



● —||— ● —||— ● **ÉCRAN / ENNEMI**

**TERRORISMES ET GUERRES DE L'INFORMATION**

**FRANÇOIS-BERNARD HUYGUE** ● —||— ●

[www.00h00.com](http://www.00h00.com)

l'Édition en ligne

Écran / Ennemi

François-Bernard Huyghe

## Écran / Ennemi

Terrorismes et guerres de l'information

Éditions 00h00  
Z É R O H E U R E  
[www.00h00.com](http://www.00h00.com)

*COLLECTION STRATÉGIE*  
*DIRIGÉE PAR PIERRE FAYARD*

Retrouvez ce livre et l'ensemble des éléments proposés autour,  
notamment les liens recommandés, ainsi que les commentaires des  
lecteurs sur le site des Éditions 00h00.com :

<http://www.00h00.com>

ISBN : 2-7454-0587-X

© Éditions 00h00, Paris, 2002

© Conception graphique : Isabelle Roulet

Ce texte publié par les Éditions 00h00 est protégé par les lois et traités internationaux relatifs aux droits d'auteur. Son impression sur papier est strictement réservée à l'acquéreur et limitée à son usage personnel. Toute autre reproduction ou copie, par quelque procédé que ce soit, constituerait une contrefaçon et serait passible des sanctions prévues par les textes susvisés et notamment la loi du 11 mars 1957 sur la protection des droits d'auteur.

Éditions 00h00.com  
24, rue Feydeau 75002 Paris France  
Tél. : 33 (0)1 42 36 61 61  
Fax : 33 (0)1 42 36 83 34  
[contact@00h00.com](mailto:contact@00h00.com)

## À propos de l'œuvre

Sur l'écran des télévisions ou des ordinateurs, éclatent des conflits inédits — terrorisme-spectacle, guerres séduction sans dégât cathodique collatéral, mais aussi des formes nouvelles de désinformation, de mésinformation, d'infoguerre, économique, civile, culturelle...

Notre société se réclame sans cesse de l'information et la communication, mais les stratégies de dominance par l'information ou de communication par la terreur y prolifèrent. Les réseaux clandestins et la Toile, les fatwas et l'utopie d'un *soft power* américain, des souris et des bombes, tels risquent d'être les symboles du monde de demain.

Ce livre nous aide à comprendre la logique des affrontements à venir. Une logique où les moyens de transmission se transforment en moyens de destruction et de perturbation.



## *À propos de l'auteur*

Docteur d'État en Sciences Politiques et habilité à diriger des recherches en Sciences de l'Information et de la Communication, ex-réalisateur de télévision, puis fonctionnaire international, François-Bernard Huyghe enseigne notamment au Celsa Paris IV ainsi qu'à l'École de Guerre économique.

Ses recherches actuelles portent sur les rapports entre information, conflit et technologie, avec la publication de *L'Information, c'est la guerre* (Panoramiques), et de *L'Ennemi à l'ère numérique, Chaos, Information, Domination* (P.U.F.).

Il a fondé l'Observatoire d'infostratégie.

François-Bernard HUYGHE  
infostrategie@paris.com





## Préface

« Ceci n'est pas transparent ! »

Vingt heures, après l'énoncé des titres, les images ! Une tour s'effondre, des visages hagards, des sirènes de pompiers, la voie off du correspondant à New York... Dans un tableau célèbre représentant une pipe, René Magritte avait écrit « ceci n'est pas une pipe ». Les images de l'impact des avions de ligne sur les Twins de Manhattan ne sont pas l'événement, dramatique, en lui-même mais un message ou un « massage » comme aurait dit Mc Luhan. Etrange massage de l'opinion publique à travers le petit écran, dont la dimension stratégique traverse les frontières et se rit des boucliers anti-missiles et des légitimités territoriales.

Longtemps, la stratégie se jouait et se payait en espace. A la fois protection et enjeu, il en représentait aussi le principal ralentisseur que l'art des communications s'efforçait de réduire. De la voie romaine au chemin de fer, de la galère à la marine à vapeur puis dans les airs et l'espace, l'effort de réduction de la durée des transports reflète la course livrée par le temps à l'espace en matière de stratégie. Avec les technologies actuelles et plus particulièrement avec les réseaux électroniques et les satellites, la prééminence de la première de ces dimensions semble à présent assurée. La distance ménageait la sécurité et la frontière départageait entre *le même* et *l'autre*.

L'espace physique, garantie du secret, donnait le temps du filtrage, du décodage, de la sélectivité voire de la manipulation. Avant que la vérité des faits ne se diffuse, un belligérant pouvait avoir créé l'irréversible et on pardonne plus aisément au vainqueur qu'au vaincu ! Dans l'espace réticulé, s'affirme désormais le règne d'une simultanéité sans borne. Tout point peut être connecté, articulé et mobilisé en quelques secondes. Les marges de liberté d'action se règlent sur des rythmiques accélérées, l'économie des moyens compose avec la dimension virtuelle et les concentrations ont la planète pour échelle. Comment penser ces nouvelles conditions de l'interaction des volontés, et notamment sur le terrain des médias ?

C'est à cette tâche de stratéguiste que François-Bernard Huyghe contribue remarquablement dans ce troisième ouvrage d'une collection qui se propose de publier des textes rendant compte des relations entre information, communication et stratégie. Le panorama qu'il balaye est ambitieux. La documentation est riche. L'abondance et la précision des liens hypertextes de la version numérique de l'ouvrage en fait un véritable outils pour l'étudiant, le chercheur ou le professionnel désireux de poursuivre par lui-même. Par respect pour son lecteur, François-Bernard Huyghe ne livre pas de prêt-à-penser mais donne à réfléchir en faisant œuvre d'intelligence. Il décrypte la tectonique de l'iceberg dont l'écran n'est que la face visible et il invite à comprendre en élargissant le champ de la vision et en opérant des coups de projecteurs sur des aspects mal connus ou ignorés des voies et moyens de la stratégie. Tel Alice, le lecteur est convié à pénétrer, par delà l'écran, dans le Pays des Nouvelles Violences Symboliques et Techniques pour en découvrir les logiques sous-jacentes et les modes de fonctionnement. C'est en ce sens une excellente stimulation.

Bonne lecture à tous !

## Introduction

Première page des journaux, un jour au hasard<sup>1</sup> : des Français assassinés au Pakistan par des islamistes, la Marseillaise sifflée par des *supporters* corses. Le lecteur, surtout s'il ne se sent ni très « croisé », ni très « jacobin », a pu s'indigner de voir ses compatriotes massacrés ou son hymne national conspué par des gens à qui il n'a rien fait. Le point de départ de ce livre est différent, plus distancié : de tels faits — et ils sont fréquents — seront envisagés comme symptômes d'un bouleversement plus vaste, touchant à toutes sortes de conflits<sup>2</sup> à venir.

D'une part, nous ne nous regardons comme les adversaires de personne, et surtout pas de nos voisins contre qui nous sommes si souvent battus. Faute de rival à l'Est, nos armées n'interviennent plus qu'à titre judiciaire et humanitaire, pour sauver des vies et arrêter des guerres\*, avec mandat international. *Exit* la guerre, *exit* l'hostilité ?

Mais, d'autres, « eux », nous considèrent comme leurs ennemis\* : ils nous combattent non pour ce que nous avons fait comme individus, mais pour ce à quoi nous appartenons<sup>3</sup>.

Or cette hostilité ne se manifeste pas de façon « classique », mais par ce qu'il faut bien appeler des « Nouvelles Violences Symboliques et Techniques ».

1. Week-end du 11 et 12 mai 2002. Si nous avions choisi le week-end suivant, cela aurait donné : alerte générale aux Etats-Unis, où des informations, basées sur l'interception de communications au sein du réseau al Quaida, font craindre une nouvelle vague d'attentats et nouvelle cassette de Ben Laden.

2. \* Les mots suivis d'un astérisque sont expliqués dans le glossaire.

3. Cette question a fait l'objet de notre précédent ouvrage, *L'Ennemi à l'ère numérique Chaos, Information, Domination*, aux P.U.F., en 2001.

*Nouvelles*, pour autant que nos catégories anciennes en rendent mal compte : guerre et paix, politique et économique, communication\* et conflit, technique\* et idéologique, national et international...

*Violences* au sens où, même si elles ne détruisent pas toujours des corps, elles visent à une contrainte ou un dommage.

*Symboliques\**, par ce qu'elles impliquent toujours un élément de croyance partagée, et comme moteur et comme cible<sup>1</sup>.

*Techniques*, puisqu'elles font intervenir systématiquement des moyens modernes de destruction et de transmission.

Ces moyens, nous les percevons à travers ce qui est l'emblème même de notre époque : *l'écran*. Dans les deux exemples précités, il joue un rôle crucial dans la mesure où il reproduit les événements et les amplifie, mais aussi parce que ces événements, bombes ou *lazzi*, ont été mis en scène, organisés pour être vus et connus, bref formatés pour l'écran.

L'écran est à entendre ici dans des sens bien différents, depuis la cohabitation d'écrans cathodiques, la télévision, média de masse par excellence, et d'écrans numériques, ouvrant sur les mondes virtuels\*. Ce qui peut se décliner ainsi :

- l'écran *reflète*, bien ou mal, la réalité.
- l'écran est le lieu de *projection*, y compris de celle des fantasmes et des pulsions agressives.
- l'écran *fait écran* : il nous *sépare* aussi d'une vie, voire d'une mort, que nous éprouvons à distance.
- l'écran vaut *carte* : c'est sur les écrans que s'exercent *surveillance, modélisation* et *contrôle\**.
- l'écran vaut *territoire* puisqu'il s'agit aussi de le *conquérir*

1. Le lecteur qui s'indignerait que l'on considère comme « symbolique » de faire sauter un autobus, verra au chapitre suivant, en quoi le terrorisme est toujours symbolique : il veut envoyer un message et s'en prend aux représentations d'un ordre qu'il déteste, fut-ce par l'intermédiaire d'une victime innocente. Ce point de vue n'implique ni insensibilité morale, ni amalgame entre des sifflets et des bombes.

## Introduction

— l'écran fait *interface* : il sert à agir à distance, mais aussi à partager. Il est entre *monde des choses* et *monde des représentations*, technique, imaginaire et cultures.

Nous avons tendance à considérer l'écran soit comme l'emblème de la modernité — et à penser en termes d'impact des technologies\* — soit comme une lucarne déformante. Dans le second cas, nous lui reprochons souvent une perte, un défaut de transparence ou de vraisemblance : sa restitution de la réalité serait faussée. Ainsi, il n'est actuellement question que de la façon dont les médias\* présentent l'insécurité. Par ses excès, elle nourrirait les fantasmes ; par incitation, elle provoquerait une contagion de la violence. Or, quel que soit l'intérêt politique ou pratique de tels débats, ce n'est qu'un des aspects du problème.

À force d'insister sur ce que ces technologies nous font, nous oublions ce que nous nous faisons par leur intermédiaire et ce n'est pas toujours tendre. Nous négligeons leur dimension stratégique : l'usage délibéré dans les affrontements de l'information, sous toutes ses formes, d'un algorithme\* à un communiqué de presse, d'une photo à un virus\*.

De la stratégie\*, il a été dit que c'était la dialectique des intelligences, dirigeant des forces pour résoudre leurs conflits ; le mot évoque d'abord la guerre. Or les nouvelles violences n'emploient pas seulement des forces, mais aussi messages et savoirs dangereux. Les machines à communiquer valent des machines de guerre : l'expansion des technologies douces s'accompagne de conflits durs où l'information sera à la fois arme, enjeu et cible.

Voici que resurgissent des guerres archaïques, tribales, ethniques, de ces guerres où l'on sait pourquoi l'on tue, puisqu'on tue son voisin. Guerres de riches par écrans interposés : guerres glacées et sans passion, guerres technologiques à alibi moral, de punition ou d'affirmation de puissance, mais aussi guerres imprécises où l'on peine à distinguer hostilité, dissuasion,

dominance, prévention, répression, violence faite aux choses, aux idées et aux gens<sup>1</sup>. Guerres de pauvres à hauteur d'homme : guerres brûlantes, morts exhibés, passions surchauffées, haines identitaires, outils rustiques, foi ardente. Ni les premières, ni les secondes ne s'expliquent simplement par les aberrations de la nature humaine, ni par les lois de la géopolitique.

Les textes qui suivent explorent les bizarres interactions entre violence et communication, information\* et conflit, modes de destruction et modes de transmission. Pour cela, il faut déborder du domaine des violences armées et de leur représentation médiatique pour aborder des conflits économiques, techniques, culturels. Même s'ils ne sont pas de « vraies guerres », ils impliquent déjà bien plus que de la concurrence ou de la rivalité.

Une première partie « Quand l'ennemi *occupe* l'écran. La maîtrise du visible » examine deux formes des nouvelles violences symboliques et techniques. La première, le terrorisme\* qui retourne les écrans de son adversaire contre lui et les emploie pour relayer son propre message. La seconde violence, celle qui se voit à l'écran, détermine comment nous nous représentons l'ennemi, la victime, et autres figures de l'antagonisme.

Une seconde partie « Quand l'écran *occulte* l'ennemi. La maîtrise dans l'invisible » étudie la situation inverse : celle où les conflits politiques, économiques, idéologiques se déroulent *derrière* l'écran. Les trois thèmes du secret\*, de la désinformation\* et de la « guerre de l'information »\* illustreront ce paradoxe : conflictualité et invisibilité vont de pair.

Le tout ne forme qu'un seul *leitmotiv* : il faut penser simultanément le stratégique, le symbolique, le technique. La médio-

1. Elle se redouble d'une guerre sémantique. Ce n'est pas un mince enjeu, on le verra, que de décider si on doit parler de « guerre de l'information », de « guerre économique » ou de « guerre de la connaissance » voire de « guerre au terrorisme ».

## Introduction

logie\*, dont se réclame l'auteur, s'y efforce<sup>1</sup>. Une polémologie\* de l'information, encore à inventer, pourrait y contribuer. Le néologisme d'infostratégie<sup>2</sup> se répand. Mais quel que soit le nom de la chose ou de la discipline, la question de l'hostilité ne peut plus se penser dans les catégories anciennes.

1. Voir le site <http://www.mediologie.com>.

2. Voir le glossaire en fin de livre pour l'explication de cette terminologie. Sur l'infostratégie, voir aussi (<http://www.strategic-road.com/intellig/infostrategie/infostra.htm>).





## Première partie

### Quand l'ennemi occupe l'écran La maîtrise du visible

Le terrorisme est, par essence, spectaculaire. Le village global lui a offert une scène à sa mesure<sup>1</sup>. Il peut tout à la fois se justifier par des discours, proclamer ses objectifs et ses revendications, s'organiser, notamment sous la forme du réseau et infliger un dommage en actes et en symboles à des sociétés technologiquement vulnérables.

Dans le même temps, une des plus anciennes expériences humaines — voir mourir et voir la guerre — devient un enjeu politique et stratégique majeur. Quand la représentation de la violence est gérée avec autant d'attention que la violence même, le conflit implique le contrôle des flux d'images. Généraux et terroristes en ont un même souci. Les premiers pour gérer des guerres sans cadavres apparents. Les seconds pour produire un maximum d'images de cadavres. Avec, en arrière-plan, une longue histoire technique et culturelle, du daguerrotypage au numérique\* : la rencontre des vecteurs de destruction et de reproduction.

1. Voir le n°13 des *Cahiers de médiologie* (<http://www.mediologie.com>) *La Scène terroriste*, dirigé par Catherine Bertho-Lavenir et François-Bernard Huyghe, Gallimard 2002.



# Chapitre I

## Terrorisme : stratégie d'irruption

Il faut s'habituer à cette idée que nous, les Occidentaux, ne faisons plus la guerre qu'à la seule Terreur. Nous ne tuons des gens que pour éviter des massacres pires encore. Que faisons-nous d'autre au Kosovo, en Bosnie, en Somalie que de combattre « l'intolérable » : purification ethnique, déportations et crimes de Terreur ? Qu'a fait Bush en Afghanistan sinon « *War against Terror* », comme le sous-titrait C.N.N. ? Qu'a fait Sharon sinon une « guerre totale au terrorisme » ? Que feront demain les États-Unis face à l'Irak ou autre pivot de l'axe du mal ? Et à quoi servira l'OTAN après sa réconciliation avec la Russie, sinon à se tourner vers les « vrais ennemis » du genre humain : les terroristes<sup>1</sup> ?

Ici, on voit cligner de l'œil ceux qui ne croient guère au discours du « plus jamais ça » : illusion, manipulation, idéologie\* ! Ils dénoncent la puissance de l'hyperpuissance derrière l'alibi du Droit. Les condamnations des États « voyous » et les réseaux\* terroristes émanent, rappellent-ils, de ceux qui ont

1. <http://www.nato.int>

encouragé ailleurs ou en d'autres temps des États ou des groupes tout aussi criminels<sup>1</sup>. Bref, la politique humanistico-pénale dissimulerait une politique des intérêts sous des bons sentiments. Peut-être !

Nul n'est assez naïf pour croire que nos guerres angéliques d'ingérence et de contrôle marquent le triomphe définitif de la « Morale ». Cela fournit une belle occasion de jouer aux jeux préférés des intellectuels : découvrir des gisements de pouvoir caché, se jeter des victimes au visage et se reprocher mutuellement de n'avoir pas autrefois dénoncé assez fort et avec assez d'équanimité des crimes politiques flagrants. Notamment lorsque Ben Laden était un « *freedom fighter* », ou que les USA toléreraient de plus effroyables terrorismes d'État pourvu qu'ils aillent dans le bon sens<sup>2</sup>.

La question n'est pas vraiment là. Elle est dans la rencontre des mots « guerre » et « terrorisme ». De la guerre, tout le monde a compris qu'elle n'a plus rien à voir avec le modèle dit *clausewitzien*<sup>3</sup> : États souverains luttant jusqu'à ce que l'un cède et que l'on signe une paix. Quant au terrorisme, il prend là une singulière pesanteur, d'autant qu'il est tout sauf facile à définir<sup>4</sup>. Mais renoncer au mot, sous prétexte qu'il se prête à des usages idéologiques, terrifiants, répressifs ou trompeurs, ne nous laisserait que des substituts comme « violence politique » ou « formes de lutte armée non conventionnelles » sans gagner

1. Exemple cité souvent : l'UCK, placée sur la liste des organisations terroristes établie par les États-Unis, en est retirée en 1999, lorsqu'elle se retrouve dans le bon camp durant la guerre du Kosovo.

2. Les dénonciations de Noam Chomsky en fournissent d'assez bons exemples voir <http://www.zmag.org/chomsky>.

3. Sur la critique des conceptions de Clausewitz, inapplicables aux modernes conflits dits « de faible intensité », voir Martin van Creveld, *Transformation de la guerre*, Éditions du Rocher 1998 (Free Press 1991 *The Transformation of War*).

4. Pour une anthologie de ces définitions voir : Schmid, Alex P., Jongman Albert J. *Political terrorism: a research guide to concepts, theories, data bases, and literature*. Amsterdam, Pays-Bas ; New Brunswick, NJ, USA : North-Holland Publishing ; Transaction Books, (*Centrum voor Onderzoek van Maatschappelijke Tegenstellingen*).

pour autant ni précision intellectuelle ni critères plus objectifs. La chose existe, le mot aussi, il faut faire avec.

## Terrorisme et violence de l'autre

### *Qu'est-ce que le terrorisme ?*

Faut-il le définir par ses effets moraux ? Il est censé répandre le sentiment de terreur, impressionner, créer un « climat de terreur » ? Sa caractéristique est-elle de troubler « gravement » l'ordre public comme le suggère notre code pénal<sup>1</sup> ?

Cet emploi illégitime de la violence politique s'opposerait-il à des usages légitimes, tels que guerre ou maintien de la paix publique ?

Et ses victimes innocentes ? C'est souvent le critère des définitions américaines qui rapprochent le terrorisme tuant des non-combattants du crime de guerre<sup>2</sup>. Par le choix de cibles prises au hasard ? D'où tout un débat sur ce qu'est une victime innocente, à une époque où toute guerre tue plus de civils que de militaires.

Les intentions de ses auteurs ? Elles ne seraient pas que criminelles — intérêt ou plaisir de détruire — mais idéologiques voire métaphysiques. Ainsi, le nihilisme proteste contre l'ordre du monde en général<sup>3</sup>.

1. Murielle Renar, *Les Infractions du terrorisme contemporain au regard du droit pénal*. Thèse de doctorat, Université du Panthéon Sorbonne, 1996, disponible sur le Web.

2. Sens dans lequel poussent aussi les instituts de recherche israéliens spécialisés dans le terrorisme : <http://www.ict.org.il>. Par ailleurs, il n'est pas inintéressant de noter que les États-Unis publient une liste d'États et de mouvements terroristes (dont l'U.C.K. a été retirée juste avant les opérations du Kosovo) mais aussi une liste d'États ne coopérant pas assez contre le terrorisme.

3. L'assimilation du terrorisme au nihilisme est notamment défendue par André Glucksman. *Dostoïevski à Manhattan*, Robert Laffont, 2002.

Le terrorisme n'est-il que la guerre, la guérilla ou la révolte du minoritaire, du faible ou du pauvre ? Il se distinguerait alors de la guerre — visant à la domination du territoire — ou de la révolution — visant à la conquête de l'État — par sa faible intensité<sup>1</sup>, son caractère accessoire ou provisoire ?

Est-ce une pratique « élitiste » ou minoritaire de la force destructrice : un maximum d'effet pour un minimum d'agents ? L'aveu d'un manque de légitimité<sup>2</sup> ou de partisans ?

« Terrorisme » est-il un jugement de valeur dénonçant la violence de *l'Autre*, comme « idéologie » disqualifie son idéal ?

Chercheurs et juristes (dont ceux de la SDN<sup>3</sup> et de l'ONU) se sont acharnés à concilier les éléments capables de caractériser le terrorisme<sup>4</sup> :

*organisationnels* : fait d'un groupe de spécialistes poursuivant des desseins historiques, le terrorisme s'apparente à la subver-

1. Quitte à choquer le lecteur, rappelons que, malgré quelques attentats exceptionnels qui ont fait des centaines, voire, comme à Manhattan, des milliers de morts, le terrorisme tue « peu » au regard des trente-deux conflits en cours aujourd'hui. Cela dit, il faut ajouter que le terrorisme tue de plus en plus (voir l'introduction au livre de Walter Laqueur, *The New Terrorism*, Phoenix Press, Londres, 1999). Pour être exact, avant le 11 septembre, le « seuil symbolique » des cent morts a commencé à être franchi de plus en plus souvent à partir de 1979 (une bombe en Iran : 477 morts) : depuis, une vingtaine d'attentats, essentiellement à la voiture piégée ou sur des avions, ont fait plus de cent victimes chacun.

2. Telle est la thèse d'Alain Wieworka, *Sociétés et terrorisme*, Fayard, 1988. Il y voit un « contre-mouvement social ».

3. La Société des Nations, ancêtre de l'ONU, définissait le terrorisme dans un traité guère appliqué de 1937 : « des faits criminels dirigés contre un État et dont le but ou la nature est de provoquer la terreur... ». Bref, le terroriste terrorise !

4. Le débat sur la définition du terrorisme après le 11 septembre (et dans le contexte des nouvelles législations américaines et européennes) se reflète même sur les sites des partis politiques. Sur celui de <http://www.demlib.com/attentats/definition.htm>, nous apprenons que « selon Jacques Baud, il existe 212 définitions dont 72 sont utilisées officiellement ».

## Terrorisme : stratégie d'irruption

sion voire à la répression, pour qui utilise la notion de terrorisme d'État<sup>1</sup> ;

*psychologiques* : la panique ou la paralysie que le terrorisme cherche à provoquer en fait la version négative de la propagande\* qui unit et rassure. Il le distinguerait de la guerre ou de la guérilla qui cherchent à détruire des forces ennemies et/ou à occuper des territoires ;

*éthiques* : son caractère clandestin, puisque le terroriste, toujours sans uniforme, se dissimule jusqu'au moment d'agir, ses victimes et sa brutalité le rapprochent du crime ;

*polémologiques* : comme la guerre, le terrorisme vise à faire plier par la violence la volonté d'un autre camp ;

*politiques* : par ses revendications, le terrorisme suppose un différend politique qu'il porte sur l'ordre de la Cité, la forme du régime, un territoire, une loi, des alliances...

Ces débats, pendant des années à l'ONU, plus récemment à la Commission Européenne après le 11 septembre ont montré que toute tentative de définition suscitait des objections<sup>2</sup> destinées à limiter un concept qui, autrement, finirait par englober toute violence politique.

Par en haut : pour certains, la qualité des intentions (résistance, lutte anticolonialiste, lutte contre des systèmes non démocratiques qui ne laissent aucune autre possibilité

1. La notion de « Terrorisme d'État » est tout sauf éclairante, puisqu'on désigne par là soit : a) l'activité répressive d'un État qui terrorise sa propre population, au sens robespierriste de la Terreur ; b) des opérations de type « service secret » visant à éliminer des adversaires politiques à l'extérieur : Trotski, Chapour Baktiar,..., et menées soit directement par les ressortissants d'un État, soit par des groupes politiques « amis » ; c) des attentats commandités par un État et visant à faire pression sur un autre État, comme ont pu en pratiquer la Libye, la Syrie ou l'Iran, et c'est alors une façon de « faire passer un message » ; d) le soutien qu'apportent des États, sous forme d'argent, de matériel, de logistique, de refuge territorial à des groupes terroristes avec qui ils partagent des objectifs politiques.

2. Une bonne question d'aborder ces débats sur Internet peut être de commencer par le site universitaire canadien : <http://agora.qc.ca/mot.nsf/Dossiers/Terrorisme>.

d'expression) doit exclure les violences politiques, imposées à leurs auteurs, du domaine honteux du terrorisme.

Par en bas : pour d'autres c'est la faiblesse des moyens employés qui distingue du vrai terrorisme un « simple » activisme, manifestation entraînant des heurts, occupation de locaux, dégradation de marchandises...

Le terrorisme est rebelle à toute définition parce qu'il se situe sur le terrain de l'exception. Robespierre, voyait dans la Terreur un moyen inédit pour une situation paroxystique car « Si le ressort du gouvernement populaire dans la paix est la vertu, le ressort du gouvernement populaire dans la révolution est à la fois la vertu et la terreur... ». De la même façon, le discours du terrorisme se réfère à une situation d'exception : tyrannie extrême, imminence de la Révolution, décrets de la Providence, menace inouïe. Il suppose des fins exceptionnelles qui ne peuvent être atteintes dans le cadre de l'ordre existant. D'où des moyens tout aussi exceptionnels et qui échappent aux lois de la paix et de la guerre. Ou plutôt, de tels moyens abolissent la distinction entre paix et guerre, combattant et non combattant, front et arrière, acte licite et illicite.

## Logiques de l'exception

Ces difficultés ont une origine historique. Le mot « terrorisme », attesté depuis 1794, désigne d'abord une Terreur exercée par l'État, un ordre politique qui repose sur l'extermination physique des opposants réels ou supposés, et l'exhibition de férocité pour paralyser les ennemis de la Révolution. La Terreur, régime qui gouverne la France de mai 1793, la chute des Girondins, jusqu'à juillet 1794, chute de Robespierre, engendre les « terroristes », ses agents. Ils la propagent dans toutes les provinces. Le « terrorisme » est leur méthode et leur but.



## Terrorisme : stratégie d'irruption

Depuis, le sens du mot s'est retourné. Il se retrouve maintenant du côté de la subversion ou du renversement de l'ordre. Désormais, la pratique de méthodes « terribles » par le Pouvoir se nommerait plutôt « répression féroce » ou « totalitarisme policier ».

Un vrai terroriste n'a ni uniforme ni bureau. Un tonton Macoute ou un tchékiste terrorisent, sans être terroristes. C'est une confusion que de parler de terrorisme du Système ou de poser une équivalence entre oppression violente et terrorisme. C'est aussi éclairant que d'embrouiller la définition de la violence, avec les notions floues de violence passive ou structurale, si bien que le terme devient synonyme de mal, haine ou inégalité. La sémantique ignore l'éthique. Déportation, épuration, massacre des opposants, camps peuvent être pires moralement que les terrorismes. Tout ce qui engendre la terreur n'est pas pour autant terrorisme.

Seconde difficulté : la désignation du terrorisme est généralement le fait du terrorisé ou du contre-terroriste. Le terroriste présumé, lui, parle de résistance, régicide, riposte des opprimés, guerre sainte, juste revendication. Il fait remarquer que s'il pose des bombes, c'est faute des bombardiers comme les États<sup>1</sup>. Sa violence, toujours seconde, répond à une terreur initiale par légitime défense ou juste vengeance. Le terroriste nous rappelle que nos écoles célèbrent ceux qui figuraient hier sur l'Affiche Rouge<sup>2</sup>. Que nos occupants appelaient terroristes nos libéra-

1. Abdel Aziz al Ramtisi du Hamas (Le Monde du 13 juin 2002) « Nous sommes dans une guerre de libération. Ce qui se passe ici n'a rien à voir avec le 11 septembre aux États-Unis. Nous ne sommes pas des terroristes. Les jeunes martyrs palestiniens ne se sacrifient pas pour un quelconque paradis ou pour retrouver je ne sais combien de jeunes vierges. Ils se battent pour libérer leur territoire avec les moyens qu'ils ont à leur disposition... Si nous avions des F-16, nous les utiliserions à la place de martyrs, mais nous n'en avons pas. »

2. L'Affiche Rouge, placardée par les Allemands en février 1944 représentait des membres du groupe de Résistance du Groupe Manouchian qui allaient être fusillés comme terroristes au Mont-Valérien.

teurs. Que De Gaulle et Mandela furent dits terroristes. Que des pouvoirs avec qui l'on traite maintenant ne sont que des terrorismes récompensés par l'Histoire, comme des religions sont des sectes qui ont réussi.

Le terroriste avoué est rare : les exemples en sont ou romantiques, tels les nihilistes sur le modèle de Netchaïev<sup>1</sup>, ou cyniques. Ainsi Trotski en théorise l'emploi, dans « Terrorisme et Communisme » en 1935<sup>2</sup>. L'organisation terroriste aime plutôt se présenter comme colonne, guérilla, armée secrète ou de libération... bref à se référer au modèle militaire du partisan, combattant sans uniforme. À moins qu'elle ne se rattache celui du parti en armes, fraction ou branche combattante d'un mouvement politique. Terroriste des champs, guérillero sans territoire, ou terroriste des villes, propagandiste armé, sont unanimes à refuser le qualificatif infamant. D'où un discours répétant que « le vrai terrorisme, c'est celui que nous subissons, l'oppression du peuple » ou que « si défendre ses droits et lutter pour la liberté est du terrorisme, alors, oui, nous sommes terroristes ».

Allons plus loin : les terroristes accomplissent des actes qui violent droit positif et droit des gens, mais au nom d'un droit qu'ils estiment supérieur. Juges, témoins, et bourreaux, ils appliquent des arrêts, convaincus de leur légitimité.

Un terroriste, c'est un juriste contrarié qui n'écoute guère les avocats. Voir les brigades rouges jugeant Aldo Moro avant de l'exécuter. Voir les auteurs d'une tentative de meurtre contre De Gaulle cherchant dans le *jus gentium*<sup>3</sup>, les raisons de sa tentative de « tyrannicide » contre De Gaulle. Voir les terroristes islamiques appliquant scrupuleusement *fatwas*, *tafkirs* (anathèmes), *diyya*

1. L'auteur du *Catéchisme du révolutionnaire* en 1869. Sa vie (et en particulier l'assassinat d'un étudiant membre de sa société secrète) ont inspiré *Les Possédés* (traduit aussi par « *Les Démon*s ») de Dostoïevski.

2. Traduction française intégrale : U.G.E. 1963.

3. Intermédiaire entre le droit naturel et le droit positif, découvert par la Raison, suivant Saint-Thomas d'Aquin : les accusés du procès du Petit-Clamart faisaient souvent de telles allusions philosophiques aux raisons de leur acte.

## Terrorisme : stratégie d'irruption

(prix du sang), *djihad* (guerre sainte proclamée) et *fiqh* (droit canon régissant l'application de la mort en cas de « nécessité »).

En arrière-plan, donc, un droit éminent : droit naturel : état de nécessité, ou légitimité de la révolte en cas de rupture du contrat social, responsabilité individuelle des séides de la tyrannie, édit divin, ordre révolutionnaire encore en genèse, commandement d'une autorité supérieure au pouvoir établi illégitime... Le terroriste châtie qui prétend le réprimer et voit une sanction où nous voyons un crime. Même l'anarchiste de la Belle Époque, Henry, qui jetait une bombe au hasard sur les clients du café *Terminus*, affirmait le principe que « Nul n'est innocent ». Aujourd'hui, des théologiens fondamentalistes expliquent que les femmes et les enfants victimes du *djihad* ne sont pas si innocents : les femmes, en payant l'impôt ou en supportant l'existence d'un État, se rendent complices de ses crimes<sup>1</sup>. Les enfants ont tendance fâcheuse à devenir adultes. Dans une logique de pureté et de culpabilité universelle, les terroristes italiens des années de plomb passèrent des attentats contre des « fascistes », vus comme actes de résistance et d'autodéfense, aux exécutions de modérés de droite puis de gauche, puis enfin des traîtres ou des repentis potentiels dans leurs rangs. Les Japonais de l'Armée Rouge en vinrent à abattre les membres de leur groupe coupables d'attitudes « contre-révolutionnaires », comme avoir des relations sexuelles.

Troisième difficulté : nature, intentionnalité et gravité sociale des menées terroristes varient suivant les époques et les cultures. Leur degré de violence et de dangerosité est jugé très différemment<sup>2</sup>.

1. Voir *Towards a Definition of Terrorism* par Ayatullah Shaykh Muhammad 'Ali Taskhiri. Vol V No. 1 (Muharram 1408 AH/1987 CE) International Conference on Terrorism called by the Organization of the Islamic Conference, Genève, juin 1987.

2. Cela pose des problèmes même aux policiers. Voir Jean-François Raynaud *Définir le terrorisme. Est-ce possible ? Est-ce souhaitable ?*, Revue internationale de criminologie et de police scientifique. N°2, 1988.

Brûler des pneus au cours d'une manifestation, séquestrer un cadre une journée ou saboter une ligne de production, est-ce du terrorisme ? Pour nous, Européens modernes, ce sont, au pire, des dérives violentes de l'action revendicative, en soi légitime. Mais en d'autres temps et d'autres lieux, cela pouvait valoir le poteau.

Distribuer de la drogue ou des images pornographiques, même au nom d'une prétendue haine de l'ordre établi, est-ce du terrorisme ? Là encore nous répondons que non. Or, les Actes de la Conférence d'Unification de Droit Pénal publiés à Paris en 1929 étaient de l'avis contraire.

Y a-t-il des actes « par nature » terroristes ? Des crimes de simple banditisme, tel un hold-up ou une prise d'otage, qui deviennent terroristes s'ils sont accomplis par des groupes organisés et visent à subvertir l'ordre social ?

Peut-on être terroriste seul ? Érostrate ou Ravailac qui n'avaient pas de complices ? Ce Suisse qui a abattu quatorze personnes au Parlement cantonal ? Là encore aucune réponse ne fait l'unanimité. Impossible de sortir de la trilogie : fins/moyens/acteurs.

Peut-on, au moins, s'accorder sur une date de naissance ? Généralement le terrorisme « moderne »<sup>1</sup> est dit remonter aux attentats des narodnystes<sup>2</sup> ou populistes russes. Ils se font connaître en 1878, par l'assassinat du gouverneur de Saint-Pétersbourg exécuté par une disciple de Netchaïev. Ce terrorisme qui frappa l'opinion européenne, inspira, en littérature, Dostoïevski, puis Camus. Mais il inspira aussi, en pratique, des imitateurs russes. En France, la presse attribue à l'influence des « nihilistes russes » ou du prince Kropotkine<sup>3</sup>, dont le nom sonne bien et que l'on confond facile-

1. George Minois (*Le Couteau et le poison*, Fayard, 1997) explique très clairement la différence entre l'ancien tyrannicide et le moderne terrorisme.

2. De *narodnaya volia*, la volonté du peuple, groupe extrémiste russe qui assassina le tsar Alexandre II en 1881. Ils sont souvent également appelés, non sans laxisme verbal, nihilistes voire anarchistes.

3. Sur cette période, y compris dans ses dimensions littéraires en France, voire Uri Eisenzweig, *Fictions de l'anarchisme*, Christian Bourgeois, 2001.

ment avec Bakounine<sup>1</sup>, la paternité morale des actions des Ravachol, Vaillant, Henry, Pauwels, et autres poseurs de bombe de la fin du XIX<sup>e</sup> siècle<sup>2</sup>. L'idée d'une incitation ou d'une participation morale au terrorisme, ou plutôt aux « menées anarchistes » naît aussi avec les « lois scélérates » de la même époque.

Certes, toute périodisation est sujette à caution : il est facile de trouver des antécédents : les sicaires bibliques, les assassins ismaéliens du Vieux de la Montagne d'Alamut, ou les attentats contre Napoléon I<sup>er</sup> et III. Il y eut des régicides, des tyrannicides, déjà théorisés par les jésuites du XVII<sup>e</sup> siècle et des complots révolutionnaires bien avant 1878.

Pourtant le terrorisme « à la russe », semble réunir tous les éléments : l'organisation, sa doctrine, son secret, ses outils de travail — la bombe et le pistolet — le rôle de la presse et de l'opinion, la contagion de l'exemple.

Ce terrorisme moderne est à la fois :

— *Épidémique*, puisque chaque attentat s'inscrit dans une série et suscite des imitateurs, en Russie et ailleurs en Europe.

— *Idéologique*, voire pesamment théorisé. Des groupes réunis par l'idée veulent tuer des idées en assassinant des gens. Ils veulent aussi et surtout réaliser des idées, ce qui est autre chose que

1. Le prince Piotr Kropotkine (1842-1921), ami d'Élisée Reclus et qui séjourna en France, écrivait en 1880 dans le journal *Le Révolté* « La révolte permanente par la parole, par l'écrit, par le poignard, le fusil, la dynamite [...], tout est bon pour nous, qui n'est pas la légalité. ». Il fut même condamné à la prison après un attentat anarchiste en 1882, mais il dénonça fermement le principe du terrorisme. Son influence intellectuelle est cependant sans commune mesure avec celle de Michel Bakounine (1814-1876), grand rival de Karl Marx. Bakounine, longtemps fasciné par Netchaïev, finira par s'en séparer avec horreur.

2. Il y eut même des attentats dont l'unique finalité était la publication par la presse ennemie d'un texte : sa lecture était censée réveiller les masses de leur sommeil. Au XIX<sup>e</sup> siècle la « propagande par le fait » se voulait un moyen d'éveiller les masses sans passer par la médiation du parti ou par la rhétorique du programme. Ici, littéralement les actes valaient discours : ils devaient émanciper ceux qui les accomplissaient autant qu'ils effrayaient ceux qui les subissaient. Voir Daniel Colson, *Petit lexique philosophique de l'anarchisme*, Poche, 2002.

châtier un tyran ou prendre le pouvoir. Jamais plus qu'en leurs débuts, les terroristes ne méritèrent le nom d'intellectuels sanglants puisqu'ils prennent théories et symboles avec un redoutable sérieux.

— *Ambivalent*, hésitant entre action et signification. Pour les narodnystes, chaque partie constituante de la dramaturgie des attentats est lourdement chargée d'un sens : elle représente toujours plus qu'elle-même. Les acteurs sont là pour exprimer une vérité ignorée, telle la révolte future du peuple, même s'il en est encore inconscient. L'organisation révolutionnaire se considère comme sa fraction éclairée. Et elle vise une cible éclairante : la victime, emblème de l'autocratie comme on disait alors. L'attentat est pensé comme un manifeste, une révolte tangible, un coup de tocsin, une étincelle destinée à se propager...

— *Instrumental*, l'acte terroriste n'est pas censé se suffire en soi. Il ne vaut que dans la mesure où il accélère un processus. Il s'agit d'aggraver la décomposition du régime et la prise de conscience des opprimés. Le terrorisme est un raccourci historique. Comme le notait Ernst Jünger, les attentats « influent moins sur l'orientation que sur le rythme de l'Histoire, tantôt l'accélégrant, tantôt le freinant. »<sup>1</sup>.

— « Altruiste » le terrorisme vise des fins qui sont supérieures aux intérêts de ses membres. Souvent les terroristes, tels *Les Justes* de Camus acceptent « d'être criminels pour que la terre se couvre enfin d'innocents »<sup>2</sup>.

Le terrorisme apparaît ainsi dès sa première phase d'expansion comme une violence politique, armée, asymétrique et non institutionnelle, clandestine. Elle vise les forces morales de l'adversaire à travers ses forces matérielles et des proclamations symboliques. Il est évident que la forme que prend le terro-

1. Ernst Jünger, *Récits d'un passeur du siècle*, Éditions du Rocher, 2000.

2. Albert Camus, *Les Justes* (1949) in Camus Théâtre, Pléiade, NRF, 1962.

risme dépend des croyances d'une époque, disons l'idéologie, mais, au moins autant, du répertoire technique disponible, les instruments de destruction et de propagation. Il dépend d'une configuration stratégique.

### **La terreur comme interaction**

Le terrorisme est une interaction<sup>1</sup>. Au même titre que la relation guerrière, elle suppose la distinction de l'ami et de l'ennemi et sépare le monde en deux camps. On connaît la phrase de Cocteau « Il n'y a pas d'amour, il n'y a que des preuves d'amour ». De même, il n'y a pas de Terrorisme, il n'y a que des manifestations de terrorisme. Elles consistent à faire et à dire pour faire dire et faire faire. Les manifestations du terrorisme — le plus souvent par des attentats — sont censées lancer une longue série de réactions et contre-réactions. Elles peuvent être positives, tel le ralliement espéré des masses, mais aussi négatives puisque l'acte terroriste est censé pousser l'adversaire à la faute, par faiblesse ou par férocité. En ce sens, tout terrorisme est une provocation : il entraîne un cycle d'actions et réactions, discours et contre-discours. Là encore, c'est un trait qui le sépare de la guerre, le terrorisme ne saurait se contenter de faire beaucoup de morts : il doit produire beaucoup de bruit et beaucoup de réactions, voire de révélations.

Ces manifestations partagent des caractères communs :

— Elles visent à une perte. Celle-ci peut se mesurer en vies humaines : chefs, responsables ou « innocents » ; en

1. Sur la notion d'interaction, fondamentale en stratégie, et pas seulement pour le terrorisme, voir Pierre Fayard, *La Maîtrise de l'interaction*, Éditions 00h00, 2000, sur <http://www.00h00.com>.

richesses : volées, consumées ou versées en rançon ; en concessions : amnistie, abandon d'un territoire... Mais ce principe de destruction se décline encore d'autres manières : perte d'organisation, de temps et d'information, en cas d'attaques contre des infrastructures, des archives, des systèmes informatiques, des mémoires. Perte des alliés découragés par les risques, perte de prestige. La cible du terrorisme, surtout s'il s'agit d'un État dit légitime, donc supposé maîtriser la violence sur son territoire, voit, de ce fait, son statut remis en cause : la question de sa légitimité n'est pas posée qu'en parole. Se présente alors une alternative. Ou bien faire cesser les pertes moralement insupportables par un abandon, en négociant, en se retirant d'un territoire... Ou bien s'engager dans une montée aux extrêmes : une lutte qui risque de légitimer *a posteriori* le terrorisme.

Le dégât peut être présent, différé ou sous condition, comme en cas de prise d'otage. Il peut être indirect, lorsque l'attentat frappe un tiers. Plus subtilement, il peut faire perdre des apparences et des prudences. Par son acte, le terroriste prétend contraindre le camp adverse à révéler sa « vraie nature », par exemple en réprimant féroce et si possible maladroitement. Ceci peut mener à des raisonnements d'une absurde complication. Ainsi a-t-on accusé l'extrême droite italienne des années soixante-dix d'avoir provoqué des attentats pour mettre en lumière la nature faible et laxiste de l'État. Le but aurait été de l'obliger à se durcir, donc à réprimer des « subversifs » potentiels. Mais le raisonnement inverse a à peu près autant de sens.

Pareil processus peut demander des sacrifices du côté terroriste. Ainsi le martyr est son propre *medium* : il témoigne, au sens étymologique, mais il transforme aussi son propre corps en vecteur du message. Il s'agit alors d'un investissement en vue d'un gain supérieur : le paradis pour le terroriste s'il est croyant, un gain de réputation et de partisans pour la cause. Le témoignage en actes, le martyr d'un des siens vaut à la cause un gain de visibilité et le poids de « l'argumentation » terroriste



## Terrorisme : stratégie d'irruption

s'en trouve renforcée. Cette arithmétique de la destruction instaure un système d'échange et de valeur d'une complexité qu'ignore le stratège « classique ».

— Les actes terroristes n'ont pas leur finalité en eux-mêmes. Ils s'inscrivent dans une continuité des desseins. « Un » acte terroriste sans suite ne serait pas plus signifiant qu'une bataille ne suffirait à faire une guerre. Il faut la promesse d'un renouvellement jusqu'à la victoire, une menace, un avertissement, une projection vers l'avenir. En ce sens, les « séries » terroristes sont à la fois économiques et stratégiques. Leur science est de gérer des ressources pour produire une plus-value, publicitaire, mais aussi de gérer les forces, dans un rapport dialectique avec des forces et intelligences adverses.

De même qu'il y a des guerres à objectifs limités et des guerres totales, la revendication terroriste peut être restreinte, négociable, ou absolue. Le terrorisme peut tenter d'infliger un dommage, essentiellement moral, à l'adversaire jusqu'à ce qu'il estime moins « coûteux » de quitter un territoire ou de céder. Ce n'est pas la même chose que de vouloir rayer son ennemi de la surface de la Terre et d'établir le règne de Dieu, comme semble être la « revendication » du 11 septembre 2001. À demande absolue, affrontement absolu.

— La manifestation terroriste doit pourtant rester rare et surprenante. Mille attentats, cela devient une guerre ou une routine. L'attentat s'apparente à la catastrophe : effondrement brusque du cours ordinaire des choses, suivi d'une période de réparation ou de retour à la normale. Une catastrophe régulière, c'est une contradiction dans les termes.

— Corollairement, ces actions sont théorisées. Le terrorisme suppose un plan, même si le recours à la terreur apparaît comme un pis-aller ou un mal nécessaire aux yeux de ses auteurs. Qui dit plan dit méthode, donc groupes structurés.

D'où le paradoxe des organisations terroristes : il leur faut rechercher l'invisibilité pour gagner la surprise ou l'impunité, dissimuler parfois les objectifs réels. L'acte terroriste recherche également une reproduction ostentatoire : multiplication exemplaire d'initiatives du même type, prolifération du désordre chez l'adversaire, mais surtout proclamation d'une « nouvelle ». Le terrorisme n'est pas un « cri », exprimant révolte ou désespoir, ou alors, il attend un écho. Son acte se veut porteur d'une riche signification et appelle une réponse de l'adversaire, de l'opinion, des neutres ou du genre humain en général.

Qu'il s'agisse de la visibilité et de l'information en général, des moyens et des statuts, des objectifs et des structures, le terrorisme est la forme de conflit la plus asymétrique, puisqu'il n'est imaginable que dans son rapport avec un adversaire absolument autre.

## **Affrontement des symboles**

Le terrorisme, modèle stratégique, applique au mieux les principes de primauté de l'offensive, d'économie et de concentration des forces, de dispersion de l'adversaire et d'augmentation de son incertitude, d'action sur les points, qui produisent un effet d'amplification. Les notions stratégiques traditionnelles s'appliquent donc, en particulier celle de montée aux extrêmes : sauf « friction » du réel qui contraire ses desseins, le terrorisme est voué à l'escalade des moyens et des initiatives.

Mais les effets de ces initiatives stratégiques terroristes ne se mesurent ni en rééquilibrage de forces ni en territoire. Il ne faut ici raisonner ni en termes de liberté d'action, ni en

termes de capacité de contraindre *l'Autre*, comme le ferait un général ou un guérillero. Contrairement à une « vraie » guerre ou à un « vrai » crime, il est souvent difficile de mesurer les objectifs réels, l'objet du conflit, ou les gains réalisés par les acteurs. Ils doivent être appréciés en termes d'information autant que de destruction ou de conquête. Ils ressortent au domaine de l'interprétation qui est aussi celui de l'imprévisible.

Le terrorisme joue toujours sur deux plans. Il y a les éléments visibles : le terroriste, l'otage, la bombe, son cratère, les cadavres, la rançon. Mais chacun de ses éléments signifie plus que lui-même et correspond à une économie supérieure du prestige, du salut, de la reconnaissance, de l'humiliation. Par là, le différend<sup>1</sup> entre les deux camps prend une autre dimension. Le terrorisme déclenche toujours quelque chose, encore faut-il savoir quoi. C'est pourquoi il est si difficile de répondre à la question classique : le terrorisme est-il efficace ? Sous-entendu : là où il échoue, n'a-t-il pas prouvé sa cruelle inutilité voire sa contre-productivité, et là où il a réussi, n'est-ce pas parce que l'Histoire allait de toute façon dans ce sens-là ?

Le terrorisme représente un modèle symbolique autant que médiologique : il vise un maximum d'efficacité, compte tenu des moyens de transmission. Son histoire fait passer du poignant au Boeing, du libelle au *live* télévisé planétaire<sup>2</sup>.

Si le dommage se double d'un message, celui-ci est à plusieurs étages :

— *C'est un témoignage.* L'acte terroriste « révèle » : l'existence, les projets ou revendications d'un groupe qui se dit représentatif d'une communauté, de l'injustice éprouvée par

1. Sur cette notion voir Jean-François Lyotard, *Le Différend*, Éditions de Minuit, 1987.

2. La « périodisation » entre armes et médias du terrorisme est traitée dans l'article de Catherine Bertho-Lavenir du n° 13 précité des *Cahiers de médiologie*.

un peuple, de leur combativité... Tel la guerre, le terrorisme est un discours pour l'Histoire, souvent pédagogique. Parfois bavard. C'est une guerre du Paraître, voire pour paraître. Combien de terroristes luttent pour « être reconnus » ?

— *C'est un outrage*. Il atteint celui à qui il s'adresse : il attende à son prestige symbolique, il en révèle les fragilités ou les contradictions. Le terrorisme procède par défi, mise en demeure. Il pose une énigme : comment interpréter l'acte, identifier les auteurs ? La transgression est renforcée par la théâtralisation. L'outrage joue aussi sur le caractère de la victime : emblématique par sa puissance et ses responsabilités, significative par son anonymat et son innocence mêmes.

— *C'est un marchandage*. Le terroriste cherche toujours un gain. Il parle sous condition : si vous me donnez tel avantage, si vous libérez Untel, si vous cédez sur tel point, j'adoucirai votre peine. Si vous me reconnaissez, vous y gagnerez. Le tout est truffé de pièges et de mystères puisqu'on ne peut être assuré ni de la promesse ni du promettant, ni des termes de l'échange.

Les actes terroristes se classent sur une double échelle.

— *L'échelle de destruction* : elle va de la violence la plus précise — un tyrannicide — à la plus générale. Si les opérations terroristes se renouvellent trop, elles finissent par ne plus se distinguer de la guérilla ou de la guerre de partisans.

— *L'échelle de propagation* : le message terroriste\* peut avoir une valeur de proclamation, destinée à éveiller le genre humain mais aussi une valeur de négociation et ne s'adresser qu'à quelques interlocuteurs et décideurs.

Il se pourrait enfin qu'il faille considérer qu'au-delà de l'atteinte aux forces adverses ou de la « publicité », le terrorisme a valeur d'expiation. La compensation du sang versé, l'humiliation du puissant, la punition tiennent une grande part dans son discours. Cela est plus vrai que jamais avec Ben Laden.

## Contrôle, images, données\*

Toutes ces grilles s'appliquent aux attentats du 11 septembre 2001. Les chercheurs discutent encore pour savoir s'ils inaugurent un « hyperterrorisme » ou s'ils ne représentent qu'un degré supérieur d'un phénomène ancien<sup>1</sup>.

Avant le 11 septembre, le terrorisme était considéré comme subsidiaire ou secondaire, il se pratiquait à la place de la guerre ou de la Révolution, voire en attendant d'en avoir les moyens. Dans la même logique, l'image était la servante de l'acte : elle amplifiait, souvent via médias de l'adversaire, la force de nuisance de l'attentat. On pouvait raisonner en termes de facteur multiplicateur. Aux yeux des terroristes, l'essentiel était de faire diffuser leur message explicatif. Est-ce toujours vrai ?

Le 11 septembre, tout commence par des images. Nous fûmes des millions à nous précipiter vers les écrans y voir et revoir s'effondrer les *Twin Towers*. Très vite, une lecture s'imposait : ces scènes étaient symboliques et stratégiques. Symboliques, elles voulaient nous *dire* quelque chose. Les tours « signifiaient » l'Amérique, l'Argent, la Culture mondiale, y compris celle des films catastrophe, la Tour de Babel... Stratégiques, ces images devaient nous *faire* quelque chose. Quelqu'un les avait produites, mises en scène, en vue d'un effet psychique et panique : une intelligence, consciente du pouvoir des médias. Il est bien connu que le terrorisme vise toujours à un retentissement psychique « hors de proportion avec ses résultats purement physiques »<sup>2</sup>.

1. C'est l'objet de la controverse entre François Heisbourg (*Hyperterrorisme : la nouvelle guerre*, Odile Jacob, 2001) et Gérard Chaliand, *L'Arme du terrorisme*, Éditions Louis Audibert, 2002. Pour suivre les travaux sur le terrorisme des équivalents français des *think tanks* américaines, voir : <http://www.frstrategie.org>, <http://www.ifri.org>, <http://www.strategic-road.com/dossiers/terrorusa/htm>.

2. L'expression est de Raymond Aron dans *Clausewitz Penser la guerre*, N.R.F., 1976.

Pourtant tout n'est pas si simple. De quoi les tours étaient-elles les « icônes » — le terme qu'emploie Ben Laden dans la traduction d'une de ses cassettes — sinon du temporel ? Comment fallait-il interpréter un attentat qui ne revendiquait rien, sinon la disparition de l'adversaire ou le règne de Dieu sur la Terre ?

Du point de vue de l'image, tout s'oppose caricaturalement. Al Jazeera contre CNN. *Cutters* contre missiles. K7 contre B52. *Low tech* contre *High tech*. Discours théologique contre discours étatique. Métaphores coraniques contre conférences de presse. Treillis contre costumes. *Ouma* contre mondialisme. Dramaturgie contre communication. Celui qui regarde le ciel contre celui qui regarde le prompteur. L'homme des grottes et du désert contre l'homme des villes et des tours. Ben Laden contre Bush.

Du point de vue stratégique, Ben Laden sait utiliser le principe des réseaux pour se protéger et retourner contre nous nos réseaux télévisuels, financiers, électroniques pour une contagion optimale. Les stratèges US théorisaient déjà *netwar*, la guerre en réseaux qu'ils distinguaient de *cyberwar*, la guerre assistée par ordinateurs<sup>1</sup>. Le Pentagone en a rêvé, Ben Laden l'a réalisé !

L'Amérique se prépare pour une « guerre de l'information » propre et politiquement correcte, gérée par ordinateurs et satellites. Les futurologues développaient le projet de la dominance informationnelle. La guerre deviendrait *cool* et séduisante. Les professionnels de la communication s'en chargeaient : zéro dommage cathodique.

C'est une tout autre « guerre de l'information » qu'a menée al Quaïda : sidération du village global par des images emblématiques en *live* planétaire, contagion de la panique boursière via la Toile, utilisation des moyens techniques adverses pour une répercussion maximale...

1. Sur ces notions voir les textes d'Arquilla et Ronfeldt sur le site <http://www.rand.org> plusieurs fois signalés dans cet ouvrage. Sur le terrorisme, la Rand propose également de nombreux textes de son meilleur spécialiste, Bruce Hoffman, partisan d'une analyse du phénomène en tant que stratégie froide et rationnelle (rationnelle au regard de ses objectifs, s'entend).

## Terrorisme : stratégie d'irruption

Le problème de l'organisation terroriste est d'être secrète et spectaculaire à la fois. Secrète, elle doit, en dépit de sa lourdeur, échapper aux détecteurs maillant la planète. Spectaculaire, elle doit produire une surprise maximale aux points de visibilité maximale. La solution de cette équation, c'est le terrorisme en réseaux, double négatif de la société en réseaux<sup>1</sup>. Il y gagne la capacité de coordonner des acteurs épars, de faire circuler leurs messages, de désigner des objectifs communs, de suivre des procédures implicites sans que ses adversaires puissent l'interrompre ou en reconstituer la structure. Dans cette configuration, le faible marque un point contre le fort.

Ben Laden et les siens comprennent les faiblesses stratégiques et techniques de l'Occident. Pourtant, reste une question : en quoi consisterait leur « victoire » politique et la recherchent-ils vraiment ? À un journaliste qui lui demandait à quoi se reconnaîtrait la victoire des USA, David Rumfeld répondit que ce serait le jour où le monde entier accepterait de ne plus s'en prendre au mode de vie américain. Cela suppose une stratégie d'annulation. Le terrorisme, l'action des États « voyous », ou des groupes mafieux, tous les troubles dans les zones incontrôlables, sont évalués dans cette optique défensive, comme crises à éviter et périls à prévenir. Il faut les éliminer, si possible en amont par la surveillance et la dissuasion, si nécessaire en aval, par une réaction immédiate.

Mais la victoire de Ben Laden ? Quel est le but ultime de sa stratégie de perturbation ? Il n'est pas difficile de comprendre ce que recherche un terroriste qui veut libérer un territoire ou renverser un gouvernement. Les objectifs de Ben Laden semblent trop universels. Est-il totalement nihiliste ou, ce qui

1. Sur la notion de réseaux on consultera Christian Marcon et Nicolas Moinet *La Stratégie réseau*, Éditions 00h00, 2000, téléchargeable sur <http://www.00h00.com>. Voir aussi Daniel Parrochia, *La Philosophie des réseaux*, P.U.F., 1993 et Philippe Forget et Gilles Polycarpe, *Le Réseau et l'Infini*, Economica, 1997.

revient au même, réclame-t-il tout : l'utopie totale, la fin de l'Histoire, la fusion du politique et du religieux ?

## Sept portes de la terreur

Résumons :

— *Le terrorisme suppose une casuistique.* Le terroriste veut justifier en conscience, et par un droit, une violence que son adversaire tente de criminaliser et de rabaisser.

— *Le terrorisme a une rhétorique.* Il tente de convaincre et son adversaire (qu'il a perdu, que sa cause est injuste...) et son propre camp (de son identité, que la victoire est proche, qu'il faut être unis...). Cette rhétorique suppose un contenu que *l'Autre* doit réfuter comme mensonger.

— *Le terrorisme s'apparente parfois à un ésotérisme,* voire à un comportement de secte, puisqu'il vit du secret. Ses ennemis, eux, prétendent toujours le démasquer.

— *Le terrorisme a une topologie : celle des réseaux.* Ils dépendent à la fois de leur capacité de fonctionner malgré les tentatives d'interruption, et d'un environnement favorable, tel un sanctuaire hors frontières par exemple. En face, le contre-terrorisme cherche à sécuriser des zones, à contrôler du territoire.

— *Le terrorisme suppose une économie :* il gère des ressources rares et tente de produire des plus-values considérables, notamment publicitaires. C'est cette logique d'échange que tentent de casser ses adversaires.

— *Le terrorisme ressortit, on l'a assez dit, au symbolique.* Il recherche une « escalade » du sens : il prétend élargir la signification de ses cibles ou de ses revendications jusqu'à atteindre des principes historiques, religieux, métaphysiques : la Tyranie, le Mal, la Révolution... Dans le camp d'en face, il faut, au



## Terrorisme : stratégie d'irruption

contraire, rabaisser le débat pour rabaisser le terrorisme, notamment le ramener à sa composante criminelle.

— *Le terrorisme est, avons-nous assez répété, stratégique.* Il repose au total sur une méthode de perturbation, — paralyser la volonté ou la capacité adverse, — plutôt que de destruction ou de conquête. Cette stratégie implique dans certains cas le concept paradoxal de « non victoire », si le but du terrorisme est uniquement d'affirmation identitaire ou de vengeance symbolique. Face à cela, il ne reste plus à son ennemi qu'à élaborer une stratégie d'annulation, dont il faut craindre qu'elle ressemble à celle des Danaïdes.



## Chapitre II

### Captures d'écran

La violence collective mobilise des moyens de destruction autant que de représentation. Ses formes et manifestations reflètent, bien évidemment, les progrès des armes. Mais nous mesurons plus mal le rôle parallèle des technologies intellectuelles qui prolongent le cerveau et non plus notre bras. Nos médias sont des armes<sup>1</sup> : ce qui transporte les hommes et les idées sert aussi à combattre. Une histoire de la violence devrait faire place, à côté du mousquet, à l'imprimerie et à la carte maritime dans la conquête du monde par les Occidentaux. Le couple train plus télégraphe — troupes et ordres circulent plus vite que les chevaux — répondrait à la synergie armes à répétition plus cartouche métallique. Ceci peut aussi se décliner de cent façons : la rencontre dynamite plus imprimerie dans l'histoire du terrorisme<sup>2</sup> ou missile plus télévision satellitaire dans les conflits contemporains.

Les machines à communiquer, les données et images qu'elles véhiculent, représentent des potentiels stratégiques.

1. Sur ce point, voir « L'Arme et le *medium* » in *Cahier de Médiologie*, n°6, *Pourquoi des médiologues ?*, Gallimard, 1998, disponible sur <http://www.mediologie.com>.

2. Cette dernière lacune commence à être comblée par l'article de Catherine Bertho-Lavenir « La Bombe, le prote et le manifeste » dans *La Scène terroriste (Cahiers de médiologie, n°13, 2002)*.

— *Ce sont des moyens d'accélération*, donc de coordination de l'action : la transmission des ordres et renseignements par des technologies sophistiquées dissipe le « brouillard de la guerre » où, suivant Clausewitz, le général n'est vraiment sûr de rien, même pas de sa propre position. Savoir et ordonner avant *l'Autre* est un avantage incontestable.

— *Ce sont des moyens d'acquisition* : de l'information pertinente, intelligence au sens large, mais aussi acquisition d'une supériorité psychologique et plus seulement décisionnelle. On songe à ces soldats irakiens, pendant la guerre du Golfe, se rendant à des simples drones, engins volants d'observation qui n'ont ni pilote ni armement. Simplement, celui qui se sait vu et filmé sur le champ de bataille se sait vulnérable. En jargon du Pentagone, sa « signature »\* est « acquise », il peut être frappé à tout moment. Apparaître sur l'écran adverse, c'est perdre.

— *Les images peuvent produire un effet d'occultation* ou de distanciation au moins pour les soldats. Le viseur puis l'écran informatique résolvent un vieux problème du dressage militaire : permettre au guerrier de voir son ennemi comme cible, lui interdire d'y reconnaître un semblable. Supprimer un point d'écran ne pose pas exactement les mêmes problèmes éthologiques que de charger à la baïonnette.

— Enfin, et c'est ici ce qui nous concerne, *les médias sont des machines de propagation* non seulement des nouvelles, vraies ou fausses, mais aussi des images et des imaginaires. Massacres de masse, manipulation psychologique des masses et *mass media*\* progressent parallèlement.

Deux questions se mêlent ici : celle de la vérité et celle des affects. Les médias sont des instruments à faire croire que... mais aussi à faire croire en..., voire à faire croire contre... Ils dépeignent la réalité avec plus ou moins d'exactitude — surtout celle de conflits — mais ils font aussi l'éprouver différemment. Le problème s'est posé dès la photographie, à la fois probante, poignante. Et bien sûr techniquement reproductible.

## Captures d'écran

Les médias rapportent des vérités de fait, souvent sous forme d'images. Le petit Mohammed, une des premières victimes de la seconde Intifada, mort devant les télévisions du monde entier a reçu ou bien une balle israélienne ou bien palestinienne. La photo par Capra d'un milicien fauché par un projectile pendant la guerre civile espagnole est ou bien authentique ou bien posée. Mais ces vérités de fait sont à pondérer en fonction de vérités politiques relatives au bien, au juste et au souhaitable (que prouvent ces documents, vrais ou truqués, sur la justesse de la cause palestinienne ou républicaine ?), mais aussi en fonction des limites de la force concluante des images. Car — pardon de rappeler ces banalités — toute image est construite, cadrée, dans un certain contexte, toute séquence est montée et découpée, toute lecture de l'image dirigée par une légende, un commentaire ou l'insertion dans un ensemble... Son point d'impact résulte d'un point de vue. Toute réalité représentée est une réalité sélectionnée, dont le sens nous est proposé. Et qui occulte d'autres réalités... Il y a ainsi des guerres d'écran et des guerres invisibles, des victimes omniprésentes et des victimes invisibles.

Quant au mode de sensibilité que créent les médias, il tient en particulier à la façon d'éprouver l'expérience de la mort d'autrui. Au-delà des catégories de la haine et de la peur, interviennent nos sentiments d'appartenance, nos relations avec des symboles collectifs. Comment nous croyons n'est pas la résultante des bons ou mauvais messages disponibles. Leur force rhétorique ne se heurte pas moins à des contraintes, celles des moyens de propagation, qu'à des limites, celles de la réception.

S'ajoute un troisième facteur. Des professionnels, s'appuyant souvent sur des connaissances qu'ils disent scientifiques, s'efforcent de calculer la balistique des messages comme celle des obus. Même sous sa forme primitive, la guerre requiert au moins deux opérations délibérées : faire accepter à des gens l'éventualité de leur propre mort et leur faire désirer celle de

gens qu'ils n'ont jamais rencontrés. Elle exige désormais la conquête d'un public. L'occupation des esprits compte autant que celle des territoires.

La presse s'est récemment émue de la découverte d'un bureau « de désinformation » du Pentagone<sup>1</sup>. D'où débat moral : quand on lutte contre l'axe du mal est-il licite de mentir à l'opinion amie ? Une brève recherche aurait pourtant suffi à rappeler qu'il existait depuis longtemps des brigades de « *psyops* »\* (opérations psychologiques de désinformation, intoxication ou « sidération »), des *spin doctors*\* et des agences de communication qui vendent de la guerre comme du yaourt ; qu'il y eut de célèbres médiamensonges durant la guerre de Bosnie et pendant celle du Golfe ; que les exercices de l'OTAN incluent maintenant l'art de ne présenter que de bons cadavres et de bonnes informations à la presse. Mais elles auraient surtout révélé l'ancienneté du couple formé par les projectiles et les projections. Il a au moins deux siècles.

## Les industries de l'enthousiasme

À l'ère industrielle, politiques et militaires comprennent très vite l'intérêt de contrôler quelle représentation de la guerre se fait une population, de plus en plus instruite, avide d'informations fraîches, de dépêches. Le public est rapidement informé ou désinformé des réalités du front. À Paris, Londres ou Berlin, la foule des boulevards réagit de plus en plus vite aux échos des tueries lointaines.

Désormais, dans tous les conflits, il faudra penser belligérance et audience. Surtout, il faut maîtriser deux flux d'informations. Les mauvaises, ce sont celles qui pourraient renseigner l'ennemi

1. Voir l'article du *Monde* du 27 février 2002 : « Le bureau de désinformation du Pentagone est supprimé » p.3. via <http://www.lemonde.fr>.

## Captures d'écran

sur l'état ou la position des forces amies, mais surtout celles qui porteraient atteinte au moral des civils. Les bonnes, ce sont les nouvelles des succès, bien sûr, mais aussi des preuves. Preuve de la vaillance de ses armées ou des atrocités ennemies.

Ici intervient très vite la photographie avec la guerre de Crimée, entre 1853 et 1856.

Pour une part, c'est encore une guerre du passé. Sur de multiples gravures et tableaux, elle est stylisée, sublimée, sur des toiles à la Horace Vernet ou à la Tabar et Charpentier<sup>1</sup>. Dans le même temps, la presse populaire, comme l'*Illustration*, dépêche des dessinateurs sur place et grave à tout va des représentations d'une guerre noble. À Paris, en province, mais aussi aux États-Unis et en Russie on raffole des panoramas<sup>2</sup>, ces spectacles qui représentent les batailles célèbres à grand renfort de toiles peintes et de machineries.

La guerre de Crimée est surtout la première guerre photographiée<sup>3</sup>, par le Français Langlois, le Roumain Szathmary et les Anglais Robertson et Fenton. Ce dernier est envoyé officiellement par la reine pour démontrer à l'opinion que ses soldats ne sont pas décimés par la maladie et font bonne figure<sup>4</sup>. Pour des raisons évidentes, temps de pose, lourdeur du matériel, la photographie est statique. Elle se complaît aux paysages et aux vues larges. Elle décrit les temps de repos et non de combat. Elle ne donne aucune idée ni de la dynamique de l'action, ni de l'atrocité des batailles. Mais le pas est franchi : pour la première fois, le spectateur voit une guerre

1. Ces peintres ont particulièrement illustré la guerre de Crimée.

2. Sur l'histoire de la représentation de la guerre, peinture, panorama, photographie, film, etc., voir l'ouvrage d'Hélène Puisseux, *Les Figures de la guerre Représentations et sensibilités, 1839-1996*, Gallimard, 1996. Nous lui devons beaucoup de l'information de ce chapitre.

3. Voir aussi *Crimée, 1854-1856 premiers reportages de guerre*, catalogue de l'exposition du Musée des Armées.

4. Plus exactement la mission de Fenton est d'opposer un démenti aux critiques du Times et de W. Russell. Sur les 360 clichés qu'il prend on ne voit pas une goutte de sang.

non idéalisée par le pinceau. Une expérience anthropologique séculaire — être en un lieu où les hommes périssent de mort violente — se vit par représentation voire par procuration. La photographie saisit le vif ; avec le reportage de guerre qui vient de s’inventer<sup>1</sup>, elle peut aussi saisir des morts. La trilogie guerrière, nos soldats, l’ennemi, les victimes, va prendre figure humaine. Les stéréotypes s’incarneront désormais de façon, croit-on, incontestable.

Lors de la guerre des cipayes en 1856, la photo montre des victimes exécutées sur les clichés de Robertson et Felice Beato<sup>2</sup>. De 1861 à 1865, la guerre de sécession américaine, guerre totale et moderne<sup>3</sup> qui fait sans doute 500 000 morts, étale ses horreurs. Et cela en grande partie grâce aux clichés, largement reproduits et source d’un commerce non négligeable ; cette fois, ils ne cachent plus les morts. Ceux de la grande boucherie de Gettysburg en 1863, les mutilés et les prisonniers ou les amoncellements de crânes et de membres que l’on retire de la terre un an après la bataille de Cold Harbor, sont d’un réalisme implacable<sup>4</sup>. Mais ce réalisme-là doit être questionné. La vérité de certaines images a été contestée, elles auraient été posées. D’autres sont déjà censurées comme celles des bagnes sudistes d’Andersonville. Et surtout, le pouvoir politique est conscient de l’intérêt de l’image photographique. Ainsi, Lincoln, le département d’État à la guerre et les services secrets encouragent et subventionnent l’immense travail de reportage de Mathew Brady.

La valeur de preuve de la photographie sera bientôt mise en évidence mais aussi ses limites. Pendant la guerre de 1870, un célèbre cliché, *Franc-tireur brûlé vif par les Prussiens*, d’une

1. Voir Alain Barret, *Les Premiers Reporters photographes, 1848-1914*, Duponchelle, 1977.

2. Il photographie des pendants de mutins en 1858, puis, deux ans plus tard, les morts d’une autre révolte : ceux du fort de Taku en Chine.

3. La photographie aussi, avec l’allègement du matériel et la réduction du temps de pose, connaît des progrès qui permettent une vision plus réaliste du conflit.

4. Tous ces clichés sont reproduits dans le livre d’Hélène Puisseux précité.



authenticité douteuse<sup>1</sup>, soulève l'indignation contre les barbares d'outre-Rhin ; certaines photos de la Commune sont visiblement gouachées... Le trucage commence. Il fleurira au vingtième siècle. On sait comment Trotski disparaîtra des épreuves où il figurait à la tribune ou près de Lénine, victime d'un coup de pinceau et de la nouvelle ligne du Parti.

### **Simulation, stimulation, dissimulation**

Sans refaire toute l'histoire de la propagande<sup>2</sup>, il faut rappeler combien la guerre de 14-18 lui donne ses caractères modernes. Sa devise semble être « Simulation, stimulation, dissimulation » : donner une image militairement ou idéologiquement correcte du conflit, stimuler les ardeurs patriotiques, martiales et morales et dissimuler par la censure tout ce qui pourrait troubler la vision officielle des événements.

D'où des innovations :

— *La propagande crée des bureaux de la foi*. Des services entiers sont affectés au contrôle de l'information disponible, expurgant tout ce qui est publié, texte ou image. Ces mêmes services sont chargés de protéger une nouvelle ressource stratégique : le « moral des civils ». Les atteintes à ce bien précieux tombent sous le coup du code pénal : gare aux défaitistes ! Et pour ce faire, les professionnels de la croyance font appel à ceux des sciences sociales ou de la toute jeune publicité.

— *La propagande déborde le domaine guerrier, c'est-à-dire la façon dont les faits relatifs à la guerre sont rapportés*. Elle tou-

1. Le document atroce est présenté par l'imprimerie dijonnaise Guibert qui en faisait commerce comme « d'après nature ». Certaines autres photos de la guerre de 1870, tels des cadavres d'enfants, sont visiblement posés et mis en scène. Voir Puiseux précité p. 154 et sq.

2. Voir Ellul J., *Histoire de la propagande*, PUF, 1967.

che au domaine des valeurs en général, de la culture, de l'esthétique (comme l'a remarqué Benjamin, elle esthétise guerre et politique<sup>1</sup>). La polarisation militaire ou militante entre eux et nous envahit tous les aspects de la vie : il ne peut rien y avoir de neutre. Tout reflète un conflit non pas historique et contingent, celui de deux États se disputant un territoire, mais une lutte essentielle entre deux types humains. Les boches sont par fatalité traîtres et cruels : c'est dans leur constitution biologique. Ils ne bombardent pas les églises par hasard, mais parce que leur barbarie déguisée en *Kultur* repose sur la haine de la Civilisation, ....<sup>2</sup>

— *La propagande est à double face*. Grande simplificatrice, elle réduit le monde à nous et eux. L'adversaire unique, à la fois cause de nos malheurs et objet de nos projections, nous resoude. Dans ce processus, le contenu de la croyance importe peut-être moins que le lien (entre nous) et la frontière (qui nous sépare d'eux). Le groupe adverse s'assimile au mal absolu dans l'ordre de la morale, de la religion, du droit, voire au laid, au non humain. Mais cet adversaire, il faut aussi lui adresser un message, ne serait-ce que pour le décourager ou le diviser. Clausewitz disait que la guerre consistait à anéantir les forces morales et physiques de l'adversaire par l'intermédiaire des secondes. Les propagandistes visent ces forces morales. Mais ils le font assez maladroitement. Les tracts lancés par-dessus les tranchées disent toujours la même chose : « Rendez-vous. Il n'y a plus aucun espoir. Vos dirigeants vous trompent. ». Les récentes reproductions de billets de banque largués d'avion en Afghanistan, portant sur l'autre face des caricatures de chefs taliban, représentent-ils un progrès ?

1. Walter Benjamin, *L'Œuvre d'art à l'époque de sa reproductibilité technique*, Carré, 1997.

2. On trouvera de nombreuses illustrations dans le chapitre *Le Vrai contre le faux* de Laurent Gervereau, *Les Images qui mentent, Histoire du visuel au XX<sup>e</sup> siècle*, Seuil, 2000. Voir aussi le site <http://www.imagesmag.net> pour une réflexion sur l'interprétation des photographies.

— *La propagande absolue suppose le crime absolu*. Il ne suffit pas que l'ennemi soit combattu ou que sa cause soit injuste, il faut qu'il soit coupable de crimes qui l'excluent du genre humain et que la guerre à mener se confonde avec une œuvre de justice. Le « Rapport de la commission Bryce sur les atrocités allemandes en Belgique »<sup>1</sup> paru à la fin 1914 et traduit en trente langues inaugure le long cycle de la judiciaireisation de la guerre, des imputations d'atrocités et de la production de preuves, souvent photographiques et filmées, de massacres.

À partir de là, l'image et la question de sa vérité deviennent cruciales dans tous les combats, militaires ou idéologiques. Certes, on n'a pas attendu la première guerre mondiale pour accuser les armées ou les partis adverses des pires horreurs : cela se pratiquait depuis l'invention de l'imprimerie et les guerres de religion, presque contemporaines. Mais l'imputation systématique d'atrocités, sa mise en scène et en images puis sa diffusion industrielle datent de 1914. Au couple des pulsions de peur et de haine, s'ajoute la relation ambiguë entre pitié ou indignation et identification. Sur les affiches, dans les films — car le cinéma est très vite mobilisé et mobilisant —, à travers des icônes du siècle, commence un long cortège de mères douloureuses, d'enfants martyrisés, de torturés, de charniers. Il hantera la mémoire visuelle collective. Le phénomène culminera pendant la seconde guerre mondiale et la question de la Shoah, irreprésentable et innommable pour les uns, mais avec, pour les autres, la conviction que si l'on avait vu, si l'on avait su, si l'on avait fourni des preuves visibles à l'opinion mondiale, les choses se seraient déroulées autrement.

Mais la guerre de l'image ne se résume jamais à la question de la preuve, qu'il s'agisse de celle de l'héroïsme des nôtres ou de la perversité de l'ennemi. Cet ennemi, encore faut-il le voir et le nommer, voire le légender comme un cliché. L'histoire visuelle de la guerre d'Algérie apparaît souvent comme celle

1. J.J. Becker et al., *Guerre et Cultures, (1914-1918)*, Armand Colin, 1997.

d'exactions révélées ou dissimulées dont nous évoquons la mémoire quarante ans après, y compris le massacre des harkis, dont ne subsiste guère d'image. Elle fut aussi celle d'un embarras à décrire des « événements » qui n'étaient ni une guerre ni une révolte, à désigner un adversaire, le fellagha qui semblait aussi invisible sur le terrain, qu'inclassable : était-il ennemi, révolutionnaire, rebelle, bandit ? Hors quelques clichés de pauvres types levant les bras, l'ennemi n'apparaît guère. L'enjeu symbolique qu'implique le point de vue sur l'image, surtout dans les guerres non conventionnelles, se révèle déjà.

## Preuves en images

Cet enjeu sera évident dans la guerre du Vietnam, riche en images. Ce sont des images qui restent dans toutes les mémoires et mobilisent les foules protestataires de l'époque, petite fille courant sous le napalm, exécution d'un civil d'une balle dans la tête, bonze se faisant brûler vif. Là aussi l'adversaire est invisible mais l'image surabondante, grâce à des correspondants de guerre équipés d'un matériel léger. Ils se déplacent sans peine et filment ou photographient ce qu'ils veulent, quitte à en payer le prix : plus de 150 d'entre eux y trouvent la mort. L'image est incontrôlée et diffusée. Car pendant que la photographie et le film fixent les grands souvenirs de la guerre pour la mémoire, la télévision fait rentrer le conflit dans les foyers. Elle y rappelle non seulement que les *boys* font des morts qui ressemblent à des civils, mais aussi que les *G.I.* qui, eux, ressemblent tant aux téléspectateurs, rentrent au pays en *Body Bags*, les sacs à viande.

Même si, côté américain, les commentaires de l'image furent globalement moins « pacifistes » qu'on ne tend à le croire<sup>1</sup>, la

1. Voir *La Télévision et la guerre du Vietnam*, in *Hermès* n°8-9.

télévision apparaissait comme facteur de démobilisation. De démoralisation, disent les militaires persuadés d'avoir perdu à cause des médias. Ils en retiennent la leçon : contrôler les images des dommages qu'on produit, mais aussi celle des pertes qu'on subit, localiser les caméras amies comme les mitrailleuses ennemies. Règles qu'appliqueront toutes les armées, y compris Tsahal en refusant récemment l'accès de Djénine à la presse.

Lors des conflits de la Grenade et de Panama, aux Malouines, règne le principe du « pas vu, pas tué » : une bonne guerre est une guerre sans morts visibles, supportable par les sensibilités télévisuelles. Les objets de notre compassion sont sélectionnés : tous les cadavres n'ont pas la même survie cathodique *post mortem*. La télévision excelle à montrer des victimes particulières et interchangeable dans leur souffrance, séparées de tout cadre de référence, de toute histoire, mais capables d'émouvoir. Mais elle les sélectionne. L'idéologie victimaire, et à l'humanitaire-spectacle, encourage l'art de montrer ou de cacher les bons morts. Et toutes ne nous touchent pas également. L'historien Walter Laqueur faisait remarquer que le terrorisme tue plusieurs milliers de personnes par an en Inde et au Pakistan et que, sauf risque de guerre nucléaire entre les deux puissances atomiques, cela émeut moins les médias occidentaux que des jets de pierre à Bethléem<sup>1</sup>.

La guerre du Golfe — on l'a écrit cent fois — fut tout à la fois une guerre vidéo, sans image, guerre en direct, guerre-spectacle, mais ce fut aussi une guerre sans victimes visibles. Elle révélait la logique de la télévision par satellite qui allait désormais nous faire vivre au rythme des catastrophes en *live*, en direct. À rebours d'une expérience séculaire, qui consistait à se vanter par des tableaux héroïques ou sur des monuments de pierre, d'avoir fait beaucoup de morts, il s'agissait aussi de démontrer l'innocuité d'une puissance, par ailleurs complaisamment éta-

1. Walter Laqueur, *The New terrorism*, Phoenix Press, Londres, 1999, p.150.

lée. Ces machins sont terrifiants, mais nous ne tuons pas vraiment de gens et bien sûr, personne ne meurt chez nous.

Depuis, la leçon a été retenue et étendue. La guerre du Kosovo, avide de visages de victimes, dissimula le corps de l'ennemi. Il fut nié par la distance, vu et frappé à hauteur de satellite, comme nié par la parole, y compris par le refus de se référer la catégorie de l'ennemi. Jamie Shea, porte-parole de l'OTAN expliquait image numérique à l'appui, que les frappes détruisaient des choses, du potentiel militaire et que les coups ne s'adressaient pas à un peuple, mais à un tyran ou à un principe.

D'où quelques nouvelles règles du jeu :

— *Les médias ne transcrivent plus l'événement, ils le font.* Ou du moins, ils le suscitent : en Somalie, comment l'*US Army* programme des guerres humanitaires sur rendez-vous avec les grands médias, mais y renonce dès que les caméras saisissent une scène non prévue par le scénario : des *boys* morts, comme au Vietnam, des indigènes bêtement mitraillés.

— *La principale fonction des médias est de dire qu'ils sont là et qu'il n'y a rien à dire,* sinon que la planète entière vibre de la même émotion et partage la même attente. L'absence d'information ne fait pas obstacle à la communication. Au contraire.

— *Désormais, la télévision contribue plutôt à une désorientation du spectateur.* La guerre devient ou trop mondiale ou trop locale. L'ennemi se dénationalise, s'identifie à une entité abstraite : Fanatisme, Haine, Totalitarisme, Purification ethnique, ou à une particularité folklorique : les Serbes n'aiment pas les Bosniaques, ni les Hutus les Tutsis, c'est comme ça chez ces gens-là. La cause des conflits s'individualise : Saddam Hussein et Milosevic sont de nouveaux Hitler, Ben Laden un fanatique nihiliste. L'intelligibilité historique est en proportion inverse de l'hystérie de visibilité dans le perpétuel présent cathodique. Et comme de surcroît, la télévision tend à dépolitiser et à montrer la « force des choses », toutes les violences deviennent égales,

dans la catégorie des catastrophes ou de l'éternelle folie des hommes, explicables par les passions archaïques.

La catégorie de l'ennemi devient pareillement problématique. L'Autre est forcément victime ou criminel, humainement touchant, moralement condamnable, toujours réduit à sa dimension affective. Sa souffrance ou sa perversité lui interdisent d'appartenir à une communauté historique.

— *La partie vaut le tout, l'individu la cause, l'exemple l'explication.* Un témoignage de victime, une mort filmée, une bavure condamnent un camp. D'où la tentation du trucage et de la forgerie : fournir à la presse ses cadavres de Timisoara, ses couveuses débranchées, ses villages bombardés, ses Madones douloureuses, ses visages émaciés derrière des barbelés. De l'image un peu esthétisée et un peu posée pour complaire aux goûts de la presse jusqu'à la pure et simple mise en scène, en passant par les images mal légendées, mal montées ou hors contexte s'ouvre le champ miné qui sépare l'erreur de bonne foi de la totale manipulation.

— *Dans la vie civile une bonne part des événements qui nous sont rapportés, sans être nécessairement faux, sont imaginés, préparés, mis en scène, précisément pour être vus.* Dès les années soixante, Daniel Boorstin présentait ce qu'il nommait les pseudo-événements<sup>1</sup> produits pour être reproduits. Il n'imaginait sans doute pas que ce principe toucherait l'événement brusque par excellence : le fait de violence, guerre ou attentat. Désormais, la cause des peuples n'est plus défendue par les poètes et les exaltés : il y a des agences de communication pour cela. Hill and Knowlton remplacent Byron et Hugo quand il s'agit de défendre les intérêts des Koweitiens ou des Bosniaques, et ces intérêts consistent à fournir aux médias leur lot d'atrocités. Les communicateurs du Pentagone, *merchandaient* fort bien une guerre humanitairement correcte : les victimes étaient d'un seul côté. Multiplier ses partisans quand on multiplie les morts suppose de cacher les seconds aux premiers.

1. Daniel Boorstin, *L'Image*, UGE, 1966.

De leur côté, les terroristes sont aussi devenus des maîtres du marketing : leur planning attentats suit leur planning médias. Ainsi le Hamas est particulièrement réputé pour sa couverture image des attentats, et il a été vite imité par les autres branches de l'islamisme. Avant, les martyrs laissent leur testament filmé sur cassette. Pendant, les combattants s'efforcent de filmer les opérations. Après, on fait circuler dans les mosquées et madrasas des cassettes montrant le châtimement des ennemis de Dieu.

— *Dernière leçon de ces guerres de l'image : certains de leurs trucages se révèlent après coup, encourageant le scepticisme de l'opinion.* Qui ne se souvient des fausses victimes de Timisoara ou des cormorans bretons englués dans le mazout d'un prétendu Golfe persique ? D'où un nouveau domaine de la guerre de l'information : la contestation des informations et images adverses, la remise en cause de leur authenticité\*, puis la contestation de la contestation<sup>1</sup>. D'où surtout, une course de vitesse, car il ne sert guère de révéler un trucage trois mois après. D'où, enfin, un effet en abîme de vraies et de fausses images.

## Violence, vision et passion

Il y aura toujours, des « médias de la haine ». La peinture, le livre, l'affiche, le journal ont toujours rivalisé en pouvoir de mobilisation. Le cinéma n'a pas moins excellé à montrer les stéréotypes les plus négatifs. Difficile de surpasser en emphase bel-

1. Dernier exemple en date : des milliers d'internautes ont pu comme l'auteur recevoir successivement par courrier électronique a) la « preuve » qu'une phrase de Jean-Marie Le Pen était recopiée d'un discours d'Hitler au Congrès du NSDAP en 1932 ; b) la « preuve » que c'était faux et que le congrès en question était imaginaire ; c) la « preuve » que tout cela était un complot. Le même jour, on répétait que des drones avaient prouvé que les Palestiniens filmaient de faux enterrements de martyrs (la « preuve » : on voyait un faux cadavre se relever), information aussitôt contestée.



liqueuse certains de ses plus grands chefs-d'œuvre comme *Naissance d'une Nation* ou *Alexandre Nevski*. On se souvient de « Radio mille collines » et de ses appels au meurtre. Au Liban, en Yougoslavie et partout où l'on se massacre, les tubes cathodiques projettent de quoi nourrir les passions les plus agressives. Les médias valent-ils ce que vaut leur contenu, vrai ou mensonger, poussant à la haine ou la connaissance de l'autre ?

À cette vision, un discours sur le pouvoir pacifiant des médias. Dans sa version simple, il affirme que nous ne nous détestons que faute de nous savoir si semblables : plus de communication (sans censure, sans frontière...) entraînera moins de violence. On connaît le programme que Jack London assignait, au cinéma : « Le temps et la distance ont été annihilés par le film magique pour rapprocher les peuples du monde. Regardez, frappé d'horreur, les scènes de guerre et vous deviendrez un avocat de la paix. »<sup>1</sup>. Version moderne : des gens qui aiment Michael Jackson et écoutent CNN ne peuvent pas vraiment se faire la guerre. Version cyber\* : grâce au Web\*, nous échangerons des données, pas des missiles. On sait ce qu'il en est advenu.

Dans une version plus sophistiquée, la télévision, *medium* froid, serait intrinsèquement apaisante. Mc Luhan soutient qu'elle est rétive aux questions brûlantes et aux personnages qui chauffent : « Hitler aurait rapidement disparu si la télévision était apparue à une vaste échelle pendant son règne. Et eût-elle existé auparavant qu'il n'y aurait pas eu d'Hitler du tout. »<sup>2</sup> La télévision, capable d'émouvoir et d'impliquer, mais non d'exciter ou de mobiliser<sup>3</sup>, serait, en somme, rétive à la rhétorique emphatique, au « sublime » qui est selon Kant le registre du discours guerrier.

1. Jack London, *Le Message du cinéma*, in *Profession écrivain*, 10/18.

2. Mc Luhan, *Pour comprendre les médias*, Points, 1977, p. 340.

3. Le même Mc Luhan note pendant la guerre du Vietnam « La guerre de la télévision signifie la fin de la dichotomie entre civils et militaires. Le public participe maintenant à chacune des phases de la guerre et ses combats les plus importants sont livrés par le foyer américain lui-même. » MC Luhan et Quentin Fiore, *Guerre et paix dans le village global*, R. Laffont, 1970.

Cette théorie du gentil *medium* revient dans l'air du temps<sup>1</sup>. On célèbre dans la télévision un des grands facteurs de dédramatisation, de désengagement, de valeurs moins martiales. Ce *medium* soft, qui marche à la séduction, nous parle le langage de l'intimité. Elle nous éloignerait de tout pathos belliqueux. Contribuant à la paix civile, fut-ce en répandant individualisme et scepticisme, mettant sous l'œil de chacun « en temps réel » toute atrocité à l'autre bout du monde, la télévision serait au service de la paix. L'argument est, en somme, que l'on meurt pour des livres, que l'on s'engage « comme au cinéma », mais qu'il est rare que l'on éteigne son poste pour courir au combat.

Possible. Mais qui rendra justice au poids des cultures dans la façon d'éprouver la crainte et l'exaltation ? Par un consensus presque spontané, les médias américains ont refusé de montrer le moindre cadavre du 11 septembre. Dans le même temps, leurs adversaires font circuler en guise de matériel publicitaire des cassettes où l'on voit décapiter un otage au Pakistan, le journaliste Pearle, massacrer des soldats algériens ou exécuter des partisans de l'Alliance du Nord, en Afghanistan. Le même écran qui a rendu la vision des victimes insupportable aux uns la rend exemplaire et exaltante pour les autres. Dans le monde de l'image la maîtrise des flux n'est pas celle de la réception. Sinon, tout le monde serait proaméricain. Le diplomate américain Richard Holbrooke se demandait : « Comment se fait-il qu'un type dans une caverne puisse gagner la bataille de la communication contre la première société de l'information\* au monde ? »<sup>2</sup> Bonne question !

Cela parce que le terrorisme moderne, guerre sans armée et crime d'écran, reflète une nouvelle relation du faible au

1. Notamment par Gilles Lipovetsky dans *L'Empire de l'éphémère*, NRF, 1987.

2. Cité par David Hoffman dans *Beyond Public Diplomacy*, in *Foreign Affairs*, mai/avril 2002 (<http://www.foreignaffairs.org>).

fort. Il a sa polémologie : l'attentat représente un rapport coût / résultat incomparable : des armes rustiques et quelques kamikazes pour un effet maximal de perturbation, d'incertitude et de dispersion des forces ennemies. Mais l'attentat a aussi sa médiologie. Le groupe terroriste, société secrète spectaculaire, compte sur les vecteurs de l'adversaire pour amplifier son message. Il lui faut, contrairement à lui, multiplier les images de cadavres. Quantitativement, puisque plus d'horreur signifie, pour le camp adverse, plus d'humiliation symbolique et un coût moral insupportable. Qualitativement, notamment par le choix de la victime. Elle est significative soit par ses responsabilités ou sa visibilité, un chef d'État, par exemple, ou un fonctionnaire « complice de la répression », soit par son anonymat qui révèle qu'aux yeux du terroriste nul n'est innocent. Dans le premier cas, la victime, physiquement touchée, et la cible symboliquement visée coïncident peu ou prou<sup>1</sup>. Dans le second, elles diffèrent au maximum, preuve que le terrorisme emploie la victime comme signe capable de produire plus de ravage politique par la publicité de sa mort que par sa mort même. Des théologiens islamistes fondamentalistes ont récemment expliqué que tuer une femme, fut-ce une simple passante en territoire ennemi, n'était pas vraiment tuer une innocente : les femmes paient des impôts qui contribuent à l'effort de guerre des oppresseurs. Et puis, si elles ne protestent pas contre l'injustice, ne sont-elles pas un peu complices de la violence des puissants, à laquelle ne fait que répondre la contre-violence du terroriste ? À ce compte-là, pourquoi ne pas massacrer les bébés : ils seraient bien capables de devenir soldats ou policiers, une fois adultes ?

1. Elles coïncident presque totalement dans le cas du tyrannicide, héritier du régicide : mais c'est une forme de crime politique, pratiqué depuis toujours, et qu'on ne peut pas qualifier de terrorisme, puisqu'il vise un homme et non une idée.

## Terreur d'écrit, terreur d'écran

L'idée que le terrorisme est une « violence aveugle », donc irrationnelle, donc nihiliste est fautive. Les poseurs de bombe ne résolvent pas des problèmes de libido ni ne manifestent une attirance métaphysique bizarre, un peu gnostique<sup>1</sup>, pour l'apocalypse. Ils appliquent une méthode rationnelle d'utilisation optimale de moyens en vue d'une fin. Cela ne signifie pas que les terroristes, individuellement, jouissent d'un équilibre psychique remarquable, ou qu'il faille considérer comme normale leur attirance pour la mort, celle des autres ou la leur (car contrairement à une idée reçue, les attentats-suicides sont très répandus tout au long de l'histoire du terrorisme). Cela signifie que, dans la bizarre comptabilité du terrorisme, du point de vue de sa rationalité instrumentale, chaque mort doit « rendre ». Ceci est vrai et en terme d'affaiblissement de l'adversaire, et en terme de plus-value publicitaire, d'amplification du message, si l'on préfère. Montrer les morts, les siens et ceux que l'on fait, est, dans cette optique, rationnel et souhaitable.

Ceci vaut pour toutes les formes de terrorisme, mais pas de la même façon. Globalement, on connaissait jusqu'à présent trois formes de terrorisme, classées en fonction de leurs objectifs politiques.

— *Un terrorisme « vertical »* (de type révolutionnaire) qui se propose de renverser l'ordre établi (l'autocratie comme disaient les terroristes russes de la fin du XIX<sup>e</sup> siècle). Dans le cadre d'une stratégie d'ébranlement du système, l'acte terroriste doit servir de préalable, voire d'accélérateur, à la mobilisation du peuple contre ses tyrans et à la révolution. Le but est de détruire l'État ou les institutions.

1. La thèse de l'origine « gnostique » du terrorisme a été soutenue, notamment par Jean Servier, *Le Terrorisme*, PUF, 1979.

## Captures d'écran

— *Un terrorisme « territorial »*, anticolonialiste par exemple, qui entend chasser un occupant, ou un groupe allogène. Ici, il s'agit d'une stratégie de découragement, qui peut être complémentaire de la guérilla et de la négociation politique : décourager la puissance étrangère jusqu'à la faire partir. L'objectif est la libération.

— *Un terrorisme instrumental de pure contrainte*. Il s'agit, dans le cadre d'une stratégie de menace et de négociation, d'obtenir un avantage précis, comme la libération d'un prisonnier, ou un renoncement (qu'une puissance étrangère cesse de soutenir telle faction ou de s'interposer dans tel conflit, p.e.). Une telle action qui peut parfaitement être commanditée par un État est en principe limitée à ses objectifs précis. En France, les campagnes terroristes de 1986 — celle de l'attentat de la rue de Rennes — et 1995 — celle du métro Saint-Michel —, l'illustrent bien. Il s'agit d'une relation de coercition, limitée dans le temps et dans ses objectifs, entre le terroriste « prédateur » et le détenteur d'une autorité ou d'une ressource qui peut être l'argent ou l'accès aux médias...

Bien entendu, ces trois modèles peuvent se mêler : on a souvent vu des groupes exercer un chantage du troisième type, dans le cadre d'une lutte de libération nationale, mais dont la finalité proclamée serait l'effondrement du capitalisme international.

Dans tous les cas, qu'il s'agisse a) de détruire l'autorité et de propager l'exemple de son propre sacrifice auprès des opprimés, ou b) de radicaliser les rapports entre deux groupes « ethniques », ou enfin c) de rendre la situation insupportable à un gouvernement ou à une institution en choquant l'opinion publique, intervient l'horreur de la mort. Elle est recherchée pour son effet direct : terroriser au sens étymologique, provoquer une peur exceptionnelle qui fait trembler, donc paralyse. Mais elle est aussi recherchée pour son effet indirect : « souligner » ou crédibiliser le message idéologique, dramatiser les relations entre deux grou-

pes, attirer l'attention de l'opinion internationale, servir d'exemple ...

En ce domaine, peut-être faudra-t-il distinguer des traditions culturelles terroristes : gens de l'écrit et gens de l'écran. À quelques jours près, en mars et avril 2002, on a pu en voir deux exemples. Les Brigades rouges italiennes (ou ceux qui prétendent reprendre leur nom et leur filiation) ont accompagné l'exécution de l'économiste Biaggi par un communiqué incroyablement verbeux de 26 pages sur copie carbone<sup>1</sup>. Quelques jours plus tard, le 15 avril 2002, al Jazeera reçoit une cassette avec une déclaration-testament d'un des terroristes du 11 septembre. Al Hazwami, sur fond de tours en flamme de Manhattan, par un montage qui chahutait la chronologie, comme un générique de film, annonçait qu'al Quaida allait porter la mort sur le territoire américain. La séquence suivante montrait Ben Laden lui-même se félicitant de cette victoire. Entre le discours abstrait de légitimation tenu par les terroristes, la façon dont ils éprouvent le résultat de leurs actes et les moyens qu'ils emploient pour le faire savoir, il y a des gouffres.

Visiblement, le nouveau terrorisme est tout à la fois mystique dans ses objectifs et pragmatique, par sa compréhension des systèmes de communication de l'adversaire et des pouvoirs de l'écran. Le 11 septembre, c'étaient d'abord des images. Comme icônes (l'expression est de Ben Laden), elles représentaient l'ennemi (les juifs et les croisés, dans sa terminologie), et, au-delà, le monde séculier. Mais ces images étaient aussi mises en scène en vue d'un effet de panique, voire d'affirmation d'un nouveau statut du terrorisme comme forme de guerre du futur.

Il se pourrait aussi que ce nouveau terrorisme échappe aux trois catégories établies plus haut et qui sont fortement mar-

1. Les amateurs, s'il y en a, trouveront l'intégrale sur <http://www.caserta24ore.it>, page du 21 mars.

## Captures d'écran

quées par une vision classique de la politique, centrée sur l'État qu'il faut renverser, chasser ou contraindre. Il se pourrait enfin que son ambition ne soit pas vraiment de l'emporter politiquement, au sens de faire céder la volonté d'un adversaire. Son but serait de se confondre avec une affirmation symbolique. Une revanche en image contre le monde de l'image ?





## Seconde partie

### Quand l'écran *occulte* l'ennemi La maîtrise dans l'invisible

Les stratèges de l'Antiquité le savaient : la meilleure façon de vaincre est d'agir sur les plans de l'adversaire<sup>1</sup>. Le tenir dans l'incertitude, augmenter son indécision est utile. Leurrer, pousser à la faute est plus efficace encore. Toute stratégie de l'action est art de la surprise : ne pas faire ce qui était attendu. Toute stratégie de l'information ou de la perception y contribue : par la vision claire qu'elle procure, comme par l'incertitude ou l'erreur où elle plonge l'adversaire. Le but est la paralysie de *l'Autre* soit directement en lui suggérant la décision erronée, soit indirectement en lui faisant perdre des soutiens. Si le stratagème consiste toujours à amener la victime à accomplir vos desseins, alors qu'elle croit qu'ils servent les siens, les technologies de communication bouleversent la façon d'appliquer ces recettes éternelles.

On ne dissimule pas les mêmes mystères avec des hiéroglyphes ou des algorithmes, on ne trompe pas de la même façon les conseillers du Prince et l'audience de CNN. On ne domine

1. Ces questions sont débattues sur un site consacré à la pensée stratégique : <http://www.stratego.tv>.

pas de la même façon à l'époque des ordres portés à cheval ou à celle des réseaux. Ce qui peut être caché, et comment et pourquoi, varie en fonction des moyens de reproduction et de mémorisation. La technologie démocratise autant la capacité de nuire et d'interdire de savoir que la capacité de savoir.

Enfin et surtout, la lutte par le secret, le leurre, le discrédit, déborde ses domaines traditionnels pour envahir l'économie ou des pratiques « culturelles » mobilisant les ressources numériques. Autre abaissement du seuil : la capacité de traiter l'information, multipliée par vecteurs médiatiques, favorise le passage au conflit, la recherche du dommage et non plus du simple avantage. De nouvelles conceptions stratégiques, et de nouveaux mots — infoguerre\*, guerre cognitive, guerre économique\*, domination informationnelle — reflètent ces bouleversements.

L'asymétrie\* caractérise ces relations de secret, de désinformation, ou de guerre de l'information, mais révèle des vulnérabilités du côté du « fort » qui est souvent aussi le visible.

Quand le pouvoir consiste à savoir avant les autres, à savoir ce que savent les autres et à faire savoir aux autres, secret, les voies d'accès à la puissance ne changent pas moins que les obstacles à la puissance.

## Chapitre III

### Secret et conflit : de la ruse à la dominance

Hors écran, hors de notre vue, où réside le pouvoir ? Les véritables batailles se gagnent-elles à notre insu ? Nos maîtres invisibles les ont-ils déjà remportées ? Cette hypothèse, un rien paranoïaque, émane de critiques radicaux comme Guy Debord qui voit dans le secret généralisé la « plus importante opération<sup>1</sup> » de la société du spectacle, son cœur même. Et le père du situationnisme d'énumérer les traits principaux du « spectacle » : renouvellement technologique incessant, fusion économique-étatique, secret généralisé, faux sans réplique, présent perpétuel. C'est une des plus brillantes variantes de la théorie du totalitarisme invisible. Elle dénonce toujours l'ordre établi comme un mécanisme de maîtrise des esprits par simulation, stimulation et dissimulation. Ce n'est pas ce qui sera défendu ici. Notamment par crainte de retomber dans le « On nous cache tout, on ne nous dit rien. Tous des menteurs » qui retentit à tous les comptoirs.

En revanche, il faut considérer l'hypothèse qu'une société qui se voue à l'élimination de l'aléa, du risque et de l'affrontement, une société comme la nôtre, obsédée par l'authenticité et

1. Guy Debord, *Nouveaux commentaires sur la société du spectacle*, aphorisme 21.

l'expression, ne favorise pas son contraire apparent. Le progrès des technologies de communication ou de *monitoring* ne fait pas reculer celles du camouflage et de la falsification. Au contraire.

## Spectacle et secret

Revenons sur cette notion ressassée d'une société « de » l'information. Société du savoir pour les optimistes : la connexion des intelligences et le partage des connaissances rendront désuète toute politique de rétention de l'information. Société du spectacle, pour les critiques : nous nous épuisons à poursuivre et consommer des signes, et sommes prisonniers des apparences. Société de l'exhibition, peut-être : à l'ère de *Loft story*, des *Web cams*, des *psysshows*, chacun, de l'homme politique au *manager* branché, dévoile sa personnalité voire son intimité. Histoire d'être « star un quart d'heure », de « changer le regard des autres » ou « d'être visible », on montre tout : âme, fesses et confesse.

Juges et caméras pourchassent les mystères. Internet\* se rit des censures et des frontières. Les hommes politiques promettent plus de clarté et moins de langue de bois. De la transparence dans la politique, nous passons à la transparence de la politique, devenue art d'exprimer et satisfaire des « demandes ». L'entreprise se veut communicante et ouverte. La vie privée fait le succès public. Quelle place, alors, pour l'archaïque secret ? Baudrillard répond : « Que deviennent les choses jadis secrètes ? Elles deviennent occultes, clandestines, maléfiques : ce qui était simplement secret, c'est-à-dire donné à s'échanger dans le secret, devient le mal et doit être aboli, exterminé. »<sup>1</sup>

Les forces dominantes, les « quatre M. » déjà évoqués, semblent bien sonner le glas du secret :

1. Jean Baudrillard, *Mots de Passe*, Pauvert, 2000, p. 44.

## Secret et conflit : de la ruse à la dominance

— *la Mondialisation* : elle fait circuler choses, gens, idées, images.

— *le Marché* : il suppose l'échange généralisé.

— *les Médias* : les médias de masse mettent tout sur la place publique du village global ; les nouveaux médias informatiques offrent toutes les données « où je veux, quand je veux, comme je veux ».

— *la Morale ou plutôt le Moralisme* triomphe : contre les systèmes autoritaires, les lois du silence ou les discriminations, il se réclame des différences et des transparences, du débat public, de la libre expression.

Pourtant, tout indique, sinon que le secret soit partout — et la vérité ailleurs — du moins que la lutte par, pour et contre le secret s'étende<sup>1</sup>. Les indices pullulent : événements étouffés, données sensibles dissimulées. Ils laissent supposer des politiques de rétention, surveillance, dissimulation, pénétration, déception\* impliquant des acteurs étatiques et infra-étatiques, économiques et idéologiques, des groupes et des particuliers.

Quelques indices :

Le nombre de documents classifiés (des millions !) augmente<sup>2</sup>.

Les révélations vraies ou fausses sur diverses formes d'Omerta dans nos sociétés : agissements de pédophiles, turpitudes financières des partis politiques ou divers scandales de type épidémies agroalimentaires.

Les fameuses « grandes oreilles » de la *National Security Agency*, qui, soit dit en passant, ont fait négliger la formidable montée en puissance de la NRO\*, *National Recognition Organization*, les « yeux » des satellites espions<sup>3</sup>.

1. Par allusion à la définition classique de la guerre de l'information comme guerre « par, pour, contre » l'information.

2. Pour les USA voir Moynihan D. P., *Secrecy : The American Experience*, Yale University Press, 1998.

3. Il suffit d'aller se renseigner à la source : <http://www.odci.gov>.

Les luttes quotidiennes des internautes pour le droit de crypter, contre le traçage, et le fichage, pour la protection de la vie privée<sup>1</sup>.

La place dans les doctrines militaires et géostratégiques<sup>2</sup> de notions comme la domination informationnelle, le *panoptisme*<sup>3</sup>, ou *l'intelligence totale*, via le cyberspace\* et l'espace stratosphérique<sup>4</sup>.

Les affaires d'infoguerre économique : elles se résument généralement à des affaires de vrais secrets violés ou de faux secrets révélés pour déstabiliser<sup>5</sup>.

Alors, vrai ou faux ? Ou encore, bon secret du citoyen, ultime refuge de la liberté, versus mauvais secret, celui du Système, de *Big Brother*\* ?

Il faut en revenir à la définition du secret, ou plutôt à sa composante conflictuelle : le secret est secret contre quelqu'un dont il faut se protéger et qui est un concurrent ou une menace.

Le secret est une information que son détenteur rend délibérément inaccessible<sup>6</sup>. C'est une relation duale et dramatique qui le place « au fond le plus intime de la puissance » pour Elias Canetti<sup>7</sup>.

1. À titre d'exemple, voir <http://www.amanet.org/research/monit/>, <http://www.delis.sgdg.org>, <http://www.eff.org>, <http://www.iris.sgdg.org>, <http://www.itinerant.qc.ca/flicage2.htm...>

2. Voir une présentation des aspects militaires, mais aussi idéologiques, économiques et sociaux de ces phénomènes dans la revue *Panoramiques* n° 52, *L'Information c'est la guerre*, <http://www.editions.corlet.fr/panoramiques/sun/>.

3. Voir glossaire pour le sens militaire de ce mot, à ne pas confondre avec le *Panopticon* ou panoptisme du philosophe Jeremy Bentham (1748-1832), popularisé par Michel Foucault dans *Surveiller et Punir*.

4. On trouve des glossaires de ce vocabulaire de la nouvelle stratégie et de la guerre de l'information sur <http://www.psycom.net/iwar.2.html>.

5. Voir Didier Lucas et Alain Tiffreau, *Guerre économique et information*, Ellipse, 2001.

6. Pour plus de détails sur cette définition voir notre propre ouvrage : Huyghe F.B. et E., *Histoire des secrets*, Hazan, 2000.

7. Voir le chapitre que l'auteur de *Masse et puissance* consacre au secret (Tel Quel, 1977)

## Secret et conflit : de la ruse à la dominance

Son essence, à suivre l'étymologie, est d'être séparé, exclu. Or, une telle opération ne se fait pas sans travail ni résistance, sans peine ni opposition. Qui a un secret a nécessairement un adversaire, fut-il virtuel, qui menacerait le secret s'il venait à en apprendre l'existence. Cet adversaire, ce peut être le détenteur du secret lui-même. La psychanalyse nous enseigne combien nos propres secrets nous menacent autant que nous les menaçons. Supposant interrelation et tension, le secret est une des formes, des causes et des moyens du conflit, au moins autant qu'un moyen de l'éviter. Ce n'est pas seulement un facteur discriminant — entre ceux qui possèdent le secret et ceux qui en sont exclus — ni uniquement une composante du pouvoir : c'est un processus.

Un secret pour personne n'existe pas, sinon sous la forme plaisante du secret de Polichinelle. Un secret sans détenteur serait une contradiction dans les termes. Un secret sans objet est apparence ou farce. N'étant ni l'invisible, ni l'ineffable, ni l'incompréhensible, ni l'inconnu même s'il en adopte les apparences, le secret n'est pas non plus le mystère. Le mystère émane de choses qui échappent, et, peut-être, échapperont toujours à notre intelligence. Le secret suppose des gens qui possèdent une information et ne la laissent pas connaître à d'autres. Il doit être connu d'au moins une personne et caché à une autre. Il doit pouvoir s'énoncer sous forme de description d'une réalité vraie ou fausse. Qu'il porte sur une information vraie ou fausse n'y change rien.

Bref, pour qu'il y ait secret, il faut qu'il y ait risque réel ou imaginaire. Valorisé négativement quand sa perte entraînerait un dommage, le secret peut l'être positivement : celui qui est seul à détenir l'information, réalise des performances particulières ou, plus simplement, vend son information rare. Mais cette valeur positive renvoie toujours à la notion de perte. Le secret ne vaut que tant qu'il est contrôlé et que l'on sait *qui* sait. Il implique une crainte : crainte d'un événement (si on savait mon secret je serais arrêté, par exemple), d'un jugement (je serais déshonoré) ou de

la perte d'une exclusivité (je ne serais plus le seul à pouvoir faire ceci). Il suppose antagonisme en puissance envers un adversaire concret ou une force abstraite Loi, Opinion, Société. Secret égale immunité, rareté ou supériorité.

Cette trilogie détenteur-contenu-menace appelle un quatrième élément : la protection. Il faut des moyens matériels pour maintenir ce rapport délibéré et asymétrique. Il se peut que l'existence même du secret soit ignorée, et que seul le détenteur puisse le trahir et se trahir par un aveu ou une maladresse. Dans ce cas limite, la situation est simple : silence égale secret. Ce serait une stratégie d'abstention qui consisterait à ne pas dire, ne pas trahir, agir sur soi, ne pas laisser filtrer d'indice. Mais elle en suggère d'autres : stratégies de rétention, contrainte, ou confusion.

Parfois, le secret requiert des manœuvres complexes : dissimulation ou protection de traces physiques — enfermer un document dans un coffre, interdire une zone d'accès — ou dissimulation des signes et signaux — chiffrement\* par exemple<sup>1</sup>, stéganographie<sup>2</sup> ou tactiques de *déception*<sup>3</sup>. Enfin, il y a la con-

1. Sur la théorie du chiffrement voir notre article « Le code paradoxal » dans *Stratégies du moins*, n° 9 des *Cahiers de médiologie*, disponible sur <http://www.mediologie.com>.

2. Art de recourir à des cachettes sur le corps humain, à des encres sympathiques, à des supports truqués, à des microfilms, bref de rendre invisible le support physique du message, par opposition avec la cryptographie qui consiste à transposer un message clair en un ensemble de signes incompréhensibles aux non-initiés, et ce par l'usage d'un code ou chiffré. C'est la différence entre la lettre volée d'Edgar Poe et son Scarabée d'or. À noter : l'affirmation selon laquelle les réseaux d'al Quaida auraient recouru à la stéganographie sur Internet, notamment en insérant des messages dans des images sur des sites accessibles à tous, n'a jamais été prouvée. Il se pourrait qu'il s'agisse d'une légende technologique. Voir <http://www.hackermag.com/indexben2.html>.

3. Au sens que tend à donner la pratique actuelle à ce mot, c'est-à-dire proche de celui de tromperie ou désinformation. Un dictionnaire stratégique américain la définit brutalement : « *Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.* » (*DOD Dictionary of Military Terms* précité).



trainte pure et simple. Elle peut consister en une menace, celle des foudres de la loi, des lois de l'honneur de l'omerta mafieuse ou de la colère divine.

Le secret repose autant sur des moyens techniques de maîtriser traces, signes ou gens, sur des organisations et sur des puissances symboliques, des croyances partagées. Ceci est d'autant plus vrai que l'on recourt à des outils ou processus de haute technologie pour conserver, transporter ou traiter de l'information<sup>1</sup>. Le secret aussi est au carrefour du technique et du symbolique, mais aussi du polémologique<sup>2</sup> puisque lié au conflit.

## Les liens du secret

Un des premiers grands sociologues, Georg Simmel<sup>3</sup>, décrivait le secret comme le contrepoint de l'interdépendance et de la confiance nécessaire dans tout groupe humain. Le secret peut porter sur le passé (qui a fait quoi), sur le futur, un plan, un traité, une conspiration (qui fera quoi) ou sur un présent virtuel (comment faire quoi) : c'est le cas des procédés qui permettent de rééditer une performance, une formule, un plan.

Surtout, il est présent comme une constante dans tout ce qui nous réunit<sup>4</sup> : la croyance, le politique, la production. En même temps, sa forme et son ampleur dépendent de facteurs historiques et technologiques.

1. On trouvera un point très éclairant sur cet aspect des technologies numériques dans Martin D. et F.P., *Cybercrime : menaces, vulnérabilité et ripostes*, PUF, 2001. Le site des auteurs : <http://www.cybercriminstitut.com>.

2. La polémologie (voir glossaire) de Gaston Bouthoul tentait d'expliquer les causes de l'explosion récurrente de violences collectives, pourquoi ne pas imaginer d'étudier de la même façon les corrélations entre les territoires du secret et les luttes qu'ils suscitent et des faits sociaux ou culturels ?

3. Simmel G., *Le Conflit*, Circé, 1995 et *Secret et sociétés secrètes*, Circé, 1996.

4. Pour d'autres exemples, voir *Secret et lien social*, dirigé par André Petitat, L'Harmattan, 2000, actes du colloque *Secret et société* de l'université de Lausanne.

Ainsi, il hante le sacré, dont le domaine déborde celui de religion, notion occidentale tardive. Des rites magiques aux théologies monothéistes en passant par les cultes à Mystères, partout une forme quelconque d'initiation, donc de secret. Suivant une tendance peut-être universelle, un enseignement conférant des pouvoirs ou un statut, comme celui du jeune chasseur africain ou de l'acousmate, celui qui a « entendu » la doctrine, de la secte de Pythagore, ne se délivre pas sans rites, épreuves et serments. La transmission est réservée à un impétrant spirituellement préparé et fiable. Faute de quoi la connaissance folle ou dangereuse serait profanée.

Souvent, une forêt de symboles, un enchevêtrement d'indices ou d'arcanes sont censés protéger le secret des dieux ou du Cosmos. Sous des formes différentes, les trois monothéismes connaissent la tentation ésotérique voire gnostique : réinterpréter l'Écriture sacrée ou la Création comme un cryptogramme. Entre l'initiation qui consiste à maîtriser la transmission pour protéger la vérité, et l'ésotérisme qui suppose un sens dissimulé derrière le sens apparent, le sacré est toujours entouré de défenses.

Ce n'est pas moins vrai pour l'économie. Le secret est un moyen de produire de la rareté, donc d'augmenter ou de conserver une valeur<sup>1</sup>. Cette rareté peut être celle des moyens. Garder le secret d'une technique, de l'emplacement d'une ressource, en constitue la forme la plus évidente. Il y a avantage à se réserver l'accès ou la fabrication de richesses. Ce fut vrai, des siècles durant, pour des matériaux ou des objets : soie, verre, épices, poudre, papier, porcelaine ont, suivant les périodes, fait la fortune de leurs détenteurs exclusifs. À l'époque industrielle, la formule du Coca-Cola ou tout autre secret protégé par des brevets ou des coffres-forts ont constitué un capital inestimable. C'est encore plus vrai avec la dématérialisation\* de l'écono-

1. Voir le dossier *Règles, ruses et usages du secret* dans le n° 50 (janvier 2002) de la revue *Veille* : <http://www.veillemag.com>.

## Secret et conflit : de la ruse à la dominance

mie. Quand celle-ci consiste, comme actuellement, à « vendre » de la connaissance ou des états de conscience, à gérer des propriétés intellectuelles, le secret devient la seule protection contre la duplication, rendue facile par le numérique, et le seul remède contre le piratage.

L'instrument de l'échange lui-même, l'argent, suppose un secret : il faut bien qu'une autorité ait le monopole de sa prolifération. Ceci peut s'obtenir par un identifiant, tel le filigrane d'un billet pour en empêcher l'imitation. Un système bancaire ou financier est une machine à gérer du secret, celui des comptes bancaires ou des transactions électroniques. Désormais, des méthodes sophistiquées combinant cryptographie\* et moyens de surveillance assurent que le paiement\* émane bien d'un tel, qu'il est bien valable, sans dévoiler pour autant la nature de la transaction, ni celle des moyens de certification.

Un domaine de l'activité humaine entretient un rapport essentiel avec le secret : le politique. C'est une activité conflictuelle opposant des groupes poursuivant des finalités inconciliables. Sa pratique incite au secret quand il s'agit de surprendre et protéger. Des conspirateurs qui se dissimulent, une censure qui recèle des documents, une police secrète, d'autant plus efficace que les citoyens en ignorent les pouvoirs effectifs et les crimes réels, trois moyens au service d'un même dessein : conserver l'avantage contre l'adversaire, fût-ce le peuple qui pourrait se soulever. Il faut dissimuler les moyens qu'on emploie, cacher ses fins, se rendre imprévisible, impressionner ceux qui ignorent la source et l'étendue de ses pouvoirs. Ces principes-là sont immémoriaux.

Des siècles avant notre ère, les philosophes chinois de l'école des « légistes » avertissaient de la nécessité politique du secret :

« Le Prince a perdu son mystère / Des tigres s'attachent à ses pas » résumait le livre de Han Fei<sup>1</sup>.

1. *Han-Fei-tse ou le Tao du Prince*, Seuil Points, 2000, in *Manifeste doctrinal* p. 107. Ce livre date du III<sup>e</sup> siècle avant notre ère.

Ce classique chinois fait l'éloge de qui « ne révèle point ses ressorts ». Notre propre tradition philosophique n'ignore pas l'efficacité de la ruse, la Métis des Grecs, ni ne néglige l'art de cacher pour surprendre.

À la Renaissance, la pensée politique européenne fait du secret une *virtu*, une qualité de l'homme d'exception. Ce caractère rend son possesseur plus redoutable (« Qui ne sait dissimuler ne sait régner » disait Louis XI). L'art du Prince est de surprendre. Ce principe est celui des « arcanes », méthodes occultes du souverain, arme d'exception répondant à des fins exceptionnelles<sup>1</sup>. Le jésuite Gracian voit dans le secret « le sceau de la capacité » car c'est « la marque d'une supérieure maîtrise de soi et se vaincre en cela est un triomphe véritable ».<sup>2</sup>

En politique, le secret politique est souvent plus trivial. Souvent, il repose sur un méta-secret : le secret de ce qui est secret. Comme l'instance politique détermine, en principe, la forme et l'intensité du conflit sur son territoire, elle contrôle le droit du secret et le droit au secret. Elle l'autorise à certains — secrets de l'intimité, de la vie privée — elle l'impose à d'autres — secret Défense ou secret d'État. Elle en contrôle les instruments. C'est ce que démontre l'interdiction faite aux citoyens de posséder ou d'exporter des logiciels de cryptologie trop puissants, au même titre que des armes de guerre<sup>3</sup>. Chaque jour, l'État dessine les territoires du secret, celui des citoyens entre eux, celui de l'État à l'égard des citoyens et celui des citoyens face à l'État.

1. Carl Schmitt, dérangeant penseur du tragique politique, donne beaucoup d'importance à ces notions, liées à l'idée d'état d'exception, dans son étude sur *La Dictature*, republiée aux PUF en 2000.

2. Baltazar Gracian, *Oraculo Manual*, n°179 dans le livre d'aphorismes repris sous divers titres dont « *Le courtisan* » ou *Manuel de poche d'hier pour hommes politiques d'aujourd'hui*, Éditions libre Hallier, 1978. On peut notamment en trouver une version sur <http://www.00h00.com>.

3. Ce fut le cas en France, jusqu'à ce que les logiciels de cryptologie (jusqu'à 128 bits) soient rendus accessibles au public en 1999.

Le régime le plus démocratique suppose de tels droits, ne serait-ce que celui du vote ou de la correspondance. Ils protègent la vie privée et l'exercice de la pensée et limitent la connaissance que les individus peuvent acquérir sur leurs vies respectives. Enfin, ce même système démocratique ne peut totalement renoncer à dissimuler, pour conserver sa liberté d'action : procédés, fonds, services, traités secrets, et autres attributs d'une raison d'État échappent au droit ordinaire. Quant aux États totalitaires, le secret leur est consubstantiel : la différence entre porteurs de secret et ignorants recouvre celle des maîtres et des esclaves. Chacun se méfie de l'autre, personne n'ose dire à haute voix des vérités connues de tous, des « secrets ouverts »<sup>1</sup>. Chacun devient complice du silence général, renforce le pouvoir qui le surveille et occulte des pans entiers de réalité la plus évidente : l'existence du goulag, ou celle des villes stratégiques dites secrètes, non mentionnées sur les cartes, en ex-URSS.

## Les luttes du secret

Tout confirme la parenté du secret et du conflit : enjeu, lutte pour connaître le secret ou le défendre, arme, dissimulation des moyens ou des objectifs, voire mode d'évitement du conflit par le secret. Le secret est une relation duale, où les objectifs de chacun des camps sont incompatibles<sup>2</sup> et où chacun s'efforce de vaincre la résistance de l'autre, passivement ou activement.

1. C'est un processus que décrit très bien Hannah Arendt dans *Vérité et politique*, in *La Crise de la culture*, Folio, 1989.

2. On pourrait objecter qu'il existe des secrets de pudeur, de plaisanterie ou des secrets « de pitié » — par exemple celui qui consiste à ne pas révéler son état désespéré à un malade — et que ces secrets n'ont rien d'agressif. Mais ils supposent, même pour la bonne cause et même sous une forme très atténuée, une forme de conflit et de tromperie.

Le rapport secret/menace/protection se retrouve à l'état pur dans une forme d'organisation qui a fasciné les esprits les plus aigus<sup>1</sup> : la société secrète. D'un côté elle touche au crime puisque toute association qui tente d'échapper à la répression ou à la dénonciation adopte peu ou prou la forme clandestine. À l'opposé, des organisations qui se proposent des buts, en principe hautement moraux, recourent à une discrétion extrême pour couvrir des activités que nul ne songe à interdire. Un compagnon du Devoir, un membre de l'*Opus Dei*, un franc-maçon peuvent difficilement se mettre dans le même sac que les triades, les hachichins ou les « dragons sublimes » du Ku Klux Klan. Pourtant ils s'engagent tous à une obligation de silence. Elle est très variable quant à ses objets. Ce peut être de ne pas révéler l'existence de la société sous peine de mort, mais aussi, bien plus banalement, d'éviter de proclamer l'appartenance d'un Maçon à la même loge que vous<sup>2</sup>, l'éventail est donc vaste.

D'un côté, la société secrète ressemble à une secte : elle fait littéralement scission du monde et dote de rites et symboles, de codes de reconnaissance, pour réserver aux élus la révélation de doctrines. De l'autre, la société secrète imite souvent l'organisation et l'idéologie d'un groupe de combat clandestin de type conspiration, armée secrète ou « branche armée ». Entre les deux, toutes les formes possibles d'entraide, de défense d'intérêts, de partage d'informations, d'influence et de réseaux, de règles implicites et de buts inavoués.

Un modèle commun est donc difficile à dresser qui inclurait aussi bien les pythagoriciens que les Tai Ping, une loge de rites écossais que les Frères de la Pureté, les *carbonari* que les *hackers* \*

1. Outre le livre précité de Georg Simmel sur *Secret et sociétés secrètes*, on trouvera d'autres réflexions sur la société secrète aussi bien chez Roger Caillois (*Instincts et société*, Gallimard, 1954) que chez Deleuze (Deleuze G. & Guattari F., *Mille Plateaux*, Paris, Éditions de Minuit, 1980).

2. Un des rares « secrets » auxquels s'engage encore le franc-maçon. Pour les autres, il y a des milliers de livres et d'articles pour les révéler.

comme les Maîtres de la déception. Restent pourtant, deux caractéristiques des sociétés secrètes ou assimilées : l'allégeance et la protection.

L'allégeance, qui suppose souvent une sorte de serment de fraternité, établit une distinction entre la loi des membres et celle des hommes ordinaires. Le membre de la société se lie à un système d'obligations, dont celle du secret est la clef de voûte. Il se soumet à des contraintes souvent bien plus exigeantes que celles qui pèsent sur le commun des mortels. Il se plie souvent avec enthousiasme à cette discipline, et c'est peut-être elle qui l'attire vers la société secrète. Quant à la protection, elle est multiforme : protéger les membres de la répression, la doctrine de la corruption, ou la stratégie suivie de la révélation. Qui dit protection dit clôture.

Ce qui nous renvoie, une fois encore, à l'hostilité comme moteur du secret, décrit par Deleuze et Guattari : « Le secret a son origine dans la machine de guerre... Une société secrète agit toujours dans la société comme une machine de guerre... Toute société secrète comporte son mode d'action, lui-même secret, par influence, glissement, insinuation, suintement, pression, rayonnement noir, d'où naissent les « mots de passe » et langages secrets... »<sup>1</sup>.

Si, par définition, nous ignorons presque tout des sociétés dites secrètes, nous constatons l'extraordinaire réceptivité de l'opinion à tout discours sur une conspiration, une main cachée qui dirigerait dans l'ombre une supposée complicité des autorités et des médias, un trucage révélé<sup>2</sup>. Cela pourrait s'expliquer par l'éternelle tendance de l'esprit humain à admettre toute explication qui suppose un arrière-monde occulte mais cohérent. Mais le phénomène se nourrit aussi de la crise de crédibilité des médias. La floraison des moyens de voir,

1. *Mille Plateaux*, précité, p. 352.

2. À titre d'exemple sur le conspirationnisme fleurissant aux USA, voir <http://www.conspire.com> : « les 70 plus grandes conspirations de l'histoire ».

savoir, de transmettre, de comparer stimule la croyance dans le secret. Pour ne prendre qu'un seul exemple : un livre qui a eu des dizaines de milliers de lecteurs, soutient qu'aucun Boeing ne s'est écrasé sur le Pentagone le 11 septembre 2001 : les dégâts auraient été provoqués par un explosif, que des « Ils » mystérieux auraient placé là. Ces gens seraient donc assez habiles pour faire volatiliser un avion et tromper des millions d'Américains et auraient réalisé un trucage si grossier qu'un internaute français l'aurait décelé sur simple photo. Toute théorie de la manipulation est bonne à prendre et à répandre pourvu qu'elle proclame que la réalité est le contraire de la vérité officielle.

Internet est le foyer de pareilles théories « conspirationnistes », surtout Outre-Atlantique<sup>1</sup>. Bref, si nous ne savons donc pas grand-chose de l'existence réelle des sociétés secrètes, nous pouvons constater leur étonnante vitalité dans le monde virtuel.

La technologie numérique rend la notion de secret plus protéiforme que jamais. Le secret protégeait depuis toujours contre l'imitation, la dénonciation ou l'anticipation — disons contre le Même, le Supérieur, l'Adversaire. Il a acquis d'autres fonctions. Désormais il garantit contre la localisation dans l'espace, le traçage dans le temps, le profilage, la prédiction de comportements, la prise de commande, celle d'un ordinateur ou d'un réseau. Loin de faire reculer le secret, la technologie lui trouve plus d'emplois que ne l'avait prévu notre imagination.

Il est des secrets dont l'unique fonction est d'être secrets. Ils identifient les possesseurs légitimes, certifient ou limitent le nombre des copies autorisées d'objets ou de données reproductibles. Tel est le cas avec un mot de passe, un marqueur caché, ou une ligne de code informatique interdisant la duplication d'un original.

1. Et de l'irrationnel. Les attentats du 11 septembre se sont immédiatement traduits par une ruée des internautes sur les prophéties de Nostradamus via [amazon.com](http://amazon.com).



## Vision globale, secret total

Une polémologie du secret devrait aussi faire la part belle aux mentalités, stratégies et idéologies. Ce que démontre l'actuelle doctrine stratégique des USA. Elle s'articule autour de la notion de domination informationnelle\* ou *infodominance*<sup>1</sup> qui sera traitée plus loin. C'est, dans l'idéal, la situation du stratège qui dispose sur le champ de bataille de capteurs perfectionnés, de satellites et instruments d'interception, de moyens de communication et réaction instantanée. Cette vision postule le *panoptisme* au profit de l'armée dominante qui sait tout de l'adversaire. Ce dernier est rendu sourd, aveugle, incapable de communiquer, ses infrastructures critiques bien vite paralysées par un bombardement chirurgical ou une cyberattaque. Sa défaite coïncide avec son incapacité de conserver le moindre secret face à la technologie moderne.

L'idée d'infodominance a débordé ce domaine strictement militaire pour devenir un projet géostratégique. Dans un monde qu'ils pensent déterminé par la révolution numérique, les USA se voient chargés d'une mission de « *monitoring* de la globalisation »<sup>2</sup>. Elle implique la détection, la prévention ou au pire la *préclusion*, c'est-à-dire la répression par la force le plus tôt possible, de tout trouble : État « voyou », opération

1. On trouvera une synthèse très éclairante dans *La Dominance informationnelle comme paradigme central de la stratégie américaine*, Séminaire de l'ADEST (association pour la mesure des sciences et techniques), École des Mines de Paris, le 14 décembre 2000 par Saïda Bédar, CIRPES/EHESS. Ce texte, et plusieurs autres se rapportant au conflit, à l'information et au secret est disponible sur <http://www.strategic-road.com/intellig/infostrategie/infostra.htm>. Du Saïda Bédar, voir également *Vers une « grande transformation » stratégique américaine ?* in Cahiers d'études stratégiques, n°31, Paris, Cirpes. Les textes du Cirpes sont disponibles sur <http://www.ehess.fr/cirpes/> : site du centre interdisciplinaire de recherche sur la paix et d'études stratégiques, dirigé par Alain Joxe, bonne source d'information sur les doctrines US en particulier.

2. Voir par exemple le discours de Bill Clinton du 27 janvier 2000 qui officialise la doctrine du « *Shapping the world* » sur <http://whitehouse.gov/WH/SOTUOO/sotu-text.html>.

mafieuse, péril écologique, terrorisme... À l'échelle militaire tactique ou géopolitique, cette ambition de contrôler toute l'information suppose une transparence totale au profit de l'acteur principal. L'infodominance, équivaut au monopole planétaire du secret. Réel ou fantasmagique, cela est une autre question.

Même obsession du secret chez des acteurs, en apparence tout à l'opposé des militaires, les internautes, libertaires ou protestataires. Pour eux, tout tourne autour du secret, celui qu'ils réclament et qu'ils veulent illimité ou le secret qu'ils soupçonnent ou dénoncent derrière toute forme d'autorité ou d'institution.

Outre l'imaginaire des *hackers*<sup>1</sup> ou les utopies des généraux, des raisons plus tangibles poussent États, entreprises, groupes militants ou particuliers à s'affronter par, pour, contre le secret.

D'abord, il existe de plus en plus d'informations stratégiques dont il y a intérêt à conserver le monopole : découvertes ou techniques performantes ou connaissances plus triviales, comme une base de données sur les habitudes de consommateurs. Même prolifération des informations dont il faut empêcher la reproduction pour des raisons patrimoniales, droits intellectuels et financiers sur des données reproductibles. La frontière s'atténue entre connaissances rares, celles que collecte l'intelligence dite ouverte, et véritables secrets protégés par la loi ou par des boucliers techniques.

À mesure que l'économie devient immatérielle, il y a intérêt à empêcher la concurrence d'accéder à des informations sensibles, un fichier de clientèle ou un projet de recherche et développement. Il faut interdire la diffusion ou l'usage de données, ou, plus brutalement encore, se défendre contre l'espionnage

1. Voir le livre-manifeste *The Hacker Ethic and the Spirit of the Information Age* (Random House, 2001) de Pekka Himanen, Linus Torvalds et Manuel Castells.

économique, la déstabilisation<sup>1</sup>. La protection du patrimoine informationnel, donc de son intégrité\*, de son authenticité, de sa pérennité ou de sa confidentialité\* deviennent une branche capitale de l'activité économique<sup>2</sup>. Comme, de surcroît, l'entreprise doit pressentir les tendances porteuses dans les innovations ou les goûts du public, et mettre en avant son image et sa réputation, toute perte du secret, de ce qu'elle sait ou de ce qu'elle est, la rend vulnérable. Le risque informationnel de ne pas savoir à temps, ou de laisser savoir engendre une insécurité obsédante. Et nous ne parlons même pas ici de l'immense domaine de l'économie criminelle, forcément clandestine.

Autrefois avoir un secret c'était avoir le monopole d'une information vraie, rare ou importante. Désormais le secret protège aussi des bases de données, et des systèmes du prélèvement ou de la falsification de l'information. Si les secrets sont désirables, ils sont aussi vulnérables et redoutables. Tous les traits que l'on prête aux nouvelles technologies — se jouer du temps et de la distance, rendre accessibles et navigables des mémoires quasi illimitées, réunir en un code unique sons, images, textes et programmes, permettre la connexion de toutes les intelligences, tout cela implique autant de possibilités et de motifs de violer des secrets.

Nos mémoires sont « externalisées » c'est-à-dire confiées à des puces de silicone et électrons invisibles. En période de « monoculture technique », si une faille apparaît dans un système de sécurité, la façon de contourner ses défenses est vite connue. Nos transactions ou communications se font à distance, électroniquement, d'où la multiplication de traces qu'il

1. L'enquête de Rémi Kauffer, *L'Arme de la désinformation Les multinationales en guerre contre l'Europe*, Grasset, 2000) en donne une inquiétante illustration.

2. Il en existe même des manuels dans la littérature du management, par exemple : Guichardaz P., Lointier P. et Rosé P., *L'Infoguerre Stratégie de contre intelligence économique pour les entreprises*, Dunod, 1999.

est possible de récupérer, rapprocher pour « profiler » les individus. Avec les télé-transactions, il est facile de se faire passer pour un autre et d'agir à sa place. Dans la mesure où nous employons les mêmes vecteurs, protocoles et logiciels, l'intérêt d'en percer le secret augmente. Dans une économie du temps et de l'accès, le secret compte toujours davantage. L'information est du temps concentré ; c'est un procédé qui permet d'économiser du temps et des ressources pour obtenir un résultat. Le secret gardé est du temps garanti.

L'effraction informatique est invisible et indolore et la pénétration si indécidable que la victime ne réalise pas que le secret a été violé. Ou, dans le cas de marquage, de *chips*, elle ignorera qu'il existe un moyen de reconstituer ses activités : il subsiste toujours une trace de tout ce que l'on a reçu et émis, un indice de tous ses mouvements physiques ou virtuels (connexions). Cookies\*, chevaux de Troie, virus, bombes à retardement... introduisent frauduleusement dans les systèmes informatiques des machines de guerre qui opèrent destruction, désorganisation, falsification, ..., mais aussi des machines de contrôle pour prélever de l'information ou exécuter des instructions. Les techniques de défense changent : il s'agit maintenant de ne pas laisser de points de passages aux signaux hostiles, de sélectionner ces signaux, de faire en sorte que l'information protège contre l'information. Dans le monde virtuel plus que dans le réel, distinguer l'ami de l'ennemi est crucial. Discriminer, c'est survivre.

Ainsi, les systèmes d'identification — authentification\* et signature — de « prouve qui tu es » répondent au besoin d'anonymat de l'utilisateur. Il vit armé de codes, obsédé par la confidentialité, menacé par des délits informationnels ou des outils de fichage. Comme citoyens nous haïssons le secret (celui de l'État, ce que nous cachent les puissants, ce que nous taisent les médias...), comme particuliers nous le réclamons : nous ne voulons plus être filmés, écoutés, décryptés... D'où de nouveaux secrets en cascade : il faut un moyen secret pour s'identifier, et un moyen secret pour être assuré de son anonymat. Ce peut être un logiciel,

## Secret et conflit : de la ruse à la dominance

un mot de passe mais aussi une signature « biométrique » via Internet : la mesure de nos impulsions nerveuses, la reconnaissance de l'iris de notre œil ou de notre voix, la transmission et vérification de nos empreintes digitales. Tous ces procédés recourent, au final à un code secret oublié : le code génétique.

Ces facteurs nouveaux — traçabilité, plus accessibilité, plus externalisation des savoirs, plus dépendance des procédés de traitement — se prêtent aussi bien à l'action hégémonique des puissants qu'à l'activité de déstabilisation des faibles. Désormais, le secret doit protéger l'information contre les risques de publicité, et, dans le même temps, en garantir la disponibilité et la lisibilité : il est indissociable du processus de traitement et de décision. La puissance se confond irrémédiablement avec la faculté de savoir ou de dissimuler.



## Chapitre IV

### De la désinformation idéologique au soupçon éthique

La ruse est une mise en scène, souvent de ses propres actes ou de sa propre apparence, pour accréditer une version fautive de la réalité. Elle mène un adversaire ou concurrent à perdre quelque chose : du temps, de l'énergie, des soutiens ou des alliés, une position favorable. L'intoxication, la déception dans le vocabulaire militaire, ne sont que des variantes de ce principe : je fais X pour que l'autre fasse B, ce qui diminue sa liberté d'action. Cela suppose un minimum de secret (ne serait-ce que pour ne pas se trahir) mais requiert aussi plus qu'un simple mensonge : outre l'énonciation d'une information non véridique, il faut calculer la réaction de la victime. Cet art de fourvoyer agit sur le contenu ou sur le contexte de l'information si bien que son destinataire adopte l'interprétation qu'on lui suggère.

Les moyens de communication introduisent un autre facteur : l'opinion. Du coup, apparaît une discipline du faux, la désinformation. Elle consiste à tromper et sur le contenu et sur la source et sur le sens de l'information : un désinformateur qui parlerait à la première personne, ce serait un propagandiste. La désinformation efficace doit aussi dissimuler le but visé : démoraliser l'opinion, discréditer l'adversaire auprès de la population, de ses alliés, des autorités. Introduisant au moins

un partenaire de plus, le public, une médiation de plus, multipliant les masques et faux-semblants, jouant sur les bandes et les rebonds, la désinformation est une forme raffinée de falsification. Elle prolifère à la mesure des réseaux d'information. Mais le mot prospère encore davantage que la chose : parler trop ou trop peu de l'insécurité ou des morts palestiniens, c'est déjà se faire accuser de désinformation par l'un ou pour l'autre camp. Or la désinformation n'est ni si vaste, ni si ancienne.

Ruses, stratagèmes, intoxication sont, depuis vingt-cinq siècles au moins, répertoriés par des auteurs chinois, grecs, hindous. Dès qu'il y a des bibliothèques, il y a des manuels de guerre et ils contiennent des recettes pour tromper l'adversaire.

La propagande remonte au minimum à Pisistrate<sup>1</sup>, ou, du moins, l'art de persuader les foules et répandre les illusions. Quand des citoyens se sont rassemblés en cités et que le pouvoir a dépendu de l'opinion, les plus malins ont découvert bien avant Hobbes que « gouverner, c'est faire-croire ». Et comme les plus malins en question étaient grecs, ils inventèrent la rhétorique et la sophistique. La pensée grecque a pesé, pensé, parfois dénoncé le pouvoir des mots, images, spectacles et illusions en des termes que nous ressasons depuis. Alors, pourquoi faut-il attendre les années cinquante pour qu'apparaisse, d'abord en URSS, puis en Occident, le mot *désinformation* ?

## Falsificateurs, vecteurs et récepteurs

La réponse la plus évidente est : à cause de la guerre froide. Un monde, divisé en deux camps, des spécialistes de l'action secrète et de l'offensive idéologique, une opinion internationale instable.

1. Pisistrate (600-527), démagogue et tyran d'Athènes, utilisa systématiquement éloquence, agents d'influence, mises en scène destinées à impressionner le peuple, et politique d'influence « culturelle » pour gagner le pouvoir.



## De la désinformation idéologique au soupçon éthique

Un camp au moins, celui du socialisme réel, dispose de relais complaisants dans l'autre. Dans le même temps, le monde devient, suivant l'expression consacrée, un village global. Or, chacun sait que dans tout village les faux bruits se répandent vite. Telles étaient sans doute là les conditions pour qu'apparaissent, sinon la chose, du moins la conscience de la chose et le mot. Et le mot est d'abord russe : *dezinformatsia*, la désinformation, dont l'URSS commence par accuser l'Occident. Le terme devient vite synonyme de « mesures actives de la stratégie soviétique »<sup>1</sup>.

Certes, les historiens signalent depuis plusieurs siècles des opérations concertées, dissimulant leurs sources, pour imputer les plus terribles forfaits soit à des individus — les libelles contre Louis XVI ne faisaient pas autre chose — soit à des communautés — comme le montre la pérennité des increvables « *Protocoles des sages de Sion* ». L'entre-deux-guerres est marqué par l'hallucination des masses à l'échelle industrielle. Mais c'est seulement après 1945 que les falsifications et mises en scène se multiplient suivant une méthode quasi scientifique.

Elles sont souvent l'œuvre du KGB. Elles visent à « incapaciter », à accréditer la résurgence du militarisme ou du nazisme en RFA, à empoisonner les rapports de l'OTAN et ses alliés par de fausses lettres de dirigeants américains, à rendre la CIA responsable de l'apparition du SIDA. Tardivement, on théorise la désinformation, sœur de la surinformation ou de la mésinformation typique des médias de masse. Elle est souvent envisagée comme manifestation d'une idéologie intrinsèquement perverse ou d'un cynisme politique sans bornes. La désinformation peut-elle s'expliquer par le complot ? Ce n'est certainement pas aussi simple.

Même aux larrons du KGB, il faut une occasion. La désinformation ne résulte pas seulement de la volonté de ses initiateurs. Personne ne pense sérieusement que les capitalistes soient « moins menteurs » que les communistes ou la CIA « plus

1. Tel est le sous-titre du livre classique sur ce sujet : *Dezinformatsia* par Richard H. Schultz et Roy Godson, Éditions Anthropos, 1985.

honnête » que le KGB Il se trouve simplement que la désinformation occidentale n'aurait trouvé au-delà du Rideau de Fer ni presse prête à la relayer, ni « idiots utiles » capables de la reprendre à leur compte. Pour que la désinformation prospère, elle a besoin de trouver des instruments adéquats et un milieu réceptif.

En termes plus savants, la désinformation, comme les phénomènes de communication en général, et comme tous ceux qu'étudie ce livre en particulier, suppose du stratégique plus du symbolique plus du technique.

— *Stratégique* : une conscience, une organisation et des méthodes. Il faut un dessein de vaincre non seulement par l'information pertinente (celle que recueillent les espions par exemple) mais aussi par l'information efficiente (celle qui est d'autant plus redoutable qu'elle trouve des récepteurs, des repreneurs ou des propagateurs). Des méthodes, des organisations, des volontés, certes, mais aussi des incertitudes : agir sur le cerveau humain est — Dieu merci — la plus aléatoire des sciences. La désinformation agit sur des cerveaux, pas sur des objets ou des données.

— *Symbolique* : le contenu de la désinformation correspond à des attentes, des catégories ou des valeurs de la cible. Nul n'est désinformé qui ne soit prédisposé à croire. Le cerveau humain est doté d'une incroyable capacité de résistance à l'évidence. La désinformation confirme souvent ce que le « croyant » est prêt à admettre : une explication des affaires du monde par des complots sulfureux ou par la perversité du Système, un arrière-monde conforme à ses fantasmes. La désinformation longtemps associée à la propagande : elle est la compagne obscure et inavouable d'une foi commune et rassurante qui se propage ouvertement. Pour le moins, elle suppose des préjugés et stéréotypes pour lui préparer le terrain.

— *Technique* : les médias ne sont pas seulement des multiplicateurs potentiels de la désinformation. Ils en font la mise en

## De la désinformation idéologique au soupçon éthique

forme et la mise en scène. C'est une chose de réfuter un opuscule distribué sous le manteau, c'en est une autre d'être confronté à l'image de prisonniers derrière des barbelés. À l'ère du téléx, on a le temps de combattre une dépêche d'agence par un communiqué, mais personne ne résiste à l'émotion mondiale *live* des images de quelque Timisoara filmé « comme si vous y étiez ». Un démenti tombe trop tard quand l'hystérie de l'actualité a remplacé un drame ou une indignation par un autre. Qu'on se souvienne des *spin doctors* qui inventaient des crimes imaginaires pendant la guerre du Kosovo : les Serbes employaient des boucliers humains, ils forçaient leurs victimes à donner leur sang, l'épuration ethnique était prévue par un plan écrit très antérieur au conflit<sup>1</sup>... Depuis, la révélation de leurs manipulations n'a rigoureusement rien changé. Comme après le Golfe, on a publié quelques bons livres, et monté quelques colloques : journalistes et universitaires ont juré qu'on ne les y reprendrait plus. Il faudra sans doute attendre quelques mois pour voir révéler trucages et bidonnages pendant la guerre d'Afghanistan. Promis, nous nous repentirons et nous ferons d'autres colloques.

L'imprécision du vocabulaire n'améliore pas les choses. Le mot « désinformation » a fini par désigner toute forme de bobard journalistique, de trucage, déformation ou simplement toute interprétation tendancieuse, à tel point que la désinformation devient l'information dont nous doutons comme l'idéologie l'idée que nous refusons. D'un côté nous sommes menacés par le Charybde paranoïaque : voir partout des complots contre la vérité et des manipulations invisibles. De l'autre, par le Sylla de l'angélisme : noyer la réalité de la désinformation dans des considérations vagues sur la relativité de toute vérité du type : toute image est sélectionnée et interprétée, tout évé-

1. Sur ce sujet maintenant très documenté voir Elisabeth Lévy, *L'Insoutenable légèreté de l'information* in Le Débat d'avril 2000 et son livre *Les Maîtres censeurs*, J.C. Lattès, 2002. Voir aussi Dominique Vidal et Serge Halimi *L'Opinion, ça se travaille*, Agone, 2001.

nement est construit. Répétons que le recadrage idéologique, le psittacisme médiatique, la myopie engagée, la construction de l'agenda\* par les médias ne doivent pas être assimilés à leur emploi tactique. Ou plutôt, la désinformation ne doit pas être confondue avec les règles du jeu qu'elle exploite<sup>1</sup>.

## Forgeries

Nous reprendrons ici une définition que nous avons déjà proposée<sup>2</sup> : la désinformation consiste à propager délibérément des informations fausses pour influencer une opinion et affaiblir un adversaire.

— « *Propager* » sous-entend un caractère public. Plus que le simple bouche à oreille ou l'usage de messages privés, il faut avoir recours à des médias et à des vecteurs.

— « *Délibéré* » demande, au moins chez l'acteur, la connaissance de sa finalité, même si les « repreneurs » et propagateurs de l'information peuvent être inconscients.

— « *Des informations* », ce qui requiert qu'il s'agisse de relations de fait, de descriptions de la réalité, non de simples jugements moraux ou opinions. La désinformation a pour base la description d'événements fictifs. Pas d'états d'âme ou théories.

— « *Fausses* » implique des affirmations contraires à la réalité ou recadrées de façon à en altérer l'interprétation. Il ne saurait s'agir de simple rhétorique ni d'exagération. De même, ceci exclut toutes les formes de construction ou explication de la

1. Pour faire le point sur les définitions de la désinformation voir le numéro 58 de *Panoramiques, La Désinformation : tous coupables ?* Mai 2002, Éditions Corlet, <http://www.editions.corlet.fr/panoramiques/sun/>.

2. Notamment dans *La Désinformation Pour une approche historique* Colloque de Montpellier 18-20 novembre 1999, UMR 5609 du CNRS, université Paul Valéry, 2001.

## De la désinformation idéologique au soupçon éthique

réalité à l'aide de stéréotypes ou catégories idéologiques. En ce cas, qu'est-ce qui ne serait pas de la désinformation ? Il y a de la désinformation « noire », celle qui ment, « grise », celle qui mêle vrai et faux, mais il ne peut y avoir de désinformation « blanche » qui ne dise que la vérité.

Le mensonge ici porte sur la réalité qu'il décrit, sur la personne ou l'appartenance de qui la rapporte et, enfin, sur le but de son énonciation qui est de produire un dommage. Cela en fait une sorte de mensonge au cube. Ce jeu à trois — initiateur, public, victime — fait souvent appel à de véritables mises en scène, à la forgerie ou à la construction d'apparences de réalité<sup>1</sup>.

La désinformation est, dans presque tous les cas, une version politique de la diffamation au sens pénal : le fait d'attribuer fausement à quelqu'un un comportement honteux. Non seulement la désinformation dit rarement du bien de ses victimes, mais elle leur impute le plus souvent de noirs complots, le plus redoutable étant d'accuser la victime de désinformer. Les imputations en question jouent dans un double registre. Elles réactivent les vieilles craintes touchant à des périls occultes tels le poison caché, la corruption clandestine, la société secrète qui manipule, le danger que les puissants nous dissimulent. Elle les réintègre dans les nouvelles catégories idéologiques : les OGM, la surveillance électronique, les contaminations alimentaires ou sexuelles, les organisations manipulant médias et gouvernements. Devant telle ou telle information malveillante, surtout sur Internet, il est difficile de trouver la source originelle, on peut toujours se poser la question. Désinformation ou simple rumeur ? La réponse est tout sauf aisée. La rumeur peut être vraie, elle a simplement une source non officielle ou non identifiée ; elle n'a pas été délibérément planifiée.

La désinformation est faite « pour influencer une opinion » : imposer une croyance ou des attitudes à un public plutôt

1. Voir la façon dont Vladimir Volkoff met en scène la dramaturgie de la désinformation et de l'influence dans *Le Montage*.

qu'une décision à un responsable, même si le premier n'empêche pas le second. Ce public peut être l'opinion adverse, des alliés, des neutres ou l'opinion internationale en général ; on peut viser les masses ou des cercles plus restreints. La première n'est possible que là où existe un espace public, avec débats et pluralité d'opinions et de connaissances. Elle n'a de sens que là où sont en concurrence diverses sources de savoir et diverses interprétations. *Big Brother* ne désinforme pas, il contrôle le présent, le passé et le futur. Il contrôle jusqu'à la langue même. Dans un système totalitaire, il y a la vérité officielle et la rumeur clandestine. Le dictateur dicte ce qui doit être su et cru. La désinformation n'est possible que s'il y a connaissance imparfaite de la réalité, non-fiction absolue.

« Et affaiblir un adversaire » : la désinformation diminue les capacités offensives de *l'Autre*, soit en divisant l'autre camp, soit en l'inhibant moralement, en le désorganisant. Toujours négative, elle diffère de l'endoctrinement, dont la finalité est d'obtenir l'adhésion. Plus simplement encore, la désinformation accroît la confusion et le désordre. Elle est le contraire de ce que devrait être l'information au sens étymologique : in-formation, mise en forme.

Partant de là, nous pouvons reformuler la question du début : que devient la désinformation de l'après-guerre froide, dans la présente configuration stratégique, symbolique et technique ?

La présence de centaines de caméras libres sur le théâtre des opérations ne garantit pas que nous soyons moins trompés qu'en 14-18. Internet, supposé paradis de l'expression non censurée et de « toutes les informations enfin disponibles », est aussi le royaume du faux triomphant et de l'insignifiance dominante.

D'une part, les médias classiques tendent à fonctionner en boucle autorépétitive et à diriger toujours leur attention de la même façon. D'autre part, Internet s'est souvent révélé le domaine où la mauvaise information chasse la bonne. Il manque des procédures

## De la désinformation idéologique au soupçon éthique

d'accréditation ou de vérification fiables. Ce que nous avons théoriquement gagné en pluralité de sources d'information, il se pourrait que nous l'ayons perdu en capacité de vérifier les sources ou en temps de réaction. Comment la vieille désinformation joue-t-elle de tant de mésinformation potentielle ?

La technique change les facilités, les fragilités et les finalités de la désinformation.

La facilité de la désinformation s'accroît.

— *La production est simplifiée.* La fabrication de faux, y compris de fausses images numériques parfaites, est à la portée de tous les logiciels. Leur introduction sur Internet, parfois de façon anonyme et plus vite que les grands médias, est accessible à tout un chacun. Plus besoin d'imprimerie ou de bureaux, plus besoin de soumettre sa prose à un directeur de publication pénalement responsable.

— *La propagation — cela va de soi — est plus commode :* les réseaux échappent à toutes les frontières ou à toutes les censures.

— *La réception rencontre moins d'obstacles.* Ici se conjuguent les facteurs psychologiques, la tendance à croire tout ce qui vient du Net, mais aussi le facteur rapidité, le facteur quantitatif : l'énorme masse de l'information disponible, plus le nombre de sites ou de médias classiques qui se recopient mutuellement. Le tout n'encourage guère l'esprit critique.

Ceci peut se reformuler en termes de vulnérabilités.

— *Dans l'espace :* sans frontière ni censure pour arrêter les rumeurs<sup>1</sup>, nul ne contrôle la diffusion d'une information sur son territoire.

1. Faute de place, nous ne pouvons traiter ici du vaste domaine de la rumeur électronique. Le lecteur que la question intéresse aura intérêt à confronter les thèses des deux stars de la « rumorologie ». D'abord, Jean-Noël Kapferer (auteur de *Rumeur, le plus vieux média du monde*, Seuil, 1987) : [http://www.hec.fr/hec/fr/professeur\\_recherche/liste/kapferer/cv.html](http://www.hec.fr/hec/fr/professeur_recherche/liste/kapferer/cv.html), mais aussi les travaux de Pascal Froisart qui soutient, au contraire, la thèse que la rumeur est un média moderne lié à nos moyens de communication récents : <http://www.chez.com/pascalfroissart/>.

— *Dans le temps*, ou plutôt à cause du temps : la vitesse de propagation est telle que toute réaction est tardive.

— *La fragilité est aussi psychologique et médiatique*. Les institutions sont de plus en plus sensibles aux affolements de l'opinion nationale ou internationale, amplifiés par les sondages et impulsés par des médias moralisateurs. Les entreprises sont dépendantes de leur image. La Bourse se panique pour une rumeur électronique<sup>1</sup>. L'air du temps est réceptif à toutes les révélations sur des épidémies, des manipulations, des catastrophes, des dangers de la technique, des secrets d'État.

Enfin les finalités changent.

Il y a davantage de raisons de recourir à la désinformation et autres armes du même métal dans le cadre d'une « infoguerre »<sup>2</sup>. Ainsi, les stratèges du Pentagone envisagent des scénarii de paralysie des infrastructures informationnelles de l'adversaire et d'opérations psychologiques sur son opinion. Quand ils ne créent pas, assez maladroitement, des structures comme l'*Office of Strategic Influence*, vite dénoncé comme une organisation destinée à désinformer les propres alliés des USA, pourtant engagés dans la « guerre au terrorisme »<sup>3</sup>.

Il apparaît, de ce fait, de nouveaux acteurs dont on ignore s'ils sont au service d'États ou d'entreprises, criminels ou militants. Ils peuvent être à la recherche d'expériences gratifiantes, comme répandre le plus gros canular ou réussir un exploit technologique, mais aussi à la poursuite de buts politiques comme « punir » un gouvernement ou une société.

1. Une société suisse aurait même produit un logiciel « traqueur de rumeurs », *rumourbot* [http://www.strategicwatch.com/intelligence/index\\_mars.php3](http://www.strategicwatch.com/intelligence/index_mars.php3).

2. Voir chapitre suivant.

3. Après la « découverte » de ce service par le *New York Times*, de nombreux journalistes se sont intéressés aux rapports du Pentagone et de l'agence Enron, à qui il verse 100.000 dollars par mois (comme au moment de la guerre du Golfe) et qui est considérée comme l'une des principales réserves de « *spin doctors* » en cas de guerre. Voir par exemple l'article « *The Pentagon's Information Warrior* » sur le site du *Center for Media & Democracy* : <http://www.prwatch.org/prwissues/2001Q4/rendon.html>.



## De la désinformation idéologique au soupçon éthique

En attendant peut-être de nous débarrasser de ce concept des années cinquante, la désinformation est à repenser. Autrefois, la difficulté était de la situer entre la lutte idéologique opposant deux systèmes et les déformations et mésinformations journalistiques.

Désormais, ce qu'il faut bien nommer désinformation avoisine trois domaines.

— *Le domaine de la « sidération »* agressive militaire ou terroriste. Il s'agit ici d'une infoguerre vraiment martiale avec ses *psyops*, opérations psychologiques, version « âge de l'information » de la guerre psychologique\* de papa. Cette stratégie-là se préoccupe aussi de « *management* de la perception », donc de proposer du « contenu », c'est-à-dire de faire circuler des informations, pas nécessairement fausses mais sélectionnées en fonction de leur capacité d'influencer les « estimations officielles » des acteurs dans un sens favorable à ses desseins. Il y aurait beaucoup à dire sur ces représentations qui tendent à ignorer combien l'efficacité du contenu de l'information dépend aussi du contexte et du code d'interprétation du récepteur. En ce domaine, il ne suffit pas de raisonner en termes de causes et d'effets : je leur « fournis » telle information et ils croient que... Il ne suffit pas de pousser dans les tuyaux, encore faut-il comprendre ce que font les tuyaux.

— *Le domaine de la rumeur*, de la *e-rumeur*, de la légende urbaine<sup>1</sup>, et autres formes de prolifération, sur la Toile, de l'information anarchique, là encore, pas forcément fausse ou malicieuse. Les communautés d'internautes sont prêtes à reprendre et amplifier toute nouvelle sensationnelle qui ne provient pas des médias « officiels », toujours suspects. Les publicitaires découvrent la puissance du « marketing viral » pour répandre l'image positive de leurs produits. C'est encore plus vrai de rumeurs négatives et autres « *hoaxes* »\* : ils prolifèrent par mil-

1. Voir Véronique Champion, Vincent et Jean-Bruno Renard, *Légendes urbaines, rumeurs d'aujourd'hui*, Payot, 2001.

liers<sup>1</sup>. La désinformation *stricto sensu* cohabite avec les virus, l'altération de données, le déni d'accès, qui consiste à sursaturer un système informatique, avec la prise de commande à distance sur des réseaux. La désinformation qui agit sur la croyance des victimes, c'est-à-dire sur leur interprétation du réel, voisine ainsi une quasi-désinformation ou anti-information : celle qui agit sur le fonctionnement des organisations et des systèmes.

— *Le domaine de l'économie*, surtout celle que l'on disait nouvelle. Les faux sites, les opérations de dénigrement par forums Internet, pseudo-associations, et pseudo-scandales interposés, les révélations et pressions composent l'arsenal de l'économie dite hypercompétitive<sup>2</sup>. Une opération de désinformation peut viser à faire perdre à sa victime sa réputation ou tout simplement un temps de paralysie, crucial dans une économie « zéro délai » en flux tendus.

D'où ce paradoxe : plus l'entreprise se dote de déontologues et de codes d'éthique, plus elle se veut citoyenne et responsable, plus elle est soumise au danger de telles opérations. Ici, la désinformation est à rapprocher de la déstabilisation, du risque informationnel. Et ce paradoxe-là pourrait bien peser lourd à l'avenir.

## Bienveillance et transparence

Là encore, il est malaisé de tracer la frontière entre vrai et faux, délibéré et spontané. Notre propos n'est pas d'absoudre les sociétés qui nous empoisonnent, blanchissent de l'argent

1. Voir <http://www.hoaxbuster.com> : site en français consacré aux rumeurs sur la Toile, <http://www.urbanlegends.com> : anthologie, depuis 1991 et en anglais, de rumeurs dans tous les domaines (politique, sexe, livres, animaux, etc).

2. Voir Rémi Kaufer, *L'Arme de la désinformation*, Grasset, 1999.

## De la désinformation idéologique au soupçon éthique

sale ou exploitent les enfants du tiers-monde. Et moins encore de leur fournir l'alibi d'un complot mené par la concurrence infoguerrière ou de la subversion désinformatrice. Cela va sans dire, et mieux en le disant : s'il n'y avait pas d'authentiques catastrophes, le problème des fausses dénonciations ne se poserait pas.

Pourtant, le « souci éthique » qui tarade si fort l'entreprise la soumet à un double péril. Soit de n'utiliser le discours moral que pour rendre plus attractive et plus *soft* une activité visant au profit et donc risque de révélation de cette opération de maquillage cosmétique<sup>1</sup>. Soit le péril, en rien incompatible, de subir mise en accusation malveillante. De telles opérations recourent notamment aux réseaux à la fois pour masquer et multiplier l'effet de déstabilisation. C'est le nouveau champ de la « désinformatique ».<sup>2</sup>

La mondialisation du risque réel — je peux être empoisonné ici par un produit fabriqué à l'autre bout de la planète — et celle du risque de réputation — une révélation faite sur un forum en Australie peut déstabiliser une entreprise européenne — renvoient à d'autres mondialisations :

— *mondialisation du marché* : la circulation des choses et des capitaux.

1. On peut trouver une virulente critique des codes éthiques des entreprises comme outil de *marketing* et alibi à la dérégulation chez Attac, par exemple. Voir le courriel d'Attac n° 295 et 307. Sans même parler des difficultés de traçabilité des produits dans des entreprises transnationales qui font appel à des sous-traitants de pays pauvres, les « antimondialisation » dénoncent ces codes comme instruments de mise en place d'une éthique privée alors qu'il existe des normes internationales (BIT ou OIT) à appliquer ou développer. Cela témoignerait, disent-ils, de l'affaiblissement de l'État protecteur au profit de la société civile, raisonnement qui n'est pas faux.

2. L'expression est empruntée à Henri Marinez. Voir son texte « La "désinformatique" à l'heure du Réseau des réseaux numériques » dans *La Désinformation, pour une approche historique* Colloque de Montpellier, 18-20 novembre 1999, UMR 5609 du CNRS-ESID, université Paul Valéry. Ce texte est également disponible sur <http://www.strategic-road.com/intellig/infostrategie/infostra.htm>.

— *mondialisation de l'opinion*, qui peut réagir ici à ce qui se produit à l'autre bout du monde.

— *mondialisation des stratégies*, notamment les stratégies commerciales qui raisonnent en termes de marché planétaire.

Derrière encore, des tendances lourdes et des valeurs dominantes. Nous vivons dans un monde obsédé par ce que Baudrillard nomme *l'évacuation totale du mal*, hors du présent, de l'avenir, voire du passé. Repentance pour nos fautes anciennes, vigilance aujourd'hui, précaution pour le futur. Éviter la catastrophe humanitaire, sécuritaire, écologique devient notre premier impératif.

Nous pensons en termes de crises : effondrement brusque et paniquant d'un ordre supposé régulier, caractère soudain de l'événement déclenchant. L'éthique dominante est celle de *minima moralia* : non plus amener le Paradis sur terre, ce qui pourrait nourrir un totalitarisme des bonnes intentions, mais faire le moins de mal possible. Quand il ne s'agit pas de troubler le moins possible l'ordre « naturel » des choses. Ainsi, il faudra rechercher un développement *durable*, une activité *soutenable* ou une production *renouvelable*.

L'impératif de réduction des contraintes, des dangers, des frictions caractérise notre société de bienveillance où les mots d'ordre semblent être « prévenir et réparer ». Et pour cela, la stratégie zéro : zéro mort à la guerre, zéro délai dans le négoce, zéro défaut dans la production, zéro risque dans la vie courante.

Si l'information équivaut à la réduction d'incertitude, la société de l'information, elle, se propose de minimiser l'aléa, et, partant, de diminuer les risques liés à sa logique de développement. Cela se manifeste sous forme d'un impératif, celui des quatre respects : respect du corps (risque pour la santé), respect de la nature (risque pour l'environnement), respect de l'individu (risque pour sa sécurité ou son intimité), respect des tribus (risque d'exclusion, d'exploitation ou de persécution de minorités, relativisme culturel). Cela pourrait tout aussi bien se résu-

## De la désinformation idéologique au soupçon éthique

mer dans la trilogie « Transparence, Tolérance, Bienveillance ». Transparence parce que tout est problème de communication, d'écoute, d'attention et d'expression. Tolérance parce que notre individualisme postmoderne glorifie la différence de masse et l'affirmation de soi comme valeurs cardinales, et qu'il répugne à tout ce qui est hiérarchique et autoritaire. Bienveillance dans la mesure où règne l'obsession hygiénique, sécuritaire, caritative, prophylactique, de l'élimination de la catastrophe et de la violence et de la protection généralisée. L'étonnant, ce n'est pas que nous croyions en ces valeurs, mais que nous soyons si scandalisés de ne pas les voir réalisées. Comme le note Gilles Lipovetsky : « Plus nous avons un pouvoir de maîtrise, d'organisation et d'efficacité, plus nous sommes voués à l'effroi, à l'exigence de protection et de précaution infinie. »<sup>1</sup>

La « dénonciation » au nom des principes de visibilité et de transparence tient un rôle important dans notre imaginaire. La judiciarisation, c'est-à-dire la tendance à faire de plus en plus appel au juge, à exiger réparation de tout et à fonder la légitimité de l'action sur la figure de la victime, joue dans le même sens. La puissance du quatrième pouvoir, les médias avides de révélations et de secrets percés, joue dans le même sens. Le tout forme un terrain idéal pour la rumeur et la désinformation, surtout quand il devient possible de passer d'une stratégie d'imputation — je fais croire que A est coupable de l'acte X — à une stratégie d'évaluation du risque — je suggère que l'initiative de A risque de produire l'effet Y dans le futur.

Après tout, même les vérités politiques peuvent se confronter à des réalités de fait. Elles ne nous disent rien de ce qu'est la liberté, la démocratie ou le meilleur des régimes, mais elles permettent d'éliminer quelques affirmations visiblement fausses. On songe au mot de Clémenceau rapporté par Hannah Arendt :

1. Gilles Lipovetsky, *Métamorphoses de la culture libérale*, Liber, 2002, p. 68.

tout est relatif en politique, mais il n'empêche qu'en 1914 c'est l'Allemagne qui a envahi la Belgique, pas le contraire<sup>1</sup>. Mais lorsqu'il s'agit de la « dangerosité » de quelque chose ? Certes, le bon sens nous suggère que le zéro risque n'existe pas, mais qu'est-ce qu'un risque acceptable ?

Dans sa *Rhétorique*<sup>2</sup>, Aristote distinguait parmi les discours destinés à convaincre : le *judiciaire* qui porte sur le passé, l'*épidictique* qui porte sur le présent, et le *délibératif* qui porte sur l'avenir. Et il ajoutait que pour convaincre en ce domaine plus qu'en tout autre, il fallait autant jouer sur la passion que sur les mœurs (pathos et ethos) de ceux à qui l'on s'adresse. C'est un schéma qui s'applique encore mieux à l'agora électronique qu'à celle d'Athènes.

La société de l'information repose sur la croyance en la prédictibilité de l'avenir et l'ambition d'éliminer l'aléa. D'autant que c'est une société qui, plus que toute autre avant elle, se pense comme société, s'examine et se commente, se dote d'une armée d'ingénieurs sociaux, de commentateurs et d'experts pour, précisément, venir à bout de ses dysfonctionnements.

Les institutions politiques, l'État le premier, les instances économiques fonctionnent à la séduction et se réclament des valeurs de transparence et d'éthique. Ce qui les soumet au risque informationnel. Le plus évident est le risque dit « de réputation », toujours en relation avec des thèmes porteurs : sécurité du consommateur, droits de l'homme, protection de la nature, dénonciation du système de surveillance.

Cette tendance trouve un terrain favorable dans le domaine économique, dans la mesure où l'esprit du temps la conçoit moins comme centrée sur la lutte contre la rareté, la production et la circulation des choses que sur la répartition de l'information et du risque. Ulrich Beck décrit très bien

1. Hannah Arendt, *Vérité et politique* in *La Crise de la culture*, Gallimard, 1972.

2. Aristote, *Rhétorique*, 1,3,1358 b 13-29

## De la désinformation idéologique au soupçon éthique

cette tendance lourde : « Dans la modernité avancée, la production sociale de richesses est systématiquement corrélée à la production sociale de risques. En conséquence, les problèmes de répartition propres à la société de pénurie et les conflits qui y étaient liés y sont recouverts par les problèmes et les conflits générés par la production, la définition et la répartition des risques induits par la science et la technique. »<sup>1</sup>

Dans le même temps, l'entreprise semble s'assimiler à un système à capter des signaux, à émettre des images et à faciliter des flux. Capturer des signaux consiste à distinguer les tendances émergentes, qu'il s'agisse de profiler une clientèle, de s'adapter à son style de vie ou d'imaginaire, de surveiller les innovations techniques ou des initiatives de la concurrence, ou encore d'anticiper les risques et les renversements.

Émettre des images se réduit le plus souvent à minimiser le risque de ne pas être éthiquement, politiquement, écologiquement, culturellement correct. Enfin, la gestion des flux de données est pensée suivant le paradigme du réseau présumé souple, innovant et économe en frictions et commutations inutiles, réducteur des hiérarchies et des contraintes.

Ce triple idéal — anticipation, séduction, répartition — ces trois modes de « bonne circulation » de l'information prend un tout autre sens dans le cadre d'une polémologie de l'information.

Les causes de ce changement — le nouvel ethos et le nouveau pathos diraient les aristotéliens — sont à chercher chez les acteurs eux-mêmes. Le premier est l'entreprise qui tient ici le rôle de l'arroseur arrosé ou du moraliste dénoncé. À mesure qu'elle préconise le réseau contre la hiérarchie, le *monitoring* contre la discipline, la sécurité contre l'agressivité, le « *ethic is good for business* » contre le « *business is business* », la volonté citoyenne contre la politique des inté-

1. Ulrich Beck, *La Société du risque*, Aubier, 2001, p. 35.

rêts, la responsabilité contre l'avidité, l'équitable contre le profitable, la chaleur communicante contre « les eaux glacées du calcul égoïste », elle se retrouve au banc des accusés. Cherchons l'erreur !

## Économie, éthique et sécurité

Tout commençait pourtant si bien. Le souci éthique, comme souci de *l'Autre* et de l'avenir, semblait promis à de tels lendemains radieux ! Le capitaliste imprégné d'esprit protestant décrit par Max Weber recevait ici-bas les signes visibles, et parfois trébuchants, des bénéfiques spirituels qui l'attendaient là-haut. Pourvu qu'il ait été sérieux, travailleur, ascétique, mobilisé. De nos jours, le *manager* éthique jouit ici et maintenant de l'avantage d'être politiquement correct, culturellement branché et financièrement prospère. Et, faut-il ajouter, dans une société où le juge a pris un tel pouvoir et le principe de responsabilité une telle extension, judiciairement « couvert ». Suivons le raisonnement...

L'attitude éthique — par exemple le refus de recourir aux *sweatshops*, ces boutiques à sueur où l'on exploite les travailleurs du tiers-monde — et la préoccupation sécuritaire sont gratifiants pour ceux qui participent à la production, donc motivants. Ce que nous appellerons désormais la « *sécuréthique* » (sécurité + éthique) s'inscrit dans une tendance générale à résoudre « les contradictions culturelles du capitalisme », expression de Daniel Bell dans les années soixante-dix<sup>1</sup>. Il entendait par là la tension entre ordre technico-économique régi par le principe d'efficacité, d'ascétisme, de discipline, l'ordre politique avec ses

1. Daniel Bell, *The Cultural contradictions of capitalism*, Basic Books Inc, New York, 1976, traduction française : *Les Contradictions culturelles du capitalisme*, PUF, 1979.



## De la désinformation idéologique au soupçon éthique

idéaux égalitaires, et l'ordre culturel voué aux valeurs d'hédonisme, d'expérimentation, d'affirmation de soi sur les ruines du modernisme culturel des avant-gardes.

La solution de ces contradictions, passe, pour parler comme une autre génération de sociologues, Boltanski et Chiapello, par la récupération de la « critique artiste » du capitalisme<sup>1</sup>. Cela se traduit par l'intégration des valeurs « post-soixante-huitardes » : dénonciation de l'aliénation, recours à l'initiative et à l'autonomie, responsabilisation des individus, refus de la standardisation, quête de « l'authenticité », par exemple par des produits naturels, différents, non polluants... Ainsi, le *manager* respectueux des règles, équilibres et différences pourra un jour rêver d'être récompensé par ses ennemis d'hier, syndicalistes, intellectuels ou autres, en recevant un prix d'une agence de notation sociale comme celle de Nicole Notat<sup>2</sup> ou en étant bien noté par un collectif comme « l'éthique sur l'étiquette ». La performance globale de l'entreprise avec ses composantes environnementales et sociales devient ainsi un atout.

Dans la même logique, du « bon pour la conscience et bon pour le profit », la *sécuréthique* attire l'investisseur. « Investir éthique », par exemple contribuer à l'échange équitable ou au renouvellement des énergies devient de plus en plus aisé grâce à des fonds spécialisés ou à des conseillers<sup>3</sup>.

Corollaire du corollaire, la valeur ajoutée *sécuréthique* constitue des arguments vendeurs : la séduction du bien s'ajoute à la jouissance des choses. Autrefois les banques proclamaient cyniquement que notre argent les intéressait, c'est maintenant notre âme qui les préoccupe, puisqu'elles proposent des cartes de crédit « éthiques » qui permettent de s'endetter tout en

1. Luc Boltanski, Eve Chiapello, *Le Nouvel Esprit du capitalisme*, NRF, Gallimard, 1999.

2. <http://www.novethic.fr/novethic/site/article/index.jsp?id=20140>.

3. Là encore, voir <http://www.novethic.fr> et ne pas manquer ses tests « Quel type éthique êtes-vous ? ».

reversant un petit pourcentage de toute somme dépensée à des associations reconnues d'utilité publique<sup>1</sup>. La pub s'idéologise et se « moralise », moitié par intérêt — rentabiliser la plus-value de la différence morale — moitié parce que ses promoteurs, *managers* et « gens de com » sont sociologiquement enclins à partager les valeurs qu'ils prônent. La nouvelle classe\* des « manipulateurs de symboles »<sup>2</sup> décrite par Robert Reich est par nature plutôt cosmopolite, tolérante, sensible à la rhétorique « bobo » (bourgeoise-bohème<sup>3</sup>) sur la qualité de vie... Dans la même logique que la publicité écologique qui vend de la nature sur fond de levers de soleil et de plages impolluées, l'entreprise peut choisir le positionnement antiraciste comme l'a fait Benetton ou les sociétés allemandes qui ont produit des campagnes pour dénoncer le racisme des *skinheads* teutons<sup>4</sup>. Cette frénésie du Bien qui peut aussi se manifester par la proclamation d'une plus-value culturelle, patrimoniale, écologique, éducative, sociale, antisexiste pour la marchandise est aussi une façon de vendre. Les nouveaux profits de respectabilité supposent donc un perpétuel effort de relégitimation.

Le *marketing sécuréthique* répond aussi à des soucis plus défensifs. Le risque d'une campagne de dénonciation ou de *boycott* inspirée par la mentalité du « No Logo »<sup>5</sup>. L'activisme s'est facilement reconverti dans la protestation contre les multinationales, comme la « pubversion » (c'est-à-dire le détournement, la subversion de la publicité), ou toutes formes d'opposition culturelle aux symboles de la mondialisation honnie. Ce militan-

1. Publicité de la Société Générale : « Profitez de tous les atouts d'une carte Visa Premier... tout en jouant la carte du cœur », en l'occurrence en versant des dons aux Paralysés de France et à la ligue contre le cancer.

2. Reich R., *The Work of Nations*, New York, Random House, 1982.

3. Nous faisons ici allusion à la description qu'en fait David Brooks dans *Bobos in Paradise*, Touchstone books, Simon and Schuster, New York, 2000.

4. Dans les années 80, Berlusconi, alors plutôt réputé à gauche, subventionnait les concerts de SOS-Racisme via sa télévision la 5.

5. Du titre du best-seller antimondialiste de Naomi Klein, *No Logo, La Tyrannie des marques*, Knopf, Canada, 2001 et Le Méac, Actes Sud, 2001.

## De la désinformation idéologique au soupçon éthique

tisme a un double avantage. D'une part, il se centre sur la vie quotidienne, sur le vécu du consommateur citoyen, de l'individualiste postmoderne. D'autre part, il fournit des récompenses symboliques plus accessibles — plus faciles que de renverser un gouvernement dans la rue par exemple.

Cette nouvelle forme de résistance au Mal fleurit, d'autant qu'elle est dispensée de l'obligation de dessiner un Bien idéal, comme un parti politique qui est censé proposer une forme d'État et de pratique concrète. Bref, c'est la conjonction du consumérisme, de l'écologie, de l'antiglobalisation qui joue à la fois sur le registre du pragmatisme et de l'idéalisme. C'est un combat où l'on gagne à tous les coups, au moins moralement, comme dans le domaine politique réduit à la défense morale systématique des victimes : personne ne peut s'affirmer contre les valeurs que vous défendez.

Donc plus une marque est visible, plus elle s'expose au sourcilieux contrôle de ces militants sans parti<sup>1</sup> : raison de plus pour désarmer la critique par un surcroît de bonne volonté. Peu de sociétés ont envie de connaître le sort de Pepsi-Cola perdant des millions de dollars à cause d'un mouvement de *boycott* en Amérique du Nord, accusé de complicité avec la dictature birmane. Ou, comme Nike<sup>2</sup>, de se voir pris dans la guerre contre les *sweat shops* qui secoua les campus en 1998. Et quelle société surveillant ses employés ou se constituant des bases de données sur ses consommateurs ne craindrait de se voir décerner un « prix technologies Brother »<sup>3</sup> ? Le positionnement éthique sert autant à surpasser ses concurrents qu'à désarmer ses opposants.

Cette « idéologisation » de l'économique n'est pas seulement par un effet de mode. Elle correspond à un double

1. Ainsi le *Council on Economic Priorities* a créé une norme de certification sociale SA 8 000.

2. Qui depuis s'est doté très ostensiblement d'un corps d'inspecteurs qui parcourent le monde.

3. <http://www.bigbrotherawards.eu.org>

changement de statut. De la marchandise d'abord, de l'économie ensuite.

Première évidence : l'entreprise ne vend plus seulement des choses mais des signes. Les biens matériels sont toujours davantage associés à des symboles, donc à de l'immatériel : information, loisirs, styles de vie, possibilités d'identification. La marchandise s'identifie moins à de l'utilité, à une promesse de jouissance ou à un symbole de réussite sociale. Elle « signifie » de plus en plus : de la santé, de l'image du corps ou de l'intelligence, de la modernité, une appartenance, du lien social, du « cool », de la différence, du politiquement correct, du générationnel, de la branchitude ou de l'américanité. La marque ne reflète plus la culture comme s'il s'agissait de s'en approprier les valeurs et les incorporer, elle *est* la culture. Elle se veut « style de vie » et « système de valeurs », certains disent religion<sup>1</sup>. L'économie se transforme en vente d'expérience et négoce d'états de conscience. La thèse que le produit nous vend l'imaginaire d'une marque et le droit d'entrée dans une communauté fantasmée gagne du terrain<sup>2</sup>. Elle implique la surexposition de la marchandise, investie de valeurs extra-utilitaires et extra-économiques. Dans cette exacte mesure, elle s'expose au conflit des valeurs.

La même chose vaut — et c'est notre second constat — pour l'activité économique tout court. Le déclin du politique, marqué par le renoncement aux grandes utopies mobilisatrices et par la réduction de l'activité politique à une sage gestion, convainc chacun de l'existence d'une économie déterminante en dernière instance, comme destin indépassable. Ainsi, la notion que l'État ne

1. Termes relevés plusieurs fois dans la très significative émission diffusée par Arte le 9 mai 2002 : *McWorld, la culture des marques*.

2. Outre Naomi Klein précitée, c'est une conception qui est défendue par quelques grands essais à succès comme *Djihad versus MCWorld*, de Benjamin Barber (Hachette 2001) ou *L'Âge de l'accès* de Jeremy Rifkin (La Découverte, 2000).

## De la désinformation idéologique au soupçon éthique

peut presque plus rien contre les règles de l'économie mondialisée est devenue un lieu commun. Quant à la résistance avant-gardiste contre l'ordre économique utilitaire, elle n'a plus grand sens depuis que marginalité, différence et contre-culture sont des arguments de vente. Du coup, il devient évident que les vrais combats auront de plus en plus pour cible des entreprises comme si la souveraineté s'était transférée dans le système économique. C'est sans doute le seul point sur lequel s'accordent les stratèges de la Maison-Blanche, qui mettent des moyens régaliens au service de la guerre économique, et les protestataires, qui ont fait de tous les sommets de type Gênes ou Porto Allegre des symboles de la lutte contre la globalisation. La politique devient apolitique en ce sens que la latitude d'action des acteurs traditionnels comme l'État est bornée par les contraintes technico-économiques et par le resserrement du spectre idéologique. Mais le non-politique, technique, production, mœurs privées, santé, devient hautement politique.

## Désigner et dénoncer

Ces données connues ont une implication très simple : la conjonction de cet arrière-fond symbolique et des possibilités de propagation sur Internet, paradis des rumeurs, ouvre d'immenses possibilités offensives. Les stratèges de la guerre économique rêvent de rééditer des cas d'école : *Body Shop* dont l'action chuta de 30 % en 1993 lorsqu'il fut révélé que cette entreprise, fêue d'écologie, employait des enfants. Ou encore Perrier qui perdit, en 1990, d'immenses parts de marché parce que des traces de benzène avaient été trouvées dans ses bouteilles.

On parle maintenant de « rumoristes » pour désigner les créateurs de rumeurs sur Internet<sup>1</sup>. Il existe également d'excel-

1. Voir le Monde Interactif du 23 mai 2001, <http://www.lemonde.fr>  
« Du simple canular à la désinformation orchestrée. »

lents manuels qui analysent les opérations<sup>1</sup> de décrédibilisation et d'infoguerre, des sites<sup>2</sup>, des écoles<sup>3</sup> qui s'y consacrent. Nous leur empruntons donc les exemples qui suivent.

Dès 1995-1996, Total est cloué au pilori dans les forums de discussion sur Internet. La société pétrolière est soupçonnée d'aider le régime totalitaire birman à combattre la guérilla, de blanchir l'argent du trafic de drogue, d'employer des travailleurs forcés. En 1999, on la dit victime d'un « rumoriste » qui fait circuler de faux courriels entre dirigeants de la multinationale<sup>4</sup>. En 1996, la filiale pharmaceutique d'Elf, Sanofi, s'inquiète de rumeurs sur Internet : elles attribuent à certains de ses produits des effets sexuels imaginaires et risquent de provoquer des catastrophes. La société Belvédère qui commercialise de la vodka polonaise est victime d'une attaque via un site Internet. L'offensive est menée par une société américaine spécialisée : Belvédère voit chuter son action sous l'effet des rumeurs.

Airbus est régulièrement confronté à des « témoignages d'experts » sur les forums d'Internet, qui remettent en cause la fiabilité de ses avions. Son modèle A320 en particulier est la cible de sites spécialisés. Des *mailing list* électroniques reçoivent les pires bruits sur la fiabilité de son ordinateur de bord, des taux effrayants d'incidents et accidents constatés... De façon plus générale, le dénigrement du concurrent est un procédé pratiqué dans l'aéronautique depuis les années soixante-dix<sup>5</sup>, mais auquel les nouvelles technologies donnent une efficacité redoutable.

1. Rémi Kauffer, *L'Arme de la désinformation Les multinationales américaines en guerre contre l'Europe*, Grasset, 1999 et Didier Lucas et Alain Tiffreau, *Guerre économique et information Les stratégies de subversion*, Ellipses, 2001.

2. Voir <http://www.infoguerre.com> ou <http://www.guerreco.com>.

3. <http://www.ege.eslca.fr> École de Guerre Économique (EGE).

4. C'est, du moins, un *rumoriste* qui s'en vante sur <http://www.examineur.com>.

5. Voir le chapitre « Duel de géants dans le ciel » dans *L'Arme de la désinformation*, précité de Rémi Kauffer.

## De la désinformation idéologique au soupçon éthique

Monsanto est déstabilisé en quelques semaines par une campagne sur Internet portant sur les OGM. En 1999, Mitsubishi, sur le point de construire au Mexique une énorme usine, en est empêché par une campagne : l'usine menacerait un écosystème indispensable à la reproduction des baleines. De fausses offres alléchantes de Nokia, provoquent engorgement, perte de temps et démentis. Dans l'affaire de l'Erika, Total se plaint de la diffusion de photos truquées et de fausses correspondances internes. Mais ce n'est rien par rapport à l'offensive qui, en 1995, empêchera Shell de couler au large de l'Écosse la plateforme pétrolière inexploitable de Brent Spar. Le tout sur la foi d'un rapport de Greenpeace dont il se révélera, mais trop tard, qu'il est sans fondement. Greenpeace reconnaîtra assez mollement son « erreur »<sup>1</sup>. En règle générale, le but d'une rumeur malicieuse est moins d'être vraiment crue que de créer une atmosphère de soupçon ou de contraindre.

Parfois il n'est pas facile de distinguer l'action de guerre économique du canular : le bruit affirmant que Kentucky Fried Chiken emploie des OGM à la place de poulet, ou la rumeur suivant laquelle certains shampoings contiendraient du sulfate de sodium Laureth, hautement cancérigène, sont-elles des farces ou des offensives de la concurrence ?

L'effet Internet joue à plein. On cite souvent l'effet d'un site<sup>2</sup> tenu par un seul individu : en relatant les difficultés de consommateurs, il a inquiété la toute-puissante Ford Company dont les ventes subirent le contrecoup. Souvent aussi, la désinformation consiste en l'envoi de faux communiqués de presse pour faire chuter le cours d'une action. Ainsi, en mars 2000, l'action de Lucent perd 3,6 % en quelques minutes de cette façon<sup>3</sup>. En octobre de la même année, c'est l'action Alcatel qui plonge jusqu'à 10 %, toujours à cause de rumeurs électronique.

1. Voir à ce sujet <http://www.greenpeace.org/odumping/oilinstall/monitorbs/remisound.htm>.

2. <http://www.blueovalnews.com>

3. Cette affaire a été jugée par un tribunal new-yorkais en 2001.

ques malicieuses. Pendant ce temps, des activistes « cyberhippies » se vantent d'avoir déstabilisé la société E-toys en quelques clics<sup>1</sup>.

La décrédibilisation de la victime auprès de l'opinion, depuis les groupes protestataires jusqu'aux consommateurs moyens, a, bien entendu, pour complément une stratégie du soupçon. Les autorités, de plus en plus liées par des normes de sécurité et par la crainte d'actions judiciaires, sont amenées à multiplier les difficultés, vérifications, refus, délais, expertises et contre-expertises qui empêchent un rival de s'installer sur un marché. Si lesdites autorités ne sont pas d'une bonne foi totale et prêtent une oreille favorable aux arguments favorables à leurs entreprises nationales, c'est mieux encore. Et s'il se trouve des relais de type ONG pour relayer l'offensive, le stratège a atteint son but.

L'intelligence économique\* dite pudiquement « offensive » a depuis longtemps traversé la ligne rouge qui sépare la quête d'information, l'organisation de leur exploitation et le domaine de l'illégal et de l'illégitime<sup>2</sup> : espionnage industriel, sabotage cybernétique ou pas, influence, corruption... Que l'on ait aussi franchi le seuil de la déstabilisation et mis au service de la guerre économique des moyens de guerre froide n'a rien pour étonner. Les spécialistes parlent maintenant de Mensonge Assisté par Ordinateur et évoquent des « logiciels de calomnie » qui naviguent sur les forums de discussion, repèrent des mots-clefs et déposent leur venin : bruit sur de mystérieux malaises à la suite de l'absorption du produit X, rapport d'experts étouffé sur les dangers de l'avion Y... La rumeur « plus vieux média du monde » est, elle aussi, devenue *high tech*<sup>3</sup>.

1. Voir <http://www.rtmark.com>.

2. Voir à ce sujet les analyses de <http://www.fsa.ulaval.ca:80/personnel/vernag>.

3. Il existe plusieurs sites francophones qui suivent cette actualité comme <http://www.ecoguerre.com> ou <http://www.infoguerre.com>, sans compter les indispensables dossiers de <http://www.strategic-road.com>



## Chapitre V

### Guerre et dominance informationnelles

Les thèmes précédents, le secret, la désinformation, évoquent tous un néologisme : la « guerre de l'information »<sup>1</sup>. Ce mot-valise regroupe des phénomènes d'affrontement inédits par écrans interposés et à l'abri des écrans. S'ils sont de divers ordres, militaire, politique, économique, sociétal<sup>2</sup>, tous mobilisent les technologies de l'information et de la communication.

La notion englobe donc un vaste domaine depuis le ravage sur des cerveaux électroniques jusqu'à la manipulation des cerveaux humains. Les pratiques qui en découlent peuvent viser à la quête d'une supériorité en termes de connaissance et de réactivité, mais incluent aussi la manipulation des perceptions et des opinions. Elles sont censées garantir le monopole de l'information pertinente, les savoirs vrais, plus la propagation de

1. « Guerre de l'information », souvent contractée en « Infoguerre » vient de l'expression américaine *Information warfare*. Sur cette terminologie, qui, on s'en doute, ne fait pas l'unanimité, on peut consulter de nombreux sites comme <http://www.defensenews.com>.

2. Il est devenu courant de parler de trois « classes » d'infoguerre : guerre de l'information « privée », plus ou moins délictueuse et intéressée, guerre économique, et guerre « globale » militaire et géopolitique par les nouvelles technologies. Voir par exemple le site/portail du créateur de cette terminologie, Winn Schwartau : <http://www.infowar.com> .

l'information utile, utile à des desseins stratégiques, s'entend, les croyances. Pour notre part, nous serions prêts à nous rallier à la terminologie de « guerre cognitive »<sup>1</sup> qui évoque davantage la valeur du savoir que les gadgets électroniques, mais à condition de préciser qu'il s'agit aussi de foi et d'illusion.

Les puristes objectent que la « vraie » guerre suppose mort d'homme. L'éventualité de la mort collective, symboliquement acceptée et techniquement organisée, fonde cette catégorie anthropologique. Mais on comprend bien en quel sens métaphorique est ici employé le mot « guerre ».

Le problème n'est pas linguistique. Il est idéologique. Le rapport entre la connaissance et la violence qui se dessine dans la nouvelle configuration technologique bouscule nos habitudes mentales.

## Gouvernement des choses et règne des signes

Nous héritons d'une tradition intellectuelle, qui remonte sans doute à Saint-Simon et à son « gouvernement des choses » : elle fait de l'amélioration des connaissances scientifiques et techniques et des moyens de communication une force par nature pacificatrice<sup>2</sup>. Son programme : réduction des obstacles que l'ignorance dresse entre les hommes, amélioration des méthodes de gestion et de prédiction sociale, abondance par la technologie, mais aussi transfert de l'essentiel de l'activité humaine depuis la production de choses vers l'accroissement des savoirs ou le maniement des signes. Cette thématique débouche au final

1. Voir à ce sujet l'ouvrage collectif *La Guerre cognitive L'Arme de la connaissance*, dirigé par Christian Harbulot et Didier Lucas, Lavauzelle, 2002, <http://www.lavauzelle.com>.

2. Armand Mattelart, *L'Invention de la communication*, La Découverte, 1994.

sur l'idée de l'abolition de la politique au profit de la technique et de la communication.

Dans les dernières décennies du XX<sup>e</sup> siècle, ce rêve, devenu celui d'une société post-industrielle, prend quelque consistance à mesure que s'affirme la puissance des technologies numériques. Bientôt, on dira société du savoir, de l'information ou de la communication<sup>1</sup>. Or ces trois notions — nous y reviendrons — ne se recouvrent que très partiellement. L'idée est que l'accroissement du savoir disponible — joint à la facilité de traitement et de partage des données — devient le moteur du changement social. Tout cela forme une vulgate ou idéologie dans l'air du temps. Le législateur se donne pour tâche d'aider la France à s'adapter à la révolution numérique<sup>2</sup>. Les économistes s'interrogent sur la réalité, la durabilité ou la désirabilité d'une nouvelle économie. Les chantres de l'ère numérique, du monde en réseaux ou de la cyberculture prospèrent. Les sciences dites de l'information et de la communication s'interrogent sur l'impact des NTIC\*. Et le débat intellectuel oscille souvent entre la célébration d'une promesse naïve, celle des paradis informationnels, et la dénonciation de l'aliénation technologique sur le ton de l'humaniste ronchon.

Car les critiques ne manquent pas : le culte, l'idéologie ou l'utopie de la communication suscitent des adversaires. La plupart protestent contre les mauvais usages de ces technologies, ou contre leur inégale répartition. Elles ne tiendraient pas leurs promesses par la faute de ceux qui en contrôlent l'usage dans un but marchand ou impérial. Les technologies auraient pour fonction de reproduire rapports de pouvoir et inégalités, voire,

1. Faute de place pour développer toutes ces notions, nous renverrons le lecteur à deux bonnes analyses historiques *Histoire de la société de l'information* d'Armand Mattelart (La Découverte, 2001) et *l'Imaginaire d'Internet* de Patrice Flichy (La Découverte, 2001).

2. <http://www.internet.gouv.fr/francais/indes.html> : pour suivre l'élaboration de la loi sur la société de l'information. Voir aussi <http://www.cnc.fr/riam> : site du RIAM qui coordonne les actions gouvernementales de recherche sur la Société de l'information.

tout simplement, de dissimuler l'hégémonie américaine<sup>1</sup>. Quand elles ne sont pas condamnées comme intrinsèquement aliénantes, formes de vie par substitution artificielle et pauvre.

Pour compliquer le débat, des faits récents justifient moins les promesses des plus optimistes. La plus si nouvelle économie a du plomb dans l'aile. La fin de l'histoire ou le nouvel ordre mondial sont repoussés *sine die*. Bref, l'allégresse technophile trouve moins de justifications. Les sociétés dites de l'information ou de l'immatériel reposaient paisiblement sur la gestion d'images séduisantes, la circulation fluide de données et le traitement performant de l'information. Du moins, c'est ce qui se disait. Le 11 septembre 2001 a montré la force des images symboliques, la fragilité des systèmes de données, l'inutilité de technologies sophistiquées dont ne résulte aucune connaissance opérante. Dans le match Djihad contre NTIC, rien ne prouve que le second l'emporte, ni que les deux soient inconciliables.

Le rêve d'Internet, paix et concorde dans un village électronique global nous paraît déjà aussi incongru qu'un autre rêve, centenaire celui-là. À savoir que le cinéma en permettant aux peuples de se connaître les empêcherait de se faire la guerre. Ou qu'une idée vieille de deux siècles : le chemin de fer entraînant la fin des conflits. Il n'y a pas de technologie bonne, pacificatrice ou démocratique, « par nature », dont il suffirait de laisser se dévoiler les heureuses potentialités, pourvu que les retards et

1. Quelques exemples de sites représentatifs : <http://www.iris.sgdg.org> Imaginons un Réseau Internet Solidaire. <http://www.itinerant.qc.ca/flicage2.htm> Site canadien sur le flicage au travail. <http://www.kumite.com/myths/home.htm>, <http://www.datafellows.fi/hox.htm>, <http://www.libertes-immuables.net> Sur les législations restrictives des libertés après le 11 septembre. <http://www.salon.com> Revue US. <http://www.assises.sgdg.org> Assises pour un Internet « non marchand ». <http://www.samizdat.net> Hébergement de sites « alternatifs ». <http://www.ctheory.com> Revue critique en anglais. <http://www.delis.sgdg.org> Droits et libertés face à l'informatisation de la société. <http://www.disinformation.com> Site américain où se retrouvent tous les adversaires des versions dites officielles que les médias donnent de l'actualité. <http://www.ecirioa.org/Observ.htm> Observatoire de la mondialisation.

## Guerre et dominance informationnelles

résistances des esprits obtus n'y fassent pas obstacle. Il y a des instruments au service de stratégies et qui rencontrent et nourrissent à la fois des facteurs symboliques.

Raison de plus pour rappeler quelques vérités anciennes. Les technologies de transmission ne changent les sociétés qu'autant qu'un milieu humain les reçoit et les accepte. (L'imprimerie n'eut pas le même impact dans la Chine confucéenne, dans le monde islamique et dans l'Europe de la Renaissance). Une technologie, avant de produire ses effets, doit s'insérer dans l'écologie des modes de transmission existants. (La télévision ne tue pas le cinéma, pas plus que l'écran ne tue l'écrit, mais ils en changent la place, l'autorité, l'usage dans une société donnée).

De même, les institutions, les mentalités ne changent pas par ères successives suivant la règle du tout ou rien. Il faut relativiser les périodisations : le plus moderne cohabite avec le plus archaïque et les taux de progression fabuleux d'Internet s'insèrent dans un environnement où la moitié des hommes n'a jamais passé un coup de téléphone. La difficulté est toujours de penser ce milieu où certains vivront comme au XXI<sup>e</sup> siècle et d'autres comme au XV<sup>e</sup>. Un monde où se chahutent le temps du changement technique, celui de l'action politique, celui des tendances lourdes démographiques et économiques et celui des cultures et mentalités. Faute de comprendre les interactions entre ces temps, tant d'anticipations brillantes se sont faites contredire par le retard de la conquête spatiale ou de l'équipement domotique, par le retour de l'archaïque. Les *futurecrates*<sup>1</sup> ne pensaient la technologie que

1. Par ce néologisme, mélange de « futurologues », qui signifie littéralement « ceux qui commandent au nom du futur », nous entendons désigner l'abondante production d'anticipations des « grandes tendances » auxquelles les auteurs, qui se trompent avec une touchante régularité, nous affirment qu'il faudra s'y adapter ou mourir. Pour un petit bêtisier, comportant notamment les plus grosses erreurs des futurologues des années 60 et 70 sur l'an 2000, voir notre ouvrage *Les Experts ou l'art de se tromper*, de Jules Verne à Bill Gates, Plon, 1996.

comme une force motrice, les changements sociaux se contentant de « suivre », avec plus ou moins de retard, la direction indiquée.

Pour notre part, nous reconnaissons volontiers que les techniques « autorisent mais ne déterminent pas », et qu'il est grand temps d'échapper au dilemme : paradis sur Terre grâce aux NTIC ou illusion et cache-sexe de la globalisation marchande. Or, une des meilleures façons de le faire, est de considérer la dimension du conflit. Un conflit qui aura l'information pour instrument, pour enjeu ou pour mesure. Il s'agira d'en contrôler le contenu, la possession ou la diffusion, à l'insu d'une victime ou au détriment d'un adversaire. Sur fond d'interrogations sur le pouvoir des *mass media*<sup>1</sup>, les Technologies de l'Information et de la Communication bouleversent les conditions de l'affrontement. Elles permettent de nouvelles formes d'hégémonie. Elles facilitent destruction et chaos *high tech*.

Le conflit est régi par les images, les croyances, les valeurs et les représentations, y compris sous les aspects d'utopies, d'idéologies ou de mythologies. Leur force d'attraction ne diminue pas avec la sophistication des techniques, au contraire.

## Plans de bataille

Ces rapports complexes entre la technique, les intérêts et les imaginaires ne se reflètent pas seulement à travers le débat sur la société de l'information. Il se trouve implicitement formulé dans un discours militaro-stratégique, économique-technique.

1. Rappelons à ceux qui pensent que la question du pouvoir des médias est « dépassée » et que les nouvelles technologies vont bientôt rendre nos craintes risibles, que dans la plupart des pays développés, la consommation de médias est la seconde activité après le travail.

## Guerre et dominance informationnelles

C'est celui de la Révolution dans les Affaires Militaires mais aussi de l'intelligence économique<sup>1</sup>.

La RMA\* (*Revolution in Military Affairs*<sup>2</sup>), doctrine officielle du Pentagone<sup>3</sup>, désigne à la fois l'adaptation du système militaire à l'ère de numérique. Elle suppose le projet d'un contrôle par les technologies de l'information et le *soft power\**, le pouvoir « doux » d'interdire tout conflit. Pareille « révolution » ne se borne pas à améliorer — mieux employer, rendre les arsenaux plus « intelligents », plus réactifs et mieux coordonnés. Elle doit faire abandonner les vieilles structures hiérarchiques et centralisatrices au profit d'un modèle, plus souple de partage des flux continus d'information. Un schéma qui n'est pas sans rappeler celle des entreprises virtuelles et des *managers* branchés.

Cette révolution bouscule les notions stratégiques. Ainsi les infrastructures adverses, civiles et militaires, les moyens de communication et de coordination deviennent des objectifs prioritaires : plus vite ils seront paralysés, plus fortes seront les chances que l'ennemi perde ses capacités perceptives, cognitives et décisionnelles, et partant de réaction effective.

Il faut anticiper, coordonner instantanément des forces dispersées, gérer des systèmes « interopérables », protéger ses propres vecteurs de communication et perturber ceux de l'autre. Il faut discriminer entre vraies données et leurres, voire amis et ennemis sur le terrain, déléguer à des niveaux inférieurs la capacité de traiter l'information et de décider instantanément. Il

1. À titre d'exemple [http://www.aracnet.com/~gtr/archive/info\\_war.html](http://www.aracnet.com/~gtr/archive/info_war.html) : *Global Technology Research, inc.* Site qui propose une bibliographie sur l'Information Warfare ou <http://www.iwar.org.uk> : consacré à l'Information Warfare, site britannique. Ou encore, pourquoi ne pas aller étudier dans une « école » comme <http://www.ndu.edu/inss/act/iwscvr.html> School of Information Warfare ou à <http://www.psycom.net/iwar.1.html> Institut d'Études avancées sur la Guerre de l'Information (*Institut For Advanced Studies os Information Warfare - IFASIW*) ?

2. Voir <http://www.geocities.com/Pentagon/7209/recherche.html>.

3. Même si la doctrine est d'origine soviétique.

faut enfin influencer et les décisions de l'ennemi, et les réactions de son opinion, et le soutien de la sienne, et la réaction des médias. Bref tout le processus stratégique serait à repenser.

La quête d'informations devient presque secondaire par rapport à la capacité à gérer de tels flux de données. L'automatisation de leur traitement en continu mène à une double fusion. D'abord entre l'acquisition de l'information, envisagée comme source de connaissance opérationnelle, et l'action. L'information, du virus informatique à la propagande ou à la déception, devient une puissance de frappe, transformant la structure de communication en cible prioritaire. Ensuite il y a fusion entre le militaire au sens strict et le diplomatique, l'économique, le médiatique. Cela suppose en amont la capacité à prévoir les risques de troubles, en aval celle de gérer les désordres postguerriers jusqu'au retour à la normale. La fonction militaire s'inscrit dans le cadre d'un projet quasiment cybernétique : réguler la planète par les technologies de l'information et presque « pour » elles. Le but de la géostratégie semble se confondre avec l'avènement planétaire de la société de l'information.

Toutes ces anticipations, et les rêveries qu'elles nourrissent sur des guerres zéro mort, menées proprement depuis des chambres de guerre, ne sont guère ou pas encore confirmées avec éclat par les faits. Après tout, quelle qu'ait été la contribution à la victoire des drones, des satellites, des marqueurs infrarouges et des ordinateurs, les Américains, en Afghanistan, ont surtout utilisé force bombardiers sur leurs adversaires taliban qui avaient la stupidité de déployer en lignes ou de rester dans les villes à attendre les missiles. Sans compter le rôle qu'ont joué les alliés au sol : les gens de l'Alliance du Nord n'ont rien d'*infowarriors* férus d'électronique. Mais, même comme mythe, la RMA reflète une étonnante mutation des mentalités. Après tout, la guerre nucléaire avec son jeu compliqué d'annonces, négociations et de contraintes proclamées ou encore l'IDS, l'Initiative de Défense Stratégique, la « guerre des étoiles » de Reagan étaient aussi des guerres purement virtuelles : personne



## Guerre et dominance informationnelles

ne savait comment elles se dérouleraient, ce qui « fonctionnerait » vraiment. De n'avoir existé que dans les cartons ne les a pas empêchées de changer la face du monde.

La plupart des remarques que nous venons de faire se transposent au monde de l'intelligence économique. Là aussi, le but ne devient plus uniquement de savoir (parfois illégalement et toujours inélegamment) ce que fait ou peut faire le concurrent. Comme en témoigne l'affaire Échelon\*, les moyens dits régaliens, notamment d'espionnage, sont reconvertis vers la guerre économique<sup>1</sup>. Guerre tout court et guerre économique subissent une commune évolution : environnement changeant, pression de l'escalade technologique, pensée stratégique en termes de sécurité, crises et périls globaux, volonté de pouvoir intervenir partout, automatisation de la gestion de l'information, décentralisation de son contrôle, exploitation de son ambivalence comme force de productivité et de destructivité, poids de l'avantage cognitif marginal (par exemple savoir un peu avant l'autre). Et le but commun, politique et économique devient la domination informationnelle<sup>2</sup>. Là encore, il faut tenir compte des vulnérabilités : celle des systèmes et structures par nature plus fragiles, celle du contenu de l'information avec le risque d'erreur, de rumeur ou de manipulation, mais aussi la dépendance des acteurs économiques à l'égard de leur image. Si l'armée adopte un modèle « civil », l'entreprise virtuelle se réclame des mêmes valeurs que la RMA : souplesse, réactivité, adaptabilité, connectivité, instantanéité. À moins que ce ne soit le contraire. Tout repose finalement sur la capacité d'anticiper des tendances, de gérer des flux et de coordonner des capacités de traitement. La guerre économique se transforme, elle aussi, en une guerre du

1. Le rapport du Parlement Européen sur Échelon est disponible sur [http://www.europarl.eu.int/stoa/default\\_en.htm](http://www.europarl.eu.int/stoa/default_en.htm).

2. Voir la très éclairante critique de ces notions par Philippe Baumard dans *Les Limites d'une économie de la guerre cognitive*, in *La Manipulation de l'Information* par C. Harbulot et D. Lucas, Éditions Lavauzelle, 2002.

temps. Il s'agit de savoir avant l'autre ce qui en tout état de cause sera vite public ou obsolète, de traiter plus vite l'information : affaire de commutation, en somme, puisqu'il s'agit de relier des éléments et des réseaux. Une même logique s'impose partout.

Longtemps, les rôles ont été bien répartis : l'autorité politique dirigeait la guerre, les militaires l'exécutaient, les civils la subissaient par contrecoup, les producteurs produisaient, les médias, chacun sur son territoire, exaltaient la justesse de leur cause et dénigraient l'ennemi.

C'est bien évidemment cette logique qui est remise en cause. Mais les raisons de ce bouleversement sont aussi dans la nature de la technique.

## **Utopie numérique, promesses des réseaux**

Le monde des NTIC, qu'on décrivait comme celui de l'invention perpétuelle, de l'intelligence collective et de l'accessibilité sans limite aux biens immatériels, a vite été hanté par l'obsession du risque, l'explosion de la capacité de nuisance, du cybercrime, de l'infoguerre, infodominance ou guerre cognitive. Dans le même mouvement, manipulation des traces, falsification des mémoires et transactions sont devenus plus accessibles au faible : le seuil d'entrée sur le champ de bataille s'est abaissé en proportion.

Facilités ? elles sont multiples. Les technologies numériques, en réduisant toute information, qu'il s'agisse d'une image animée ou d'un texte ou d'un programme, en un code unique digital (0 ou 1) permettent des modifications de la moindre de leur composante. Cette intervention peut s'effectuer à distance. En clair : toute information peut être truquée, altérée, traitée par l'usage du code numérique. Un virus remplace une bombe. Un modem suffit à rentrer sur le champ de

bataille. Un forum peut lancer une rumeur ou une désinformation. Une recette reprise sur un site transforme n'importe quel gamin (un *script kiddie*) en redoutable pirate. Une pétition sur la Toile vaut un brevet de résistance au totalitarisme. Détruire la mémoire ou la réputation d'un concurrent est moins risqué que de lui envoyer des saboteurs. Un écran vous permet de vous battre sur un autre continent. Un site « anonymiseur » suffit à assurer l'impunité. Une *page perso* vous transforme en éditeur de brûlot d'opinion. Un algorithme permet de prendre le contrôle d'une machine distante. Vos victimes ne rendent pas les coups et n'agonisent pas disgracieusement sous vos yeux. Tentant, non ?

Du coup, la possibilité d'entamer une « infra-guerre » s'ouvre à des acteurs divers, économiques, « privés », militants, délinquants ; plus besoin d'avoir le monopole de la violence légitime, caractéristique de l'État, maître de la guerre.

Faire perdre du temps, par exemple, à une entreprise peut la conduire très vite à la catastrophe. Or, au lieu d'employer le temps et l'énergie d'assaillants de chair et de sang, il est possible de les remplacer par des agents virtuels qui paralysent le site de la victime par leur seul nombre et par la répétition de nuisances qui, à une autre échelle, seraient jugées bénignes.

Le numérique implique des fragilités liées au temps. Le fait que l'information aille toujours plus vite dans nos sociétés, qu'elle fonctionne en flux tendus et qu'il faille réagir instantanément, implique aussi que nous sommes entrés dans une économie du temps. Le temps perdu ou gagné a acquis une valeur stratégique. Gagner quinze jours sur le concurrent par l'intelligence économique est un avantage important, gagner quelques secondes sur des réactions instantanées peut décider d'une guerre. Corollaire du corollaire : faire perdre du temps à l'autre, c'est lui infliger un préjudice. Quant un virus provoque un déni d'accès sur quelques sites importants (c'est-à-dire les bloque quelques heures) l'économie frémit. Faire perdre du temps par des leurres ou des ruses, c'est déjà vaincre.

Bien sûr, jusqu'à présent, la nocivité d'Internet a surtout consisté en la diffusion de légendes urbaines, canulars, rumeurs, intoxication et désinformation. Sans ouvrir le très vaste dossier du coût global de la sécurité ou de la nocivité des pirates sur la Toile, rappelons simplement que la « bombe informatique »\* dont parlait Paul Virilio<sup>1</sup> n'a jamais explosé, pas plus que l'accident suprême attendu, le chaos numérique total, ne s'est produit. Même au lendemain du 11 septembre (surtout au lendemain du 11 septembre), les spécialistes américains ont agité le spectre du cyberterrorisme\* et réclamé davantage de mesures et de millions de dollars pour protéger les infrastructures vitales<sup>2</sup>. Pourquoi le système n'a-t-il pas été gagné par le chaos ? Pourquoi des terroristes n'ont-ils jamais songé, puisque cela semble si facile sur le papier, à provoquer un « Waterloo » électronique ?

Personne ne possède sans doute la réponse parce que :

a) l'information dont nous disposons est incomplète, par souci de sécurité ou exagérée par intérêt ;

b) le déroulement d'une crise de ce type, que personne n'a jamais vécue, et qui suppose la synergie de plusieurs formes de désordre, est pour le moins hasardeux ;

c) il y a une composante psychologique ou symbolique qui nous échappe, au moins dans le cas du terrorisme (peut-il se satisfaire d'une panique informatique et si oui que peut-il revendiquer ou menacer dans ce cas ?)<sup>3</sup>.

Bref, nous ne pouvons pas évaluer l'étendue des périls. Mais il y a une chose certaine : le discours inverse, celui qui voit dans l'expansion des réseaux un phénomène par nature pacifiant est, lui, radicalement faux. Ainsi, le principe du numérique

1. Paul Virilio, *La Bombe informatique*, Galilée, 1998.

2. L'actuel « tsar » de la cybersécurité, Robert Clarke qui dirige le NIPC (Centre de protection des infrastructures nationales) créé sous Clinton, a annoncé un budget de 38 milliards de dollars en 2003, pour éviter le fameux « Pearl Harbour » informatique.

3. Voir l'annexe sur le cyberterrorisme.

## Guerre et dominance informationnelles

suppose que l'information soit appropriable, imitable, reproductible, modifiable... Ce qui engendre un énorme problème de discrimination des contenus. Mais le principe complémentaire du réseau, pose, lui, le problème des stratégies de contagion et de perturbation. Il suppose de nouvelles façons de penser : sur tout réseau, le pouvoir consiste à contrôler le flux et le contenu de ce qui circule (et d'abord l'information), mais aussi les règles et les nœuds de circulation.

Ce modèle du réseau est réputé adapté à la circulation des biens immatériels : vitesse, répartition en tout point des ressources et des accès, détachement des contraintes territoriales, relations aisées entre acteurs, reconfigurations rapides. La dimension politique du réseau (ou plutôt le fonctionnement de communautés sur le modèle du réseau) n'a pas non plus échappé aux chercheurs. Manuel Castells, qui nomme « société en réseaux » ce que d'autres baptisent société de l'information, remarque : « Les réseaux sont parfaitement appropriés à une économie de type capitaliste reposant sur la flexibilité et l'adaptabilité ; à une culture de la déconstruction et de la reconstruction sans fin ; à un système politique conçu pour traiter instantanément des valeurs et humeurs publiques changeantes ; à une organisation sociale visant à la négation de l'espace et à l'annihilation du temps. La morphologie du réseau opère néanmoins de spectaculaires réorganisations des relations de pouvoir. Les commutateurs qui connectent les réseaux (par exemple, les flux financiers qui prennent le contrôle d'empires médiatiques exerçant une influence sur les processus politiques) sont les instruments privilégiés du pouvoir, et ceux qui manient les commutateurs détiennent le pouvoir. »<sup>1</sup>

Ceci est vrai pour l'économie. La mythologie contemporaine, notamment celle du discours *managerial*, exalte le réseau, intelligent, créatif, souple, fonctionnant à l'immatériel, à la

1. Manuel Castells, précité, Tome I, p. 527

coopération et à l'innovation. Il s'oppose facilement au hiérarchique, au fixe, au rigide, aux anciennes contraintes du temps et de l'espace, à la « vieille » entreprise ou à la vieille organisation. On rappelle que celles-ci reposaient sur le monopole de l'autorité et de la connaissance, donc sur leur circulation verticale, quasi militaire : les informations remontent, les ordres descendent. Bref le réseau serait postmoderne et démocratique, et branché. En témoigne l'image de l'entreprise virtuelle, à la fois mondialisée et décentralisée, éclatée par la multiplication du télétravail ou des communautés créatives temporairement orientées vers un projet, sans horaires fixes, reliant des groupes de créatifs en perpétuelle ébullition, échangeant des données instantanées entre hommes terminaux, et vivant finalement la vitesse de rotation de son capital intellectuel. Dans ce portrait, tout contredit la vision traditionnelle d'une entreprise où certains, en des lieux et des moments appropriés, se colletent à la matière, répétant les gestes appris, tandis que les autres les dirigent et conçoivent.

De fait, les débats sur l'impact d'Internet témoignent de trois approches des relations entre réseaux et politique. La première insiste sur les facilités que les premiers apportent à des pratiques politiques plus anciennes : accès des citoyens à l'information publique, économie de paperasseries, possibilités d'expressions pour les associations et mouvements de la société civile. La seconde voit plutôt dans le réseau la source de nouvelles pratiques de la politique : vote électronique ou démocratie directe « en ligne »\*, voire la « diplomatie des réseaux » que prônait Brezinski, conseiller du Président Carter à la fin des années soixante-dix, ou encore « e-contestation » des réseaux protestataires anti-mondialisation. Bref des façons de court-circuiter des institutions et médiations plus anciennes. Les plus utopistes ou les plus audacieux voient dans le modèle du réseau une façon d'abolir la politique, ou d'y échapper : constitution de communautés virtuelles ou de ce que Hakim Bey, le pape des cybercontestataires américains,

nomme des « Zones d'autonomie temporaire ». Le réseau serait alors hors territoire, hors loi, hors État, symbole et instrument d'une affirmation individualiste : chacun crée son cybermonde.

## Le réseau vulnérable

La même grille peut s'appliquer au réseau et au conflit. Le réseau peut-il faciliter la pratique du conflit ? en transformer la nature ? Supprimer le conflit ?

Tout réseau, en un premier sens, est une structure faite de liens multiples formant entrelacement. Le réseau est censé faciliter l'interconnexion souple et rapide, permettre la meilleure liaison entre tous les points, en particulier pour l'information. Il a des caractéristiques formelles (les interactions possibles) et téléologiques (il est orienté vers une finalité). La fonction du réseau serait alors de faire circuler des flux au mieux. Mais, en un second sens, le réseau évoque des communautés, des solidarités obscures, voire des sociétés occultes, produisant, via ce mode de transmission réticulaire, un échange d'avantages et de savoirs. Cet échange est plus ou moins clandestin, ou, du moins, incompréhensible au non-initié. Il en résulte souvent une clôture au monde extérieur : un réseau pédophile, terroriste, ou un réseau basé sur des solidarités idéologiques ou sur l'intérêt. Même les réseaux les plus « innocents », chapelles intellectuelles, bandes de copains, anciens de ceci ou de cela, reposent sur un système d'exclusion, sur des codes et protocoles implicites, sur des solidarités propres. Dans la pratique, les deux caractères se mêlent : les performances des vecteurs techniques nourrissent des pratiques sociales. Celles-ci supposent des règles souvent difficiles à formaliser, de l'implicite, des intérêts, des coopérations, mais aussi des exclusions et des secrets. Contrôler un réseau suppose que l'on contrôle un contenu, ce qui circule, une structure de circulation et des règles ou protocoles.

Le réseau est difficile à interrompre : Arpanet, ancêtre d'Internet, n'avait pas d'autre raison d'exister que de résister à des tentatives d'interruption du système de communication militaire US. En revanche, il est facile à contaminer : ce qui y entre une fois tendra à y demeurer ou à y proliférer. C'est, par excellence, le domaine du dérèglement épidémique aux origines incertaines et à la propagation incontrôlable. Le conflit obéira donc à des règles différentes, selon que l'on lutte pour le réseau (pour le préserver en bon état de marche), contre le réseau (pour le perturber) ou sur le réseau (pour infliger un dommage à un autre acteur). Tous ces points prennent toute leur importance en une période où l'on parle de plus en plus de guerre en réseaux et de terrorisme en réseaux, après avoir célébré l'entreprise en réseaux, le savoir en réseaux<sup>1</sup>. Enfin, la structure du réseau n'est pas nécessairement « égalitaire » ou démocratique au sens où tout ce qui circulerait serait accessible à tous, partout. Elle recèle des nœuds de pouvoir, comme elle suppose des nœuds de circulation : c'est le pouvoir des commutateurs<sup>2</sup>. Le pouvoir de diriger et de sélectionner les flux, y compris les flux d'attention du public, la capacité d'être aux points bien innervés, de combiner les éléments, devient un mode d'influence redoutable, même s'il n'est plus le plus visible.

Tout rêve de *Pax Electronica* se heurte à une double contradiction. À toute technologie de contrôle s'oppose une technologie plus récente de prédation, de dissimulation, de perturbation. En particulier sur des réseaux qui valent ce que vaut leur maillon le plus faible, la faille technologique est immédiatement connue et exploitée. Mais le contournement par le bas n'est pas moins redoutable. Le « progrès » technologique est aussi impuissant à éradiquer le ressentiment de ses ennemis qu'à contrer leurs

1. Le lecteur intéressé trouvera de nombreux textes des deux pontes de la « netwar », Arquilla et Ronfeldt sur le site de la *Rand Organization* : <http://www.rand.org>.

2. Cette notion très éclairante a été développée par Marc Guillaume dans *L'Empire des réseaux*, Descartes et Cie, 1999.



méthodes. On peut avoir les meilleurs satellites et *espionciels* et se trouver démuni devant des barbus enturbannés. Le réseau mondial voué à la prévention des risques, à la réadaptation, à la dissémination du pouvoir d'initiative, à l'intériorisation des objectifs par les acteurs est une sorte de grosse machine cybernétique fragile face aux micro-réseaux offensifs.

Nous avons vu que la société en réseaux se trouve confrontée au terrorisme en réseaux. Déterritorialisée, faisant aisément circuler capitaux, armes et combattants d'un pays à l'autre, d'un groupe de soutien à un second, capable de se concerter sans doute largement via le Web, mais aussi par des liens beaucoup plus archaïques ou informels (réseaux tribaux ou familiaux par exemple), n'offrant aucune cible, les atteignant toutes, l'organisation terroriste donne là une terrible leçon de stratégie postmoderne.

Dans un autre registre — et sans faire d'amalgame — des coordinations mondiales contre la mondialisation semblent aussi illustrer le vieux slogan « marcher séparément, frapper ensemble » revu à la mode cyber. Beaucoup ont été surpris par la capacité offensive de groupes dispersés, donc difficiles à repérer et à anticiper, dépourvus de structures lourdes mais capables de converger vers un objectif commun, les protestations anti-mondialisation de Gênes par exemple, pour une action brève et intense. Pareille capacité dépend entre autres facteurs, outre les motivations idéologiques, la communauté d'objectifs et la souplesse des modes de décision, de l'instantanéité de la coopération et d'un accès à l'information en tout point. Donc, d'Internet. Ici l'outil ne se contente pas de faciliter l'action militante par des liaisons plus rapides, il en change les modalités et les acteurs. Le léger offensif l'emporte sur le lourd pataud.

Quand se combine le mode de diffusion pyramidal des *mass media* (un émetteur, une multitude de récepteurs), plus, le mode de propagation « viral » des nouveaux médias (tous émetteurs, tous récepteurs, tous connectés), le résultat est redoutable. Contrôler les flux d'informations positives ou

négatives devient le ressort le plus intime de la véritable hégémonie, qu'il s'agisse de nouvelles du monde, d'ordres de Bourse, de ce qu'il est convenu d'appeler « économie de l'attention », de connaissances scientifiques.

Les vulnérabilités sont d'abord organisationnelles. La solidarité de fait des structures vitales d'un pays (transport, communication, approvisionnement énergétique), la monoculture technologique évoquée plus haut, notre dépendance de circuits informationnels fiables pour la coordination ou les transactions, les interrelations incessantes et les transferts de données décisives, la possibilité au moins théorique d'acquérir un pouvoir sur la vie d'un citoyen en corrélant des bases de données, parfois isolément très triviales et innocentes. Ce sont autant de possibilités de mini catastrophes. Les réseaux sont sensibles à la contagion, à commencer par celle du désordre. À preuve, l'obsession américaine d'une paralysie de ses réseaux informatiques, financiers, routiers, énergétiques.

Faut-il pour autant tomber dans le catastrophisme symétrique ? Décréter que l'internaute est un loup pour l'internaute ? Que le réseau implique la lutte de tous contre tous et le principe de chaos ? Que nous perdrons sur tous les plans en vertu du principe d'addition ? Que nous allons vers un monde où il y aura et des boucliers antimissiles et des gosses qui se massacrent à la machette, et *Big Brother* et la barbarie archaïque, et des *hackers* et des bandes urbaines ? Disons pour faire simple : hégémonie *high tech* plus barbaries *low tech* ?

Pour répondre à cette question, nous n'avons que deux hypothèses crédibles. Nos anticipations technologiques seront fausses, nos motivations symboliques seront déterminantes.

Nos anticipations des capacités de manipulation ou de dérèglement de nouvelles technologies sont fatalement erronées. Personne n'a jamais lancé une cyberguerre, ni n'a signé une cyberpaix. Nous ignorons l'efficacité des moyens de guerre de l'information, pour le moment virtuels, mais nous connaissons les faiblesses de ce qui existe déjà. Il suffit de suivre l'actua-

lité. Parallèlement, la gravité de la guerre de l'information économique se révèle tout aussi difficile à estimer : ni les victimes qui n'ont pas intérêt à révéler leurs pertes, ni les auteurs qui par définition n'avouent jamais, n'ont de raison de dire la vérité. Il n'existe guère de cybergendarmerie pour faire des constats. Pour savoir si telle affaire de déstabilisation, de déni d'accès ou d'intelligence économique (euphémisme pour espionnage), si telle manipulation ont vraiment produit de tels dommages. Pour évaluer la gravité des pratiques « hypercompétitives »\* (autre bel euphémisme), il faut se rabattre sur le sensationnalisme journalistique et sur les marchands de sécurité. Nous en savons autant qu'un général qui, en guise de batailles, n'aurait disputé que des *kriegspiels* pour soldats de plombs. Retenons que nos anticipations des guerres de 2010 ont autant de chances d'être ridicules que nos anticipations de l'an 2000 faites vingt ou trente ans avant.

Seconde leçon : le symbolique se venge. Un conflit, militaire, idéologique, économique, peu importe, ne se réduit jamais à un calcul de forces techniques et moins encore à la mise en œuvre de puissances matérielles. Tout ce qui est techniquement possible ne sera pas pratiquement réalisé, mais plus de technologie, implique aussi plus d'idéologie.

Que nous dit là-dessus l'actualité récente ? Que croyance et volonté sont à la fois cible et moteur des conflits. Que la foi n'est pas soluble dans les données. Que l'art de montrer des victimes est plus important que celui de faire des victimes. Que la science de la guerre est d'abord celle de faire-croire. Que les masses comprennent davantage les blessures et sacrifices emblématiques que les statistiques. Que le plus technologique peut se mettre au service du plus archaïque. Qu'une technique qui agit sur les choses n'est rien sans une pragmatique qui agit sur les gens. Et, qu'en ce domaine, on n'a inventé que deux sortes d'outils : des armes et des médias. Outre le fait d'agir, comme les outils ordinaires sur la matière et l'énergie, ceux-là agissent sur les chairs et les cerveaux.

## Infodominance

Or, précisément, ces outils-là sont pensés par les stratèges contemporains en termes d'infodominance.

En un sens initial, « infodominance », ou dominance informationnelle, est un néologisme d'origine militaire désignant un avantage tactique, opérationnel. Il se réfère surtout aux moyens techniques de connaître le champ de bataille et de plonger l'*Autre* dans le brouillard. L'infodominance repose sur une différence de savoir entre adversaires. Il faut, en amont, des technologies de surveillance, ou intégration visant à la localisation et l'anticipation de l'initiative adverse, puis une réaction instantanée et ultra ciblée. Au moment de la décision, il faut pouvoir modéliser l'affrontement, agir sur le territoire comme sur une carte. Outre cela il faut pouvoir priver l'adversaire de cette même aptitude, pervertir ses moyens de perception et d'organisation. Simuler, stimuler, dissimuler. Et ce, à un tel point que la différence de capacité confère une différence de statut. L'un des adversaires a acquis omnipotence, omniscience et ubiquité ; l'autre, idéologiquement ou juridiquement criminalisé, est traqué plutôt que véritablement combattu.

Du moins en théorie ! Car la pratique révèle les limitations de cette vision fondée sur une guerre de la certitude et de l'incertitude. D'une part, cette perspective confond agir sur les choses et agir sur les gens. L'adversaire n'est pas une donnée ou une chose, c'est un acteur. Il n'est pas long à découvrir les failles des systèmes technologiques : une vulnérabilité dans un modèle technique repéré par un attaquant est vite connue dans des systèmes de monoculture technique. Ou encore, par des tactiques de perturbation, telles que leurres, faux signaux, dissimulation, il peut affoler des systèmes ultra sophistiqués, à supposer qu'ils ne s'affolent pas eux-mêmes à

## Guerre et dominance informationnelles

tout vouloir prévoir et prévenir. Le faible, le petit, le souple, le rapide, le rustique, le clandestin se réadaptent très vite et surprennent les grosses machines coûteuses.

En un second sens, plus géostratégique, « infodominance » désigne un objectif économique et politique global : la gestion du monde par et pour les technologies de l'information. Par et pour le contrôle des perceptions, volontés, savoirs et modes de relation de ceux qu'il faudra bien appeler les infodominés. L'infodominance devient programme. Il ne s'agit plus du gain d'un avantage dans le conflit, mais de la transformation des règles du conflit, voire au stade ultime de l'abolition du conflit (le règne des choses et du droit). Ceci au prix d'une extension. Il est désormais question de contrôler les normes, les standards, les réseaux qui servent à la répartition de l'information. Voire proposer à la planète entière un ensemble de croyances et d'objectifs. Le passage à la société de l'information, envisagé comme perspective d'un nouveau déterminisme historique.

L'infodominance est une utopie en trois étapes :

— *au stade 1, les NTIC améliorent les outils traditionnels du conflit* et donnent un avantage décisif (cognitif, opérationnel, organisationnel) à une puissance à la pointe de l'évolution.

— *au stade 2, l'infodominance ainsi acquise transforme la nature du conflit*. Il devient nécessairement asymétrique et multiforme. Asymétrique, les acteurs n'ont plus le même statut (acteurs infra étatiques, criminels ou États criminels contre la puissance internationale). Le territoire n'est plus le même : les locaux affrontent depuis leur glèbe les globaux qui jouissent d'une sorte d'ubiquité. Le conflit devient multiforme. Les anciennes instances, politique, militaire, économique, culturel, se confondent.

— *au stade 3, l'infodominance est parachevée* : elle prévient le conflit. Il disparaît au profit du règne des techniques. Fin de partie, fin de l'histoire !

Bien évidemment cette conception appelle des critiques :

— *même au stade 1, opérationnel, l'efficacité absolue des NTIC est loin d'être prouvée.* Les bombardements du Kosovo ou le conflit actuel montrent les ratés des systèmes de surveillance, leur tendance à l'emballement, leur vulnérabilité aux leurres, leurs surprenantes déficiences face aux technologies rustiques, leur négligence du facteur humain, psychologique ou culturel.

— *la propriété d'une technologie, c'est de pouvoir se reproduire :* celui qui dispose des mêmes connaissances et des mêmes moyens peut réaliser les mêmes performances. Corollairement, la « faiblesse » d'une technologie peut être répandue une fois détectée : elle affectera alors tous les systèmes recourant à la même technologie. Traduction : il suffit d'un bon cerveau et de quelques ressources pour s'emparer de la technologie de l'adversaire et pour en exploiter toutes les failles.

Croire qu'il n'existe plus d'ennemis et qu'on est en charge de l'Histoire, de tout contrôler, est le meilleur moyen de devenir l'ennemi de tout le monde, ou plus exactement de tous ceux qui croient que vous êtes effectivement le responsable de l'état du monde. C'est offrir le plus puissant ressort à l'idéologie : la croyance en une cause unique du mal. Mais c'est aussi, se condamner à assumer tous les désordres de la planète. C'est offrir à l'adversaire la possibilité de jouer et de vos faiblesses techniques et de ses forces symboliques. L'hyperpuissance devient l'hypercause, explication et objectif de tous les ressentiments. Si le système est présent partout il semble responsable de tout.

Plus le modèle « tout technologique » prétend s'exporter, en vertu du principe que tous les problèmes sont techniques et que les hommes sont partout fondamentalement les mêmes, animés par les mêmes besoins rationnels, plus il suscite son contraire. Dans le même mouvement, le puissant se condamne à être global, à assurer une défense tous azimuts contre les risques de désordre, bref à garantir un monde zéro

## Guerre et dominance informationnelles

défaut. À expulser ainsi la notion d'ennemi, on s'expose au risque du retour de l'ennemi, ou plutôt au danger de devenir le seul ennemi possible.





## Conclusion

Les Nouvelles Violences Symboliques et Techniques que nous avons décrites sont sous le signe du paradoxe.

Elles sont politiques : elles mettent en jeu le pouvoir et les règles de son fonctionnement. En cela, elles reflètent une politisation de domaines comme la religion, l'usage des technologies, le crime organisé, l'activité économique. Il n'est pas faux de dire, pêle-mêle, que les *hackers*, la secte *Aum*, *Unabomber*, la NSA\*, les militants *anti-Big Brother*, les cyberhippies, la fondation Soros, les narcotraficants colombiens proches des FARC, CNN, les membres du réseau d'information antiglobalisation Indymedia, ou le Chaos Computer Club « font » de la politique. Si l'on entend par là qu'ils sont animés par des visions d'un état du monde souhaitable, qu'ils s'organisent pour agir sur les décisions publiques — pour certains en refusant l'existence de décisions publiques — et que, directement ou indirectement, le résultat de leur activité sera que des hommes obéiront à d'autres hommes, alors, oui, il s'agit de politique.

Mais, par rapport à nos conceptions classiques des acteurs, des motivations ou des méthodes politiques, tous ces phénomènes s'expliquent avec difficulté et se classent malaisément. Ils paraissent hybrides et incertains. Il n'est pas commode de retrouver les distinctions entre privé et public, national et international, civil et militaire... Qu'est-ce qu'al Quaïda : une secte, un parti clandestin, une nébuleuse de groupes de combat ? Comment décrire le « message » des « miliciens » auteurs de l'attentat de 1995 à Oklahoma City ? D'extrême

droite, de religieux-fondamentalistes, de paranoïaques-millénaristes ? La guerre économique traduit-elle la privatisation de moyens étatiques ou l'intervention de moyens régaliens au service d'intérêts privés ? Les instances politiques contrôlent-elles quoi que ce soit dans le cybermonde ? Le pouvoir des médias est-il au service d'une idéologie et d'intérêts ou les médias sont-ils l'idéologie ?

Une partie de la réponse est dans la distinction entre politique et étatique. À l'évidence, la figure traditionnelle de l'État ne correspond guère aux changements que nous avons décrits. Il s'y adapte mal dans l'espace à cause de la mondialisation des flux et de l'anarchie des territoires. Il s'y adapte mal dans le temps : le rythme du changement technologique échappe à l'autorité ou à la réglementation. Il s'y adapte mal psychologiquement. Un fonctionnaire, fut-il de la Défense, n'est pas vraiment préparé à comprendre la mentalité d'un kamikaze salafiste, d'un gangsterroriste, des membres d'une cybercommunauté... Il appréhende mal des gens qui ne cherchent pas à renverser un système ou à libérer un territoire : leur but est bien au-delà de la sphère étatique (établissement de la loi islamique sur Terre, écologie « fondamentale », millénarisme, révolution cybernétique planétaire) ou encore, ils cherchent la poursuite d'intérêts, criminels, économiques, communautaires, culturels, dans un cadre « postpolitique » où l'État n'existe plus, ni ne compte plus.

Certes, on ne peut pas exactement dire que, dans cette enquête, nous n'en ayons pas rencontré au moins un, l'État américain, ses soldats, ses communicants, ses espions, ses satellites... Mais, cet État-là, d'une certaine façon, semble confondre sa propre cause avec celle de la Mondialisation, du triomphe de la société de l'information, du *monitoring* global, de l'infodominance, du règne du Bien et de la Technique et de la fin de l'Histoire. En ce sens, ses buts sont foncièrement antipolitiques : ils visent à l'abolition de la relation politique et nationale.

## Conclusion

Si nous remontons en amont, c'est-à-dire vers la relation de conflit, ce sont les catégories politiques du conflit qui changent. Nous avons vécu quelques siècles sur l'idée qu'il existait trois sortes de violences organisées. A) Les États, détenteurs du monopole de la violence légitime, se font la guerre entre eux, de territoire à territoire, pour résoudre des querelles politiques ; B) Sur le territoire des États, les groupes poursuivant des objectifs politiques s'affrontent soit par des moyens conventionnels et limités (lutte démocratique des idées, par exemple) — et l'État fonctionne — soit par des armes — on peut alors parler de guerre civile et l'État ne remplit plus son rôle ; C) des groupes emploient la violence armée à des fins particulières, et il s'agit de crimes que l'État doit interdire.

Les nouvelles violences collectives sont d'un quatrième type : elles sont hybrides par leurs motivations (criminelles/politiques, millénaristes/politiques, économiques/politiques), hybrides par les acteurs qui les mènent, qui ne sont ni des partis, ni des armées, et, bien sûr, par leurs méthodes qui mêlent les forces de la croyance, les instruments de la communication, et la brutalité crue.

Valéry disait que deux choses menacent le monde : l'ordre et le désordre. C'est vrai plus que jamais. D'un côté le danger de contrôle en douceur par les systèmes planétaires de gestion de l'information. De l'autre, le péril d'un chaos qui résulterait autant des usages anarchiques ou délictueux des technologies, que des violences erratiques comme la privatisation de la guerre ou le terrorisme. L'instance politique sera-t-elle capable de s'adapter à ces nouvelles menaces qui remettent en cause son fondement même ? Pour cela, il faudrait d'abord commencer par penser une violence qui remette en cause toutes ses certitudes.



## Annexe I :

### Ben Laden sur les écrans de *Big Brother*

Révélation du 11 septembre : l'inefficacité des systèmes de surveillance. Les signaux d'alerte n'avaient pas manqué : avertissements des services européens, indications sur des individus suspects d'appartenir au réseau al Quaida, rapports négligés. Ni l'idée de s'en prendre au *World Trade Center*, ni celle de précipiter des avions détournés sur des bâtiments n'étaient nouvelles<sup>1</sup>. En aval, les apprentis terroristes avaient agi avec un étrange manque de discrétion. Leurs images filmées, leurs fiches dans des dossiers, leurs relevés de cartes bancaires et leurs visites chez les stripteaseuses : autant de cailloux qui permettraient de reconstituer, mais trop tard, leur itinéraire. Les propos alarmistes menaçant la *homeland security*, la sécurité du territoire, les scénarii ingénieux décrivant d'éventuelles attaques, les analyses subtiles sur les conflits asymétriques ou les menaces transnationales peuplaient des rayons de bibliothèque<sup>2</sup>. En vain.

1. CNN vient même de révéler que le synopsis du 11 septembre (sans doute avec beaucoup d'autres) figurait parmi les scénarios catastrophe d'un « rapport inter agence » demandé du temps de Clinton et conservé à la Librairie du Congrès : <http://www.cnn.com/2002/US/05/17/bush.sept.11/index.html>. Tout aussi ironiquement, un rapport du CRS (Congressional Research Service) de la veille de l'attentat prévenait que Ben Laden était susceptible de frapper sur le sol des USA.

2. Même si, il faut le reconnaître, la plupart des analystes avaient plutôt tendance à se concentrer, les prédictions sur l'usage des armes de destruction massives (*WMD Weapons of Mass Destruction*) ou du cyberterrorisme. Voir par exemple : Jessica Stern, *The Ultimate Terrorists*, Harvard University Press, 2000.

Bref, l'événement le plus imprévisible paraissait avec le recul inéluctable : comment avait-on pu ne pas prévoir ? Où était l'erreur ? De là, ce qu'il est convenu d'appeler aujourd'hui la crise du renseignement<sup>1</sup>. Pour l'expliquer, on avance généralement trois types de raisons qui, du reste, ne s'excluent pas : le politiquement correct, la bureaucratie, la technocratie. La première aurait empêché la CIA de faire son travail qui ne consiste pas à fréquenter des enfants de cœur<sup>2</sup>. La seconde aurait empêché la coordination des services. La troisième aurait incité la « communauté de l'intelligence »<sup>3</sup> à tout miser sur des logiciels et des satellites, et à négliger qu'il fallait aussi des gens qui connaissent le terrain et parlent arabe ou pachtou<sup>4</sup>.

Les fameuses sociétés de contrôle ne contrôlent pas mieux le prion que les terroristes. Ces gens qui croient tous aux rêves prémonitoires et argumentent par fables, apologues et proverbes, sont capables de mettre en échec la technologie sophistiquée ; Il y a des explications : trop d'information tue l'information. Trop d'alertes tuent la vigilance. Trop d'anticipation tue la prévision. Plus une machine gère de données, plus elle est sujette aux fausses alarmes, par auto emballement ou parce que ses ennemis sont assez habiles pour l'intoxiquer et la leurrer. Plus il y a de données, moins on se décide à temps. Plus on étudie de scenarii, moins on est prêts. La vision totale multiplie les points aveugles. La question n'est pas seulement d'avoir des moyens de surveillance, elle est de ne réagir qu'aux bons signaux, de n'être ni intoxiqué, ni surexcité. Et surtout de savoir à temps : reconstituer après

1. Voir Bauer A. et Rauffer X., *La Guerre ne fait que commencer*, J.C. Lattès, 2002.

2. C'est la thèse soutenue dans un livre à succès de Richard Baer, *La Chute de la C.I.A.*, Jean-Claude Lattès, 2002.

3. Treize agences américaines de renseignement, dont Bruce Hoffman, faisait récemment remarquer que leur budget de 30 milliards de dollars était supérieur au budget de défense de tous les États du monde sauf six.

4. Voir en particulier *La Guerre Cognitive*, précité.

## Annexe I : Ben Laden sur les écrans de Big Brother

coup le moindre déplacement ou la moindre dépense d'un suspect ne sert guère<sup>1</sup>. Et les logiciels sont impuissants devant les sourates : écrit un, écran zéro !

1. Ce paradoxe de l'ignorance de celui qui a toutes les données illustre le caractère paradoxal qui caractérise la stratégie des moyens, voire la stratégie tout court. Voir à ce sujet l'ouvrage classique d'Edward Luttwak, *Le Paradoxe de la stratégie*, Paris, Odile Jacob, 1988.





## Annexe II : Le cyberterrorisme, objet virtuel

Les juristes traitent de *cybercrimes via Internet* : récemment, le Congrès américain a voté une loi sur la *cybersécurité* et la Commission Européenne une convention sur la *cybercriminalité*. Les techniciens cataloguent les méthodes pour prélever, falsifier, contrôler ou détruire données ou systèmes informatiques. Elles vont du virus, au déni d'accès qui rend un site inutilisable par saturation.

Le *hacktivisme\**, sorte de *cybercontestation*, est aussi avéré. Ses motivations idéologiques, dénonciation de *Big Brother* et de la mondialisation, ses formes sont bien connues. Les *hacktivistes* recourent au Réseau, soit pour mobiliser l'opinion par des actions spectaculaires, soit pour « punir » institutions ou entreprises. Cela va depuis le fait de modifier un site par un slogan rageur jusqu'à provoquer une faillite.

Mais le *cyberterrorisme* ? Il existe, à en croire les centaines de publications d'experts qui, avant et après le 11 septembre, prédisaient un « *Pearl Harbour* » informatique<sup>1</sup>. L'idée est que le pays le plus puissant peut être mis à genoux par des attaques cybernétiques touchant ses systèmes de communication dépendants de l'informatique : financiers, électriques, distribution de l'eau, du gaz et de l'essence... Les États-Unis dépensent des millions de dollars pour protéger leurs infrastructures

1. Munro Neil, *The Pentagon's New Nightmare : An Electronic Pearl Harbor* Washington Post, juillet 95, [http://vislab-www.nps.navy.mil/~sdjames/pentagon\\_nightmare.html](http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html).

vitales contre ce péril<sup>1</sup>. Sa définition serait selon Dorothy E. Denning de Georgetown University : « La convergence du cyberspace et du terrorisme. Le mot recouvre les opérations de piraterie informatique à motivation politique, destinées à provoquer de graves pertes, vies humaines ou dégâts économiques considérables. ».<sup>2</sup>

Seul problème : personne n'a jamais rencontré un *cyberterroriste*, sauf à considérer comme tels les internautes qui, lors de récents conflits s'en sont pris aux sites de l'OTAN, de l'US Army, de Tsahal ou du Hamas, du gouvernement serbe, indien... Sans grand dommage ni grand écho, d'ailleurs.

Admettons que les experts aient raison et que des groupes terroristes puissent acquérir la compétence et les moyens de mener ces attaques qui causeraient un temps considérable de désorganisation. Pourquoi ne le font-ils pas ?

Une partie de la réponse pourrait être d'ordre stratégique et politique. Les « avantages » théoriques du cyberterrorisme sont connus : anonymat, action à distance, faible coût, faible risque. Mais il y a des inconvénients. Le premier est la subsidiarité : une telle agression, pour avoir un impact plus important que quelques heures de désordre (équivalent à celui de grèves ou d'une panne d'électricité), devrait préparer d'autres initiatives et atteindre simultanément les réseaux vitaux d'un pays. Ce type d'offensives semble plutôt destiné à relayer par un effet de désordre une violence à grande échelle. Il faut donc raisonner sur un scénario de science-fiction : une offensive dont personne ne connaît l'efficacité, dont nul ne sait la valeur de menace ou de dissuasion, ou la possibilité de réparé-

1. C'est le rôle du *National Infrastructure Protection Center* : <http://www.nipcc.gov>.

2. Tout ce débat est évidemment très documenté sur Internet, particulièrement sur les sites américains. On peut commencer ses recherches par <http://www.cybercrime.gov> ou par le portail de Winn Schwartau : <http://www.infowar.com>.

## Annexe II : Le cyberterrorisme, objet virtuel

tion, ni qui seraient vraiment les victimes. Ce ne sont pas de minces inconvénients pour le terrorisme qui suppose impact psychologique et force démonstrative. Autre limitation : impossible de revendiquer l'attentat, donc risque qu'il soit attribué à un autre. Et, pour le cyberterrorisme d'État, le danger d'être affecté par un désordre, bancaire par exemple, qu'il aurait déclenché.

Le cyberterrorisme pourrait pâtir de son défaut de visibilité, et de son déficit symbolique et spectaculaire. Les cadavres et cratères, plus leur image filmée, ont une valeur contagieuse. Un attentat qui s'en prend à des informations et à des bits numériques agit-il de la même façon et sur l'imaginaire de la victime et sur celui de l'auteur ? Le terrorisme a peut-être aussi besoin de corps pour prendre corps.



## Annexe III : Sens et valeur de l'information

L'information est une différence qualitative, une variation. Elle est différemment évaluée suivant l'interprétant.

L'information est donc une différence qui produit une différence pour quelqu'un. C'est ce que résume l'apologue « Vous vous promenez dans la rue ; vous donnez un coup de pied à une brique, elle bouge : vous lui avez transmis de l'énergie. Vous donnez un coup de pied à un chien, vous lui transmettez de l'information, la douleur. Il réagit différemment soit en fuyant, soit en grognant, soit en vous mordant... »<sup>1</sup>. L'information ne vaudrait en positif ou en négatif, que pour un récepteur : votre pied n'apporterait pas la même information à un éléphant ou à un ordinateur.

Que l'information soit une valeur semble évident aux tenants de la théorie dite de l'information de Shannon et Weaver de 1949 : sa fonction est précisément de mesurer la valeur « en information », dans une vision probabiliste. Son maximum, sa plus grande densité, correspond à une réduction des choix possibles entre des éléments susceptibles d'être discriminés. Plus large est le choix, par exemple plus les éléments ont une probabilité égale d'apparaître, donc plus forte est l'entropie, plus riche est la capacité de réduire l'incertitude de chaque élément faisant différence. « Information est un nom pour désigner le contenu de ce qui est échangé avec le monde extérieur à mesure que nous

1. Voir Lucien Sfez, *Critique de la communication*, Seuil, 1987.

nous y adaptions et que nous lui appliquons les résultats de notre adaptation » disait Wiener in *Cybernétique et société*, témoignant ainsi de l'expansion que subit le concept. Bien sûr, il existe toutes sortes d'objections à la généralisation philosophique de cette théorie, à commencer par le fait que ce n'est pas une théorie de l'information, mais une théorie mathématique de la communication voire de la signalétique. Qu'elle est fort utile pour résoudre des problèmes techniques d'utilisation optimale des signaux, mais pas pour comprendre le sens véhiculé par les messages, sa réception, ses effets psychologiques et sociaux. Qu'elle implique ce paradoxe : le message le moins signifiant puisque le plus aléatoire serait le plus riche en information. De la restitution des variations à la reconnaissance des formes s'ouvre le gouffre du sens.

Enfin et surtout, ladite théorie ne nous dit pas ce qu'est ce concept bouche-trou : l'information existe puisqu'on la mesure ou plutôt qu'on mesure le coût de l'acquérir ou de la dupliquer<sup>1</sup>. Or l'information est un processus. Nous ne le connaissons que par ses effets qui sont tout sauf simples. Il faut bien qu'il y ait de l'information puisqu'il y a communication, donc victoire de l'information sur les distances, mais aussi transmission, donc succès contre le temps et l'oubli et enfin propagation, donc lutte de l'information contre l'information, ou

1. Chaque symbole ne véhicule pas le maximum de bits d'informations qu'il pourrait (au sens du nombre de choix binaires entre deux possibilités). Cela désole peut-être le spécialiste de la compression numérique, mais importe assez peu dans la vie quotidienne où il nous est plus facile de deviner un message dans lequel un élément fait défaut ou est altéré. L'économie d'effort compense en relation ce qui se perd en contenu. Ces notions ont une formulation mathématique. Si un alphabet de 26 lettres était employé de manière absolument équiprobable, en lisant un texte, il y aurait une chance sur 26 de deviner la lettre suivante, comme à pile ou face il y a une chance sur deux de deviner le prochain coup, même si le joueur croit distinguer des séries signifiantes. L'information de chaque lettre serait égale au logarithme de 26 soit 4,7 bits. Dans la réalité, il en va tout autrement. Une langue comme l'anglais est très redondante, quasiment aux trois quarts, et une lettre n'y apporte qu'un bit d'information en moyenne.

plutôt contre les résistances du déjà acquis et du déjà cru. L'information est quelque part sur ce triple front et réside dans ce triangle des Bermudes.

## De l'archive à l'action

L'information « se présente au regard tantôt comme mémoire, tantôt comme savoir, tantôt comme message, tantôt comme programme, tantôt comme matrice organisationnelle » suivant Edgar Morin. Elle est *data*, *knowledge et news* pour les anglo-saxons : données, connaissances, nouvelles. Or, elle ne peut se réduire aux données, des unités de variation stockées ou traitées quelque part et qui produisent des traces. Ni aux messages qui lui permettent de circuler et n'en représentent qu'une forme d'existence temporaire. L'information ne peut pas non plus être assimilée à la connaissance qui en résulte lorsqu'un cerveau relie des informations pour faire émerger une forme mentale d'un fond. Enfin, l'information, ce ne sont pas non plus les programmes (ceux des logiciels ou ceux de notre code génétique) qui contiennent en puissance d'autres états de la réalité et agissent comme des commandes. L'information c'est tout cela à la fois. C'est le processus qui explique la continuité de ces quatre états.

Assez vite, la théorie de l'information, puis ses déclinaisons cybernétiques donnent lieu à une valorisation d'un autre ordre : la conviction que la « bonne » société repose sur un bon usage ou un bon partage d'une information disponible en pleine croissance. L'optimisme des premiers penseurs de l'information n'a pas d'autre source. Voir Shannon définissant une bonne gestion « cybernétique » du politique comme remède à la barbarie. Voir H.D. Laswell, pape de la sociologie des médias d'après-guerre, exaltant la société

démocratique comme capable d'assurer la répartition des connaissances donc des pouvoirs<sup>1</sup>. Or c'est négliger trois ambiguïtés.

D'abord, celle qui porte sur le rapport entre données et connaissances. Il est évident que la disponibilité de données, ou les instruments qui en permettent le stockage, le traitement, le transport, ne garantit pas un savoir (une représentation organisée de la réalité, la rendant plus intelligible). Le savoir consiste aussi à éliminer, hiérarchiser, classer les données accessibles, non à les accumuler. L'information, processus d'acquisition d'éléments in-formés au sens étymologique, ne repose qu'en partie sur la multiplication des modes et objets de représentation.

Une autre ambiguïté porte sur les rapports entre information et communication. Il y a une certaine contradiction entre information, nouveauté demandant un effort d'acquisition et d'intégration et la communication comme effusion ou communion. D'où, comme le dit Daniel Bounoux, « l'antagonisme de l'information et de la communication, néanmoins contraintes de cohabiter dès lors que celle-ci (la communauté, la connivence participative ou la chaleur du massage) est la condition et le préalable obligé de celle-là (le message qui ouvre, qui complique ou éventuellement contredit nos mondes propres). »<sup>2</sup>

Une troisième ambiguïté porte sur la réduction de l'incertitude et la réduction du conflit. Ceci suppose l'idée fort ancienne que les affrontements résultent d'une ignorance et qu'une véritable connaissance mènerait sinon à l'harmonie des intérêts du moins à la réduction des hostilités. Tout nouveau moyen de communication est accompagné de prédictions humanistes et de phrases immortelles sur l'humanité qui, rapprochée et tout ébahie de se découvrir si semblable en toutes ses composantes, ne pourrait bientôt plus se

1. Voir le texte de Laswell, *Structure et fonction de la communication dans la société*, in *Sociologie de l'information*, Larousse, 1973, textes réunis par Francis Balle et Jean G. Padioleau.

2. Daniel Bounoux, *L'Information contre la communication*, Hachette, 1996.



## Annexe III : Sens et valeur de l'information

faire la guerre. Victor Hugo n'y a pas échappé davantage que Bill Gates. Le télégraphophone, le cinématographe ou le dirigeable ont suscité autant de discours prophétiques avant 14-18, qu'Internet avant l'hécatombe des start-up. Avec le succès que l'on sait.

Deux éléments contribuent à répandre dans l'esprit du temps la notion d'une valeur intrinsèque de l'information.

Avec les *mass media* et les industries culturelles, le négoce d'états de conscience devient une activité économique et sociale cruciale. La valeur de l'information devient une évidence entre économie du savoir, économie de séduction.

Enfin, il se constitue dès les années soixante d'une idéologie « postindustrielle » représentée par quelqu'un comme Daniel Bell puis par des épigones moins subtils de type Alvin Toffler. Elle nourrit ce qu'il est convenu d'appeler « l'utopie de la communication ». Sa vulgate prédit le passage à une société dite indifféremment de l'information, de la communication, du savoir, des réseaux — comme si ces termes étaient équivalents.

Dans cette vision, l'information est substantifiée, considérée comme une ressource difficile à produire mais de plus en plus facile à stocker, circuler et dupliquer, bonne par nature puisque génératrice de possibilités nouvelles : seule sa rétention pourrait produire des effets de pouvoir ou de manipulation. D'où le double idéal d'une société plus rationnelle, égalitaire et protectrice et d'un individu répondant à l'impératif généralisé d'expression de soi et d'authenticité...

## Les choses, les gens, l'information

Dans l'optique stratégique, l'information représente un pouvoir sur les choses, sur les gens et sur l'information elle-même.

Sa valeur dépend de sa capacité de limiter la complexité des choix au profit de la décision. Cette connaissance porte sur les conditions extérieures du déploiement de l'action, mais aussi

sur les plans de l'adversaire (qui sait souvent qu'il en est ainsi et peut penser ses « coups » en fonction de leur prédictibilité). Sun Zi y ajoutait la connaissance de soi et de ses propres forces : « Connaissez-vous et connaissez l'adversaire et jamais ne serez vaincus en cent guerres »<sup>1</sup>. Ces modes d'acquisition de l'information (avec leur corollaire, les procédures de protection du secret, d'intoxication ou de déception des décideurs adverses, voire de dégradation de leurs systèmes d'information) caractérisent la relation conflictuelle. Un savoir stratégique ne saurait être pure technique, moyens garantissant une fin et permettant une économie de temps ou de ressources. L'avantage informationnel dépend de l'opportunité juste et donc du temps (éventuellement de la capacité de faire perdre du temps à l'adversaire et d'accroître son incertitude). Pareil avantage peut être très éphémère. Il peut être aussi très marginal dans la mesure où il dépend de l'état des connaissances d'un adversaire ou d'un concurrent, plus de l'anticipation de l'effet de cette différence sur son comportement. Le problème de discrimination de l'information pertinente est donc crucial.

L'information agit aussi sur les gens : nos représentations nous possèdent autant que nous les possédons. D'être facteur d'adhésion met l'information/croyance au centre d'un processus complexe entre relation (croire, c'est souvent rentrer dans une communauté), opposition (la croyance suppose un refus d'autres représentations concurrentes tenues pour fausses ou perverses, et bientôt la construction), mais aussi « focalisation » (croire, c'est diriger son attention sur un énoncé ou un thème et d'une certaine façon se fermer à d'autres possibilités ou à d'autres ouvertures sur le monde). La bonne nouvelle c'est que tout ceci ne se laisse guère réduire en équations et que la persuasion, pragmatique et non technique, est le plus aléatoire des arts. Les mystères de la réception et les pièges

1. Il existe une version de *L'Art de la guerre* de Sun Tse sur <http://www.00h00.com>.

### Annexe III : Sens et valeur de l'information

de l'interprétation ont guéri plusieurs générations de chercheurs de définir les recettes de la manipulation des esprits, mais pas les pratiquants de persévérer en dépit de cette imprédictibilité des effets.

Enfin, l'information agit sur l'information. Positivement d'abord. Des informations qui mettent en ordre les données enregistrées, des connaissances qui hiérarchisent et relient des connaissances, des moins de signes qui produisent des plus de sens, simplifier les structures pour ouvrir le champ des possibles, cela définit assez bien le travail de l'intelligence. Mais cette valeur peut être affectée du signe négation : l'information, à rebours de son étymologie — in-former, mettre en forme — peut être un facteur de désordre et détruire l'information. Tel est le cas du virus informatique. Reste aussi le cas où la valeur de l'information sur l'information est purement conventionnelle : le mot de passe ou l'identifiant ne valent en rien par leur contenu et leur signification nulle, mais uniquement par leur rareté organisée.

De là, trois usages offensifs :

— *Une appropriation non désirée, rançon de sa durabilité.* Que l'information soit relative à des choses (techniques autorisant des performances, connaissances déterminant des stratégies) ou qu'elle concerne des acteurs (localisation, repérage, surveillance), l'information égale le pouvoir.

— *Une pénétration dommageable, rançon de sa transmissibilité.* L'information est une force agissante. Elle crée des choses ou des relations et en détruit. Elle produit de l'ordre et du désordre. En particulier l'information fausse, déstructurante, occulte la vérité, enlève la capacité de réagir de façon appropriée. L'information menace l'information.

— *Une propagation périlleuse rançon de sa reproductibilité.* Le monopole de sa diffusion fait obstacle à la pensée critique et interdit toute possibilité de réponse. L'information menace alors la communication.

Il n'existe ni recette, ni technologie qui garantisse la réussite dans les trois domaines, et qui confère ce que l'on pourrait résumer comme capacité d'agir sur la réalité, capacité d'agir sur les cerveaux, et capacité d'agir sur la capacité. Il ne suffit pas d'acquérir de l'information (de monopoliser des représentations vraies et opérationnelles de la réalité, comme dirait le stratège, de produire, distribuer ou répartir des biens informationnels, comme dirait l'économiste). Bref, l'accumulation de données, fussent-elles fournies par des machines sophistiquées peut être autant un handicap qu'une force. Le problème est également de diriger l'information, et enfin souvent de l'éliminer, soit pour se protéger de l'information fausse ou étouffante, soit pour interdire sa propagation. Il est enfin, idéalement, de décider des modes d'acquisition de l'information et, en somme, de ce qui sera considéré comme information.

## Glossaire

**Agenda** : La « fonction d'agenda » ou *agenda setting* est une notion héritée de la sociologie des médias. Elle désigne le pouvoir propre aux *mass media* de déterminer ce qui fera débat, de sélectionner les événements et sujets auxquels s'intéressera le public (et/ou les décideurs). Plus subtilement, « faire l'agenda » est un élément d'une stratégie *décisionnelle* dans le domaine médiatique, intellectuel ou politique. Faire l'agenda, c'est choisir le terrain, diriger l'attention, voire décider de ce qui sera une information.

**Algorithme** : Ensemble des règles opératoires propres à un calcul ou à un traitement informatique. Les algorithmes permettent à l'information d'agir comme programme, productrice virtuelle de réalité.

**Analogique** : Signal électrique dont les variations forment une courbe périodique (comme les ondes de la voix ou celles des couleurs, par exemple, reproduites par les variations d'un sillon de microsillons ou les taches chimiques sur une pellicule). Par extension, est dit analogique tout mode de représentation qui repose sur la ressemblance (ne serait-ce qu'en intensité) entre l'objet représentant et le représenté. Cette idée s'oppose surtout à celle de numérique.

**Asymétrie** : Relation entre deux acteurs ou éléments, au-delà de la simple dissymétrie (inégalité quantitative, de forces ou de ressources par exemple), elle reflète un saut qualitatif, une différence de statut ou de catégorie entre ces acteurs ou éléments.

**Attaque logique** : Utilisation non autorisée des éléments d'un système informatique pour y produire un préjudice (bombe logique, virus, cheval de Troie).

**Authenticité** : Qualité de ce qui émane réellement de l'auteur auquel on l'attribue. Par vol de code et connexion à distance, il est de plus en plus facile d'emprunter des identités et de réaliser par des moyens informationnels (transmission et collecte de données) des opérations non autorisées ou délictueuses...

**Authentification** : Acte de prouver son identité à son correspondant, notamment en exécutant une « performance » qui démontre que l'on possède des connaissances, telle la clef d'un code. On peut également authentifier par transmission à distance d'éléments biologiques (donc par son code génétique et non plus physique) : pupille de l'œil, influx nerveux...

**Back door** : Littéralement « porte de derrière », créé par le programmeur d'un système informatique, pour pénétrer dans le système à l'insu de son légitime propriétaire.

**Big Brother** : « Naturellement, il n'y avait pas de moyen de savoir si à un moment on était surveillé. Combien de fois, et suivant quel plan, la Police de la Pensée, se branchait-elle sur une ligne quelconque, personne ne pouvait le savoir » George Orwell, 1984.

**Bombe informatique** : On attribue à Einstein la formule selon laquelle le futur serait menacé par trois bombes : atomique, démographique et informatique.

**Bombe logique** : Programme ou morceau de programme, placé dans un ordinateur capable de détruire ou modifier des données dans certaines conditions (par exemple lorsqu'un certain mot est saisi).

**CNA** : *Computers Network Attack*. Concept stratégique américain : utiliser le *medium* des réseaux informatiques comme aire de combat. La nouvelle stratégie américaine vise donc à « militariser » le cyberspace au moins autant que l'espace stratosphérique est censé l'être par la *National Missile Defense*.

**Cheval de Troie** ou **Back Orifice** : Programme introduit subrepticement dans un ordinateur, souvent sous couvert d'un programme officiel et légal, il en permet l'administration à distance, de type client/serveur, c'est-à-dire le contrôle à l'insu du légitime propriétaire

**Chiffrement** : Transformation d'une information pour en assurer le secret.

**Clef publique** : Chaque acteur dispose d'une clef privée A qui ne sert qu'à décoder et d'une clef publique B qui ne sert qu'à coder, reliées entre elles par une relation mathématique asymétrique. Tout texte clair codé par B (donc par n'importe qui en ayant pris connaissance) ne peut être déchiffré que par A sans que cela permette de déduire quoi que ce soit sur A.

**Clef secrète** : Si le texte clair est chiffré par clef secrète et algorithme, l'application de la même clef au chiffré permet de restituer le clair.

**Communication** : Concept aussi difficile à définir qu'information. Le verbe communiquer est transitif et intransitif, et l'on peut communiquer quelque chose ou communiquer tout court. Selon le cas, la communication renvoie à la transmission de ou à la relation avec, voire à l'expression de soi. Les activités économiques liées à la manipulation de signes et symboles, les techniques de conservation et de consultation des savoirs, la place des médias dans les relations entre les hommes, les valeurs dominantes dans nos sociétés, négociation et séduc-

tion, voilà au moins quatre niveaux de réalité différents que recouvre la catégorie de la communication.

**Compétition hypercompétitive** : Véritable militarisation de l'économie.

**Confidentialité** : Caractère d'une information qui n'est connue que d'un nombre restreint de personnes.

**Conflit informationnel** : Pratiques par lesquelles un groupe vise à la suprématie sur un autre par le contrôle, la modification ou la destruction de ses savoirs et de ses voies et moyens d'information. Son champ recouvre tout usage de l'information, entendue comme bien immatériel, mémorisable, inscriptible et reproductible pour infliger un dommage, exercer une force ou acquérir un avantage contre le gré de l'autre.

**Conflit** : Relation consciente et contradictoire entre individus ou groupes où chacun cherche à vaincre la résistance de la volonté de l'autre et à obtenir de lui un renoncement durable, éventuellement par la violence physique, voire par la suppression de l'adversaire.

**Contrôle** (société de) : Notion que Gilles Deleuze oppose à celle de sociétés disciplinaires : « Les sociétés disciplinaires ont deux pôles : la signature qui indique l'individu, et le nombre ou numéro matricule qui indique sa position dans la masse.(...) Dans les sociétés de contrôle, au contraire, l'essentiel n'est plus une signature ou un nombre, mais un chiffre : le chiffre est un mot de passe, tandis que les sociétés disciplinaires sont réglées par des mots d'ordre. » (in *Pourparlers*, 1990.).

**Convergence** : Une des caractéristiques de l'évolution technique, qui se manifeste aujourd'hui par la fusion de l'informatique, des télécommunications et de l'audiovisuel.



## Glossaire

**Cookie** : Ces espions, des lignes de code informatique, déposés dans votre ordinateur par un navigateur Web à la demande d'un site permettent à ce dernier d'identifier un visiteur et de garder des données sur lui.

**Cryptanalyse** : Étude des procédés de décryptage et de la sécurité des procédés cryptographiques.

**Cryptographie** : Étude du chiffrement et du déchiffrement et des procédés permettant d'assurer l'intégrité, l'authentification et la signature.

**Cyber** : Issu de la science-fiction, l'adjectif est devenu préfixe pour qualifier les objets, lieux ou événements liés de près ou de loin à Internet. On parle ainsi de cyberespace, cyberculture, cyberpunk...

**Cyberespace** : Métaphore désignant le domaine des interactions entre données et réseaux et accessible par ordinateurs, puis au sens large le monde global de tous les ordinateurs et système connectés par Internet.

**Cyberterrorisme** : Attaque délibérée par un adversaire militaire ou civil, organisation ou particulier, contre les systèmes informatiques cruciaux d'un pays pour les contrôler ou les rendre inefficients. Existe surtout sur le papier. Voir l'annexe à ce sujet.

**Déception** : En terminologie militaire mesure de tromperie, trugage, falsification, mise en scène. Elle est destinée à amener l'adversaire à agir de façon préjudiciable à ses propres intérêts. Repris dans le vocabulaire économique.

**Déchiffrement** : Retrouver l'information initiale contenue dans le message chiffré à l'aide de la clef secrète appropriée.

**Décryptage** : Restitution en clair d'une information sans avoir accès à la clef secrète qui permet son déchiffrement normal.

**Dématérialisation** : Jamais totale (même sur Internet), la dématérialisation désigne l'allègement et la mobilité croissante des supports d'inscription, la mutation des traces et la rupture des contacts physiques autrefois liés à l'échange.

**Déni de service** : Attaque logique paralysant une ressource informatique, par exemple en saturant artificiellement les services d'un site sur Internet.

**Désinformation** : Mot se prêtant à un usage abusif, surtout lorsqu'il finit par désigner toute opinion diffusée par les médias et que l'on croit fausse ou biaisée. La désinformation consiste à propager délibérément des informations fausses pour influencer une opinion et affaiblir un adversaire. Voir le chapitre IV.

**Données** : Toute représentation de fait, d'idées ou d'instructions de manière formalisée permettant sa communication, son traitement ou son stockage par un cerveau humain ou artificiel.

**Échelon** : Gigantesque système d'interception des transmissions hertziennes installé en Grande-Bretagne et contrôlé par la puissante NSA (*National Security Agency*) américaine. Considéré comme un instrument d'espionnage économique au service des pays qui ont créé ce système : les États-Unis, le Canada, la Grande-Bretagne, la Nouvelle-Zélande et l'Australie.

**Ennemi** : Le grec sépareit *extros* (ennemi particulier), de *polemos* (celui envers qui il peut être fait appel à la guerre et plus seulement à la lutte) ; le latin distinguait l'*inimicus* privé (contraire de l'ami et donc non aimé) de l'*hostis* (qui en même temps pourrait être l'hôte, voire demain l'allié). La langue française ignore

la nuance mais la tradition philosophique et juridique connaît cette distinction. Ainsi pour Vattel au XIX<sup>e</sup> siècle : « L'ennemi particulier est une personne qui cherche notre mal et qui y prend plaisir ; l'ennemi public forme des prétentions contre nous, ou se refuse aux nôtres, et soutient ses droits, vrais ou prétendus, par la force des armes. »<sup>1</sup>

**En ligne** : Synonyme de « sur le réseau ». On trouve des boutiques en ligne, des romans en ligne, des magazines en ligne...

**Firewall** : « barrière de feu ». Mesure de sécurité pour protéger un réseau d'ordinateurs des accès (et des attaques) externes : les paquets de bits informatiques sont filtrés de façon à n'autoriser que certains types d'accès.

**Géoéconomie** : Suivant le stratège Edward Luttwak, économie de combat au service d'un seul pays ou d'un seul groupe de pays.

**Guerre** : Conflit armé, collectif, organisé et durable. Dans la mesure où les guerres tendent à prendre, du côté des forts, la forme d'interventions « de maintien de la paix » plus ou moins policières ou judiciaires, et, du côté des faibles, celle de guerres chaotiques, guérillas, guerres mi-civiles, mi-ethniques, mieux vaut oublier la vision « classique » de la guerre en uniforme entre États Nations se déclarant la guerre et signant la paix.

**Guerre classique** ou « **clauswitzienne** » : Les experts sont donc d'accord pour proclamer la disparition de la guerre classique dite « trinitaire »<sup>2</sup> qui suit le schéma : a) des entités souveraines représentées par les autorités politiques décident de la guerre en fonction d'un objectif et d'un désaccord politiques, puis b)

1. Cité à l'article ennemi de *L'Univers philosophique*, *Encyclopédie universelle*, PUF.

2. Ainsi : Martin van Creveld, *La Transformation de la guerre*, Éditions du Rocher, 1998.

des professionnels de la violence, les armées, tentent de réaliser cet objectif politique par la force c) les civils subissent et, si possible, s'enthousiasment pour leur juste cause. Hors cela, si des groupes en armes se battent, cela est censé être une guerre civile, pour s'emparer du pouvoir d'État, ou de la criminalité (violence privée que l'État souverain a pour fonction de maîtriser).

**Guerre de l'information** : Toute activité destinée à acquérir données et connaissances (et à en priver l'adversaire) dans une finalité stratégique, soit par ses systèmes (vecteurs et moyens de traitement de l'information), soit par le contenu, en assurant une domination informationnelle (voir ce mot). Sous son aspect offensif : toute opération recourant à la rumeur, à la propagande, à un virus informatique qui corrompt ou détourne le flux des informations ou données d'un adversaire qu'il soit un État, une armée, une entité politique ou économique...

**Guerre économique** : Désignation métaphorique des méthodes d'attaque et de défense auxquelles sont confrontées les entreprises dans la compétition économique mondiale.

**Guerre électronique** : Terminologie militaire, utilisation guerrière du spectre électromagnétique, de l'interception et de l'identification des émissions électromagnétiques à l'emploi de cette énergie pour altérer les systèmes de communication ennemis.

**Guerre psychologique** : Terminologie militaire un peu datée désignant les moyens d'influencer l'opinion, les sentiments et comportements d'éléments adverses pour les modifier dans un sens de la réalisation de ses objectifs militaires.

**Hacker** : Nouveaux pirates qui accèdent via Internet, à des sites protégés par jeu ou lucre, y font des prélèvements ou des modifications, copient, vendent ou offrent illégalement des logiciels payants.

**Hactivisme** : Activité militante recourant aux techniques des hackers.

**Hoax** : Faux bruit sur Internet, sorte de canular électronique ou légende se répandant par courrier électronique, groupes de discussion et parfois repris par des sites ou des médias classiques.

**Humint** : Jargon de la « communauté de l'intelligence » US. Intelligence humaine, c'est-à-dire méthodes traditionnelles de renseignement par indicateurs, correspondants... par opposition à *Comint* ou *Signint*, l'interception des communications ou des signaux par des moyens *high tech*.

**Hyperclasse** ou **Nouvelle classe** : Nouvelle élite, composée non de détenteurs du capital ou du pouvoir politique, mais des catégories contrôlant les moyens de communication et les flux d'attention, habiles à manier signes, images et nouvelles technologies, ayant la capacité de mobiliser capital et compétences pour des projets éphémères.

**Hypertexte** : Document contenant des liens vers d'autres documents. L'hypertextualité, le fait de pouvoir « sauter » d'une page d'un site à une autre, à l'autre bout de la planète, en fonction d'une corrélation logique explique une très grande partie du succès d'Internet.

**Idéologies** : Définition banale de l'idéologie : fumées (idées de l'autre), utopies, délires, rêveries, idées contre réalité... Définition chic : représentation du monde apparemment rationnelle (mais partielle et faussée) que se font des acteurs en fonction de leur position et de leurs intérêts (notion qui permet d'expliquer pourquoi l'idéologie dominante, ô surprise, domine les médias). Rappel : « une » idéologie, ça n'existe pas. Mais il y a des idéologies, des systèmes d'idées polémiques traquant des évaluations et visant à des effets concrets ; ils se

heurtenant à d'autres systèmes et visent à se propager dans d'autres têtes.

**Infodominance ou dominance informationnelle** : Au sens tactique, strictement militaire : moyens essentiellement technologiques de connaître les forces adverses et l'environnement et désorienter l'*Autre* par l'acquisition, la rétention ou l'altération de données, tout en coordonnant instantanément ses propres forces. Donc supériorité en terme de savoir débouchant sur la maîtrise de l'espace (ubiquité), du temps (instantanéité) et des forces (« projetables » en tout lieu). En un second sens, plus géostratégique, « décisionnel » désigne un objectif économique, technologique et politique global : la gestion du monde par et pour les technologies de l'information. Voir chapitre V.

**Infoguerre** : De l'anglais *infowar*, lutte pour le contrôle de l'information, visant notamment à dégrader les informations et fonctions informationnelles adverses pour pervertir son système de décision. Cette notion, encore mal précisée du fait de ses usages civils et militaires, semble souvent recouvrir toute forme d'agression via Internet et les systèmes informatiques. Certains distinguent même trois degrés : les sabotages d'infrastructures (électriques, de télécommunications, bancaires) aboutissant notamment à un « déni de service » (paralysie), la guerre psychologique via des données informatiques (p.e. « pourrir » la vie d'un individu en faussant les données qui le concernent), et enfin la guerre politique consistant surtout en dissémination de rumeurs via Internet.

**Information** : Sur cette notion, qui pose plus de problèmes qu'elle n'en résout, voir l'annexe plus haut.

**Infostratégie** : L'infostratégie est l'étude des conflits (modalités, occurrences, motivations et finalités) liés aux systèmes de transmission et communication dans la société dite « de

l'information ». Le champ de l'infostratégie peut se définir comme l'étude des invariants et des changements régissant les rapports entre conflit et information.

**Intégrité** : Caractère de données non modifiées. Assurer l'intégrité de données consiste à permettre la détection de leurs modifications volontaires, telles celles qui découlent de la possibilité informatique d'altérer physiquement des informations-données dans une mémoire et/ou d'y introduire des instructions ou algorithmes qui fassent échapper la machine au contrôle de son maître.

**Intelligence compétitive** : Techniques de gestion des sources ouvertes d'information pour s'assurer un avantage par rapport à la concurrence.

**Intelligence économique** : Ensemble des actions coordonnées de recherche, de traitement, de distribution et de protection de l'information utile aux acteurs économiques et obtenue légalement (Commissariat général du plan). Trois fonctions majeures la caractérisent : la maîtrise du patrimoine scientifique et technologique, la détection des menaces et des opportunités, l'élaboration de stratégies d'influence au service de l'intérêt national et-ou de l'entreprise.

**Internet** : Réseau de réseaux d'ordinateurs interconnectés où l'information, découpée en « paquets », peut transiter par des milliers d'ordinateurs (au départ, cette fonction avait une finalité militaire : éviter que le système puisse être interrompu par des attaques en des points stratégiques et faire que les messages puissent transiter par tout point du réseau). Internet englobe notamment le Web, le courrier électronique et les groupes de discussion.

**Mass media** : Mot hybride d'anglais et de latin. Appareils de diffusion d'information, construits sur le modèle « un-tous »,

apparus avec les rotatives : presse grand public, radio, télévision... Vecteurs de messages reproduits en masse.

**Médias** : Moyens de diffusion, de distribution ou de transmission de signaux porteurs de messages écrits, sonores, visuels (presse, cinéma, radiodiffusion, télédiffusion, vidéographie, télédistribution, télématique, télécommunication). Dans l'usage courant, le terme média recouvre des réalités différentes : des formes culturelles d'expression, comme le cinéma, la publicité, la navigation sur Internet, des institutions et organisations (la presse, les journalistes...), des moyens de conservation et de transport des signaux (des ondes, des câbles, des pellicules), des techniques (des outils et machines à communiquer comme une caméra ou un téléphone) plus des opérations effectuées par des individus dotés de compétences spécifiques (monter, filmer, taper sur un clavier...), des usages, pratiques et attitudes (le fait que des individus écoutent un baladeur ou regardent la télévision), des codes qui s'enchevêtrent souvent (code filmique, code linguistique, code numérique).

**Médiasphère** : Milieu technique déterminant un certain rapport à l'espace (transport) et au temps (transmission). Se décline en logosphère, graphosphère, vidéosphère... Chaque médiasphère s'équilibre autour d'un *medium* dominant (la voix, l'imprimé, l'image-son).

**Médiologie** : Néologisme récent (1979) dû à Régis Debray. Il désigne des études qui traitent des fonctions sociales supérieures (religion, politique, mentalités, idéologies) dans leurs rapports avec les structures techniques de transmission et de transport (matériaux, supports, vecteurs de communication) et avec les formes institutionnelles.

**Message terroriste** : Soit l'hypothèse que le terrorisme est message : il est tout sauf simple (surtout s'il est formulé explici-



tement en un texte, souvent bavard, accompagnant l'acte). Que doit-il « dire » en effet ? Idéalement, proclamer, désigner, réclamer et émaner. Proclamer ? Même l'attentat que l'on dit « gratuit » ou « absurde » prétend énoncer une thèse (le règne de Dieu est proche, les jours des puissants sont comptés, il faut faire la Révolution...). Désigner ? Le message ne s'adresse pas indistinctement à tous les destinataires : il y a ceux qui doivent en pâtir (les oppresseurs, les occupants...) et ceux qui doivent le reprendre à leur compte. Réclamer ? Discours pour faire (ou pour faire faire), le terrorisme exprime une demande directe (« Répondez à nos revendications. ») ou indirecte (« Montrez votre vrai visage. »). Le but est d'infliger à l'adversaire un dommage moralement insupportable, jusqu'à ce qu'il cède ou qu'il crée les conditions de sa propre perte (en menant une odieuse politique de répression, par exemple). Émaner ? Le terrorisme implique signature. S'il revendique, il se revendique aussi. Là encore, ceci se fait soit directement (une organisation qui affirme son droit d'auteur), soit indirectement (un camp, une cause). Sans oublier, l'usage de la fausse revendication ou de fausses organisations, « cache-nez » de services secrets.

**NRO** (*National Recognition Organisation*) : Agence responsable des satellites de vision. Les yeux les plus perçants de l'Histoire.

**NSA** (*National Security Agency*) : Agence responsable des interceptions de communications, les plus grandes oreilles de l'Histoire.

**NTIC** : Nouvelles Technologies de l'Information et de la Communication (certains suppriment le « Nouvelles » et disent TIC). L'ensemble des médias qui sont nés, dans la décennie 1970, du rapprochement entre la radiotélévision et les télécommunications, via le câble et le satellite, puis dans les années 1980, du rapprochement entre les télécommunications et l'informatique, c'est-à-dire la télématique et le service en ligne,

et enfin, depuis 1990, de la convergence entre l'audiovisuel, l'informatique et les télécommunications ; on parlera alors du multimédia en ligne et hors-ligne. On parle aussi de nouveaux médias, issus du rapprochement des techniques de l'informatique, de la télécommunication et de l'audiovisuel.

**Numérique** : Caractéristique des signaux codés sous forme de données binaires (0 ou 1), équivalent de l'anglais *digital*.

**Paiement sécurisé** : Systèmes sophistiqués, censés garantir que votre numéro de carte de crédit ne tombera pas en possession d'escrocs.

**Panoptisme** : Concept militaire adopté par des gens qui n'ont jamais lu Bentham ou Foucault : la capacité de surveiller la planète pour pouvoir punir d'éventuels États « voyous » (*Rogue States*), délinquants, purificateurs ethniques, mafieux troublant le nouvel ordre mondial.

**Phreaking** : Piratage du réseau téléphonique (par exemple pour faire des appels longue distance gratuitement). Par extension, passer outre les sécurités d'un système quelconque (par exemple dans des réseaux de communication).

**Polémologie** : Discipline créée par Gaston Bouthoul et qui se proposait d'étudier les guerres comme des faits sociaux, susceptibles d'obéir à des lois, à des régularités. Il y a quelques années, la polémologie avait fait le projet d'établir des constantes sociales, psychiques, culturelles, voire démographiques qui présidaient à l'explosion des conflits armés. Pour d'évidentes raisons d'époque, ce projet avait largement sous-estimé la dimension informative des conflits (sauf à traiter de l'incitation à la violence de nos représentations) et ignoré les Nouvelles Technologies de l'Information et de la Communication alors balbutiantes. Enfin, elle était largement polarisée par l'idée d'une fonctionnalité

(essentiellement démographique) du conflit armé. Ces remarques faites, rien n'interdit de s'inspirer de l'esprit ou de l'ambition de la polémologie en les appliquant à l'information.

**Propagande par le fait** : Notion héritée des révolutionnaires russes dans les années 1870 et abusivement réduite aux attentats nihilistes : volonté de propager l'idée anarchiste par les actes exemplaires de révolte et non par les paroles.

**Propagande** : Toutes les informations, idées, doctrines, appels, communiqués pour influencer l'opinion, les émotions, les attitudes ou le comportement de tout groupe particulier dans le but d'obtenir un bénéfice direct ou indirect (définition officielle de l'OTAN). Pour nous : moyens de faire croire une communauté en un contenu idéologique dans le cadre d'un conflit avec une autre communauté et d'autres croyances.

**Psyops** (*Psychological operations*) : En terminologie militaire américaine : actions politiques, militaires, économiques et idéologiques destinées à créer, sur une opinion neutre, amicale ou non hostile, des attitudes émotionnelles ou comportements favorables aux objectifs visés.

**Réseaux** : Ensemble de nœuds de circulation (d'énergie, d'informations, d'argent, de drogue) reliés par des connexions plus ou moins stables et explicites. Mode de relation représentable des lignes entrelacées comme voie d'accès pour des flux.

**RMA** (Révolution dans les affaires militaires) : Transformations dans la conduite de la guerre résultant sur le plan instrumental, stratégique, organisationnel et doctrinal des progrès des technologies de l'information.

**Sanctuarisation** : La stratégie d'après-guerre froide suppose, après la disparition du « compétiteur égal », une protection

tous azimuts des USA contre des acteurs asymétriques : guérillas, terroristes, mafieux, armées privées, groupes *infra* étatiques aux motivations ethniques, économiques ou idéologiques mal définies.

**Secret** : Une information que son détenteur rend délibérément inaccessible.

**Serveur** : ordinateur dont les informations peuvent être consultées à distance par d'autres ordinateurs (ou par Minitel).

**Signature** : Donnée de taille faible qui, jointe à un message, prouve l'identité de l'émetteur du message. En terminologie militaire : trace détectable (visuelle, thermique, sonore, électromagnétique) que laisse un objectif sur le terrain, ce que résume la formule : « Sur le champ de bataille, la signature c'est la mort »

**Société de l'information** : Expression assez largement acceptée, en dépit ou grâce à son flou, apparue au tout début des années quatre-vingt. Signifie suivant le contexte : a) Société où une part croissante de la valeur économique résulte de la production, de la distribution et de la demande de données, images ou symboles ; b) Société où les machines et dispositifs informationnels se multiplient, et où chacun est confronté sans cesse à un nombre de messages sans commune mesure avec ce qu'ont connu les générations précédentes ; c) Société dont le destin serait lié au développement téléologique d'une sorte de principe historique du nom d'information, par contraste avec les sociétés agraires ou industrielles, phase radieuse de l'histoire de l'espèce.

**Soft power** : Le pouvoir « doux » d'amener la planète entière à adopter le modèle de la société démocratique et mondialisée du marché et de l'information. Se sentant investis de la mission

historique de « façonner la mondialisation » (*monitoring the globalization*), c'est-à-dire de faciliter par tous les moyens économiques, culturels, diplomatiques (et très accessoirement militaires) la transition vers cet état heureux, les géostratèges US déclaraient que les notions d'ami et d'ennemi étaient obsolètes.

**Spin Doctors** (de *to spin* : donner une pichenette, pousser) : Surnom des spécialistes de la communication, de plus en plus employés en cas de conflit, pour « vendre » la guerre comme du yaourt à l'opinion.

**Stéganographie** : Art de recourir à des cachettes sur le corps humain, à des encres sympathiques, à des supports truqués, à des microfilms, bref de rendre invisible le support physique du message, par opposition avec la cryptographie qui consiste à transposer un message clair en un ensemble de signes incompréhensibles aux non initiés.

**Stratégie** : Art de diriger des forces et des informations dans une relation dialectique et conflictuelle, dont l'issue est en principe la victoire d'un des acteurs.

**Symbolique** (du grec *sumballein*, jeter ensemble) : 1/ Ce qui relie des réalités séparées. 2/ Ce qui représente autre chose que soi-même.

**Système d'information** : Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire de l'information. (Arrêté relatif au vocabulaire informatique, JO du 17 janvier 1982.)

**Technique** : Toute utilisation de moyens, recettes et instruments concrets, par lesquels nous modifions notre environnement conformément à nos buts.

**Technologie** : Anglicisme, superlatif savant de technique, pour désigner les techniques et systèmes techniques les plus récents.

**Télécharger** : Copier, grâce à Internet, un fichier, une image ou un programme stocké sur un ordinateur distant.

**Terrorisme** : Hybride entre faire et dire, le terrorisme est une « proclamation ». Elle est orientée, vise des forces morales, celles du « fort », l'adversaire qu'elle s'efforce de décourager, contraindre ou démasquer ; mais le message s'adresse aussi à d'autres forces morales, celles du « faible », une communauté (le Prolétariat, le peuple occupé, les vrais croyants, les vrais patriotes, les opprimés, la race menacée) que le terrorisme prétend ressouder, dynamiser, pousser à la révolte, et venger au nom de qui il agit... Dans ce but, il recourt à des actions, notamment les attentats, qui sont pour lui presque des « performances ». Elles sont parfois sous-titrées par un discours pédagogique et explicatif (la revendication). Surtout, elles sont investies par leurs auteurs d'une richesse de sens : ainsi la victime du terrorisme « représente » le système honni, l'attentat « prouve » que nul n'est à l'abri, ou encore, il « annonce » la contagion de la révolte. La cible matériellement touchée n'est jamais l'objectif ultime visé, ni la signification totale symbolisée. Le mot « terrorisme » n'est employé que par ses adversaires pour disqualifier une violence qu'ils désignent par là comme illégitime. Ou, si, exceptionnellement, quelqu'un se reconnaît « terroriste », c'est toujours pour comparer son terrorisme à un autre plus puissant et, pire encore, qui le provoque et le justifie. De plus, la définition du terrorisme est rendue aussi difficile que sa répression, de par son caractère multiforme. Nous avons connu un terrorisme révolutionnaire, celui des nihilistes et anarchistes du XIX<sup>e</sup> siècle, un terrorisme indépendantiste ou anticolonialiste, un terrorisme instrumental, souvent international visant à contraindre un pouvoir sur un point précis. Nous connaissons ou connaissons des terrorismes mystiques

## Glossaire

ou apocalyptiques, tel celui des sectes, des « gangsterrorismes », des « écoterrorismes », des terrorismes inspirés par toutes les causes, même celle des animaux, ou l'idéologie du *New Age*.

**Veille** : Opération de surveillance, souvent par simple collecte et analyse de documentation, composante essentielle de l'intelligence économique. Elle se subdivise en veille technologique, concurrentielle, géopolitique, sociétale...

**Virus** : Programme informatique qui réplique son code dans la mémoire des ordinateurs et éventuellement passe de l'un à l'autre.

**Virtuel** : « Est virtuel ce qui existe en puissance et non en acte. Contrairement au possible, statique et déjà constitué, le virtuel tend à s'actualiser. Il ne s'oppose donc pas au réel mais à l'actuel : virtualité et actualité sont seulement deux manières d'être différentes. » Pierre Lévy, *Qu'est-ce que le virtuel ?*

**Web** (*World Wide Web*) : En français : la toile d'araignée mondiale. Une métaphore souvent employée : un filet tendu sur la planète, dont chaque maille serait un ordinateur et chaque fil une ligne de téléphone.

**Zones grises** : Celles où sévissent des conflits intermédiaires entre politique, économique, idéologie, délinquance, ou encore « conflits asymétriques » (terroristes contre État, entités criminelles ou économiques, groupes « privés » ou religieux, organisations internationales s'affrontant de façon chaotique).





# Bibliographie

## Généralités sur l'information et la communication

BOUGNOUX D., *Sciences de l'information et de la communication*, Larousse, 1993.

BOUGNOUX D., *Introduction aux sciences de la communication*, La Découverte, 1998.

CINÉMACTION (revue) N° 63, *Les Théories de la communication*, 1992.

CAHIERS FRANCAIS (revue), *La Communication et Les Médias* Documentation Française, 1992.

CAHIERS DE MÉDIOLOGIE (revue), *Pourquoi des médiologues ?* N° 6, 1998.

DEBRAY R., *Transmettre*, Odile Jacob, 1997.

DEBRAY R., *Introduction à la médiologie*, PUF, 2000.

SFEZ L., *Critique de la communication*, Seuil, 1988.

WATZLAWICK P. (dirigé par), *L'Invention de la réalité. Comment croyons-nous ce que nous croyons savoir ?* Seuil, 1992.

WOLTON D., *Penser la communication*, Flammarion, 1997.

## Textes classiques

BAUDRILLARD J., *Simulacres et simulation*, Galilée, 1981.

DEBORD G., *La Société du spectacle*, Buchet Chastel, 1967.

ECO U., *La Guerre du faux*, Grasset, 1985.

MARCUSE H., *L'Homme unidimensionnel*, Éditions de Minuit, 1968.

MC LUHAN M., *Pour comprendre les media*, Mame, 1968.

- MC LUHAN M., *La Galaxie Gutenberg*, Mame, 1967.  
MORIN E., *L'Esprit du temps*, Grasset, 1976.  
RIESMAN D., *La Foule solitaire (anatomie de la société moderne)*, Arthaud, 1964.  
SENETT R., *Les Tyrannies de l'intimité*, Seuil, 1990.  
TCHAKHOTINE S., *Le Viol des foules par la propagande politique*, Gallimard, 1952.

### **Le pouvoir des médias**

- BALLE F., *Médias et Société*, Montchrestien, 1997.  
BERTHO-LAVENIR C., *La Démocratie et les médias au XX<sup>e</sup> siècle*, A. Collin, 2000.  
BOURDIEU P., *Sur la télévision*, Liber, 1997.  
BRETON P., PROULX S., *L'Explosion de la communication*, La Découverte, 1989.  
CAZENEUVE J., *L'Homme téléspectateur*, Denoël, 1974.  
DEBRAY R., *L'État séducteur*, Gallimard, 1993.  
DERVILLE G., *Le Pouvoir des médias*, PUG, 1997.  
KAPFERER J-N., *Les Chemins de la persuasion*, Gaultier-Villars, 1978.  
MATTELART A., *Histoire des théories de la communication*, La Découverte, 1995.  
NEVEU E., *Une Société de communication ?*, Montchrestien, 1994.  
POPPER K., *La Télévision : un danger pour la démocratie*, Anatolia, 1995.  
SCHWARZENBERG R.G., *L'État spectacle*, Flammarion, 1979.  
WOLTON D. et MISSIKA, *La Folle du logis*, Seuil, 1982.

### **Nouvelles technologies et société de l'information**

- BRETON P., *Le Culte d'Internet*, La Découverte, 2000.  
CASTELLS M., *L'Ère de l'information*, 3 tomes, Fayard, 1998.  
FINKIELKRAUT A. et SORIANO P., *Internet l'inquiétante extase*, Mille et une nuits, 2001.

## Bibliographie

- GUILLAUME M., *L'Empire des réseaux*, Descartes et Cie, 2000.
- HUITEMA C., *Et Dieu créa Internet*, Eyrolles, 1995.
- LÉVY P., *Qu'est-ce que le virtuel ?*, La Découverte, 1995.
- LÉVY P., *Cyberculture*, Odile Jacob, 1998.
- MATTELART A., *Histoire de l'utopie planétaire*, La Découverte, 2000.
- MATTELART A., *Histoire de la société de l'information*, La Découverte, 2001.
- MARCON C. et MOINET N., *La Stratégie réseau*, Éditions 00H00.com, 2000.
- NEVEU E., *Une Société de communication ?*, Montchrestien, 1994.
- RAMONET I., *La Tyrannie de la communication*, Galilée, 1999.
- RIFKIN J., *L'Âge de l'accès*, La Découverte, 2000.
- VIRILIO P., *Cybermonde la politique du pire*, Textuel, 1996.

### Guerre de l'information et infostratégie

- ADAMS J., *The Next world war*, Simon & Schuster, 1998.
- ARQUILLA J. et RONFELDT D., *Networks and Netwar : the Future of Terror, Crime and Militancy*, Rand, 2002, téléchargeable sur <http://www.rand.org>.
- BAUMARD P. et BENVENUTI J.A., *Compétitivité et système d'information*, Dunod, 1998.
- CAMPBELL D., *Surveillance électronique planétaire*, Allia, 2001.
- FAYARD P., *La Maîtrise de l'interaction*, Éditions 00H00, 2000.
- FONVIELLE D., *De la guerre économique*, PUF, 2002.
- GUICHARDAZ P., LOINTIER P., ROSE P., *L'Infoguerre*, Dunod, 1999.
- GUISNEL J., *Guerre dans le cyberspace*, La Découverte, 1995.
- HARBULOT, C. LUCAS D. (dir.), *La Guerre cognitive*, Lavauzelle, 2002.
- HUYGHE F.B., *L'Ennemi à l'ère numérique Chaos, information, domination*, PUF, 2001.
- KAUFFER R., *L'Arme de la désinformation*, Grasset, 1999.

## Écran / Ennemi

LUCAS D. et TIFFREAU A., *Guerre économique et information*, Ellipses, 2001.

MARTIN D. et F.-P., *Cybercrime : menaces, vulnérabilités et ripostes* P.U.F., 2001.

MURAWIEC, L., *La Guerre au XXI<sup>e</sup> siècle.*, Odile Jacob, 2000.

PANORAMIQUES (revue n° 52), *L'information, c'est la guerre*, 2001.

TOFFLER A. et H., *Guerre et contre-guerre*, Fayard, 1994.

VIRILIO P., *Stratégie de la déception*, Galilée, 2000.

WAUTELET, M., *Les Cyberconflits*, Bruxelles, GRIP / Complexe, 1998.

# Table

<i>À propos de l'œuvre</i> .....	5
<i>À propos de l'auteur</i> .....	7
Préface .....	9
Introduction.....	11
Quand l'ennemi occupe l'écran	
La maîtrise du visible.....	17
Terrorisme : stratégie d'irruption.....	19
Captures d'écran.....	43
Quand l'écran <i>occulte</i> l'ennemi	
La maîtrise dans l'invisible .....	65
Secret et conflit : de la ruse à la dominance.....	67
De la désinformation idéologique au soupçon éthique .....	87
Guerre et dominance informationnelles.....	113

## Écran / Ennemi

Conclusion .....	137
Annexe I :	
Ben Laden sur les écrans de Big Brother .....	141
Annexe II :	
Le cyberterrorisme, objet virtuel .....	145
Annexe III :	
Sens et valeur de l'information .....	149
Glossaire .....	157
Bibliographie.....	177

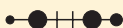
## Dans la même collection

*La Maîtrise de l'interaction*, Pierre Fayard, 00h00

*La Stratégie réseau*, Nicolas Moinet, Christian Marcon, 00h00

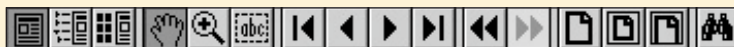
*L'exemplaire numérique est livré dans un format nommé PDF (Portable Document Format), développé par la société Adobe®, qui permet d'avoir une vraie mise en page à l'écran et offre certaines fonctionnalités très utiles qui sont détaillées ci-après.*

- [1] COMMENT NAVIGUER DANS L'EXEMPLAIRE NUMÉRIQUE ?
- [2] COMMENT FAIRE UNE RECHERCHE DE MOTS DANS UN PDF ?
- [3] COMMENT AMÉLIORER LA LECTURE À L'ÉCRAN ?
- [4] COMMENT SAUVEGARDER UN PDF REÇU PAR E-MAIL ?



## [1] Comment naviguer dans l'exemplaire numérique ?

Vous venez de recevoir votre exemplaire numérique et vous l'avez ouvert en double-cliquant dessus. Celui-ci va ouvrir automatiquement le logiciel Acrobat Reader® que vous avez téléchargé auparavant. Dans Acrobat Reader, vous trouverez la barre d'outils suivante :



Affiche la page seulement.



Affiche à la fois la table des matières et la page. Vous pouvez ensuite cliquer sur le titre de chapitre pour aller directement à la première page du chapitre désiré.



Affiche à la fois les vues miniatures du document et la page.





Permet, au même titre que les curseurs, de faire défiler la page de haut en bas ou de gauche à droite.




Affiche la première page.



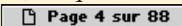
 Affiche la dernière page.

 Affiche la page précédente.

 Affiche la page suivante.

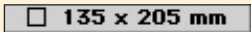
 Équivalent du « **back** » : retour à l'écran précédent.

 Équivalent du « **forward** » : retour à l'écran suivant.

Pour aller d'une page à l'autre, vous pouvez utiliser les outils ci-dessus ou bien utiliser l'ascenseur sur la droite de l'écran. Vous verrez les numéros de pages s'afficher si vous montez ou descendez le bouton de l'ascenseur. Ces numéros de pages sont également lisibles en bas à gauche de l'écran (exemple : page 4 sur 88...). Pour aller directement à une page précise, cliquez sur le symbole de la page, en bas à gauche de l'écran: 

Vous verrez s'afficher le message « **aller à la page** ». Saisissez le numéro de la page désirée et cliquez sur « **OK** ».



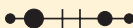
Si vous souhaitez régler le mode de défilement de la page, cliquez sur le bouton : 

- L'option « **une seule page** » permet de faire défiler le texte page par page.
- L'option « **continue** » permet de faire défiler le texte de façon continue.
- L'option « **continue page double** » permet d'afficher côte à côte le recto et le verso de la page.

## [2] Comment faire une recherche de mot dans l'exemplaire numérique ?



Lorsque vous cliquez sur cette icône, une fenêtre apparaît dans laquelle vous pouvez saisir un mot, une expression, une phrase et même un racine verbale ; cliquez ensuite sur « **Rechercher** » et Acrobat Reader va parcourir tout le document pour trouver les occurrences du texte que vous avez saisi.



## [3] Comment améliorer la lecture à l'écran de l'exemplaire numérique ?

Pour choisir votre taille de page visible à l'écran, utilisez les outils suivants :



Affiche la page courante dans une taille intermédiaire.



Affiche la totalité de la page courante à l'écran.




Affiche la page courante en occupant toute la largeur disponible pour un plus grand confort de lecture à l'écran (recommandé).



Sélectionnez cet outil et cliquez sur un passage du texte quand vous voulez en agrandir la taille des caractères.

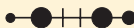


Ce bouton remplace le précédent:  lorsque vous appuyez sur la touche « **Ctrl** » (PC) ou « **alt** » (Macintosh) pour réduire la taille des caractères ou « zoomer » en arrière.

### Confort de lecture:

Pour votre confort de lecture vous pouvez sélectionner ou non l'option « **Lissage du texte et des images monochromes** » dans le menu *Fichier/Préférences/Généralités*.

Cependant, pour éviter une légère impression de « flou » due au lissage des polices lorsque cette option est sélectionnée, nous vous conseillons de lire les ouvrages en mode « **pleine largeur** ».



## [4] Comment sauvegarder un PDF reçu par e-mail ?

- **Sur PC** et pour la plupart des programmes de mails, qu'ils soient intégrés au navigateur ou non, lorsque vous cliquez sur l'icône du fichier attaché dans l'e-mail, celui-ci va s'ouvrir grâce au programme Acrobat Reader que vous aurez préalablement téléchargé et installé. Une fois ouvert dans Acrobat Reader, dans le menu « **Fichier** » cliquez sur « **Enregistrer sous** » et spécifiez l'endroit où vous désirez enregistrer votre PDF. Vous pouvez également sauvegarder très rapidement votre PDF en maintenant la touche « **Shift** » (Majuscules) appuyée tout en cliquant sur l'icône du fichier attaché dans votre e-mail ; une fenêtre de dialogue s'ouvrira alors et vous demandera où vous désirez enregistrer votre PDF.

- **Sur Macintosh** : vous pouvez effectuer les mêmes opérations que celles décrites ci-dessus, mais vous pouvez également sélectionner l'icône matérialisant le fichier attaché dans votre e-mail et la faire « **glisser** » sur le bureau ou dans le répertoire que vous désirez. Par la suite, un simple double-clic sur le fichier déclenchera son ouverture dans Acrobat Reader.

*Remarque générale : Le programme Acrobat Reader contient un Plug-in qui, une fois installé, vous permet de lire directement les PDF dans les navigateurs Internet Explorer et Netscape (à partir de la version 3 pour chacun d'entre eux). Si vous avez installé ce Plug-in et que rencontrez des difficultés pour ouvrir et lire un PDF sauvegardé, vous pouvez essayer de le lire en déposant son icône sur celle de votre navigateur.*

### **Remarque concernant les notes en fin d'ouvrage :**

Dans certains textes les notes sont en fin d'ouvrage et un hyperlien permet d'y accéder (il suffit de cliquer sur l'appel de note pour accéder à la page des notes). Pour revenir au texte source, cliquez sur la note.