais Internet est le moyen idéal pour diffuser n'importe quoi, en citant une source imaginaire mais crédible. Le réseau est d'autant plus dangereux que l'internaute standard n'a aucune possibilité d'identifier la source. Bien que l'information n'ait pas pu être vérifiée, elle détient cependant une parcelle de vérité puisqu'on ne soupçonne pas *a priori* la source comme étant un moyen de désinformation. Le temps passant, la fiabilité se renforce, comme cela se passe pour une rumeur.

En utilisant le fait qu'il est présent partout et utilisable à toute heure, un groupe quelconque, dès lors qu'il s'organise, peut utiliser Internet pour agir sur les masses, en vue d'abattre, de contraindre ou d'empêcher un adversaire désigné. Pour cela, il existe un certain nombre de possibilités :

- *l'appel aux instincts élémentaires* : il s'agit de faire peur, d'intimider, de faire naître l'inquiétude ou la panique. Des messages alarmistes, en provenance de sources multiples et aptes à terroriser la population, sont envoyés sur le réseau mondial, au début à des internautes sélectionnés (journalistes, relais d'opinion, associations écologistes, organisations non-

<sup>86</sup> Voir l'article *Ecran total*, paru au quotidien *Libération* du lundi 6 mai 1996.

<sup>87</sup> Voir l'étude de l'IHEDN, op. cit., séance I de M. Bélorgey.

<sup>88</sup> Voir *Internet : vitrine, source d'information, lieu de circulation (donc d'interception)*, de Claude Esmein, dans le n° 60 de la revue *L'armement* de décembre 1997-janvier 1998.

gouvernementales, etc.) puis de manière beaucoup plus étendue (*Newsgroups*, listes d'abonnés). Chaque action doit être menée en fonction de la sensibilité de la population : par exemple, la diffusion d'une (fausse) révélation de Nostradamus suscitera le sourire amusé du journaliste sérieux mais l'affolement parmi les membres d'une secte. Par ailleurs, il faut utiliser au maximum les *Newsgroups* afin de créer la discussion, d'apporter de l'intérêt au contenu du message, d'amplifier le phénomène.

En temps de crise, des sites peuvent facilement présenter des images chocs, même si elles sont censurées par les opérateurs, mais jamais assez vite pour éviter que certains les aient déjà copiées. Ainsi, en montrant la situation dramatique qu'une population connaît, sous les bombardements, à cause d'un embargo ou au milieu des combats, on peut atteindre un effet comparable à celui de la télévision. Cet effet de masse a pour objectif de "produire l'émotion"<sup>89</sup>. On accroche alors à coup sûr l'internaute. Le message qui suit peut gagner l'opinion. Il ne reste plus qu'à laisser germer le mécontentement.

Internet est assurément un instrument fabuleux de destruction des meilleures légitimités, qu'elles émanent de l'ONU ou d'ailleurs.

- *la propagande* : il s'agit ni plus ni moins d'influencer le jugement universel en diffusant non pas de fausses informations mais des informations ciblées, relatives à une doctrine précise, menant l'opinion à penser de manière uniforme. On peut mythifier une idole, répandre des slogans<sup>90</sup>, faire la publicité d'un événement<sup>91</sup>, transporter des informations illégales, pratiquer la provocation en comptant sur la répression pour déclencher la sympathie, rapprocher les croyances pour provoquer l'adhésion<sup>92</sup>...

Internet peut être utilisé par des réseaux islamistes, par des sectes, par la mafia, par des mouvements révolutionnaires. On peut également utiliser les logiciels de recherche pour distribuer des prospectus aux particuliers. Une seule lettre, 100 000 (é)lecteurs... La technologie du *push* permet d'expédier directement l'information chez l'utilisateur, sans qu'il ait à venir la chercher. C'est une intrusion pure et simple, un démarchage à domicile sans pouvoir verrouiller sa porte. Internet peut être aussi utilisé par une entreprise pour favoriser l'émergence d'un mouvement d'opinion qui serve ses intérêts. Il suffit d'utiliser des listes de diffusion, correspondant, par exemple, aux internautes s'étant connecté au site de la firme, en associant aussi les journalistes, les relais d'opinion ou les organisations non-gouvernementales ou transnationales intéressées par un bon scandale chez le concurrent<sup>93</sup>.

- *la désinformation et l'intoxication* : c'est le mensonge organisé. Guy Durandin considère qu'elle se présente sous six formes<sup>94</sup>:

<sup>89</sup> Voir *La persuasion de masse, guerre psychologique/guerre médiatique*, op. cit., p 57.

<sup>90</sup> François Géré expliquait récemment "qu'Internet est une arme parmi d'autres dans la panoplie de la guerre de l'information, qu'il a une très grande souplesse car il s'apparente à de la guérilla". Grâce à l'atelier de recherche qu'il a créé en 1997 sur ce thème, il a décelé les fausses informations que le mouvement zapatiste diffusait sur le réseau, selon lesquelles l'armée mexicaine massacrait les populations favorables aux Zapatistes.

<sup>91</sup> Bob Denard a ouvert un site ([www.bobdenard.com](http://www.bobdenard.com)) pour donner sa version personnelle des différents coups de main qu'il a menés, avec photos, documents et films à l'appui. En ayant pris connaissance, un rapporteur de la Commission européenne a fait allusion à la possibilité offerte par Internet de recruter des mercenaires.

<sup>92</sup> Un groupe de chômeurs, en janvier 1998, a créé une antenne Assedic virtuelle sur Internet (voir l'article [www.altern.org/antenneassedic](http://www.altern.org/antenneassedic) de Yves Eudes dans *Le Monde* du 29 janvier 1998). Il y est rapporté la profession de foi, résolument anarchiste, suivante : "... esprit contributif, absence de hiérarchie, non-rétention de l'information..." Les messages envoyés à 800 internautes bien choisis, comme des journalistes ou des militants, ont permis aux chômeurs de coordonner leur action dans l'occupation de lieux symboliques. Il a assurément servi à faire converger les sympathies, voire à déclencher des mouvements "spontanés".

<sup>93</sup> Qui dit que "l'erreur" de Greenpeace, lors de l'affaire de la plateforme pétrolière Shell en mer du Nord, n'a pas été habilement suggérée - amplifiée à travers Internet puis relayée par les médias classiques - par une entreprise concurrente ?

<sup>94</sup> Voir le livre *L'information, la désinformation et la réalité* de Guy Durandin, PUF, p 27.

- une différence entre la connaissance de la réalité et le discours,
- l'intention de tromper,
- les motifs du mensonge,
- les objets (faits, intentions, valeurs, opinions, croyances et idéologie),
- les destinataires,
- les procédés.

A travers les forums de discussion ou les sites de diffusion de médias écrits, un internaute peut directement prendre pour cible les décideurs ennemis ou tromper une population, en analysant une information réelle, avérée, mais partielle<sup>95</sup>. On pousse ainsi la victime à participer involontairement à sa propre méprise. M. Durandin<sup>96</sup> utilise une expression tout à fait révélatrice à ce sujet : l'intoxication évoque "le cheminement d'un corps étranger dans un organisme". Ce que le réseau mondial apporte, c'est la possibilité de contaminer des millions de personnes ! Un logiciel astucieux<sup>97</sup> permet de savoir automatiquement si tel ou tel utilisateur est présent en même temps que vous sur le réseau. Dans ce cas, il est possible d'engager la conversation en direct, d'échanger des données, d'expédier des fichiers... On peut s'en servir pour désinformer en direct<sup>98</sup>.

En outre, il suffit d'exprimer son opinion plusieurs fois en signant de manière différente à chaque fois pour faire croire que les sources sont différentes, disséminées partout dans le monde. L'effet de masse étant atteint, on peut orienter la discussion dans le sens choisi, c'est techniquement très facile. De nombreux internautes se laissent abuser et l'institution ou la société attaquée n'a souvent pas les moyens de dénoncer suffisamment tôt la tentative de manipulation, dès lors que certains s'y sont déjà associés fort honnêtement.

Internet n'est certes pas l'apanage des organisations non-gouvernementales ni des mouvements anarchistes mondiaux. Cependant, on remarque que les forums de discussion abordent des thèmes chers à une certaine population protestataire. En effet, on peut tout dire, tout écrire, tout montrer, bref faire n'importe quoi. Sa présence au sein des forums est tangible et son implantation au sein des ONG agissantes telles qu'Amnesty International ou Greenpeace est une menace, dès lors qu'on la laisse s'exprimer librement, sans contrepartie réaliste<sup>99</sup>. Internet est pour le milieu anarchiste un lieu idéal de désinformation.

- *la subversion* : il s'agit de jeter le discrédit sur des autorités<sup>100</sup>, de culpabiliser un peuple ou un homme<sup>101</sup>, de semer le trouble et d'atteindre à la cohésion d'une communauté, en répandant

<sup>95</sup> Après l'explosion du vol TWA 800, en juillet 1996, au large de New-York, Internet a été le lieu de nombreuses rumeurs quant à l'implication des militaires américains. Une thèse a été lancée par Ian Goddard et Pierre Salinger - ex-porte-parole du président Kennedy - s'appuyant sur des témoignages mettant en cause un missile tiré par la marine américaine. Le 5 novembre dernier, Ian Goddard a avoué aux enquêteurs du FBI qu'il s'agissait de faux documents. Le site en question a été vidé de son contenu.

<sup>96</sup> Voir *L'information, la désinformation et la réalité*, op. cit., p 150

<sup>97</sup> Il s'agit par exemple du logiciel ISQ, ou *I seek you* : "Je te cherche".

<sup>98</sup> *France soir*, le matin du 19 septembre 1997, a publié une photo censée représenter Lady Di dans la carcasse de sa voiture. En réalité, cette photo était un canular mis en place sur un site contestataire pour piéger les médias, ce qui réussit.

<sup>99</sup> On croit qu'Internet a aujourd'hui des effets très limités. C'est faux, ou, plutôt, ce n'est plus vrai. Un exemple montre les effets d'une campagne habilement menée sur le *web* : en 1992, Jody Williams lançait une campagne internationale pour l'interdiction des mines antipersonnel uniquement sur Internet. En 1998, elle a rallié un millier d'ONG disséminées dans une soixantaine de pays, avec, à la clef, le prix Nobel de la paix 1997 et un traité d'interdiction signé par une centaine de pays. On sait que l'organisation Amnesty International, longtemps manipulée par Moscou pendant la guerre froide, dispose aujourd'hui de 35 sites Internet, avec la possibilité de lancer des pétitions, des lettres de protestation... Les pays montrés du doigt par cette ONG réagissent immédiatement. De même, Greenpeace utilise le réseau pour ses campagnes (20 sites, 10 listes de diffusion pour 2000 internautes) et le surveille 24 heures sur 24 pour lancer des opérations "coup de poing" auprès des forums de discussion.

<sup>100</sup> Voir en annexe le site officiel de la présidence de la République française ([www.elysee.fr](http://www.elysee.fr)) et le site pastiche ([www.elysee.org](http://www.elysee.org)).

des calomnies ou des rumeurs, en soutenant financièrement - puisqu'il est possible de faire circuler par le *Web* des sommes importantes d'argent - des partis politiques, des ONG, des associations culturelles... Il s'agit de diffuser le plus largement possible son point de vue pour qu'il s'impose.

### 311-3 L'intervention sur l'architecture du réseau

L'architecture du réseau mondial et son fonctionnement sont très vulnérables car il n'est pas organisé, ou très peu, et il n'existe pas de filtres institutionnels, sauf à travers quelques fournisseurs d'accès. La menace est multiple :

- pollution volontaire de sites hostiles,
- intrusion dans les réseaux privés pour en extraire des informations classifiées,
- intrusion dans les réseaux privés pour transformer les informations,
- interception de paquets d'informations pendant leur transit,
- attaque contre les fournisseurs d'accès,
- prise de contrôle de systèmes se trouvant à des milliers de kilomètres de distance<sup>102</sup>.

Ces menaces émanent de plusieurs types d'agressions :

- *la recherche de pénétration* : Internet est un champ d'expérimentations informatiques quasiment sans limites ; il offre aux génies informatiques de quoi exercer leur imagination. Songer qu'on puisse pénétrer impunément à l'intérieur d'un ordinateur situé à l'autre bout de la planète, dès lors qu'il est branché sur le réseau, qu'on puisse y lire ce qui est écrit et violer ses secrets constituent une tentation forte pour ces internautes talentueux.

Il est même amusant de remarquer qu'Internet devient quelquefois un lieu de compétition entre "pirates informatiques"<sup>103</sup>. Sur le *web*, un véritable vocabulaire guerrier s'instaure entre les spécialistes des réseaux : on parle déjà d'*infowar*, de bombes logiques capables de frapper des sites ciblés... Il n'est pas rare que certains dénient, sans les dénoncer, ceux qui sont parvenus à pénétrer un réseau pourtant réputé inviolable. Ceci est difficile car la société violée n'en fait généralement même pas état. Cela prouve toutefois que les internautes laissent des traces de leur passage.

Quotidiennement, de nombreux *hackers* tentent de s'introduire dans les réseaux les plus secrets et les mieux protégés du monde (CIA, Pentagone, MITI, etc.). Parmi eux, certains réussissent. En effet, il suffit qu'un seul ordinateur soit sous-tension - même sans être en fonctionnement - et connectable sur un réseau accessible, pour qu'on puisse pénétrer le système en son entier et tous ceux qui s'y rattachent. Ce caractère de quasi contagiosité est le talon d'Achille d'Internet<sup>104</sup>. On imagine que les plus grandes entreprises ou les grandes organisations se

<sup>101</sup> A l'occasion du procès Papon, les parties civiles ont ouvert un site ([www.matisson.com/affaire.papon](http://www.matisson.com/affaire.papon)) sur lequel on ne trouvait bien évidemment que les griefs reprochés à l'ancien secrétaire général de la préfecture de Bordeaux. C'était occulter une partie de la vérité, orienter l'opinion publique contre Maurice Papon et influencer par là implicitement les jurés. On aurait pu opposer le fait que la défense pouvait faire de même. Certes, mais tous les accusés pourraient-ils en faire autant ? Ne serait-il pas plus juste que ce soit le ministère de la Justice lui-même qui se charge du site relatant les audiences, avec les interventions de chacun, ni plus ni moins, et non pas un site se proclamant indépendant ?

<sup>102</sup> Une équipe de militaires américains, mandatée par le Pentagone, est parvenue à télécommander à distance, *via* Internet, une batterie de missiles embarqués sur un bâtiment de surface de l'US Navy naviguant au large.

<sup>103</sup> On les appelle aussi des *hackers*.

<sup>104</sup> Voir l'étude de l'IHEDN, op. cit., séance 6, avec M. Philippe Breton : "Les sociologues de l'information estiment que les pirates informatiques sont mus par des considérations idéologiques de type anarchiste. Ils prônent une société sans Etat, sans armée, gouvernée par les réseaux. Pour eux, l'information doit être libre et il ne doit pas y avoir de sécurités, de verrouillages. Ils ont donc un comportement de destructeur des sécurités alors qu'ils n'utilisent pas l'information protégée. Ainsi, l'alliance entre un génie du piratage et un service chargé d'actions psychologiques est à redouter"...

protègent contre ces intrusions. C'est effectivement vrai mais, comme la vieille histoire de l'arme et de la cuirasse, tout moyen de protection électronique est un jour ou l'autre dépassé<sup>105</sup>.

- *l'attaque aux racines du réseau* : il existe un autre danger, non celui du pirate qui recherche à s'introduire dans un ordinateur, mais celui qui recherche à dégrader le fonctionnement du réseau à des fins personnelles ou terroristes. C'est ainsi qu'au début du mois de février 1998, le quotidien *Le Monde*<sup>106</sup> a annoncé qu'un des pionniers d'Internet, Jon Postel, était parvenu à détourner le trafic des demandes d'adresses, pourtant géré par le gouvernement américain. L'intéressé n'est pas le premier venu puisqu'il est "considéré comme le père du système d'adressage des sites sur Internet" en charge de l'IANA<sup>107</sup>. Il a rerouté l'ensemble du trafic pendant 48 heures au nez et à la barbe du gouvernement américain... et de milliers d'internautes qui ne se sont rendus compte de rien.

Comme le souligne le chroniqueur du *Monde*, "ce détournement souligne le caractère archaïque des structures actuelles du réseau mondial, qui mettent une responsabilité énorme dans les mains d'un seul homme", et, par conséquent, sa fragilité face à une action de désinformation...

- *la dérive vers le renseignement* : les "pirates du cyberspace" s'ingénient surtout à pénétrer les réseaux sans pour autant chercher l'information classifiée qui y est entreposée. Mais les organisations criminelles et des institutions tout à fait connues engagent des *hackers* afin de profiter de leurs talents informatiques et faire du renseignement. Par exemple, les services secrets japonais développent actuellement des logiciels automatisés qui ont pour fonction d'intercepter, de trier et de stocker des informations pêchées dans les banques de données *on-line* à partir de mots préprogrammés<sup>108</sup>. M. Shigeta, chargé de la guerre des codes au Johohondu - agence centrale de renseignement militaire japonaise, annonce franchement la couleur : "Internet va devenir l'un de nos grands chantiers".

- *les fournisseurs d'accès* : les fournisseurs d'accès détiennent de nombreux renseignements sur leurs abonnés, comme l'adresse et le numéro de téléphone par exemple. Un sous-marinier américain en a récemment fait la triste expérience : diffusant des messages homosexuels, en utilisant un pseudonyme - *Boysrch*, soit "recherche-de-garçons" -, il a fait l'objet d'une dénonciation auprès de l'*US Navy* qui a pu, par téléphone, récupérer chez son *provider* - *America on line* - le nom et l'adresse du sous-officier. Ce dernier a alors fait l'objet d'une demande de renvoi<sup>109</sup>. Comme le rappelle Yves Eudes, "tous les clients d'AOL sont en droit de se demander si leur anonymat est respecté ou si leur identité peut être révélée à n'importe qui, y compris à des personnes mal intentionnées, sur un simple coup de téléphone". AOL a enfreint la loi fédérale américaine<sup>110</sup> qui garantit la protection de la vie privée sur les réseaux. On peut imaginer le nombre d'informations personnelles que l'on peut récupérer via internet dans le but d'exercer des pressions sur un homme, ou au moins d'étudier son caractère.

<sup>105</sup> Aux Etats-Unis, un concours de déchiffrement de clés est organisé chaque année : après la phrase à découvrir de 40 bits, déchiffrée en 3 heures, puis celle de 48 bits, déchiffrée en 13 jours, il a fallu 210 jours pour déchiffrer celle de 56 bits et remporter les \$ 10 000 mis en jeu par la société RSA. Les 72 millions de milliards de possibilités ont été essayés par un système équivalent à 26 000 microprocesseurs *Pentium 200* travaillant en parallèle. La machine qui a trouvé la bonne clé, située non pas au *Massachusetts institute of technology* mais dans le département informatique d'une université bruxelloise, était capable de tester 7 milliards de clés par seconde...

<sup>106</sup> Voir l'article *Un pionnier d'Internet démontre la fragilité des structures de la Toile* de Michel Alberganti, dans *Le Monde* du 4 février 1998.

<sup>107</sup> Voir le paragraphe 222-2 *Matériel nécessaire*.

<sup>108</sup> Voir l'article *Le Japon dans la guerre secrète* de Roger Faligot, dans la revue *Planète Internet* n°25 de décembre 1997-janvier 1998, p 51.

<sup>109</sup> Voir l'article *Les mésaventures du sous-marinier McVeight* d'Yves Eudes, dans *Le Monde* TV-radio-multimédia des 25 et 26 janvier 1998.

<sup>110</sup> Il s'agit de l'ECPA, *Electronic communications privacy act*.

Car les *providers* recensent automatiquement les connections effectuées par chacun de leurs abonnés, afin de demander le règlement de la facture. "Dis-moi qui tu lis et je te dirai qui tu es..." Ces informations peuvent être utilisées pour déterminer les centres d'intérêt de l'internaute, pour discerner sa personnalité, ses vices, donc ses faiblesses. Les actions psychologiques seront d'autant plus efficace que la personne a bien été ciblée.

### 312. Comment se prémunir des actions psychologiques ?

#### 312-1 Les problèmes à résoudre

M. Durandin estime que pour se protéger du mensonge, il faut au préalable en avoir une idée distincte. Or, le mensonge peut revêtir une multitude de formes, donc il est irréaliste de penser pouvoir cerner le problème. En revanche, on sait qu'il est organisé par quelqu'un (à définir) dans un but bien précis (*idem*). Ce sont ces deux réalités qu'il faut appréhender avant de parvenir à contrer l'action psychologique.

En outre, il existe partout dans le monde de nombreux vides juridiques quant à l'utilisation frauduleuse du réseau (transfert d'argent sale, pornographie, pédophilie, etc.). Le jour n'est pas encore venu où les nations s'entendent sur des mesures communes réprimant ces pratiques. Pour quelques années encore, il est donc possible d'envisager des actions illégales sur le réseau.

Enfin, la confidentialité des informations et la sécurité des réseaux semblent difficiles à acquérir, compte tenu des capacités intrusives des informaticiens.

Nous sommes donc en présence de trois problèmes distincts :

- qui cherche à manipuler, à pénétrer ou à entraver le fonctionnement du réseau ?
- quel est l'objectif recherché ?
- peut-on, dès le temps de paix, trouver un moyen légal ou technique pour le contrer ?

#### 312-2 Quelques solutions...

- ... à la *première question* : en temps de crise, savoir de qui provient l'attaque n'est pas compliqué. Il convient cependant de relever au moins le contenu du message puis d'identifier celui qui le diffuse. En France, la CNIL en est capable, mais uniquement pour les ordinateurs se connectant en France métropolitaine<sup>111</sup>. Cette capacité d'action n'est pas difficile à contourner puisqu'il suffit de travailler à l'étranger ou d'utiliser, occasionnellement, un site sur lequel on peut travailler quelques heures et disparaître. On peut encore se poser la question de savoir si la CNIL pourra longtemps dépister un pirate parmi les millions de récepteurs attendus dans les prochaines années. Toutefois, puisqu'on ne peut pas laisser le champ libre aux diffusions illicites, il faut que cette "police française du cyberspace" s'entende avec celle de ses voisins, quant elles existent.

Lors de la Seconde Guerre mondiale, on a tenté des deux côtés d'intercepter les communications de l'ennemi. Aujourd'hui, il faut adapter les moyens de guerre électronique et confier aux spécialistes la mission de veille et d'interception des messages insolites.

Les véritables champs de bataille, ce sont les forums de discussion. Pour éviter les messages de désinformation, il faut surveiller les *Newsgroups* et disposer de logiciels permettant de retrouver les personnes qui signent sous des noms d'emprunt différents. Il faut également pouvoir compter sur des outils permettant de détecter une campagne d'opinion lancée sur Internet, par exemple dès que certains se mettent à diffuser à peu près les mêmes choses sur un même thème. Des sociétés civiles se sont lancées sur le marché de la défense contre le dénigrement économique *via* Internet. Par exemple, l'entreprise DATOPS propose les services de "surfeurs" professionnels dont la stratégie de contre-information peut éviter le phénomène de réaction en chaîne très préjudiciable à une marque ou une organisation. Les ministères de la Défense et de l'Intérieur doivent absolument s'intéresser à de tels procédés.

<sup>111</sup> Voir plus loin 312-3 Ce que font les autorités étatiques en la matière.

On assiste ensuite auprès des internautes à une prise de recul assez positive, en ce qu'il se développe chez l'individu un sentiment de méfiance au regard des informations recueillies çà et là. En effet, on se méfie d'autant plus des positions prises qu'elles sont peu nuancées donc moins crédibles, puisque le *quidam* n'est pas forcément manipulateur professionnel, et que cela se voit aisément. Instiller des informations manifestement fausses, voire grotesques, permettrait de noyer les messages de désinformation et ainsi de leur enlever leur efficacité.

Enfin, on évoque souvent la recherche de l'anonymat. Faire appel aux services d'*anonymizers*<sup>112</sup> accessibles au grand public présente des effets pervers. En effet, cela ouvre forcément la porte à des abus ou à des trafics. C'est la raison pour laquelle certains de ces services ont déjà fait l'objet d'une fermeture pure et simple.

- ... à la deuxième question : il convient d'apprécier convenablement la situation du temps de crise et d'en tirer les objectifs de l'ennemi. En fonction de telle action ou de telle décision, des argumentaires doivent en permanence être diffusés. Il s'agit d'utiliser ni plus ni moins la même stratégie que pour les médias classiques, mais sans attendre l'attaque. Pour ne pas laisser le doute s'installer, il faut occuper le terrain et être présent au sein des discussions des *Newsgroups*. Toutefois, les pays démocratiques ne pouvant pas se permettre de recourir au mensonge pour contrer le mensonge, ils doivent sans cesse rappeler la vérité. Les actions psychologiques ne doivent pas être menées par les services reconnus de communication, mais par des officines "privées".

- ... à la troisième question : il faut contrôler le média "Internet". Thierry Régnier, chef du service informatique du CEDOCAR<sup>113</sup>, estime que c'est possible car ce sont les opérateurs qui disposent des câbles, des satellites et des liaisons par lesquelles transite l'information. Ces opérateurs s'interconnectent entre eux, en fonction d'accords internationaux ou d'alliances économiques. Les Etats ou des sociétés bien identifiées détenant les moyens adéquates contrôlent donc les chemins empruntés par les liaisons Internet<sup>114</sup>. On peut ainsi surveiller l'information et son contenu. Toutefois, étant donné l'explosion du trafic sur le réseau mondial, il devient impossible de tout suivre, donc de tout contrôler. Et si l'opérateur censure trop l'accès à certains sites cela peut lui faire perdre un marché... donc la faculté de contrôle ! C'est pourquoi le suivi d'Internet est une affaire très sensible<sup>115</sup> ! Cela demande également d'intervenir avant la crise, car, une fois celle-ci commencée, fermer un site serait mal perçu par l'opinion publique.

Devant la multiplication des sites sources, les moteurs de recherche constituent un moyen quasi incontournable pour un internaute pour rechercher d'une information. Il ne faut donc pas abandonner à un seul pays ou à un seul opérateur le monopole des moteurs de recherche, ce serait toujours vers les mêmes sites, les mêmes entreprises, les mêmes opinions que se dirigeraient les "surfeurs. Il y a là également un problème d'indépendance nationale qui doit être pris en compte au plus tôt pour éviter d'être victime "d'influence".

Quant aux décideurs, pour rendre leur surveillance électronique plus difficile, il leur faut souvent changer d'identité (électronique), ne procéder qu'à des requêtes très larges et poser des questions assez éloignées des domaines d'intérêt réels. Il faut pouvoir également se surveiller soi-même afin de déceler celui ou ceux qui écoutent ou lisent ce qui se raconte sur l'ordinateur utilisé. Il y a une indispensable sensibilisation et formation de nos élites.

Ensuite, pour sauvegarder des informations et ne les communiquer qu'à des personnes ayant besoin de les connaître, de nombreuses sociétés font appel à la cryptographie. Les Etats sont

<sup>112</sup> Un *anonymizer* est un système proposé aux utilisateurs d'Internet, permettant l'anonymat le plus complet.

<sup>113</sup> Le Centre de documentation de l'armement dépend de la Délégation générale pour l'armement (DGA).

<sup>114</sup> Voir l'article *Internet et la guerre de l'information* de Thierry Régnier, dans la revue *L'Armement* n° 60 de décembre 1997-janvier 1998, p 106.

<sup>115</sup> Aux Pays-Bas, un fournisseur d'accès à Internet (XS4ALL) a refusé de coopérer avec la police et d'exercer une "planque électronique" sur le compte d'un de ses abonnés, sous le prétexte que la demande manquait de base légale.

restés longtemps hostiles à ces pratiques qui rendent la surveillance du réseau plus difficile. Aujourd'hui, étant donnée l'ampleur que prend le réseau, elles sont autorisées.

On peut, toujours dans un souci de protection, faire également appel à des codes d'accès, mais si la source et la destination sont bien protégées, ce n'est pas le cas du support de l'information qui, lui, n'est pas soumis au même niveau de protection. C'est pour cela que les mesures de cryptographie sont nécessaires. Même dans ces conditions, les systèmes de sécurité sur le réseau lui-même ne semblent pas suffisamment efficaces et sérieux pour qu'un Etat puisse faire transiter des informations de Défense. En revanche, il semble possible de jouer sur les connections entre les Intranets et Internet : cela éviterait qu'un ordinateur branché sur l'un puisse être pillé par un hacker connecté sur l'autre. Des efforts sérieux de protection peuvent donc être faits.

### 312-3 Ce que font les autorités étatiques en la matière

Aux Etats-Unis, le *Communication decency act* (CDA) devait déterminer le niveau de "criminalisation" des échanges de propos offensants dans toute les communications électroniques. Pourtant votée par les deux chambres du Congrès et signée par Bill Clinton, cette loi a été invalidée par la Cour suprême, considérant qu'elle était anticonstitutionnelle. Pour contourner cet obstacle, les législateurs américains parlent d'insérer des puces de filtrage au sein des ordinateurs ou d'avoir recours à des logiciels de censure.

En outre, pour éviter des incidents comme le détournement du trafic des adresses par Jon Postel, le gouvernement américain<sup>116</sup> propose de créer une entreprise privée - 100 % américaine, il s'entend - à but non lucratif qui reprendrait en main la gestion des numéros assurée par l'IANA, et serait dirigée par un conseil composé de quinze membres représentant équitablement les intérêts des différents acteurs d'Internet, à l'exclusion des gouvernements ou des organisations internationales. Cette solution n'est bien évidemment pas convenable car, elle officialise l'assujettissement du réseau au contrôle de la seule puissance américaine. Ce plan va totalement à l'encontre des propositions de l'Union internationale des télécommunications (UIT)<sup>117</sup> qui tente de faire sortir le centre de gravité d'Internet du giron américain, en confiant à 28 entités différentes, réparties sur la planète, la gestion de l'ensemble des adresses. On voit par cet exemple que les Etats-Unis cherchent à garder le maximum de contrôle sur le réseau.

En France, en novembre 1996 a été annoncée la création de l'Observatoire des autoroutes de l'information, regroupant l'ensemble des acteurs industriels, socio-économiques, politiques, scientifiques... concernés par le développement d'une société informationnelle<sup>118</sup>. La démarche gouvernementale française s'inscrit dans une action de développement du commerce électronique sécurisé, donc de la recherche en matière de cryptologie, et la promotion par l'éducation des Nouvelles technologies de l'information et de la communication (NTIC). Il est nécessaire que la Défense s'investisse dans de tels projets.

De son côté, la Commission nationale informatique et liberté (CNIL) a ouvert un site<sup>119</sup> expliquant comment on pouvait être pisté sur Internet. L'anonymat n'est donc pas la règle : on peut être suivi, surveillé, voire espionné. Comme le dit la CNIL, l'anonymat demande des efforts et il n'est jamais absolu. L'exemple fourni en annexe B correspond à une connection effectuée à partir du bureau de M. Yves Calmejanne, de la société TF 1 : la CNIL a pu reconstituer les adresses de la machine utilisée, le système d'exploitation employé, la date de la dernière connection, etc.

En ce qui concerne le filtrage des informations, le ministère de l'Education donne l'exemple avec le réseau Renater. Il a décidé de "rationaliser l'usage d'Internet par les étudiants à des fins

<sup>116</sup> Par la voix d'Ira Magaziner, conseiller Internet du président Clinton.

<sup>117</sup> Dépendant aujourd'hui de l'ONU, l'UIT est la petite-fille de l'Union télégraphique créée en 1865, la plus vieille institution internationale.

<sup>118</sup> Voir l'étude de l'IHEDN, op. cit., séance n°1 de M. Bélorgey.

<sup>119</sup> Son adresse est "www.cnil.fr".

plus académiques". En effet, comme pour le Minitel, on peut se connecter à un site rose, extrémiste, terroriste ou à un site informationnel sérieux. Une sorte de "cybergendarme" est mis en place sous la forme d'un filtre. Il existe déjà à la faculté de Jussieu une machine<sup>120</sup> et un logiciel servant de filtres. Il en faudrait une dizaine pour filtrer efficacement Internet, d'après Stéphane Borztmeyer, administrateur à l'Institut Pasteur<sup>121</sup>. On éviterait peut-être ainsi l'intoxication et la désinformation des élites. Cette espèce de censure, pourrait être également étendue aux familles, ce qui empêcherait que l'appel aux instincts élémentaires (faire peur, intimider, faire naître l'inquiétude ou la panique) n'ait de réelles répercussions sur le moral de la population. Néanmoins, il faudrait que ce soit des sociétés françaises ou européennes qui créent leur propre logiciel car, actuellement, les "listes noires" de sites interdits sont établies selon les normes américaine<sup>122</sup>.

On assiste donc un peu partout à un désir de censure, ou au moins de filtrage, de la part des Etats, afin de protéger la population des effets pervers d'une communication tous azimuts incontrôlable. Il faut, de toute évidence, que la France participe activement aux recherches permettant de faire évoluer le réseau selon sa sensibilité, sinon les normes anglo-saxonnes s'imposeront et, dans les périodes de crise, un décalage grandissant existera entre la volonté gouvernementale et la "sensibilité" exprimée sur le réseau.

### Conclusion partielle.

Internet est-il une arme redoutable pour la désinformation ? Aujourd'hui, en tout cas, il est devenu incontournable pour la vie des entreprises et des chercheurs. Il est certain que, dans quelques années, il le sera pour une vaste partie de la population refusant d'être "infopauvre".

Toutes les branches d'activité des pays industrialisés seront à terme reliées à Internet et posséderont chacune des Intranets connectés entre eux. Le défi est clairement lancé aux Etats. Ceux-ci doivent agir dans trois directions et n'en oublier aucune, sous peine de laisser s'installer une sorte d'anarchie informationnelle, prélude à leur disparition :

- recouvrer impérativement la fonction régalienne de surveillance de l'information ;
- se donner les moyens techniques aptes à exercer cette surveillance ;
- se donner les moyens légaux de censure par entente internationale sur le sujet.

Internet va encore certainement évoluer. Il est même prévisible que tous les médias se retrouveront un jour ou l'autre au sein d'un immense système planétaire les combinant entre eux. Quand on constate le bouleversement que la numérisation provoque dans le monde de la télévision, on imagine l'ampleur du phénomène si on l'associe à Internet. En effet, d'après Joel de Rosnay<sup>123</sup>, les modifications liées à la technologie du numérique vont entraîner d'importantes modifications industrielles et créer un nouvel espace impliquant des regroupements dans l'édition, la téléphonie et des intégrations sectorielles. Il pense que, dans trois ou quatre ans, on assistera sans doute à :

- un accroissement considérable des débits multimédias, grâce à l'entrée en jeu de satellites à orbite basse ou polaire ;
- la fusion de la télévision numérique et d'Internet (le *webtv*) ;
- l'avènement du *webcasting* (par analogie au *broadcasting*), c'est-à-dire l'envoi et la mise à jour sélective des informations, en fonction du profil d'intérêts de l'utilisateur.

C'est sans doute ce que les visionnaires nomment les "autoroutes de l'information". Il est nécessaire que la Défense s'y prépare car leur contrôle deviendra une arme indispensable.

## 32. Techniques numériques et actions psychologiques

<sup>120</sup> *Alpha 1000*, de la société Digital : elle coûte 300 000 francs l'unité et sert de cache (*proxy* en langage informatique).

<sup>121</sup> Voir l'article *Les étudiants dans les mailles du filet ?* de Jérôme Thorel, *Planète Internet* n°25 de décembre 1997-janvier 1998, p 36.

<sup>122</sup> Par les sociétés Cyberpatrol, Surfwatch, ou Webtrack.

<sup>123</sup> Voir l'étude de l'IHEDN, op. cit., séance 8 de M. de Rosnay.

### 321. Apport du numérique et actions psychologiques

Il s'agit de déterminer en quoi la rapidité et la qualité du traitement de l'information télévisuelle peuvent influencer sur les méthodes déjà connues de manipulation de l'image. Nous l'avons vu, si on associe numérisation à compression et miniaturisation, les problèmes auxquels est confrontée une équipe de reporters sont moins délicats qu'auparavant parce que :

- les matériels emportés sont beaucoup moins encombrants ;
- les capacités de mémoire et de traitement sont bien plus étendues ;
- la vitesse de transmission est très supérieure.

En fonction de la chaîne "mère" (TF 1, FR 2... ou LCI, CNN...), la méthode de travail est sensiblement différente. En effet, on est désormais en présence de trois niveaux d'urgence :

- le premier correspond à l'urgence absolue : les chaînes d'information continue peuvent diffuser immédiatement un reportage à peine arrivé, qui n'est alors pas vérifié au préalable, et les chaînes classiques peuvent suspendre les programmes en diffusant un flash<sup>124</sup> ;
- le deuxième est celui du moyen terme, lié au journal télévisé classique<sup>125</sup> ;
- le troisième est celui des émissions à thème ou à vocation "reportages"<sup>126</sup>.

Les menaces à prendre en compte se réfèrent donc à un de ces trois niveaux.

Nous l'avons dit, le temps de crise est celui du temps réel. Au XXI<sup>e</sup> siècle, le public n'acceptera pas d'être informé avec des heures de retard. Ainsi, les effets recherchés par une équipe chargée de mener des actions psychologiques seront :

- de frapper l'opinion publique par des images chocs, en s'adressant aux instincts élémentaires de la population ;
- de pousser la population visée à s'interroger grâce à des prises de vues surprenantes, à des fins de propagande, de désinformation ou d'intoxication.

Dans le premier cas, la demande d'images impose des délais les plus courts possibles. On peut alors truquer l'image proprement dite ou la substituer par une autre au moment de sa transmission. Cela nécessite cependant des moyens performants, capables de réduire au minimum la durée du délit et utilisant des procédés les moins complexes possibles : l'imposture d'image<sup>127</sup> ou le montage mensonger<sup>128</sup>. Si les conditions le permettent, on fera appel à la superposition<sup>129</sup>.

En outre, il est possible de jouer sur le fait qu'aujourd'hui, grâce aux techniques de transmissions numériques, les images parviennent très rapidement aux rédactions, voire simultanément avec l'événement. Elles risquent donc de ne pas être visionnées avant diffusion. La pression de l'actualité, la concurrence avec les autres chaînes, l'attrait de l'image choc et un rédacteur en chef saturé ont vite fait de laisser diffuser des images trafiquées.

Dans le deuxième cas, les délais accordés aux manipulateurs sont beaucoup plus longs. La manipulation peut donc se montrer plus insidieuse, ne cherchant pas à afficher directement mais tachant de créer un malaise, une critique ou une préoccupation. Des procédés plus complexes sont alors employés, faisant appel à toute la puissance du traitement numérique : méthodes utilisant l'incrustation point à point<sup>130</sup>, la détection de contour<sup>131</sup>, voire la création d'images de synthèse<sup>132</sup>.

<sup>124</sup> C'est le cas lors de la disparition de personnalités comme le pape, un chef d'Etat, une princesse...

<sup>125</sup> Le "20 h 00" détient manifestement la palme toutes catégories de l'audience et de l'impact auprès du public.

<sup>126</sup> Comme *Envoyé spécial* sur France 2, *Zone interdite* sur M 6, etc.

<sup>127</sup> Les techniques numériques sont aptes à transformer une image d'archives en la remettant au goût du jour.

<sup>128</sup> De la même manière, il est possible d'effacer des indications gênantes afin de donner à une succession d'images, provenant de sources différentes, l'apparence de l'unité spatio-temporelle.

<sup>129</sup> Par exemple, on place un soldat américain au milieu d'un combat de rue, ce qui tend à prouver l'intervention directe des Etats-Unis dans un conflit.

<sup>130</sup> Par exemple, on peut introduire l'image d'un représentant de l'ONU ou d'un militaire de l'OTAN à une réunion de l'exécutif serbe de Bosnie, en présence, cette fois-ci bien réelle, de Radovan Karadzic. Sans en faire état dans le commentaire, l'image sera diffusée sans problème, tout le monde ne connaissant pas le visage de tout le monde. Il faudra alors prouver l'impossibilité de la présence et le trucage du film.

Enfin, même si cela ressemble à de la science-fiction<sup>133</sup>, il doit être envisagée la possibilité d'intervenir directement sur un canal de télévision, par substitution du signal technique. Si les prévisions de Joel de Rosnay se réalisent, c'est-à-dire la fusion de la télévision (numérique) et d'Internet (le *webtv*), la puissance d'un ordinateur associée à celle du traitement numérique pourra demain être capable d'accomplir une telle opération. C'est la conséquence directe de l'interconnexion des moyens d'information. On sera alors confronté à un nouveau phénomène de piratage aux manifestations spectaculaires.

### **322. Dispositions et précautions à adopter**

Agir sur le deuxième niveau d'urgence semble difficile car la qualité des moyens de visionnage des reportages augmente au même rythme que celle du matériel de montage - ce dernier bénéficie également des progrès du numérique. On peut alors penser qu'un bon technicien, sensibilisé au danger de la manipulation des images et connaissant parfaitement les techniques modernes associées, sera encore en mesure de reconnaître un montage douteux<sup>134</sup>. Des logiciels de reconnaissance de trucages pourraient être mis au point, comme il en existe pour dépister des virus informatiques. Encore faut-il se donner les moyens de le faire. Quant au troisième niveau d'urgence, il n'est par réellement utilisable en temps de crise.

Il convient donc de s'intéresser à l'urgence absolue. La technologie numérique ne change pas radicalement les procédés de trucage. Elle instaure un autre rythme de travail, des formes de menace nouvelles, donc des mesures de protection différentes. Le temps de crise offre des opportunités à ceux qui doivent mener des actions de déstabilisation. Bien que leur champ d'action soit très étendu, on cerne sans difficulté les dangers auxquels les télévisions sont confrontées. La primauté de l'image, la "dictature" du temps réel sont des impératifs auxquels il ne faut donc pas sacrifier. Une sensibilisation devra être entreprise<sup>135</sup> :

- à la source, on emploiera des méthodes de protection (cryptage, transfert doublé des images *via* deux supports différents) ;
- à l'arrivée, on vérifiera la provenance de la transmission (griffe du chef d'équipe, codes personnels) ;
- on ne diffusera pas de reportages qui n'aient été préalablement vérifiés.

S'agissant d'une éventuelle capture de faisceau, il devra être toujours possible à une chaîne de brouiller le canal qui lui est concédé.

Après ces paragraphes sur les techniques disponibles, il ressort que le mariage de la technologie numérique et de la miniaturisation multiplie les possibilités de prise de vue, de conception, de transformation et de transmission des images vidéo.

S'agissant de la diffusion de l'information, une évolution vers une plus grande fluidité et une plus grande facilité d'accès est prévisible. Demain, plus qu'aujourd'hui, il sera possible d'alerter le téléspectateur partout, tout le temps et de diffuser des images vieilles de quelques minutes.

Toutefois, le consommateur sera saturé par le flux et par la masse d'informations qui lui seront données. Leur impact s'en ressentira fatalement, ce qui signifie que la manipulation aura des répercussions moindres si elle n'est pas de grande ampleur.

<sup>131</sup> On peut jouer sur l'environnement en remplaçant un pommier en fleurs par un arbre sous la neige, tendant à prouver qu'un événement s'est déroulé en hiver.

<sup>132</sup> Tout est désormais possible, tant cette technique a évolué depuis quelques années.

<sup>133</sup> On se rappelle des films de James Bond ou de bandits masqués réussissant à prendre la parole lors d'un journal télévisé, en parvenant, pendant quelques secondes, à court-circuiter la transmission de la chaîne.

<sup>134</sup> Actuellement, pour ce qui est du journal de 20 h 00 de TF 1 par exemple, environ quinze sujets de dix secondes à deux minutes sont diffusés chaque soir.

<sup>135</sup> Sous la forme d'une conférence aux membres des rédactions. Par exemple : comparaison entre images truquées ou non, démonstration de procédés de manipulation, etc.

### 33. Un concept d'actions psychologiques

Les progrès techniques, comme nous venons de le voir, ont eu pour effet d'accroître de manière exponentielle la quantité d'informations, erronées ou non, qui circule. La révolution informatique, la multiplication des satellites, la profusion des réseaux et des bases de données, sans compter les technologies de traitement, de transmission et de distribution de l'information; font qu'aujourd'hui, aucune crise ne peut être gérée sans prise en compte de l'information.

"Quelle que soit la forme que puissent revêtir les conflits modernes - guerre ouverte ou larvée opposant des armées "conventionnelles", des forces armées structurées à des armées locales résiduelles, des milices, voire un mercenariat, dans un cadre espace-temps limité ou élargi, leur règlement ne peut se suffire du seul poids des armes. Un accompagnement "psychologique", plus ou moins prononcé, en direction des acteurs sur le terrain et des populations est plus que nécessaire pour vaincre... Dans ces conditions, le besoin de restaurer, sous certaines conditions, l'action psychologique se pose encore avec plus d'acuité depuis l'apparition d'une violence débridée, aussi bien en Europe qu'en Afrique..." C'est bien en ces termes que le colonel Ritchoufftz<sup>136</sup>, de la Délégation aux affaires stratégiques, explique l'importance des actions psychologiques en tant que nouveaux moyens qui permettent, dit-il, de gagner autrement.

Mieux encore, il ne suffit plus de prendre en compte l'information dans la gestion des crises, mais il faut la penser, la concevoir en fonction d'objectifs clairement affichés, la préparer, de façon à pouvoir anticiper sur les événements.

### 331. Un concept nécessaire

Prévoir des répliques médiatiques, incluant des actions psychologiques en fonction de l'analyse des risques et des actions que peut mener l'adversaire ou certains médias hostiles est indispensable. Certains, parmi ceux qui n'ont pas encore saisi les enjeux de l'information, continuent à crier au scandale. Néanmoins, il s'agit de ne pas se laisser bercer par les principes déontologiques illusoire, ce qui implique de perdre beaucoup de sa naïveté au profit d'un réalisme et d'un pragmatisme à toute épreuve. François Géré attire notre attention sur les dangers d'une moralisation utopique d'une médiatisation que la France risque d'être seule à vouloir défendre : "On évoque la désinformation soviétique et, plus récemment, l'action psychologique américaine dans la guerre du Golfe ; on retient le faux témoignage devant le Congrès d'une dignitaire koweïti et les manipulations dont auraient été victimes les journalistes via le *pool* de presse mis en place durant la campagne. Le résultat est que nous serons bientôt les seuls à nous détourner de l'action psychologique, attitude qui, non seulement nous place en position de vulnérabilité, mais devient franchement absurde si l'on considère les profondes mutations qui affectent le cadre général dans lequel se développera désormais l'action psychologique..."

#### 331-1 Une structure et des missions

Dans le domaine de la gestion des crises, l'improvisation doit être proscrite. En amont des crises, une analyse du problème doit être tentée car la rapidité de réaction et la cohérence de la réponse sont primordiales. Lorsque la crise éclate, l'essentiel, si ce n'est le tout, aura déjà été fait auparavant.

C'est pourquoi il devient nécessaire de disposer au niveau stratégique d'un organe de conception et de planification médias (OCPM) qui dépendrait directement des plus hautes autorités de l'Etat. Il serait permanent parce que les travaux à mener sont nombreux et afin de mieux roder les circuits d'information et de travail, nécessairement complexes car interministériels et pluridisciplinaires.

L'organe chargé de la planification médiatique devra, pour les besoins d'efficacité et de cohérence, travailler conjointement avec toutes les parties prenantes ou pouvant être intéressées

<sup>136</sup> Voir son article paru dans la revue *L'Armement* n° 60 de décembre 1997- janvier 98, p 16.

de près ou de loin par la gestion d'une crise, tels l'Etat-major interarmées de planification opérationnelle, les Renseignements généraux, le ministère des Affaires étrangères...

Il serait en quelque sorte saisi par les ministères compétents et, dès les prémices de la crise, il travaillerait sur des scénarios médiatiques, incluant l'action psychologique, possibles et réalistes. Naturellement, des experts pourraient être associés temporairement aux travaux des cellules permanentes.

Le rôle de cette structure serait de conduire, dès le temps de paix, la réflexion sur la façon dont les crises futures pourraient être gérées. Parallèlement aux planifications opérationnelles et à la lumière des enseignements tirés des crises survenues à travers le monde (Golfe, Afrique, Moyen-Orient, ex-Yougoslavie, Asie, etc.), elle élaborerait des projets de manœuvre médiatique. Comme pour les crises intérieures et sur renseignement des services compétents, l'organisme tenterait non pas de prévenir une crise mais de préparer l'opinion publique à soutenir la position du gouvernement sur le problème.

Elle constituerait également une banque de données médiatiques, étayée par diverses études politiques, économiques, sociologiques, historiques, linguistiques... à même de faciliter une prise de décision et qui, le jour J, constituerait une panoplie d'options pour les décideurs. Evidemment, au déclenchement d'une crise, il faudrait mettre à jour et adapter le plan au nouveau contexte. Pour ne pas surcharger l'organisme, la conduite de l'action psychologique au cours et à la fin de la crise devrait être confiée à un organisme différent.

Enfin, parallèlement à ce travail d'accumulation des données, il serait à même d'analyser les flux d'informations<sup>137</sup>, de façon à détecter une possible action psychologique visant à entraver l'action gouvernementale. Il pourrait ainsi orienter les services compétents sur la surveillance des réseaux qui lui semblent suspects. Bien que sensibiliser les acteurs des nouveaux médias sur les risques encourus et les mesures à prendre pour sécuriser les réseaux soit une action capitale, il ne semble pas nécessaire que cette mission supplémentaire lui soit confiée, cette action pouvant être menée par des organismes privés.

### **331-2 Un souci : l'anticipation**

Pendant une crise, il ne faut pas se laisser devancer par l'adversaire ou par les événements. Pour cela, il s'agit de faire en sorte que le moment où se déclenche la crise soit favorable chaque fois que possible à une action gouvernementale. Certes, il est souvent difficile de commander les événements, leur déclenchement échappant à notre volonté pour des considérations internationales qui nous dépassent, par exemple. Mais lorsque cela est possible, le choix du moment opportun est une condition de succès car il permet, en disposant de l'initiative du déclenchement de l'action psychologique, d'influencer les médias en leur donnant une vision, une norme propre au lieu de subir la leur<sup>138</sup>.

Nous sommes ici dans le domaine de l'influence. Il faut, répétons-le, une volonté politique claire, si possible constante, pour ne pas brouiller le message, afin que les sujets qui préoccupent nos concitoyens soient abordés par les médias d'une façon "favorable" au gouvernement.

Comme nous l'avons dit, la conduite de la communication de crise devrait être confiée à un autre organisme. Comme le Service d'information et de relations publiques des armées (SIRPA)

<sup>137</sup> Bien que difficilement imaginable, ceci semble possible à la lumière d'une étude du *Scientific and technological options assesment*, commission présidée par M. Pompidou, de la Direction générale de la recherche au Parlement européen. Ce rapport révèle l'existence d'un réseau d'écoute baptisé *Echelon*, chapeauté par la *National security agency*, agence américaine placée sous la responsabilité du directeur de la CIA.

<sup>138</sup> La campagne d'EDF de promotion de l'énergie nucléaire est quasiment un cas école. La production d'électricité par la filière nucléaire civile est critiquée par de nombreux acteurs (pays, ONG, personnalités...). Sans connaître le jour, on peut s'attendre à une campagne de grande envergure, organisée contre cette filière pourtant primordiale économiquement pour EDF (et pour la France). C'est donc bien une action psychologique avant la crise que finance EDF avec des spots télévisés, asseyant son choix dans l'opinion publique.

ne doit pas participer officiellement à une action psychologique, afin de ne pas brouiller son image, l'action doit être menée de façon indirecte. L'art consiste à fabriquer l'information puis à la "vendre" aux divers médias, sans passer en priorité par le canal traditionnel. C'est toutefois un danger puisque, menée par un nombre restreint de personnes, la manipulation peut atteindre les équipes gouvernementales.

En dépit des efforts de détection des crises, certaines éclatent sans prévenir, surtout les crises nationales. Le rôle de l'organisme serait alors, après que les spécialistes en communication ont déterminé les axes à exploiter :

- d'identifier au plus vite les actions à mener ;
- de vérifier dans la banque de données si des indices permettent de penser que la crise est dirigée (et si oui, par qui ?), mais prendre garde à ne pas tomber dans la paranoïa ;
- de monter un plan d'action psychologique complet incluant les retombées de l'après crise.

### 331-3 Une nécessité : la surveillance

Aujourd'hui nous constatons que les Américains, particulièrement en pointe en ce qui concerne les réseaux, songent sérieusement à créer un organisme dépendant du Conseil national de sécurité, c'est-à-dire tout près du Président américain. Son rôle serait de veiller en permanence sur la sécurité des réseaux et de l'information. Dans un article paru le 16 mars 1998 dans l'hebdomadaire *Defense News*, on peut ainsi lire sous la plume de George I. Seffers :

"Washington - Protecting the United States against what one expect called an « electronic Pearl Harbor » is the purpose of an historic directive expected to be signed in April by President Bill Clinton. It includes a series of far-reaching initiatives to bolster the nation's protections against computer attacks, including the creation of an Office of National Infrastructure Assurance, which a president's commission recommended reside within the National Security Council to focus the nation's intelligence hierarchy on cyber security and infrastructure protection.

Under the catastrophic electronic scenario feared by many national defense experts, a terrorist group or foreign government could, theoretically, launch a series of computer attacks against the US information infrastructure, blocking banking and finance transactions, bringing Wall Street to a screeching halt, disrupting traffic signals in major cities, altering flight paths for airplanes and drawing the country into a Third World war with cyberspace as the front line..."

La création d'une telle structure répond au besoin de sécuriser le réseau lui-même. Il impose d'améliorer la surveillance des échanges et de pouvoir repérer les cyber-attaques. Ceci n'est qu'une partie du travail, car si les *hackers* peuvent visiter des sites sensibles et modifier des données, l'action psychologique peut prendre des formes plus souples. Il faut donc être à même de détecter, de pister les intervenants sur un sujet sensible, de façon à établir la validité d'une information et son origine. Ce travail seul permettra de pouvoir détecter des actions hostiles, mais que l'on peut qualifier de "douces" puisqu'il n'y a pas d'effraction.

Il est donc nécessaire de développer deux structures distinctes :

- l'une surveillant "physiquement" le réseau et les agressions et proposant des mesures de protection ;
- l'autre orientant les recherches, analysant le flot des informations, détectant les attaques et mettant au point des plans d'action médiatique que d'autres mettraient si nécessaire en œuvre. C'est bien de cette dernière dont nous parlons.

En France, des dispositions pour surveiller les échanges sur le réseau ont déjà été prises. Toutefois, il n'est pas certain que les actions soient coordonnées, ce qui fait met en cause leur efficacité. Ayant décrit des missions qui pourraient être confiées à différents organismes, il s'agit maintenant de procéder au recensement de ce qu'il faut comme moyens humains et matériels à l'organisme qui conçoit ou détecte les actions psychologiques.

### 332. Recenser les moyens nécessaires

### 332-1 Les moyens humains

Imaginer des plans d'action psychologique nécessite des compétences très diverses. Certes, il faut des spécialistes des médias - dans le cas qui nous intéresse, il leur faudrait même maîtriser les nouveaux médias, mais également des experts en psychologie, des chercheurs sur l'impact des messages<sup>139</sup>, des sociologues, des ethnologues, des communicateurs... Tous concourent à une bonne compréhension du milieu et, par conséquent, à l'adaptation des sources, des canaux et des messages aux cibles choisies. Des experts en réseau sont naturellement indispensables de manière à prendre la mesure des possibilités offertes par les réseaux. Ensuite, des compétences particulières sont à trouver dans le domaine des images de synthèse, des graphistes... Ces personnes doivent enfin constituer des équipes en nombre suffisant.

D'après Toffler, les journalistes qui travaillent pour le Pentagone n'ont que des connaissances rudimentaires du milieu et des langues étrangères, ce qui constitue pour l'avenir un grand handicap. Il faut naturellement éviter cet écueil. L'arme psychologique étant utilisée même entre alliés, il importe pour la France de conserver une certaine indépendance dans l'acquisition des informations. Par exemple, l'agence AFP permet de ne pas dépendre entièrement de la sphère anglo-saxonne. Le gouvernement doit donc soutenir autant que possible cette agence. Elle complète de façon indispensable les réseaux gouvernementaux (diplomates, services de renseignement, etc.).

Enfin, l'organisme doit pouvoir s'appuyer sur des centres de recherches et d'études menant à son profit (exclusif ou non) des enquêtes et des expérimentations.

### 332-2 Les moyens matériels

Ce sont des moyens matériels importants qui ont permis au SIRPA de mener à bien sa mission et de gagner la bataille médiatique contre Greenpeace, lors de la crise des essais nucléaires. Nous avons là un exemple concret de ce qu'une volonté politique affirmée, soutenue par le couple homme/matériel peut réussir. Ce qui est performant techniquement aujourd'hui ne le restera pas forcément demain. D'où la nécessité d'une veille technologique pour rester compétitif, non seulement avec les autres pays mais aussi avec les médias nationaux dont les moyens financiers sont énormes. Il y a bien évidemment pour les armées un problème de budget. Si les responsables politiques peuvent faire des économies sur certains matériels de guerre, il ne peut en être de même pour ce qui est des moyens médiatiques.

Alvin Toffler affirme que "les gens qui réfléchissent le plus sérieusement à la guerre du futur savent qu'une partie des combats les plus importants de demain se déroulera sur le champ de la bataille des médias"<sup>140</sup>. Cela a déjà commencé avec CNN. C'est pourquoi, le SIRPA doit disposer en qualité et en quantité suffisantes de ce qui est nécessaire pour pouvoir mener ses missions d'information en tout temps et en tout lieu, à savoir :

- de moyens de couverture médiatique (caméras, magnétoscopes, etc.) ;
- de moyens de retransmission en direct (antennes, téléphones cellulaires, liaisons satellitaires, etc.) ;
- de moyens de montage sur place et de réalisation d'effets spéciaux. La seule déontologie qui compte est le succès de la mission. D'où la nécessité, non seulement d'être au fait des nouvelles possibilités techniques dans le domaine de la désinformation, mais surtout d'encourager nos propres inventions en la matière.
- de moyens de déplacement rapide sur les différents théâtres susceptibles d'intéresser la manœuvre médiatique (hélicoptères équipés de moyens de transmission, par exemple). La chaîne doit être complète jusqu'aux moyens terminaux d'information. Mais, comme nous l'avons déjà dit,

<sup>139</sup> Lors d'un colloque organisé par le Centre d'études en sciences sociales de la Défense, les 1er et 2 octobre à Paris, sur les influences psychologiques, un chercheur s'est étonné du manque d'intérêt pour le sujet !

<sup>140</sup> Toffler, op. cit. p 233.

dans le domaine de l'action psychologique, le SIRPA ne peut être qu'un acteur inconscient. L'organisme chargé de déterminer le plan médiatique - communication plus actions psychologiques, par exemple - doit disposer en amont de matériel bien différent, essentiellement informatique.

- de moyens de stockage de données (textes, images réelles ou virtuelles, sons) ;
- de moteurs de recherche pour naviguer sur Internet ;
- de filtres permettant de sélectionner des messages selon des mots codes ;
- de capacités de déchiffrement et de décryptage ;
- de logiciels de conception d'images virtuelles : le travail définitif serait effectué par les équipes en charge durant la crise, mais des esquisses initiales sont nécessaires pour imaginer les actions).

### **333. Les modes d'action**

L'effet principal devant être constamment recherché à travers l'action psychologique doit être la légitimité politique et juridique de l'action que la nation entend poursuivre à travers son engagement. Du degré de cet engagement et du niveau d'implication des intérêts nationaux qui sont en jeu, dépend la nature du mode d'action à envisager. Dans tous les cas, modes d'action défensifs et modes d'action offensifs peuvent être souvent menés de pair. Ces modes d'action ne sont nullement exhaustifs. Nous tenterons néanmoins de les regrouper en fonction des expériences et, pour des besoins didactiques, en actions défensives et offensives.

#### **333-1 Actions psychologiques défensives**

Il s'agit de sécuriser les réseaux. Avec le développement des techniques de traitement de l'image et du son, l'information est devenue un simple signe, qui peut être modifié ou altéré. L'un des moyens destinés à en assurer la protection consiste à développer les systèmes de tatouage et les techniques de contrôle du *copyright* pour s'assurer leur authenticité. Cette sécurisation suppose également la capacité de contrôler ce qui est diffusé au public *via* les réseaux devenus de plus en plus accessibles aux particuliers ou aux organismes privés. Avec le nombre de caméscopes et les nouvelles techniques de numérisation, des personnes peuvent montrer n'importe quoi, à n'importe qui et quand ils le désirent. Ainsi, une simple cassette tournée par un amateur américain montrant des policiers de Los Angeles brutalisant un Noir provoqua des émeutes sanglantes. Le mouvement Chiapas agissant *via* un site Internet réussit à attirer l'attention de l'opinion publique. On s'est aperçu par la suite qu'il s'agissait de fausses informations, mais le mal était déjà fait aux autorités mexicaines.

Cette technique permet donc rapidement aux responsables politiques de dénoncer une tentative de manipulation.

#### **333-2 Actions psychologiques offensives**

Elles sont destinées à assurer le succès de l'action et reposent principalement sur des modes d'action et des postures "agressives" pouvant prendre l'une des formes suivantes :

- occuper l'espace en premier comme le SIRPA l'a fait contre Greenpeace lors de l'opération *Nautile II* au moment de la crise des essais nucléaires. Ce mode d'action très payant nécessite de disposer, comme nous l'avons déjà souligné, de moyens adéquats en personnel et en matériels et requiert une réactivité extrême en termes de délais de transmission et de diffusion de l'information. Cette réactivité permet un certain degré de monopole dont CNN a bien su profiter lors de la guerre du Golfe.

- recourir à la rétention par le biais du système des *pools* au cas où la sécurité des opérations l'exigerait, comme cela a été employé pendant la guerre du Golfe. Il faut rappeler tout de même la nécessité d'un usage modéré de cette technique car l'opinion publique finit par perdre

confiance et risque de passer d'une désaffection progressive à une opposition totale à l'action. L'efficacité de ce mode d'action dépend donc d'un savant dosage entre le verrouillage total et l'ouverture sur l'information lorsque celle-ci ne met pas d'intérêts essentiels en jeu. Lors d'une crise interne, cette technique est quasiment impossible avec le développement des nouveaux médias. Il faut donc au contraire songer à noyer le réseau avec des nouvelles vraies mais tronquées ou des nouvelles discréditant la thèse hostile.

- fournir au public une version des faits différente de la réalité. Pour cela, les équipes engagées doivent préparer toutes les images possibles à l'avance (archives ou trucages) en s'appuyant sur les banques de données, de façon à produire des montages d'images "prêts à consommer", en fonction des besoins. Si la crise est arrivée de manière totalement imprévisible, à charge pour ces équipes de travailler au plus vite.

### **34. Les méthodes**

Il n'y a pas à proprement parler de méthode qui constitue une panacée à toutes les crises. Chaque situation porte en elle sa particularité et doit être de ce fait traitée différemment, en fonction du contexte, du temps, du degré de sensibilité et de la possibilité de réactivité ou non de l'opinion avec cette crise. Même face à une crise qui se répète et dont les enjeux sont restés les mêmes, un traitement médiatique nouveau s'impose. La méthode de gestion des médias employée par les Etats-Unis pendant la guerre du Golfe n'aurait pas pu être reproduite telle quelle si les Américains avaient été amenés à conduire des frappes contre l'Irak lors du dernier bras de fer qui les a opposés en février 1998. Les motifs politiques ne sont plus les mêmes, les membres du Conseil de sécurité ne sont pas tous unanimes, etc. Ainsi, chaque crise appelle un traitement particulier. Néanmoins, l'analyse des conflits récents permet de dégager des constantes qui semblent valables de façon générale.

Ces instruments ont fourni la preuve de leur efficacité et peuvent donc servir de base pour l'élaboration de stratégie d'actions psychologiques. Dans ce cadre, on peut distinguer deux types de méthodes : celles qui sont valables dès aujourd'hui et celles qui relèvent plutôt du futur.

#### **34.1. Méthodes pour aujourd'hui**

L'une des méthodes les plus couramment utilisées aujourd'hui consiste à accuser d'atrocité l'ennemi : si ces atrocités ne sont pas avérées, il faut les créer. L'exemple de la jeune koweïtienne de quinze ans qui témoigna devant le Congrès américain en parlant de vol de matériel médical est assez patent. On peut s'interroger sur la complicité passive des organismes de sécurité de l'Etat qui ne signalèrent pas qu'en réalité, la jeune fille était une fille d'ambassadeur. Les images montrées sur CNN avaient en fait - à son insu - été fabriquées par une agence indépendante américaine. Concept particulièrement intéressant qui permet de dégager le gouvernement de toute responsabilité quand le mensonge est découvert. Notons d'ailleurs que le même principe est utilisé pour des raisons de sécurité : les services officiels ne sont pas engagés mais des agences "indépendantes" se chargent d'instruire et d'encadrer les armées de pays africains<sup>141</sup>. Dans une crise intérieure, il ne faut pas aller si loin, mais l'adversaire peut être déconsidéré dans son action.

On peut également effectuer un gonflement hyperbolique des enjeux, en faisant croire aux gens que ce à quoi ils tiennent le plus est menacé : ordre mondial, démocratie, religion, liberté, etc. Ceci peut se faire assez facilement par le biais des *Newsgroups* sur Internet.

On peut encore dévaloriser l'adversaire en utilisant des sites spécialisés : dans ce cas la puissance de l'image peut simplifier volontairement le problème. Ceci est toutefois risqué dans une crise où l'opinion publique n'a pas encore exprimé son opinion<sup>142</sup>.

<sup>141</sup> Comme c'est le cas au Rwanda, par exemple.

<sup>142</sup> Ainsi, dans le conflit des chômeurs, une telle attitude était difficile à lancer. Le gouvernement a tenté de discréditer le mouvement en dénonçant sa politisation mais cela n'a que partiellement réussi. Une action

Ensuite, la méta-propagande permet de jeter la suspicion totale dans l'opinion publique sur tout ce qui provient de l'adversaire. Cette méta-propagande est l'un des instruments les plus puissants et les plus efficaces puisqu'elle permet d'immuniser l'opinion publique contre toute action psychologique menée par l'adversaire. Cela nécessite des équipes scrutant en permanence les déclarations de l'adversaire, relèvent les contradictions et les dénonçant. Mais encore une fois, il faut différencier le type de crise. Dans le cas d'une crise interne, cette méthode n'est utilisable qu'en partie, l'opinion publique pouvant se reconnaître plus ou moins dans les manifestants.

### **342. Méthodes pour demain**

Depuis la guerre du Golfe et Timisoara, les opinions publiques semblent se méfier davantage des médias, au point que la manipulation est devenue une chose compliquée et risquée. Les journalistes ont également pris conscience de leurs responsabilités. Ils se doivent de vérifier plus que jamais les informations s'ils veulent demeurer crédibles aux yeux des lecteurs.

Quand une crise se déclare, la maîtrise de l'information, afin de s'assurer le soutien de sa propre population - ou de celle où l'on intervient, est, nous l'avons constaté, compliquée par les évolutions techniques récentes (la disponibilité des réseaux, des techniques de numérisation, des satellites commerciaux et des téléphones cellulaires, les possibilités pour les amateurs avec des moyens miniaturisés de témoigner, etc.). Il convient donc de chercher de nouvelles orientations en restant conscient que, très souvent, on ne peut que proposer des informations modifiées, mais que l'exploitation en sera faite par des partenaires indépendants (individus, médias nationaux ou internationaux).

Actuellement, certains chercheurs américains préconisent, pour l'avenir, des méthodes qui rompent avec les usages anciens. Constatant que les opinions publiques ne sont pas aussi dupes et dociles, ces chercheurs étudient de nouvelles méthodes. Ces méthodes jouent sur la qualité du message, le "ciblage" du public ou, carrément, l'accélération du temps de transmission de l'information.

#### **342-1 Démassification de l'information**

Il s'agit ici de l'information ciblée avec précision, au même titre que le sont les nouvelles générations d'armes guidées laser. Voyons ce qu'en dit Alvin Toffler : "Quand ils viseront un public précis dans les sociétés de la troisième vague, les manipulateurs médiatiques de demain, comme les agences de publicité de demain, devront démassifier leurs messages, en concocter des versions différentes pour chaque segment de public : une version pour les Noirs américains, une autre pour les Asiatiques, d'autres encore pour les médecins, les mères célibataires, et ainsi de suite. Nul doute que les histoires truquées d'atrocités seront un jour manipulées de la sorte, les victimes étant présentées différemment dans chaque version, de manière à inspirer un maximum de sympathie ou de haine à chaque ensemble de spectateurs". Ce type de manipulation n'est bien sûr pas possible au niveau mondial mais reste parfaitement réalisable par le biais du réseau, afin d'influencer les relais classiques de la société civile. Il s'agit là d'adapter le message à la cible et de sélectionner, par et *via* le réseau, les destinataires.

#### **342-2 Individualisation de l'information**

Une telle segmentation de l'information n'est en réalité qu'une phase de transition vers un nouveau type de message beaucoup plus infinitésimal : l'individualisation ou la personnalisation de l'information. Grâce aux réseaux et aux bases de données, il sera possible d'identifier ce que chaque élément, faisant partie du réseau a besoin d'entendre et de modeler en conséquence le message qui lui sera destiné en fonction de sa psychologie, de ses préférences, etc.

---

psychologique importante, visant les journalistes de la grande diffusion et appuyant cette dénonciation, aurait sans doute été nécessaire auparavant.

Ceci est déjà exploité sur le réseau. Suivant les centres d'intérêts repérés automatiquement lors des incursions sur Internet par une personne, des pages de publicité s'affichent directement sur l'écran.

On peut donc exploiter le même système en orientant les individus sur des groupes de discussion, en affichant systématiquement des images ou des textes préparés par un groupe chargé d'actions psychologiques.

### 342-3 Accélération du temps réel par création d'irréel

Dans *Guerre et contre guerre*, Toffler estime que "les nouveaux médias ne changent pas seulement la réalité, mais aussi et surtout la perception que nous en avons, et donc le contexte dans lequel s'affrontent la propagande guerrière et la propagande pacifiste"<sup>143</sup>. Les nouveaux médias jouent énormément sur cette confusion entre perception et réalité.

Les sensations de proximité et d'immédiateté sont renforcées par les nouvelles techniques. On peut donc assez facilement jouer sur la peur en rapprochant artificiellement des événements extérieurs. Le temps et les distances sont effacés, sans que les connaissances des journalistes soient plus importantes. Ils sont alors d'autant plus susceptibles d'être trompés par la manipulation.

### 343. La nouvelle stratégie américaine du savoir

Pour les Américains, les évolutions de perception constatées dans l'opinion publique et l'idée que celle-ci commence à se faire des médias imposent la mise en place d'une nouvelle stratégie prenant en compte ces évolutions. Dans ce cadre, Alvin Toffler estime que "le côté plus souriant de toute cette évolution est qu'un public accoutumé à se servir de la simulation à bien d'autres fins, à la maison, au travail ou pour jouer, peut apprendre que voir ou même sentir n'est pas croire. Avec le temps, le public a toute chance de devenir de plus en plus averti vis-à-vis des médias - et, partant, on peut l'espérer, plus sceptique."<sup>144</sup> On revient aux capacités naturelles de créer des défenses de la part des individus.

Ceci a donc conduit ces chercheurs à tenter de développer une nouvelle méthode qui tire les enseignements des évolutions que connaît la société américaine. Puisqu'il ne s'agit plus de manipuler l'opinion publique en permanence, il faudrait donc tirer le maximum de profit des avantages de la liberté en cherchant à amadouer les médias et non en leur imposant un contrôle absolu tel que cela a été jusqu'à présent pratiqué. Ainsi, Alvin Toffler pense que "toujours est-il que, malgré les frustrations et les tensions du Pentagone vis-à-vis des médias et vice versa, la plupart des guerriers du savoir militaires avec lesquels nous avons pu parler était d'accord avec les médias sur un point essentiel. Ils croient en effet que le contrôle totalitaire des médias est, en soi, une stratégie vouée à l'échec et que, d'une manière générale, la tradition américaine d'une information relativement ouverte est militairement payante. Qu'ils portent ou non l'uniforme, beaucoup ont sincèrement soutenu que l'esprit d'innovation, l'initiative et l'imagination qui jaillissent d'une société ouverte l'emportent de beaucoup sur les avantages, quels qu'ils soient, qu'un Etat totalitaire pourrait trouver à sa mainmise sur les médias. Avoir une stratégie du savoir, ce n'est pas imposer un contrôle absolu, mais user à de meilleures fins des avantages intrinsèques de la liberté. Mais gagner, perdre ou amadouer les médias, y compris des chaînes ou des technologies que l'on n'imagine pas aujourd'hui, seront une arme de première importance pour les combattants des guerres comme des contre-guerres du futur : un élément clé de la stratégie du savoir."<sup>145</sup>

<sup>143</sup> Toffler. op. cit. p 224.

<sup>144</sup> Toffler. Op-cit. page 246

<sup>145</sup> Toffler. Op-cit. pages 247-248.

Le gouvernement doit s'employer, sur certains sujets, à développer ce que Suren Erkman dénonce sous le titre "journalistes sous influence"<sup>146</sup>. Il prend l'exemple de l'effet de serre qui devient à la mode en 1988, simplement parce que plusieurs articles lui furent subitement consacrés par des scientifiques, qu'un soi-disant rapport confidentiel déniché par le *New York Times* sur Internet en dénonçait les dangers. Or ce rapport de trois volumes n'était pas confidentiel mais très circonspect sur le sujet. Il est certain que s'appuyer sur un rapport confidentiel est extrêmement intéressant pour l'action psychologique car le public ne verra dans les dénégations officielles que la poursuite de l'effort fait pour lui cacher la vérité. Or le réseau se prête tout particulièrement au "vol" de documents.

#### 344. L'utilisation des faiblesses des médias

Comme cela fut relevé précédemment, la course au direct, et à l'image que se livrent les médias offrent des opportunités. En construisant des images sur une crise en cours, en les mettant à la disposition des internautes et des (ou d'un) grands médias, on multiplie artificiellement les chances que des informations favorables à l'action du gouvernement soient publiées. Il faut également prendre soin de répondre à un besoin et de fournir des images essentiellement émotionnelles qui gardent leur force d'impact même si leur origine devient litigieuse.

---

<sup>146</sup> Suren Erkman, *Manière de voir*, bimestriel de mars-avril 1998, p 86.

## CONCLUSION

**Si l'action psychologique ne vous intéresse pas, elle s'intéresse à vous.**

En conclusion, nous ne suivrons pas point par point le plan de ce devoir, mais nous tenons à rappeler quelques vérités essentielles à propos de l'action psychologique.

Tout d'abord, c'est une nécessité dans nos démocraties où le pouvoir doit de plus en plus légitimer son action, qu'elle se situe dans ou en dehors de ses frontières. Les plans médiatiques actuels qui visent déjà à modeler l'opinion publique afin qu'elle soutienne son gouvernement ne tiennent pas assez compte du côté émotionnel de plus en plus marqué de la présentation de l'information.

L'action psychologique pose un problème éthique dans nos démocraties. Il semble toutefois possible d'exercer un contrôle politique, de façon à éviter toute dérive comme celle qu'a connue le "5e bureau". Ce problème étant caduc, l'arme psychologique reste surtout une arme particulièrement adaptée aux exigences actuelles car elle permet de convaincre et de contraindre sans effusion de sang. Cela permet de "coller" à la doctrine zéro mort que les Anglo-saxons développent et qui, bon gré mal gré, devient une référence. Enfin, c'est une arme utile même entre alliés, de façon à défendre la politique et la vision du monde d'un pays. Certains ne se privent pas de réfléchir sur le sujet. Il serait donc dangereux que, cédant au poids de l'histoire, la France ne veuille pas investir sur ce terrain. Le sujet ne doit pas être tabou.

Les développements techniques récents, qui se poursuivent d'ailleurs sans qu'on sache exactement vers quel type de société ils nous mènent, rendent possibles des opérations impensables il y a quelques années. La mise en place d'un réseau planétaire, qui modifie radicalement les rapports entre l'homme et l'Etat, la facilité avec laquelle les informations peuvent être acquises, modifiées puis transmises, rendent possible une information continue et en temps réel d'un nombre croissant d'habitants. Il n'y a donc quasiment plus d'obstacles techniques à la manipulation de cette information.

Il faut réfléchir aux moyens d'utiliser ces nouvelles techniques et aussi de s'en prémunir. Il est d'abord nécessaire de mettre en place des organismes, réunissant divers spécialistes, qui soient en mesure de surveiller les actions d'intrusion sur le *web*. La France se doit donc d'avoir une parfaite connaissance des réseaux pour en connaître les capacités. Mais il faut également se doter de moyens pour surveiller les flux d'informations, identifier les sources, analyser les discours tenus dans les forums d'échanges. Incidemment, elle doit conserver une capacité indépendante d'acquisition de l'information sans influence extérieure, sinon son intoxication serait facilitée. Ces actions de surveillance amènent à constituer d'importantes banques de données qui peuvent être exploitées pour des actions psychologiques. Un organisme doit être en mesure de structurer des réponses, de les faire approuver, puis de les mettre en œuvre. Nous ne reprendrons pas ici les actions concrètes à mener mais les opportunités nouvelles de manipulation de l'image, de surveillance électronique individuelle et les faiblesses du système médiatique permettent d'envisager des actions coordonnées.

Il faut toutefois garder à l'esprit que l'action psychologique n'est pas une arme totale, mais doit être incluse dans un système médiatique cohérent. En effet, l'opinion publique a parfois des réactions imprévisibles que les meilleurs chercheurs ne savent toujours pas anticiper !



<b>BIBLIOGRAPHIE:</b>
-----------------------

- Le monde diplomatique, Médias et contrôle des esprits, Manière de voir 27 août 1995 trimestriel.
- Capitaine CAUDE, Propagande et guerre psychologique. Revue de défense nationale 2<sup>o</sup> semestre 1995
- Le monde diplomatique, Internet l'extase et l'effroi, Maniere de voir, hors série, ,
- Lt Cl T. L. THOMAS, Dangers without border,. military Review, may-june 1997
- L'état des médias, La découverte médiapouvoirs CFPJ, 1991, 460 p
- K. POPPER, La télévision: un danger pour la démocratie, bibliothèques 10/18, 1997.
- P. BOURDIEU, Sur la télévision, Liber, 1997.
- F. GERE, La guerre psychologique, Economica, 1997.
- L'ARMEMENT, Revue bimestrielle- Décembre 1997- Janvier 1998, DGA,
- G. DERVILLE, Le pouvoir des médias, PUG, 1997, p.158.
- S. P. HUNTINGTON, Le choc des civilisations, Editions Odile Jacob, 1997, p 402.
- F. FAUCON, Guerre de l'information ou opérations d'information?, in Défense nationale, revue mensuelle, Mars 1998.
- *Les télés entre chiens et loups*, Michel Richard, *Le Point*, n° 936, août 1990
- *La bataille de l'information, les médias dans la guerre du Golfe*, entretien avec le général Germanos, chef du SIRPA, *Armées d'aujourd'hui*, n° 157, février 1991
- *Une journée au Sud de Bagdad*, Bernard Estrade, *La Croix, l'Événement*, février 1991
- *La coalition des médias*, Thierry Garcin, *Stratégique*, n° 51, 3e trimestre 1991
- *Les fonctions de restrictions imposées par l'armée américaine pour la couverture de la guerre du Golfe*, Pascale Combelles, bulletin d'information du CERSA, automne 1992
- *L'information, la désinformation et la réalité*, Guy Durandin, Presses universitaires de France, juin 1993
- *Une stratégie de l'information, l'exemple américain*, Anne-Chantal Lepeuple, revue *Défense*, n° 66, décembre 1994
- *Armées d'aujourd'hui*, n° 216, décembre 1996-janvier 1997

- *Infosphère, espace stratégique ?*, synthèse des travaux du groupe intercomités n° 3, IHEDN, 49e session nationale, mai 1997
- *Sony Vision*, mensuel de "l'audiovisuel Broadcast et professionnel" de la société Sony, n° 26, octobre 1997
- *Planète Internet*, n° 25, décembre 1997
- *Internet : vitrine, source d'information, lieu de circulation (donc d'interception)*, Claude Esmein, *L'armement*, n° 60, décembre 1997-janvier 1998
- *Internet et la guerre de l'information*, Thierry Régnier, *L'armement*, n° 60, décembre 1997-janvier 1998
- *WWW.altern.org/antenneassedic*, Yves Eudes, *Le Monde* du 29 janvier 1998
- *L'information sous influence*, Christophe Labbé et Olivia Recasens, *Le Monde* des 18 et 19 janvier 1998
- *Armées d'aujourd'hui*, n° 227, février 1998
- *Internet détourné*, Michel Alberganti, *Le Monde* du 4 février 1998
- *La persuasion de masse, Guerre psychologique/guerre médiatique*, sous la direction de Gérard Chaliand, Robert Laffont
- *Guerre et contre-guerre. Survivre à l'aube du XXI<sup>e</sup> siècle.* Alvin et Heidi TOFFLER. Ed Fayard.
- *Les manipulations de l'image et du son. Pluriel FED.* Rencontres Internationales. MEDIA-DEFENSE 95 IMAGINA. Ed.HACHETTE. 1996
- *L'ARMEMENT.* Revue de la DGA. N° 60 décembre 97- janvier 98.
- *L'événement international et les médias.* Thiery Garcin. Défense Nationale. N°10. Oct.1997
- *Libres propos sur la manipulation.* Michel Klen. Défense Nationale. N°4. Avril 1997
- *Guerre de l'information ou opérations d'information.* M. Klen. Défense Nationale. N°4. Avril .97.
- En attente des actes du colloque du Centre d'Etude en Sciences Sociales de la Défense sur la manipulation des 1er et 2 octobre 1997.

<b>CONTACTS PRIS A L'EXTERIEUR</b>
------------------------------------

- Novembre 1997 : visite à Thomson pour capacité d'écoute et d'interception.
- Novembre 1997 : entretien avec le lieutenant-colonel Batiste, COPID.
- Décembre 1997 : visite à CNN Paris, radio Proche-Orient.
- Mardi 13 janvier 1998 : entretien avec le major Gallo, services techniques de l'Etablissement cinématographique et photographique des armées, Ivry
- Mardi 13 janvier 1998 : entretien avec M. Jean-Pierre Quittard, rédacteur en chef, TF 1, Boulogne-Billancourt
- Mercredi 14 janvier 1998 : visite à l'agence AFP.
- Mercredi 21 janvier 1998 : entretien avec M. Yves Calmejanne, responsable Internet de TF 1, Boulogne-Billancourt
- Jeudi 22 janvier 1998 : entretien avec M. Humbert, services techniques de TF 1, Boulogne-Billancourt
- Lundi 26 janvier 1998 : démonstration de télévision virtuelle, société Syma vision, Paris
- Mercredi 28 janvier 1998 : entretien avec M. Patrick Robin, directeur de la société Imaginet, Paris.
- Mercredi 11 février 1998 : présence à la soutenance de thèse de doctorat en sciences de l'information et de la communication par le lieutenant-colonel Chauvancy  
sujet : « L'information, arme stratégique des démocraties: nécessité et légitimité d'une stratégie de communication ».

**ANNEXE A.**

**Exemple de site pirate.**

# Présidence de la République

10 avril 1998

DISCOURS  
DU PRÉSIDENT

COMMUNIQUÉS DE  
CONSEIL DES MINISTRES

LE MAGAZINE DE L'ACTUALITÉ  
PRÉSIDENTIELLE  
ET L'AGENDA DE LA SEMAINE



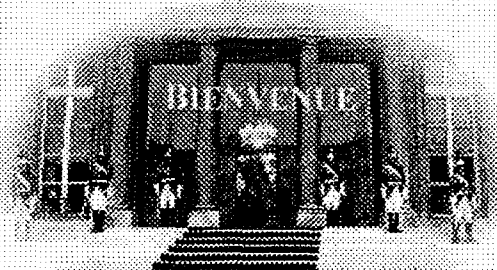
LES INSTITUTIONS



LE PRÉSIDENT

LA FRANCE ET  
L'EUROPE

DEUTSCH ENGLISH ESPANOL



Remise de décorations  
aux sportifs olympiques  
et paralympiques



ÉCRIRE  
AU PRÉSIDENT



RECHERCHE

Sommaire Europe-Asie



Visite en Bosnie-Herzégovine





# Les Amis du Président de la République



Ce site est hébergé gracieusem  
(et amicalement) par :



« Ça m'en touche une sans faire bouffer l'autre... »

LE PRÉSIDENT



JACQUES CHIRAC :  
UNE VISION POLITIQUE



LA FRANCE  
DANS LE MONDE



LA BIBLIOTHÈQUE  
NATIONALE



QUOI DE NEUF ?



Meilleurs voeux !

ÉCRIVEZ-NOUS

**ANNEXE B.**

**Les traces sur Internet.**



- Anonyme sur internet ? Pas si sûr...
- Démonstration
- Comment ça marche ?
- Les enjeux





## Anonyme sur internet ? Pas si sûr...



Se connecter à Internet est devenu, pour la plupart des internautes, un acte quotidien. En quelques clics, la connexion est établie et en quelques autres, vous lancez votre logiciel préféré pour aller visiter tel ou tel site web. Peut-être téléchargerez-vous des programmes ou des fichiers, peut-être irez-vous lire quelques messages dans les "newsgroups" sur les sujets qui vous intéressent, sans doute consulterez-vous votre messagerie. Peut-être même discuterez-vous en temps réel avec des personnes situées à l'autre bout du monde...

Que vous alliez sur Internet dans le cadre de vos activités professionnelles ou depuis votre domicile, confortablement installé dans votre fauteuil, vos déplacements dans ce monde virtuel, si vaste et si riche, vous donnent sans doute une impression de liberté. Et le fait est que vous êtes libre d'aller n'importe où sur le réseau. Est-ce cette impression qui donne à de nombreux internautes le sentiment de naviguer en étant parfaitement anonyme ? L'absence d'intermédiaire visible ne renforcerait-elle pas le sentiment d'absence de surveillance ? La méconnaissance du fonctionnement des réseaux couplée à une surdose d'optimisme ne serait-elle pas plutôt à l'origine de cette conviction - fautive - que les connexions ne laissent pas de traces ? Le préjugé très répandu qu'Internet est complexe ne donnerait-il pas l'assurance, hâtive, que si traces il y a, les moyens de les exploiter sont disproportionnés au regard de l'intérêt qu'on aurait à le faire ?

La réalité est autre.

Non, l'anonymat n'est pas la règle sur Internet et l'absence de traces l'est encore moins. Oui, il est possible d'être sinon espionné, du moins surveillé, peut-être pas étroitement, mais suffisamment pour qu'un marché des outils de surveillance existe et que cette surveillance puisse être le fait d'acteurs de nature très diverses...

Attention, il ne s'agit pas d'affirmer que si l'anonymat n'est pas la règle, la surveillance le serait. Restons dans la réalité. Et si nous cessions un instant de qualifier Internet de "virtuel" et autre "cyber", pour le considérer sous son angle bien réel, informatique et technique, nous constaterions qu'en matière d'anonymat, Internet fonctionne exactement comme tout autre lieu du monde : l'anonymat demande des efforts, il est rarement absolu et garanti. La surveillance nécessite également des moyens, parfois importants; elle n'est pas infaillible, mais elle est toujours possible.

Sur cette question aux contours plutôt flous pour la plupart des internautes, le meilleur moyen d'être clair consiste à montrer directement aux internautes connectés au site de la CNIL ce que nous sommes en mesure de collecter comme traces de leur passage.

Mieux, nous avons souhaité expliquer de la façon la plus simple possible comment nous avons procédé techniquement, en soulignant les difficultés de l'exercice, et les

enjeux des techniques utilisées.

Ce que le site de la CNIL permet de faire, avec des moyens techniques limités, peut être fait par tous les sites auxquels vous vous connectez habituellement.

Cette démonstration constitue une manière de dévoilement de ce qui se fait, parfois, à votre insu.

La partie "**Démonstration**" exploite cinq techniques élémentaires qui permettent d'obtenir des informations sur les internautes. Jugez-vous mêmes ! Certaines techniques peuvent ne pas fonctionner dans votre cas, selon l'ordinateur, le système d'exploitation, le navigateur ou encore la configuration réseau que vous utilisez pour vous connecter. Dans ce cas, nous vous indiquerons quelques-unes des causes qui peuvent être à l'origine d'un échec.

La rubrique "**Comment ça marche ?**" vous apprendra comment nous avons procédé. Vous découvrirez qu'aucune des techniques mises en oeuvre dans la démonstration n'est particulièrement lourde ni ne nécessite d'investissements colossaux. Bien au contraire.

#### "Les enjeux" :

- **Constater** qu'aucune de ces techniques n'a été conçue à l'origine pour nuire aux internautes ou porter atteinte à leur vie privée mais qu'elles ont chacune leur justification et leur utilité;
- **Indiquer** que chaque technique employée a ses limites;  
Evoquer éventuellement d'autres modalités de traçage qui peuvent également être utilisées sur Internet;
- **Rappeler** l'attitude qu'il paraît important d'adopter lorsque l'on fait d'internet un outil de travail, de divertissement ou d'information quotidien.

L'expérience montre que l'on est beaucoup plus conscient d'un risque si l'on en comprend les ressorts, s'il nous a été non seulement affirmé mais également expliqué.

Sur les "autoroutes de l'information", l'enjeu, c'est la protection de votre vie privée. Le meilleur moyen de ne pas avoir d'accident de l'inforoute, c'est de connaître les risques et d'agir en conséquence. En un mot, d'être responsable. Sur Internet comme ailleurs.

Nous espérons que ce site vous y aidera.

---

[Glossaire](#) | [Anonyme](#) | [Démonstration](#) | [Comment ça marche](#) | [Les enjeux](#)



## Démonstration

### Votre configuration

Saviez vous que l'**adresse IP** de votre machine est : 194.196.254.10  
et que votre **adresse DNS** est : ns.tfl.fr

Nous pouvons voir que votre ordinateur utilise : Microsoft Windows NT  
comme **système d'exploitation**.  
**Votre navigateur** a comme nom de code : Mozilla/2.0 (compatible; MSIE 3.01;  
Windows NT)  
mais c'est en fait : Microsoft Internet Explorer 3.01 .

**Pour accéder à cette page, vous avez cliqué sur un lien situé à l'adresse suivante**  
:  
<http://www.cnil.fr/traces/demonst/demo.htm>

Cette page montre comment le serveur peut exploiter les variables d'environnement  
de votre navigateur.

Cette démonstration n'a peut être pas fonctionné. Dans ce cas, **découvrez pourquoi**.

### Comment ça marche

**Pour obtenir des informations sur votre configuration et l'URL précédemment visitée, nous avons utilisé les variables d'environnement qui sont définies dans votre navigateur et que ce dernier envoie systématiquement au serveur.**

#### *Quelques explications simples ...*

- Comparaison n'est pas raison
- HTTP, Javascript et Cie

#### *Plus techniquement...*

- Adresse IP, adresse DNS et signature du navigateur
- Lien précédemment suivi

#### 1 . Comparaison n'est pas raison

Si l'on tentait de schématiser l'ensemble des règles et procédures à suivre pour établir une communication téléphonique, on pourrait aisément distinguer deux niveaux de ce qu'il convient d'appeler des protocoles. Le premier niveau, le plus bas, est indispensable à l'établissement

physique de la communication, c'est le niveau le plus technique qui permet, entre autres, de composer le numéro d'un correspondant, de générer une sonnerie sur son poste, d'établir la communication, de maintenir le transfert de la voix dans les deux sens et en même temps au travers de la ligne et enfin de terminer la communication. Le second niveau, supérieur au précédent car plus accessible aux locuteurs, n'est pas indispensable à la communication technique proprement dite mais à la communication humaine : il part d'un accord sur la langue utilisée par les deux locuteurs en passant par les conventionnels "Allô ?", "Qui est à l'appareil ?", etc.

Sur Internet, on pourrait faire la même observation. Pour que les informations soient correctement transférées de votre ordinateur au serveur, un protocole est nécessaire afin que les différents appareils situés entre vous et lui soient à même de les transporter. Il s'agit du protocole TCP/IP. On représente généralement l'architecture d'un protocole en couches. Tout en bas, la couche matérielle correspond (schématiquement) aux câbles et aux cartes utilisés (Ethernet par exemple), puis la couche réseau gère la circulation des paquets à travers le réseau (IP), la couche transport gère le flux de données entre deux machines (TCP), enfin, la couche supérieure, la couche applicative, gère les détails de communication d'une application particulière entre le serveur et le client (HTTP, par exemple, si vous êtes "sur le web", ou bien FTP, pour le transfert de fichiers, ou encore NNTP pour les newsgroups). La couche supérieure correspond au dialogue établi entre les deux applications client/serveur, comme par exemple votre navigateur et le serveur web.

## 2 . HTTP, Javascript et Cie

Au niveau HTTP, donc, chacune de vos requêtes contient un certain nombre d'informations, à commencer par ce que vous avez à demander : l'adresse d'une page web généralement. Mais elle contient également de nombreuses informations sur l'environnement de votre ordinateur. Ces informations sont systématiquement transmises dans chaque paquet qui part de votre ordinateur vers le serveur. Lorsque le paquet arrive sur le serveur, un processus système est créé sur la machine, processus qui intègre ces informations sous forme de variables d'environnement et exécute la requête demandée.

Autant d'informations que le serveur peut ajouter à celles dont il pourrait disposer également par ailleurs.

Concrètement, voici les variables d'environnement et leur contenu tel que nous l'avons reçu de votre navigateur :

```
REMOTE_HOST      = ns.tf1.fr
REMOTE_ADDR      = 194.196.254.10
HTTP_USER_AGENT  = Mozilla/2.0 (compatible; MSIE 3.01; Windows NT)
HTTP_REFERER     = http://www.cnil.fr/traces/demonst/demo.htm
```

Un script sur le serveur les a analysées pour vous les présenter plus clairement :

```
Votre adresse DNS      : ns.tf1.fr
Votre adresse IP       : 194.196.254.10
Votre système d'exploitation : Microsoft Windows NT
Votre navigateur       : Microsoft Internet Explorer 3.01
Votre page précédente  : http://www.cnil.fr/traces/demonst/demo.htm
```

## 3 . Adresse IP, adresse DNS et signature du navigateur

Un script CGI analyse les variables d'environnement suivantes :

**REMOTE\_HOST, REMOTE\_ADDR et HTTP\_USER\_AGENT**

**REMOTE\_HOST** et **REMOTE\_ADDR** retournent au serveur l'adresse DNS et l'adresse IP de votre machine.

Si l'adresse DNS n'y figure pas, c'est que votre machine n'a pas été enregistrée dans le serveur de DNS.

**HTTP\_USER\_AGENT** est la signature du navigateur client. A partir de celle-ci, nous déterminons quel est le système d'exploitation, quelles sont les caractéristiques du navigateur (marque, modèle et, éventuellement, numéro de version) et la version linguistique du navigateur. Pour obtenir ces informations, nous utilisons une table de correspondance entre les éléments de la signature du navigateur et les signatures connues (par exemple, nous savons que la chaîne de caractère "WinNT" est contenue dans la signature d'un navigateur Netscape tournant sous Microsoft Windows NT ou que "Windows 95" est contenue dans la signature d'un navigateur Internet Explorer tournant sous Microsoft Windows 95).

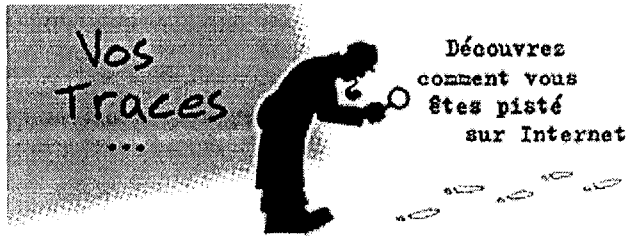
Il est également possible pour le serveur de récupérer ces variables à l'aide d'un Javascript. Javascript est un langage de script dont les instructions s'intègrent sous forme textuelle à l'intérieure des pages HTML et que le navigateur exécute lorsqu'il charge la page. **Attention, ne confondez pas Javascript et applet Java.**

#### 4 . Lien précédemment suivi

Un script CGI est chargé d'analyser la variable d'environnement **HTTP\_REFERER**, et d'en extraire les informations suivantes sur la dernière page vue par le navigateur client : protocole utilisé, adresse DNS ou IP du serveur, chemin d'accès à la ressource, et ressource demandée (page, image, cgi ...).

---

### Les enjeux de cette technique



## Démonstration

### Un peu de météo ...

Bonjour ! C'est la 2<sup>ème</sup> fois que vous consultez cette rubrique.

La dernière fois que vous êtes venu, c'était le 21 janvier 98 à 12:32:54



La dernière fois que vous lui avez indiqué quel temps il faisait chez vous, notre détective en a déduit sa tenue du jour.

Vous déclariez : C'est tout blanc

Mais le climat a peut être changé depuis...

Notre détective a de la mémoire. Indiquez-lui le temps qu'il fait chez vous, il s'en souviendra et s'habillera en conséquence la prochaine fois que vous reviendrez sur cette page.

Quel temps fait-il chez vous ?

Ajoutez une phrase de commentaire. Ex : "Noël au balcon, Pâques au tison"

Cette page montre comment un serveur peut exploiter les "cookies".

Si cette démonstration n'a pas fonctionné, [voici peut-être pourquoi.](#)

## Comment ça marche

Pour compter vos passages, nous rappeler de la date de votre dernière visite et pratiquer la météo avec notre détective, nous avons utilisé des cookies.

### *Quelques explications simples...*

- Qu'est-ce qu'un cookie ?
- Un peu plus de détails ?
- Cookies et navigateurs

### *Plus techniquement...*

- L'écriture des cookies
- La lecture et l'affichage des cookies par un CGI
- Le répertoire qui contient les cookies

## 1 . Qu'est-ce qu'un cookie ?

Pour aller à l'essentiel, on peut dire qu'un cookie est un enregistrement d'informations par le serveur dans un fichier texte situé sur l'ordinateur client (le vôtre), informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement. La technique des cookies repose sur le protocole HTTP, c'est-à-dire le protocole du web. Il ne faut donc pas voir de cookies partout : seul un serveur web peut en envoyer.

Plus précisément, un cookie se compose d'un ensemble de variables (ou de champs) que le client et le serveur s'échangent lors de transactions HTTP, lesquelles variables sont tout simplement stockées sur la machine cliente dans un simple fichier texte. Un cookie est obligatoirement rattaché à un nom de domaine et un ensemble d'URL de telle sorte que seule une requête provenant du même serveur pourra y accéder.

Par exemple, grâce à un programme CGI, le serveur a la possibilité de mettre à jour ou d'effacer un cookie. Mais pour cela, il doit spécifier tous les attributs du cookie, par conséquent seul le serveur qui a créé un cookie peut le modifier ou le supprimer.

Un même "client" peut stocker un maximum de 300 cookies, dont 20 maximum pour un même serveur, chaque cookie pouvant atteindre jusqu'à 4000 octets (env. 4 Ko).

Le paragraphe suivant donne quelques précisions sur le fonctionnement des cookies dont vous pouvez éventuellement vous dispenser si les détails techniques vous rebutent. Sachez simplement que leur fonctionnement est extrêmement simple : le fichier stocké sur votre PC est un fichier texte écrit et lu par votre navigateur. Vous pouvez le lire, le détruire, le copier, le modifier à la main si vous le souhaitez. Il ne peut pas contenir de virus ni être exécuté, il n'est pas actif.

## 2 . Un peu plus de détails ?

Un cookie est envoyé par le serveur par insertion d'une directive dans l'en-tête du message de réponse HTTP dont la syntaxe est la suivante :

Set-Cookie : Nom=valeur; expires=date; path=chemin; domain=nom\_domain; secure

Grâce à l'information Nom=valeur, (ex: "datenaissance=01011964". C'est vous qui avez tapé "01011964" dans un formulaire) chaque cookie porte un nom ("datenaissance", dans notre exemple) auquel correspond une valeur définie par le serveur sous forme d'une chaîne de caractères et qui, précisément, sera renvoyée au serveur lors des connexions suivantes ("01011964"). Le champ Expires indique la date d'expiration du cookie. Une fois cette date dépassée, le logiciel client n'insérera plus le cookie lors des transactions HTTP. Le serveur peut

donc effacer un cookie en substituant à sa date initiale d'effacement une date antérieure à la date du jour. Le champ path indique quelles pages peuvent accéder au cookie à partir du serveur spécifié dans domain=nom\_domain, où l'on retrouve le nom de domaine du serveur qui a posé le cookie (www.cnil.fr, par exemple). Par défaut, ces deux dernières valeurs correspondent à la page et au domaine qui ont initialisé le cookie. Enfin, secure est utilisé pour n'assurer l'application du cookie que lorsque la connexion client-serveur est sécurisée, par le protocole HTTPS par exemple. En l'absence de ce champ, le cookie est transmis quel que soit le protocole utilisé.

**Par exemple, lors de la démonstration, vous nous avez envoyé les informations suivantes :**

```
temps="Neige"  
phrase="C'est tout blanc"
```

**Nous vous avons renvoyé les cookies suivants :**

```
Set-Cookie: Temps=Neige; expires=Wednesday, 21-Mar-98 12:33:25 GMT;  
domain=www.cnil.fr; path=/  
Set-Cookie: Phrase=C'est tout blanc; expires=Wednesday, 21-Mar-98 12:33:25 GMT;  
domain=www.cnil.fr; path=/;
```

Lorsque le client accède à une URL, il recherche parmi ses cookies celui ou ceux qui correspondent à l'URL. Il insère ensuite dans la requête HTTP une ligne contenant tous les couples "nom=valeur" correspondants. Les cookies posés par un serveur sont donc systématiquement envoyés à ce serveur sans qu'il ait besoin de les réclamer.

Un cookie peut être posé et lu grâce à un programme CGI exécuté sur le serveur ou par un javascript intégré dans une page HTML (attention : ne confondez pas javascript et applet Java).

### 3 . Cookies et navigateurs

Les principaux navigateurs du marché reconnaissent les cookies mais les navigateurs plus anciens ou moins performants les ignorent. S'agissant des produits de Netscape et de Microsoft, leur méthode de stockage des cookies est légèrement différente. Là où le Navigateur enregistre tous les cookies dans un seul fichier, l'Explorateur crée un fichier cookie par serveur qui contient tous les cookies de ce serveur, lequel fichier est situé dans un répertoire cookies. La présentation interne du fichier est également différente mais on retrouve toutes les informations et il s'agit toujours d'un simple fichier texte.

A vous de vérifier les cookies envoyés par la CNIL.

**Attention !** : Les cookies ne sont sauvegardés sur votre disque dur que lorsque vous quittez votre navigateur.

### 4 . L'écriture des cookies

Nous utilisons deux scripts CGI : un CGI pour collecter les informations (que l'utilisateur aurait éventuellement saisies lors d'une précédente visite), et un CGI chargé de mettre à jour les cookies lorsque l'utilisateur a fini de remplir le formulaire.

- Collecte des informations : le premier script se charge de la collecte de deux cookies ("Temps" et "Phrase") et affiche leurs valeurs dans la page.
- Mise à jour du cookie : le deuxième script CGI effectue les opérations suivantes : il récupère les informations saisies par l'utilisateur grâce au formulaire, puis insère dans l'en-tête d'un message HTTP les cookies suivants :  
Set-Cookie: Temps=Neige; expires=Wednesday, 21-Mar-98 12:33:25 GMT;  
domain=www.cnil.fr; path=/  
Set-Cookie: Phrase=C'est tout blanc; expires=Wednesday, 21-Mar-98 12:33:25 GMT;

domain=www.cnil.fr; path=/;

Le contenu du message HTTP renvoyé est un indicateur de retour sur cette page.

## 5 . La lecture et l'affichage des cookies par un CGI

Bonjour ! C'est la 2<sup>ième</sup> fois que vous consultez cette rubrique.

La dernière fois que vous êtes venu, c'était le 21 janvier 98 à 12:32:54

Nous utilisons deux scripts CGI : un premier script est chargé de collecter les cookies concernant le nombre de visites et la date de dernière visite. Un second CGI va se charger de mettre à jour les cookies.

- Collecte des cookies : le script CGI récupère les cookies que lui envoie le navigateur client, puis extrait de ces derniers ceux qui correspondent aux nombres de visites de l'utilisateur, et la date de dernière visite. La dernière opération consiste à afficher
  - 1) la valeur du cookie +1 (la visite en cours),
  - 2) la valeur du cookie contenant la date de dernière visite.
- Mise à jour du cookie : le deuxième script CGI effectue les opérations suivantes : il formate la date courante pour le cookie `Derniere_visite=d` et collecte, analyse et incrémente le cookie `Nombre_visite=n`.  
Ensuite, il renvoie au client les nouvelles valeurs des cookies sous la forme `Nombre_visite=n` et `Derniere_visite=d` dans l'en-tête du message HTTP. Le contenu du message HTTP renvoyé est une image d'un pixel transparent (donc invisible par l'utilisateur).

## 6 . Le répertoire qui contient les cookies

La sauvegarde des cookies est organisée différemment selon le type de navigateur que vous utilisez. Si nous considérons les deux principaux navigateurs existants :

- **Microsoft Internet Explorer** gère un répertoire "Cookies" dans lequel se trouvent des fichiers au format texte. Les cookies sont enregistrés dans des fichiers ayant comme nom le DNS du site qui vous les a envoyés.  
L'emplacement du répertoire "cookies" dépend de votre système d'exploitation.

Système d'exploitation	Répertoire
Windows 95	C:\Windows\Cookies\
Windows NT	C:\WinNt\Cookies\
Unix	/home/.microsoft/Cookies home : Chemin d'accès à votre répertoire personnel.
Macintosh	folder:Preferences Panel:Cookies folder : Dossier dans lequel est installé votre navigateur.

- **Netscape Navigator/Communicator** enregistre les cookies au sein d'un seul fichier : "cookies.txt". Ce fichier au format texte contient l'ensemble des cookies, quel que soit le site vous les a envoyés. L'emplacement de ce répertoire dépend du répertoire dans lequel vous avez installé votre navigateur.

Navigateur	Système d'exploitation	Répertoire
Navigator	Windows 95	C:\Program Files\Netscape\Navigator\Cookies.txt
Navigator	Windows NT	C:\Program Files\Netscape\Navigator\Users\name\Cookies.txt name : "Default" ou nom d'utilisateur sous lequel

		vous vous connectez.
Communicator	Windows 95 Windows NT	C:\Program Files\Netscape\Communicator\Users\ <i>name</i> \Cookies.txt <i>name</i> : "Default" ou nom d'utilisateur sous lequel vous vous connectez.
Navigator Communicator	Unix	<i>home</i> /.netscape/cookies <i>home</i> : Chemin d'accès à votre répertoire personnel.
Navigator Communicator	Macintosh	<i>folder</i> :MagicCookie <i>folder</i> : Dossier dans lequel est installé votre navigateur.

---

### Les enjeux de cette technique