



STRATÉGIE ET SURVEILLANCE DES ENVIRONNEMENTS CONCURRENTIELS

Ph. BAUMARD
Professeur de S. DESPES

MASSON 

Introduction

Pourquoi l'entreprise, en cette fin du XX^e siècle se passionne-t-elle de nouveau pour la surveillance ? En quoi cette discipline intéresse-t-elle l'économiste et le manager ? Jeremy Bentham¹ se serait certainement étonné d'une telle question ! Pour lui, la surveillance est la clef de voûte du profit. Elle remédie aux limites du pouvoir de l'entrepreneur par l'assujettissement des forces productives. Elle augmente la productivité. Elle instaure et maintient l'ordre dans la production, fédérant ainsi l'industrie toute entière. L'inspecteur Bentham était-il un utopiste, ou le précurseur de l'économie industrielle du XXI^e siècle ?

Que nous prépare l'industrie ? La grande firme, détenant le management du projet, n'assujettit-elle pas les petites et moyennes entreprises qui font le réseau de sa production ? Déléguer ses compétences, ce n'est pas forcément déléguer toute son autorité. Si la petite firme, qui a en charge certains modules de la production, a en effet toute latitude pour décider de certains procédés, elle dépend de la firme ensemble² pour l'essentiel : l'information. Finalement, la petite industrie est un module de compétences nécessaires à la grande firme, mais ses compétences n'ont pas de valeur économique si elles ne sont pas transformatrices d'information, si elles n'appartiennent pas à une combinatoire de production dont la surveillance est du ressort de son chef de file.

Détenir un savoir-faire, une invention, ou la maîtrise d'une technologie, c'est finalement détenir un pouvoir. Les industries qui ne possèdent que les équipements, celles dont les bureaux d'études préparent les plans de la grande firme, ne sont plus que des relais neutres dans le réseau productif³ : il faut acquérir l'information pour sortir de la domination. Cette compétition pour l'information gagne tous les espaces de la firme, sur le territoire de la commercialisation, comme sur celui de la conception, de la recherche fondamentale et des hommes. Les firmes « filialisent » leurs activités dans ce seul

¹ Jeremy BENTHAM, né à Londres en 1748, est l'auteur du panoptique, une architecture pour voir sans être vu. Cf. *Œuvres de Jeremy Bentham, jurisconsulte anglais*, Edition Dumont, Bruxelles, Louis Hauman & Cie, 1829-1834, 4 volumes.

² La firme ensemble : firme qui décide de la combinatoire de la production, et qui a la responsabilité de l'ensemble du projet productif.

³ En terme de pouvoir, cette organisation n'a pas la possibilité de négocier avec le chef de file, sinon discuter des détails techniques, des échéanciers ou un vingtième de point de marge.

but : dynamiser l'acquisition d'informations, enclencher le processus novateur. Les espaces de la compétitivité sont ainsi délocalisés, puis mis en réseaux{ XE "réseaux" }. Il faut coûte que coûte être le novateur, le premier à avoir découvert un procédé, une combinatoire, une matière et parfois même un slogan.

Mais être le premier, cela suffit-il ? Une fois la connaissance acquise, il faudra de toute façon la valoriser, et très vite. A ce niveau, il y aura deux types de firmes : celle qui n'a pas intégré de stratégies informationnelles à son projet de développement, et celle dont les combinatoires technologiques et les réseaux de compétences sont prêts à agir, dès que le besoin s'en ressent. Dans ce second cas, on imagine la grande firme, bénéficiant de son expérience, en train de déléguer son autorité à des unités combattives, tactiquement placées aux connexions du marché et de la production, dans l'ingénierie, l'intermédiation scientifique, le lobbying... Mais n'est-ce pas faire fausse route ?

En fait, nul n'est épargné par l'incertitude. Elle gagne toutes les formes d'organisation, de la petite industrie au complexe industriel intégré. A tous les niveaux de son environnement, la firme est constamment mise en jeu, par une innovation qui dérange définitivement ses projets de commercialisation, par un partenariat inconnu qui bouleverse ses stratégies transactionnelles avec ses partenaires... La compétition coûte de plus en plus cher tandis que l'imperfection gagne aussi bien l'information financière, que l'information politique, économique ou technologique.

C'est pourquoi la firme a besoin d'une approche nouvelle de l'information, orientée vers l'accomplissement d'objectifs stratégiques pour son développement. Il lui faut concevoir différemment ses rapports avec son environnement, en quittant les schémas classiques de rapports de domination. Il lui faut lier sa capacité d'innover à sa capacité d'appréhender une rationalité limitée. Il lui faut bâtir, hors des sentiers battus, une dynamique nouvelle de la compétition.

L'ensemble de l'analyse qui va suivre prend donc pour hypothèse de départ que l'information *ne circule pas librement* sur le marché et entre les firmes. C'est uniquement autour de cette idée de « *disponibilité limitée et coûteuse* » de l'information qu'il faut entreprendre la lecture de cet ouvrage⁴. De même, l'information dont il est question ici n'est pas un prix. C'est un *élément de connaissance*, à propos de l'environnement de la firme, ou des firmes partenaires et adverses, dont la *codification* permet son acquisition, son transfert et sa conservation. Cette information peut être tout autant relative à un procédé, à une technologie, qu'à toutes innovations, qu'elles soient commerciales, sociales, culturelles ou technologiques. La notion d'*imperfection* sous-tend ainsi tout notre développement. Il n'y a, pour nous, de problématique réelle de la surveillance qu'en dehors des schémas néoclassiques de concurrence pure et parfaite. Car,

⁴ Avec une référence tacite et permanente aux travaux de Donald J. TEECE, (*The Market for Knowhow and the Efficient International Transfer of Technology*, Annals of The American Academic Journal of Political and Social Science, novembre 1981), et de O. WILLIAMSON, (*Markets and Hierarchies: Analysis and Antitrust Implications*, New York, The Free Press, 1975).

enfin, quel est l'intérêt de surveiller si ce n'est pour la réduction, ou l'augmentation, d'une asymétrie des niveaux d'information entre les firmes ?

De même, la compétition dont nous discuterons n'est pas une compétition *par les prix*, mais une *compétition globale* autour de l'acquisition, du transfert et de la protection *d'une information telle que nous venons de la définir*. C'est une compétition qui s'organise *dans un objectif d'innovation* et qui s'accompagne d'une stratégie bien définie d'acquisition et de transfert de technologies. Quand nous parlerons de *compétitivité*, il faudra l'entendre sous cet aspect : le maintien d'une asymétrie vis-à-vis des firmes concurrentes.

C'est ainsi que toutes les définitions « classiques » du mot « *surveiller* » ne sauraient s'adapter à la firme que nous évoquerons. Si elle observe, *une firme est aussi observée* : « *voir sans être vu* », n'est plus, en 1991, qu'un vieil adage du panoptisme⁵. Firme et environnement entrent désormais *en interrelation* si bien que des notions telle que *l'obsolescence d'une information* sont devenues bien relatives. On peut toujours émettre l'hypothèse qu'il existe un lieu, à un moment donné, où l'information pourra être exploitée. Une réaction « rationnelle » pourrait être de *conserver toute information* (puisque un jour utilisable) et de *n'en divulguer aucune* (puisque exploitable par d'autres).

Mais d'un point de vue économique, il n'est pas possible de *tout conserver* et de ne rien *divulguer*. D'une part, on ne peut pas tout conserver car la quantité d'informations disponibles a pris une taille inconsiderée; une firme ne peut donc pas raisonnablement envisager de ficher tout ce qu'elle apprend de son environnement. Et d'autre part, on ne peut non plus envisager de ne rien divulguer car l'acte de commerce s'accompagne toujours d'une divulgation d'information, dont la valeur d'échange est prise en compte dans la transaction. Refuser de divulguer toute information, c'est s'interdire toute possibilité de partenariat stratégique (joint-ventures, fusions, rachats) et par là même compromettre sa compétitivité.

C'est au niveau de cet arbitrage entre la protection du savoir de la firme et la nécessité de le partager dans le cadre de partenariats stratégiques, que se dessinent les axes de recherche les plus attrayants. La surveillance y joue à la fois le rôle *défensif* de protection du savoir-faire et le rôle *offensif* d'acquisition de connaissances sur l'environnement. Nous nous sommes passionnés pour deux aspects essentiels de cet arbitrage : la relation entre *surveillants et surveillés*, et la *stratégie du surveillant* à proprement parler.

Une firme doit toujours, un jour ou l'autre, jouer l'un de ces deux rôles. Qu'elle y soit préparée nous paraît être une priorité pour son développement stratégique. C'est au niveau de cette *préparation* du partage, du transfert et de l'acquisition de connaissances, que nous essayerons de formuler une réponse adaptée aux contraintes actuelles de la compétition. Nous essayerons ainsi de renouveler l'approche, non seulement de la surveillance, mais également du *management*

⁵ Pour une étude du panoptisme, voir Michel FOUCAULT, *Surveiller et punir*, Gallimard, 1975, pages 197-229.

stratégique dans l'ère des technologies de l'information. Il s'agira d'en définir les enjeux, les besoins et les contraintes dans le cadre des objectifs suivants :

1) Cerner les concepts de veille et d'intelligence et étudier leurs spécificités par rapport à d'autres fonctions de la firme. En quoi la surveillance de l'environnement est-elle devenue stratégique ? Pourrait-elle devenir la clef de voûte de l'orchestration des compétitions et des coopérations d'entreprises ?

2) Présenter et analyser de manière critique le fonctionnement de l'intelligence. En quoi *la circulation de l'information* délimite-t-elle les possibilités de surveiller l'environnement ? En quoi le facteur *discipline* modifie-t-il les performances d'un réseau de veille stratégique ?

3) Lier le fonctionnement de la surveillance à l'évolution de *son contexte* : en quoi la nouvelle économie industrielle modifie-t-elle les enjeux de la vigilance ? Quels sont les rôles joués par *la crise, la technologie et la violence* dans le jeu des surveillants et des surveillés ?

4) Apporter des éléments de réflexion pour la mise en œuvre d'un système de veille stratégique au sein d'une organisation dont les besoins et les contraintes naissent de sa nécessité d'être « en intelligence » avec son environnement.

Cette approche débouchera d'elle même sur de nouveaux facteurs clés pour le développement de l'intelligence d'entreprise et sa pratique efficiente au sein des organisations.

CHAPITRE I

Méthodologie

1.1. Concepts et méthodes de l'intelligence

1.1.1. Surveiller la surveillance

Pour mieux appréhender la question de la surveillance environnementale, l'entreprise a tout intérêt de réaliser une recherche approfondie sur les approches existantes, et notamment celles pratiquées par ses concurrentes. La bibliographie produite sur le thème central et toutes ses implications, présentée à la fin de cet ouvrage, pourra l'y aider. Chacun est libre de s'investir dans les références qui lui sembleront les plus proches de ses intérêts.

Parmi tous les domaines à surveiller, celui des méthodologies{ XE "méthodologies" } de la surveillance elles-mêmes, est certainement le plus passionnant et important pour l'entreprise. Veiller est un métier. Il ne s'agit pas de métamorphoser complètement les entreprises en organisations de renseignement mais il existe toutefois un « seuil minimal de veille » en dessous duquel l'entreprise menace sa compétitivité. Tous les acteurs économiques sont d'ailleurs plus ou moins directement concernés par l'information et la surveillance. Entrepreneurs, chercheurs, ingénieurs et gestionnaires font tous de la « surveillance » sans en être forcément pleinement conscients. Ce livre pourra certainement les aider à améliorer leur connaissance{ XE "connaissance" } théorique de cette discipline, sans pour autant oublier que rien ne remplace l'expérience. On ne peut pas projeter de construire des réseaux relationnels si on n'en a jamais fait partie, si on ignore les réalités de leur fonctionnement, de leurs possibilités et de leurs limites. S'intéresser à la veille, c'est tôt ou tard faire le choix de s'y impliquer. Et c'est pourquoi il est sage de « surveiller la surveillance »... Sans en négliger la pratique.

Il existe cependant plusieurs types de « veille ». En suivant la typologie présentée par Jean-Michel Ribault et Bruno Martinet⁶, nombreux sont ceux qui distinguent la veille commerciale{ XE "veille commerciale" }, la veille concurrentielle{ XE "veille concurrentielle" }, la veille technologique{ XE "veille technologique" } et la veille environnementale. Cette distinction est difficile à maîtriser par l'entreprise dans la mesure où l'évolution de l'environnement{ XE "environnement" } concerne aussi bien la commercialisation de produits existants que la recherche de nouveaux produits. Technologie, concurrence et environnement ne sont que très rarement dissociables. La veille est ainsi abordée, dans ce qui suit, sous son aspect global, intégrant aussi bien la technologie que la concurrence, le politique{ XE "politique" } que le social. Pour mener à bien plusieurs des analyses présentées, la veille technologique a tout de même présenté l'intérêt, d'une part, d'être pratiquée depuis longtemps (d'avoir ses experts, ses méthodologies) et d'autre part, d'être fortement liée à l'utilisation des nouvelles technologies de l'information. L'analyse infographique de la parution de brevets à partir d'une base de donnée scientifique en constitue un bon exemple⁷.

La veille technologique recouvre cependant elle-même un domaine très vaste, concernant aussi bien la surveillance de l'évolution de la recherche fondamentale⁸, que la surveillance des procédés de fabrication⁹ et des matières premières. Parmi ces différents aspects, la surveillance dédiée *aux transferts de connaissances* est plus particulièrement intéressante. D'une part, les transferts industriels présentent l'atout de mettre en œuvre un nombre important de technologies de l'information{ XE "technologies de l'information" }. D'autre part, — et parce que la recherche fait de plus en plus appel aux technologies de l'information dans sa pratique professionnelle¹⁰ — l'évolution des systèmes d'information a désormais un impact sur l'avancée de la science, par une plus grande et plus rapide diffusion de ses résultats¹¹.

1.1.2. Veille technologique, science et industrie

⁶ Bruno MARTINET, Jean-Michel RIBAUT, *La veille technologique, concurrentielle et commerciale*, Editions d'Organisation, 1989.

⁷ Voir à ce propos Henri DOU, PARINA HASSANALY, « Infographic Analytical Tools for Decision Makers », *Scientometrics*, Vol. 17, Nos 1-2, pp. 61-70.

⁸ Nouveaux résultats, dépôts de brevets, orientations possibles des axes de recherche, possibilités de liens interdisciplinaires.

⁹ Matériaux, filières, et méthodes de transformation,

¹⁰ Bases de données scientifiques, communication par réseaux informatiques entre centres de recherches et centres industriels.

¹¹ Le destin d'un résultat de recherche est autant lié à la technologie qui va le transporter à travers le monde qu'à sa valeur intrinsèque. Les stratégies de valorisation de la recherche sont avant tout des stratégies informationnelles.

La veille technologique que nous évoquerons est ainsi sous-tendue par un nouveau défi de *synergie*¹² entre la science et de l'industrie. Parce que l'industrie se rapprochera de la science, elle agrandira sa connaissance fondamentale et augmentera ses possibilités de mettre en œuvre des combinatoires génériques de technologies.

De son côté, la science élargira sa perspective sur *une autre recherche, qui a ses propres rituels*, et dont l'expertise est tout aussi intéressante que celle de la recherche fondamentale. Ce sont deux communautés aux habitudes sociales et aux normes de groupe¹³ différentes qu'une pratique réfléchie de la veille technologique a pour mission de rapprocher.

Cette mission de rapprochement des deux communautés scientifique et industrielle est confiée à ce que nous appellerons des « médiateurs science-industrie ». Au service de l'entreprise, ou au service d'une organisation de recherche, leur mission est d'augmenter le flux d'échanges entre les deux communautés. Pour l'entreprise, ces médiateurs lui permettent d'être proche des centres d'innovation{ XE "innovation" } et de créer des liens qui lui permettront de revendiquer une priorité sur l'acquisition d'une éventuelle découverte du laboratoire. Pour la recherche, de tels médiateurs permettent d'augmenter les flux contractuels (*deal flow*) avec l'industrie.

LE MEDIEATEUR SCIENCE - INDUSTRIE		
MISSIONS	FLUX	MOYENS
veiller	d'informations	colloques et partenariats
lier	contractuels (<i>deal flow</i>)	financement de recherches
rapprocher	informels	persuasion
influencer	décisionnels	prise de leadership
acquérir	financiers	budgets de transfert industriel

¹² Terme emprunté au psychologue français François GAUCHET pour désigner la concaténation, puis la fusion d'un groupe dans la réalisation d'un projet commun. Ses principaux atouts sont le gain de temps et la cohérence dans la réalisation des objectifs des deux parties en interrelation.

¹³ Kurt LEWIN, *Readings in Social Psychology*, Holt Rinehart & Winston, New-York, 1947, pages 197-211.

Le réseau des médiateurs est une structure{ XE "structure" } de veille, un environnement qui facilite l'accès, le partage et l'analyse commune de l'information, entre deux communautés : scientifiques et industriels. Etudier de telles organisations permet de comprendre ce qui amène l'entreprise à se rapprocher de la recherche fondamentale, mais aussi comment est envisagée la veille technologique dans cette nouvelle perspective. Des liens étroits entre « capacité d'écoute » et capacité d'innovation ont pu ainsi être mis en relief.

De fortes disparités peuvent ainsi être relevées dans le niveau d'utilisation des nouvelles technologies d'information selon la taille des industries, exceptions faites des « petites industries de la matière grise ». Il existe en effet des groupes d'experts d'une dizaine de personnes qui ont quitté la grande industrie pour créer leurs propres sociétés. Très équipées en technologies et positionnées sur des « niches », ces P.M.I. ont mis en place des combinatoires de compétences concentrées dans une poignée d'hommes qui remettent en question l'effet de la taille des entreprises sur leur excellence technologique.

1.2. Description des méthodes utilisées

1.2.1. Retracer l'histoire de la surveillance

La surveillance est le point de rencontre nécessaire entre plusieurs disciplines, parmi lesquelles l'économie industrielle{ XE "économie industrielle" }, la sociologie{ XE "sociologie" } des organisations, l'économie de l'information, la stratégie{ XE "stratégie" } et le management.

Elle est une *discipline de l'économie industrielle* dans la mesure où la surveillance s'exerce avec des objectifs de *compétitivité*, de *veille technologique*, d'*acquisition et de transferts de connaissances*. Pour étudier ce point, nous ferons référence à des auteurs comme Schumpeter¹⁴, dont l'analyse du processus de l'innovation, stimulée par des combinaisons de facteurs de production — *et qui se développe en « grappes »* — correspond tout à fait à la thèse que nous essayerons de développer. Nous associerons en effet *le déploiement* de la surveillance à la diffusion des technologies telle que l'envisage Joseph Schumpeter : en refusant une coupure trop stricte entre le court terme et le long terme, entre l'économique et le social. Mais il nous faudra contester, avec Joan Akerman¹⁵, *l'aspect exogène* du progrès technique de Schumpeter. Les inventions ne jaillissent pas spontanément. En niant l'autonomie du progrès technique vis-à-vis de l'évolution économique, nous essayerons de montrer qu'il existe *des structures favorisant l'innovation* et que la *surveillance* peut en être une des forces motrices. Pour que la surveillance ait un rôle à jouer, il faut également sortir du cadre utopique d'une

¹⁴ Joseph Aloys SCHUMPETER, (1883-1950), *Business Cycle*, 1939, *Capitalisme, Socialisme et Démocratie*, 1942, *History of economic analysis*, 1954.

¹⁵ Joan AKERMAN, *Structures et cycles économiques*, 1945.

concurrence pure et parfaite telle qu'a pu la définir Adam Smith ¹⁶, ou par la suite, Léon Walras ¹⁷. La concurrence{ XE "concurrence" } ne sera pas pure, car nous nous placerons le plus souvent dans des hypothèses d'asymétrie de niveaux d'information entre acheteurs et vendeurs. De plus, pour que le transfert d'une technologie{ XE "technologie" } *d'une firme à une autre* soit justifié, il faut considérer qu'aucune autre technologie ne lui est substituable. L'hétérogénéité des biens et des structures est une condition *sine qua non* à notre approche. De même, *la concurrence sera imparfaite* car si l'information circulait librement, quelle serait l'utilité tactique de la surveillance ?

La surveillance est aussi *une discipline de la sociologie des organisations*. Il y a encore peu de temps, surveiller, n'était rien d'autre *qu'assujettir*. C'est bien le rôle que Taylor ¹⁸, Fayol ¹⁹ ou Bergery ²⁰, confiaient à la surveillance au sein de la firme : *le maintien de l'ordre productif*. Mais la démarche sociologique, c'est aussi expliquer les « *mécanismes* » de la surveillance en termes de *relations de pouvoir*, de *schémas relationnels* de négociants à négociants. Une nouvelle voie d'analyse est ouverte par François Perroux ²¹ qui intègre *le pouvoir* à l'économie, dans la propagation du progrès technique aussi bien que dans la structuration de l'espace{ XE "espace" }. Mais c'est surtout à des auteurs comme Jeremy Bentham ²², Michel Foucault ²³, Michel Crozier ²⁴, Erhard Friedberg ²⁵ ou même René Girard ²⁶, que nous emprunterons le plus de notions. La surveillance a évolué. Elle a principalement changé de méthodes, de formes et de présence. Ces différents auteurs nous aideront à comprendre comment elle est entrée dans le jeu quotidien des firmes dans le cadre des relations intra industrie.

La surveillance, enfin, est tout autant *une discipline de l'économie de l'information*, qu'un des domaines d'étude du *management* et de la *stratégie*. Nous aurons ainsi l'occasion d'explorer les écrits de Michaël Porter ²⁷, d'Harold

¹⁶ Adam SMITH, (1723-1790), *Recherche sur la Nature et les Causes de la Richesse des Nations*, 1776.

¹⁷ Léon WALRAS, (1834-1910), *Abrégé des éléments d'économie politique*, réédité par Leduc, Paris et Lausanne, 1938.

¹⁸ W. TAYLOR, *La Direction des ateliers*, Dunod, 1919.

¹⁹ H. FAYOL, *Administration industrielle et générale*, Dunod, 1920.

²⁰ C.L. BERGERY, *Economie industrielle*, Tome III, « La conduite d'une fabrique », Metz, 1831

²¹ F. PERROUX, *Pouvoir et Economie*, Dunod, 1974.

²² J. BENTHAM, « Le Panoptique », in *Théorie des peines et des récompenses*, Edition Dumont, Genève, 1811.

²³ M. FOUCAULT, *Surveiller et Punir*, Gallimard, 1975.

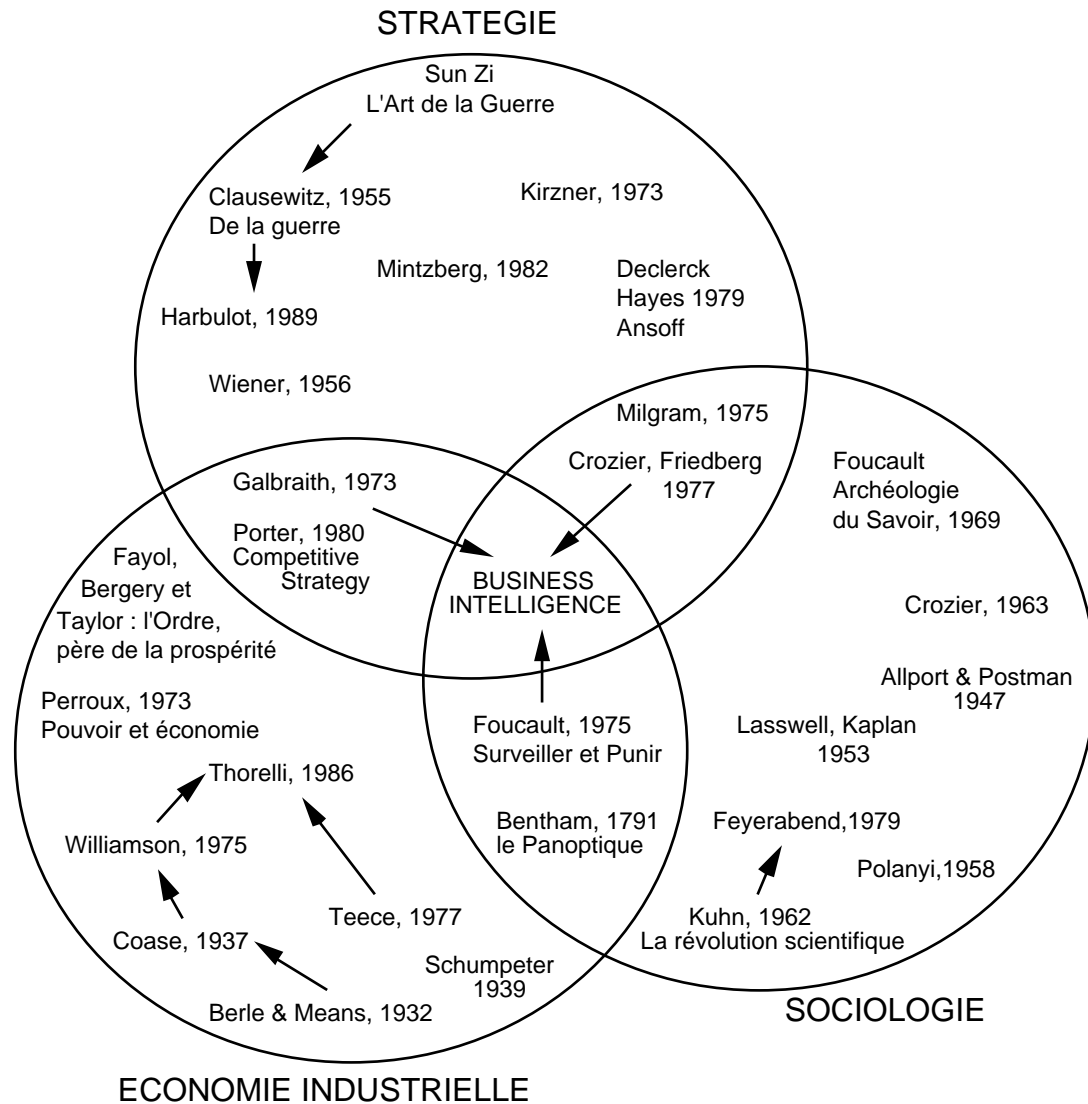
²⁴ M. CROZIER, *Le phénomène bureaucratique*, Editions du Seuil, 1963.

²⁵ Erhard FRIEDBERG, Michel CROZIER, *L'acteur et le système*, Editions du Seuil, 1977.

²⁶ René GIRARD, *La violence et le sacré*, Grasset, 1972.

²⁷ Michaël E. PORTER, *Competitive Strategy*, McMillan, 1980.

Lasswell ²⁸, de Donald Teece ²⁹, ou encore de Thorelli ³⁰, en essayant toujours de faire le lien entre stratégie de l'entreprise et utilisation de l'information. Notre propos sera ici d'étudier quelles *utilisations stratégiques* la firme peut faire de l'information, mais aussi de définir quelles sont les structures stimulant au mieux ces utilisations.



²⁸ Harold D. LASSWELL, « The function of propagandists », pp. 258-268, The International Journal of Ethics, Vol. 38, University of Chicago Press, 1927.

²⁹ Donald J. TEECE, « The Market for Know-how and the Efficient International Transfer of Technology », *Annals of the American Academic Journal of Political and Social Science*, November 1981.

³⁰ H. THORELLI, « Networks: between markets and hierarchies », *Strategic Management Journal*, Vol. 7, 1986.

Cela nous amènera à étudier aussi bien l'aspect offensif{ XE "offensif" } de la manipulation de l'information{ XE "manipulation de l'information" }, avec des auteurs comme Sun Tzu ³¹ et Allport ³², que son aspect défensif{ XE "défensif" } : transfert de connaissances, ou protection du potentiel technologique. Sur ce constat de *multidisciplinarité*, la recherche historique sur la surveillance s'est tout naturellement orientée selon les axes suivants :

(1) La genèse de la surveillance quand elle n'avait pas d'autre objectif que d'économiser le pouvoir de répression, c'est-à-dire lorsqu'elle était un *instrument disciplinaire*, avec Bentham, Beccaria, Bergery, Taylor, Fayol et Foucault.

(2) La définition *d'un nouveau concept de firme industrielle*, avec Scherer, Thorelli, Johanson et Williamson.

(3) L'étude des étapes de la *connaissance* que la surveillance se propose d'acquérir comme de défendre, avec Feyeraabend, Foucault et Kuhn.

(4) L'étude de la surveillance économique{ XE "surveillance économique" }, cette fois-ci, et notamment celle qui se consacre à *l'environnement de la firme*, avec Aguilar, Ansoff ou encore des praticiens comme Jakobiak, Villain et Lesca.

(5) L'analyse du rôle de l'information dans les relations entre firmes, avec l'approche des notions de flexibilité, de réputation ou de dissuasion, avec Gremaq, Cohendet ou Llerena.

(6) La description des utilisations détournées de l'information, comme la rumeur, la propagande, la désinformation, avec Lasswell, Allport, Postman, Doving et Hovland.

(7) La description des relations de pouvoir dans l'organisation avec l'apport de la cybernétique de Wiener, Ashby et Milgram, mais aussi l'apport d'approches nouvelles comme celles de Crozier et de Friedberg.

(8) L'étude du rôle des informations nouvelles et plus particulièrement, du rôle de l'innovation technologique dans la compétitivité{ XE "compétitivité" } des firmes, ce qui nous permettra de décrire une fonction stratégique de la surveillance avec Teece, Kamien, Ramantsoa et Abernathy.

(9) La synthèse, enfin, d'une surveillance conçue à la fois comme l'un des éléments conceptuels d'une nouvelle firme industrielle, et comme stimulatrice de la dynamique de l'innovation, c'est-à-dire dans *son acception stratégique*, avec Ansoff, Porter, Declerck, Kirzner ou Zimmermann.

Les ouvrages ainsi consultés sont regroupés, à la fin de cet ouvrage, selon les neuf domaines d'analyse que nous venons de décrire.

1.2.2. Entretiens avec des professionnels de « l'intelligence »

³¹ SUN TZU, *L'art de la guerre*, « De l'utilisation des espions », Traduction de Niquet-Cabestan, Economica, 1988.

³² G.W. ALLPORT, L.J. POSTMAN, *The Psychology of Rumor*, Holt & Co Publishers, New York, 1947.

Surveiller, c'est mettre en œuvre plusieurs expertises d'horizons très divers : observations, recoupements, interview de réseaux relationnels ou acquisitions de rapports de recherche fondamentale... La surveillance fait l'objet d'une coordination{ XE "coordination" } de plusieurs expertises détenues par des chercheurs, des hommes du marketing, des planificateurs ou des gestionnaires.

Les entretiens qui ont été menés ne doivent donc, en aucun cas, être considérés comme représentatifs d'une population ou d'une profession. Leur finalité est principalement *qualitative*. L'objectif était de mettre en valeur des divergences ou des convergences de points de vue plus *significatives que représentatives*.

Un guide d'entretien délibérément très ouvert a été le support de l'ensemble de ces entrevues. La principale difficulté rencontrée a été la *réticence* des praticiens à fournir l'information recherchée. Ce refus des personnes à livrer une information précise concernant de telles activités est peu contournable. Il s'agit, en fait, de ne pas s'éloigner trop souvent des centres d'intérêts de l'interlocuteur. De même, le terme de « surveillance » s'est révélé ambigu pour la grande majorité des praticiens. On lui préfère la notion floue de « veille ». Le verbe « surveiller » se rapportant à l'univers carcéral, juridique et policier, tandis que le mot « veille » semble dénué de connotations à *utilités négatives*, c'est-à-dire contraignantes, et rallie ainsi conseillers et praticiens.

Ces entretiens avec des praticiens ont eu plusieurs objectifs. Il s'agissait de faire le point sur la situation française de la veille, d'en connaître les *acteurs*, les *qualités* et les *défauts*, mais aussi de prévoir ce qu'elle pourrait devenir, grâce aux nouvelles technologies de l'information, en termes de coût, de méthode et de pratique.

1.2.3. Expérimentation du concept sur réseau

Le réseau{ XE "réseau" } informatique tient une place essentielle dans cet ouvrage en tant qu'objet d'étude, d'expérimentation et de communication. Grâce au réseau interuniversitaire BITNET mis en place par la société IBM, qui relie à travers 26 pays plus de 2600 centres de recherche et universités, la création d'un groupe de discussion autour du thème « Strategic Information and Management » a pu être réalisée.

Ce groupe réunissait, dès le 9 décembre 1989, près de 100 participants d'horizons très divers³³. L'hétérogénéité du réseau BITNET, c'est-à-dire sa possibilité de connecter des ordinateurs de constructeurs différents, offre l'opportunité de créer des groupes très variés dans le cadre des « distribution lists ». Le principe en est assez simple : des utilisateurs ayant un intérêt commun peuvent se regrouper dans une liste de distribution de messages. Cette liste est alors considérée comme un utilisateur du réseau capable de redistribuer tout message qui lui est envoyé. La liste en question s'appelait « Apogées ».

³³ Massachusetts Institute of Technology, Wharton School of Business, London School of Economics, ... (voir encadré).

L'utilisation de ce type de liste est fondée sur le respect mutuel, c'est-à-dire qu'il n'y a pas de protection à l'entrée des messages. Ainsi, les interventions de chaque participant n'engagent qu'eux mêmes et ne sauraient être représentatives du lieu physique ou organisme, à partir duquel les messages sont envoyés. Des centaines de listes existent déjà sur ces réseaux, avec des sujets très variés (anthropologie, marketing, sociologie...).

Une liste d'une centaine de correspondants, comme celle d'Apogées, est l'occasion de tester la validité du concept de « veille sur réseau ». La croissance très soutenue que connaissent les réseaux informatiques est souvent associée à la possibilité d'une nouvelle forme de surveillance. Ce raccourci un peu aisé ne prend pas en considération la *nature* des informations susceptibles d'être obtenues sur un réseau, ni leur important *trafic*, ni la nécessité d'*adapter* les méthodologies classiques à ce nouveau médium. La liste Apogées a également permis de comparer les différentes acceptions du concept « d'information stratégique{ XE "information stratégique" } » pour chaque participant.

CHAPITRE II

Hypothèses de travail

2.1. Hypothèses relatives aux concepts

2.1.1. La firme comme un « nœud » de contrats

Pour soutenir notre analyse, la firme sera prise dans son acception d'*agence*. Il faut évoquer, pour justifier ce choix, l'évolution de la théorie de la firme depuis sa conception néoclassique jusqu'à la théorie de l'agence. Considérée comme une sorte de « boîte noire », la firme néoclassique, en répondant à la demande, n'avait d'autre mission de maximiser le profit et d'augmenter sa valeur intrinsèque. Une première novation du concept est apportée par les travaux de Berle et Means³⁴ qui proposent d'opérer une distinction entre les motivations des dirigeants et des propriétaires de la firme. La question du *pouvoir de décision* est pour la première fois soulevée. Les hypothèses de Berle et Means considèrent que le capital{ XE "capital" } étant fortement diffusé, la possibilité d'en posséder une fraction importante est faible, que les cadres dirigeants{ XE "dirigeants" } sont le plus souvent dans ce cas de figure et que, finalement, leurs intérêts divergent de ceux des propriétaires majoritaires de la firme.

Cette amélioration de la théorie ne nous permet cependant pas d'étudier la problématique du *partenariat* et du *partage de l'approche stratégique des activités de la firme*. De plus, elle favorise le dirigeant à qui elle confère la primauté du pouvoir de décision, laissant en retrait l'actionnaire qui *surveille* la cohérence des choix opérationnels avec les choix capitalistiques (investissements et profitabilité à long terme). Cette conception du partage de la décision dans la firme est trop fonctionnelle et laisse peu de place à des relations de négociant à négociant (relations de pouvoir et de conflit entre actionnaires et dirigeants).

³⁴ BERLE and MEANS, *The modern corporation and private property*, 1932.

La seconde novation conceptuelle nous vient de Coase³⁵ qui repose sa conception de la firme sur la base juridique de sa propriété. C'est en comparant les caractéristiques de la propriété privée (exclusivité dans l'usage du bien et libre transfert de ce droit) au droit de décider dans la firme que l'auteur met en évidence l'*aspect contractuel* de la décision. L'entreprise est alors perçue comme un « nœud de contrats », c'est-à-dire un canevas relationnel construit sous la motivation{ XE "motivation" } du gain et orienté dans un objectif de réalisation commune. Cette conception, qui se rapproche de celle du réseau, peut supporter aisément l'étude de la circulation de l'information en fonction de différents schémas disciplinaires.

2.1.2. Les espaces de la compétition

Notre première hypothèse de travail décrit l'environnement de la firme comme un *espace* soumis à des contraintes endogènes et exogènes de compétitivité. On entend par « espace » *l'ensemble des relations*³⁶ qu'entretient la firme avec les *domaines d'activité*, où son passé, son présent et son devenir sont impliqués. L'espace est donc pris ici dans une acception large. On pourra parler d'espaces économiques, comme d'espaces sociaux, historiques, juridiques, technologiques, politiques et culturels. Cette notion de l'espace permet d'élargir la notion de *contrainte de l'environnement* à l'écologie des systèmes, à la sociologie des organisations, ou encore à la psychologie{ XE "psychologie" } des acteurs. L'environnement, dans cette définition, tolère une rationalité limitée. Plus proche du concept de paradigme que de celui de territoire, l'espace auquel nous ferons référence, dans le cadre de nos analyses, rend possible l'*identification* des multiples contraintes auxquelles est soumise la compétitivité de la firme. Il permet de les *appréhender* dans le cadre commun d'un *seul schéma directeur*. Ce en quoi il se rapproche de la notion d'*environnement pertinent* de Crozier et Friedberg : « Dans l'accomplissement de ses objectifs, toute organisation, quelle qu'elle soit, doit négocier avec *son environnement* »³⁷.

2.1.3. Le nouveau paradigme de l'information

Quant à notre hypothèse centrale, elle est construite autour de l'émergence d'un nouveau paradigme{ XE "paradigme" } de l'information. Le paradigme, c'est avant tout l'exemple de référence (*paradeigma*), ou encore, un schéma pour l'acquisition des connaissances, mais avec Thomas Kuhn, « on réalisera

³⁵ R.H. COASE, « The nature of the firm », *Economica*, Vol. 4, Londres, novembre 1937, pages 386-405.

³⁶ Un ensemble de relations me paraît plus signifiant que des frontières géographiques. Le concept de « relation » met en relief la mouvance, et la fragilité, de l'environnement de la firme. Il suggère que la totalité de cet environnement se modifie sous la pression des relations de pouvoir que la firme entretient avec lui, de négociant à négociant.

³⁷ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Ed. du Seuil, Paris, 1977, page 164.

rapidement que le sens de *modèle* ou de *schéma* qui permet l'appropriation n'est pas tout à fait le sens de la définition du *paradigme*³⁸ ». C'est pourquoi le paradigme doit plutôt être considéré comme le *cadre de référence* d'un groupe donné de chercheurs, de scientifiques et/ou de praticiens. Il est constitué d'un ensemble de modèles, de méthodes et d'acquis qui ne sont plus discutés, permettant de résoudre des problèmes propres à ce groupe. Un paradigme est un *temps de stabilisation dans la démarche* du groupe. L'appartenance à un paradigme signifie que l'on adhère, que l'on défend et que l'on pratique cet ensemble de schémas stabilisés de résolution de problèmes. Cela implique aussi une *attitude commune* dans la conception et la gestion, qui s'étend à tous les concepts d'efficacité pour la production, aux modèles mis en œuvre et aux relations intra-industries.

Dans ses applications classiques, le paradigme fonctionne « en permettant de *reproduire* des exemples dont n'importe lequel pourrait, en principe, le remplacer³⁹ ». Ce qui n'empêche pas ce paradigme d'être « rarement susceptible d'être reproduit⁴⁰ » parce que toujours « destiné à être *ajusté et précisé* dans des conditions *nouvelles ou plus strictes*⁴¹ ». A l'instar d'un modèle, le paradigme génère lui-même sa contradiction, et une fois ajusté, se régénère en modèle. Les technologies de l'information ont ainsi connu trois de ces « modèles ». Il s'agit des trois paradigmes suivants :

— **Le paradigme de la centralisation**{ XE "**centralisation**" }, pendant lequel les informations étaient systématiquement dirigées vers des sites centraux et traitées par lots. Accessibles seulement dans des formats fixes et avec de longs temps de traitement, l'information était gérée de façon statique : on appréhendait une succession d'états, ou de phases de calcul, sans pouvoir encore envisager d'autres approches. Tous les espaces d'activité de la firme n'étaient pas couverts par le système qui était le plus souvent focalisé sur des questions scientifiques (calculs, recherches et développements).

— **Le paradigme de l'interactivité**{ XE "**interactivité**" } **partielle**, avec l'apparition de la mini-informatique interactive. Les informations sont encore centralisées mais accessibles en secondes au lieu d'heures. Les temps de transfert restent cependant longs et les formats fixés à l'avance. Le développement des applications est réalisé par des analystes et restent hermétiques à l'utilisateur final.

— **Le paradigme de l'individualisation**{ XE "**individualisation**" }. L'information et son traitement sont plus fréquemment décentralisés, au moyen de micro-ordinateurs, mais les informations essentielles à la firme, ses bases de données, son patrimoine technologique, appartiennent encore au premier ou au second de ces trois paradigmes. En fait, selon le stade d'évolution de la firme elle-

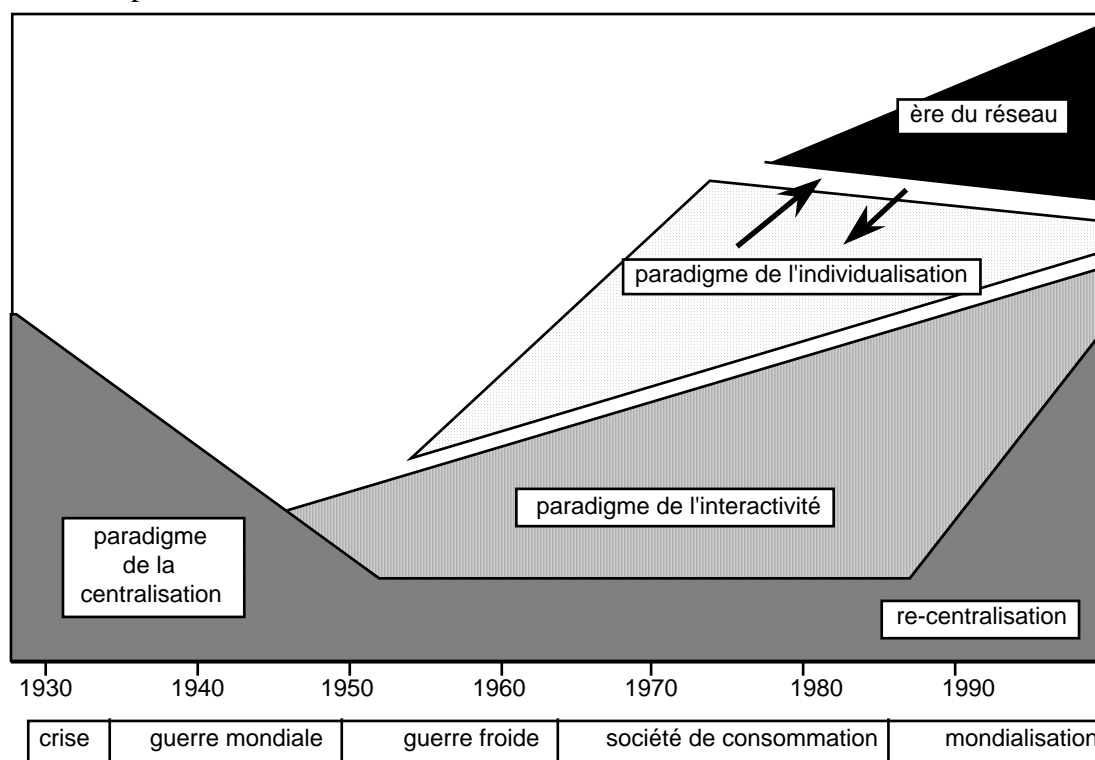
³⁸ Thomas KUHN, *La structure des révolutions scientifiques*, Flammarion, 1983, p. 45.

³⁹ Thomas KUHN, Op. Cit., p. 45.

⁴⁰ Thomas KUHN, Op. Cit., p. 45.

⁴¹ Thomas KUHN, Op. Cit., p. 45.

même, il y a *coexistence* de paradigmes, avec leurs spécialistes, leurs défenseurs et leurs praticiens⁴².



On peut expliquer cette coexistence par trois contraintes majeures d'ordres historique, économique et technologique. Il y a eu contrainte historique, car le premier paradigme se « cristallise » dès l'après-guerre et il faudra attendre plus de vingt ans avant d'accéder au stade de *l'interactivité partielle* (guerre froide, peur du partage, peur de l'espion). Une contrainte économique est venue surenchériser ces difficultés car chaque passage d'un paradigme à un autre est coûteux et plus l'aspect novateur du paradigme est grand, plus ce *coût* est important. On ne peut pas transférer, du jour au lendemain, plusieurs dizaines de millions d'informations centralisées vers des sites délocalisés et encore moins, vers des micro-ordinateurs dont les capacités de stockage sont très restreintes. C'est en cela qu'il y a aussi contrainte technologique, et il nous faut mettre en parallèle l'évolution de la technologie du semi-conducteur et celle des paradigmes.

C'est une innovation technologique qui sera à l'origine de la quatrième remise en cause, mais cette fois-ci, la problématique de la coexistence de paradigmes peu ouverts les uns aux autres semble résolue. Les nouveaux réseaux informatiques vont ainsi relier sites centraux, mini-informatique interactive et micro-ordinateurs. En laissant chaque élément (serveur, systèmes d'exploitation et applications) jouer son rôle, pour lequel il est le mieux adapté, le système

⁴² Voir à ce propos la postface à l'édition de 1962 de *La structure des révolutions scientifiques* de KUHN, publiée par Flammarion en 1983, pp. 237-284.

optimise l'accès, le partage et l'utilisation de l'information. En s'adaptant à l'accélération et à la délocalisation des espaces de la compétitivité, cette nouvelle informatique, partagée, ouverte et accessible, confère à son paradigme une dimension universelle. Elle concerne la totalité du système d'information de la firme, son mode d'activité, jusqu'à la gestion de ses ressources humaines. Tout ce qui est en rapport avec l'information (recherche, fabrication, commercialisation...), va s'intégrer parfaitement dans une nouvelle architecture{ XE "architecture" }, optimisant la coexistence de ces trois paradigmes et en les fusionnant en un quatrième : **le paradigme de l'information**.

Afin de valider ou d'infirmer l'hypothèse de ce nouveau paradigme, nous démontrerons que l'introduction de nouvelles technologies a modifié, *par ajustements successifs*, les conditions expérimentales, et par la même, les supports empiriques des théories des autres paradigmes. Ainsi, pour Thomas Kuhn, les nombreuses discussions « sur les méthodes légitimes, les problèmes, les solutions acceptables ⁴³ » sont « annonciatrices des révolutions scientifiques, *au moment où les paradigmes sont attaqués et susceptibles de changer* ». Nous décrirons l'évolution de ces débats, parallèlement à d'autres évolutions, technologiques et économiques.

2.2. Hypothèses sur le panoptisme

2.2.1 Bentham et sa technologie politique

Si l'objet d'une politique est d'organiser le pouvoir{ XE "pouvoir" } de manière à rendre plus efficace l'ensemble des pratiques et déterminations d'une organisation, alors, en un certain sens, le panoptique est un outil politique.

Etienne Dumont, l'ami de Jeremy Bentham, écrit à l'Assemblée Nationale française en 1791 : « Si l'on trouvait un moyen de se rendre maître de tout ce qui peut arriver à un certain nombre d'hommes, de disposer tout ce qui les *environne*, de manière à opérer sur eux l'*impression* que l'on veut *produire*, de s'assurer de leurs actions, de leurs liaisons, de toutes les circonstances de leur vie, en sorte que rien ne pût échapper ni contrarier l'effet désiré, on ne peut pas douter qu'un moyen de cette espèce ne fût un *instrument* très énergique et très utile que les *gouvernements* pourraient appliquer à *différents objets* de la plus haute importance ⁴⁴ ».

Dans cette introduction au panoptique, Bentham utilise les quatre mots clés de cette première hypothèse : environnement, impression{ XE "impression" }, production et instrument. Ce qu'il décrit, c'est bien un *instrument* politique, un

⁴³ Thomas KUHN, *Op. Cit.*, p. 77.

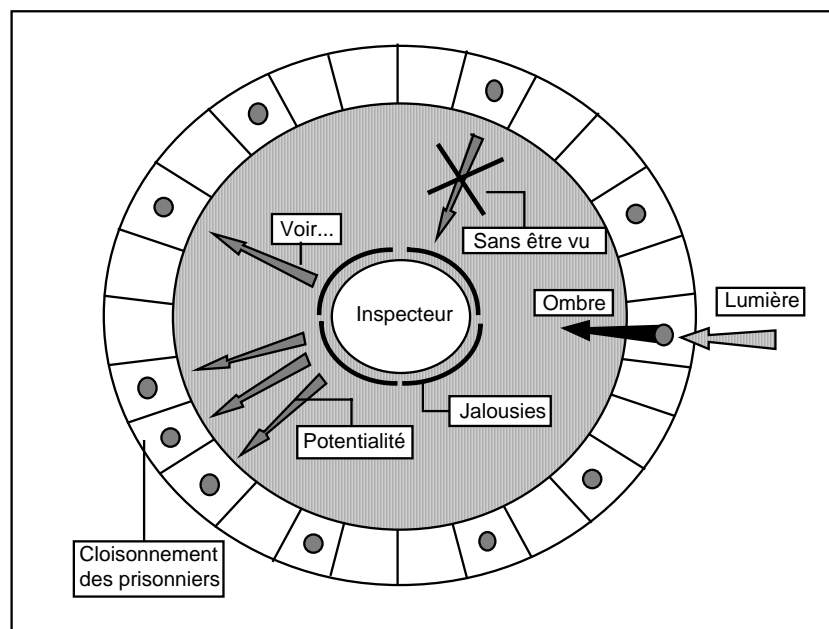
⁴⁴ M.E. DUMONT, *Mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maisons de force*, imprimé par ordre de l'Assemblée Nationale, Paris, Imprimerie Nationale, 1791.

outil du pouvoir, permettant de *produire* une *impression*, c'est-à-dire intégrant la dimension psychologique, afin de maintenir le pouvoir. Comment ? Non pas en agissant directement sur les hommes, mais sur *l'environnement tout entier*, en modifiant la *totalité de leur cadre de référence*.

C'est ce principe du panoptique{ XE "panoptique" } qui est applicable à l'information de la firme. On peut ainsi émettre l'hypothèse que la firme *perçoit* son environnement en fonction de son cadre de référence : acquis culturels, sociaux, technologiques, historiques et juridiques. La connaissance, puis la modification, de façon indirecte, de ce cadre de référence permet à la firme concurrente de *produire* une *impression*, de déstabiliser, d'augmenter le climat d'incertitude et ainsi d'augmenter son pouvoir relatif.

2.2.2 Panoptisme et technologies de l'information

Rappelons le principe du panoptique pour introduire cette seconde hypothèse. La prison panoptique est construite dans un bâtiment *circulaire*, de manière à ce que chaque cellule s'ouvre sur son centre, où est placée la tour d'inspection. Chaque cellule est ouverte à la lumière de part et d'autre, de façon à se laisser traverser par elle. L'inspecteur, placé au centre de ce bâtiment circulaire, peut ainsi voir, *en même temps*, toutes les silhouettes de tous les prisonniers. La maison de l'inspecteur, le *mirador*, sont entourés de jalousies afin que l'autorité puisse *voir, sans être vue*. « Le panoptique est une machine à dissocier le couple voir-être vu : dans l'anneau périphérique, on est totalement vu, sans jamais voir ; dans la tour centrale, on voit tout sans jamais être vu ⁴⁵ ».

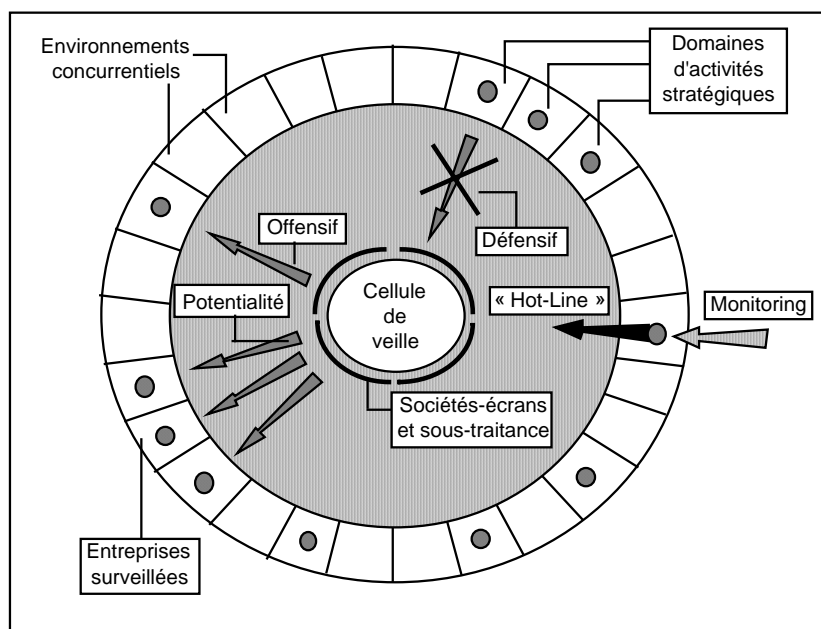


Le panoptique de Jeremy Bentham, 1787

⁴⁵ Michel FOUCAULT, *Surveiller et Punir*, Editions Gallimard, 1975, p. 203.

Le point important dans ce plan, comme l'explique Jeremy Bentham dans une de ses lettres ⁴⁶ est « que les individus sous surveillance se sentent constamment surveillés, ou, à tout le moins, qu'ils *pensent* qu'il y a des chances qu'ils le soient ». Mais, ajoute-t-il, « il n'est aucunement *le seul*. Le serait-il que le même avantage pourrait être dérivé de bâtiments de toutes formes ou presque. Ce qui, ici, n'est pas moins important, c'est que, pendant la plus grande proportion de temps possible, chaque individu *soit en fait sous surveillance* ».

Le principe d'une *visibilité* { XE "visibilité" } *permanente*, c'est-à-dire une situation de certitude { XE "certitude" } maintenue, est la base du panoptique. C'est cette *certitude* d'être visible qui constitue le frein psychologique assez puissant pour éviter toute tentative d'évasion du système. Et c'est l'incertitude { XE "incertitude" } de la présence *réelle* de l'inspecteur, ou de son regard dirigé vers le prisonnier, qui est la source d'*économie* du pouvoir. Caché derrière les jalousies de sa tour, l'inspecteur est peut-être en train de regarder ailleurs, ou peut-être est-il en train de surveiller celui-là même qui vient d'avoir cette pensée. L'inspecteur est seul, mais représente *virtuellement* un inspecteur pour chaque prisonnier. *La potentialité de l'inspection remplace son déploiement*. Certitude de visibilité, incertitude quant à la réalité de la surveillance, Bentham a inventé la machine à dissuader et a posé les premiers principes d'une économie de la dissuasion { XE "dissuasion" }. Cet ouvrage se propose, dans le sillage du panoptique, d'introduire une nouvelle notion : le néopanoptisme { XE "néopanoptisme" }.



Le néopanoptisme

⁴⁶ Jeremy BENTHAM avait choisi la forme épistolaire pour publier son « panoptique » (*Panopticon or the inspection-house*, 1787, réédition de Belfond, 1977, Lettre V, p. 109).

Selon ses propres termes, les écrits de Bentham repose « *sur une simple idée d'architecture* ». C'est cette idée qui est exploitée et du panoptisme, on retiendra tous les éléments qui permettent de mettre en œuvre une *dissuasion au moindre coût*. De l'idée d'architecture, on retiendra le modèle et on fera *abstraction* des murs, des briques, des tubes de fer blanc, pour introduire la notion de *réseau de communication* avec ses canaux{ XE "canaux" }, ses émetteurs{ XE "émetteurs" }, ses messages{ XE "messages" }, ses feed-back. La *tour* d'inspection, ce sera la firme face à ses espaces de compétition, les *cellules où sont prisonniers ses différents devenir, technologiques, économiques, politiques et culturels*. Le lien entre cette tour, la firme et les cellules de son devenir, les espaces de la compétition, ce sera le *néopanoptisme*, c'est-à-dire la faculté, pour la firme, de mettre en œuvre un ensemble de nouvelles technologies de l'information, dites *panoptiques*, pour appréhender son environnement.

2.3. Récapitulatif des hypothèses de travail

2.3.1 Hypothèse 1 : la firme-réseau

La firme est un « nœud » de contrats, entre les différents acteurs qui assurent la réalisation de ses objectifs. Elle est un *réseau de compétences* mises en œuvre sous l'égide de nombreuses relations contractuelles qui peuvent être financières, mais aussi morales, économiques, politiques et stratégiques. Cette acception de la firme, développée dans le cadre de la *théorie de l'agence*{ XE "théorie de l'agence" }, convient parfaitement à l'étude de la surveillance qui elle aussi s'organise en réseaux.

2.3.2 Hypothèse 2 : l'environnement-acteur

A l'instar de la firme, l'environnement sera considéré comme un *acteur* à part entière de la compétition. Il est défini comme l'ensemble des domaines d'activité et de leurs acteurs, avec lesquels la firme entre en relation et *négoce* son développement. Il regroupe les espaces économiques, sociaux, historiques, juridiques, technologiques, politiques et culturels.

2.3.3 Hypothèse 3 : le paradigme de l'information

Thomas Kuhn définit le paradigme comme « les découvertes scientifiques universellement reconnues qui, pour un temps, fournissent à une communauté de chercheurs des problèmes types et des solutions ⁴⁷ ». On peut rapprocher cette définition à une connaissance tacite, éprouvée et commune à un groupe établi, qui

⁴⁷ Thomas KUHN, *La structure des révolutions scientifiques*, Flammarion, 1983, p. 11.

lui permet ses recherches et lui suggère des résultats, tant que les fondements de cette connaissance ne sont pas remis en cause⁴⁸.

Il a existé trois grands paradigmes des technologies de l'information, celui de la *centralisation*, celui de l'*interactivité* et celui de l'*individualisation*. Les trois vont désormais constituer le *paradigme de l'information*, dont les caractéristiques sont issues des points communs et des confrontations (remises en causes) des trois autres paradigmes.

2.3.4 Hypothèse 4 : l'économie de la dissuasion

Le principe du panoptique, *voir sans être vu*, obtient son efficacité de la pression psychologique qu'il opère sur la personne surveillée. *Produire une impression* est la finalité de cette machine, car l'impression est omniprésente chez les individus surveillés, elle s'entretient d'elle-même, sans que cela *coûte* à l'autorité surveillante. La gestion de l'information dans un contexte fortement compétitif procède de la gestion des *impressions* offertes par la firme à ses concurrents.

2.3.5 Hypothèse 5 : le néopanoptisme

Le panoptisme repose sur une idée d'architecture. Le concept proposé de *néopanoptisme* conserve l'idée, mais supprime l'architecture réelle, avantageusement remplacée par une *architecture virtuelle* née des nouvelles technologies de l'information.

⁴⁸ Voir à ce propos la postface à l'édition de 1962 des *Structures des Révolutions Scientifiques* de KUHN, Flammarion, 1983, pp. 237-284.

CHAPITRE III

Problématique de la surveillance

3.1. Une problématique aux multiples aspects

3.1.1. Ses dimensions historiques et politiques

La surveillance est une relation de pouvoir. A ce titre, elle rémunère tout acte contribuant à son maintien, et réprimande tout autre, la remettant en cause. Mais il n'y a plus de pouvoir et par là même, plus de surveillance, sans l'ordre{ XE "ordre" } qui assujettit. Il n'y a pas non plus d'*ordre* sans le pouvoir qui l'entretient. L'ordre, c'est la structuration des contextes de l'autorité{ XE "autorité" } dans la finalité de la maintenir à sa place dominante. Le pouvoir, quant à lui, est une *relation instrumentale*{ XE "*relation instrumentale*" }, c'est-à-dire qu'il « ne se conçoit que dans la perspective d'un but qui, dans une logique instrumentale, motive l'engagement de ressources de la part des acteurs ⁴⁹ ». Ceux qui détiennent cette *capacité relationnelle*, non seulement par leur personnalité, mais aussi par leur position dans la hiérarchie{ XE "hiérarchie" } sociale, *savent très bien qu'elle est toute relative*. Comme le précisent Crozier et Friedberg, le pouvoir est une *relation non transitive*⁵⁰. Hors d'un contexte ordonné, c'est-à-dire structuré pour faciliter sa mise en œuvre, la relation de pouvoir ne se limite qu'à une poignée d'hommes, avec, pour chacun d'eux, un domaine très limité d'influence. Pour sortir de cette spécificité, l'ordre instaure un *schéma relationnel générique*, c'est-à-dire qu'il prévoit, pour chaque relation de pouvoir, comme le voleur face au policier, ou l'ouvrier face au chef d'atelier, un code de conduite et une échelle graduée des peines et des récompenses. Il génère des relations types.

⁴⁹ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Ed. du Seuil, 1977, p. 67.

⁵⁰ Michel CROZIER, Erhard FRIEDBERG, *Op. Cit.*, p. 67.

L'ordre, cependant, ne peut pas supprimer la liberté des acteurs{ XE "acteurs" }, il peut seulement *la contraindre à ne pas s'exprimer, temporairement*.

Face à ce risque irréductible de liberté, l'autorité punitive doit *savoir* « qui, où, quand, comment et pourquoi ». Elle doit sans cesse surveiller, pour corriger les lacunes de l'ordre, pour se prémunir contre les aléas des capacités relationnelles des hommes du pouvoir à maintenir leurs semblables dans l'assujettissement. L'autorité se veut savante et rationnelle. Sa grande *connaissance* des règles{ XE "règles" }, des usages et des lois, doit la rendre incontournable. Le pouvoir s'entoure d'ailleurs, tout au long de son histoire{ XE "histoire" }, de l'autorité consultative, du savant, ou de l'éminence grise. Si bien que l'on s'inquiète : du conseiller ou du Roi, qui gouverne ? Et l'homme qui gouverne a-t-il le savoir pour le faire ? Finalement, il faut bien « admettre que le pouvoir produit du savoir (et pas simplement en le favorisant parce qu'il le sert ou en l'appliquant parce qu'il est utile); que pouvoir et savoir{ XE "savoir" } s'impliquent directement l'un l'autre; qu'il n'y a pas de relation de pouvoir sans *constitution relative d'un champ de savoir*, ni de savoir qui ne suppose et ne constitue en même temps des relations de pouvoir ⁵¹ ».

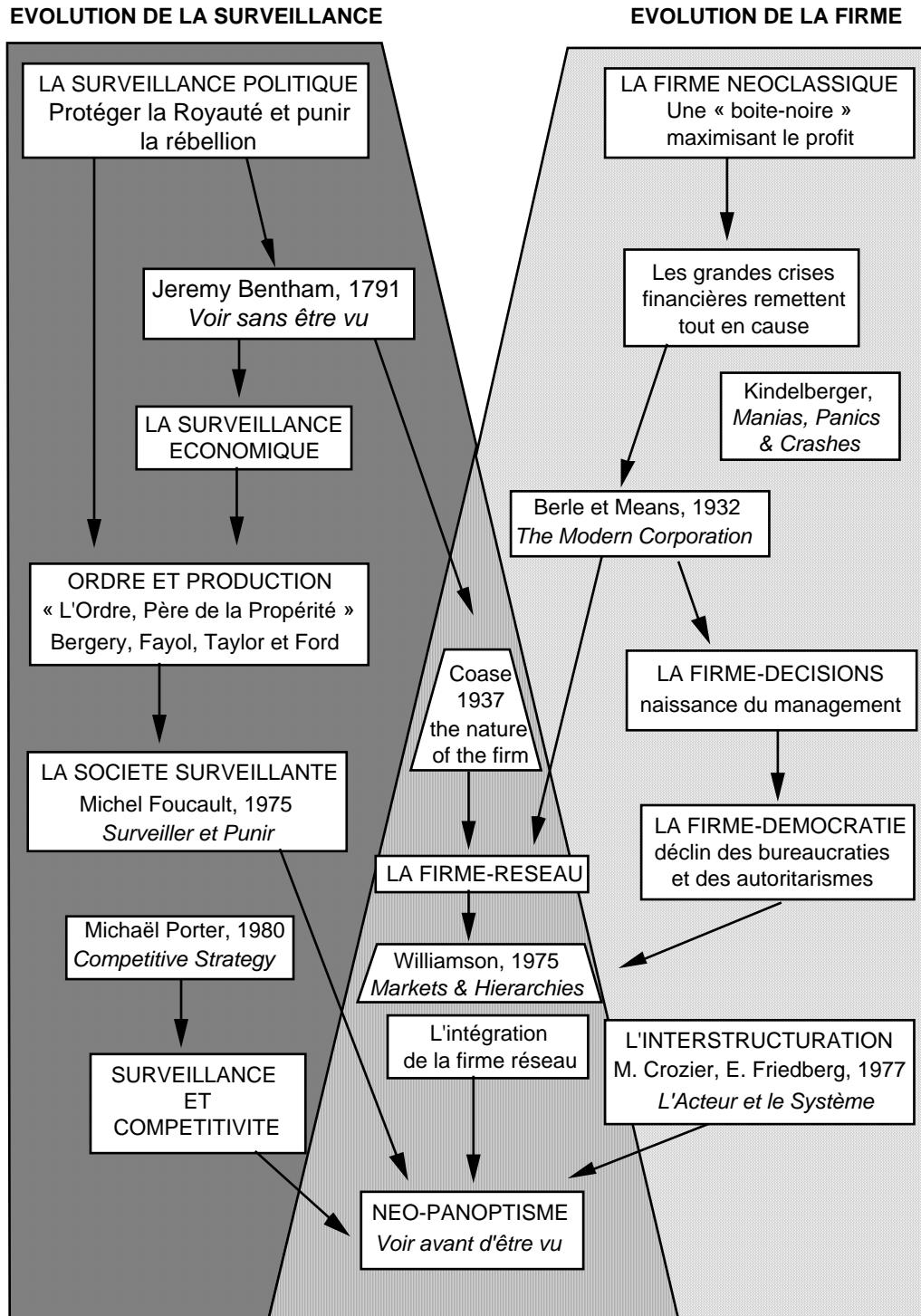
La dimension à la fois politique et historique de la surveillance, cette condition du pouvoir, est assez bien résumée par « Les deux corps du Roi » de Kantorowitz, en 1959. Michel Foucault écrit à ce sujet : « corps double selon la théologie juridique formée au Moyen Age, puisqu'il comporte outre l'élément transitoire qui naît et qui meurt, un autre qui, lui, demeure à travers le temps et se maintient comme le support physique et pourtant intangible du royaume ⁵² ». Dans ce contexte, la surveillance a eu une double mission historique. A l'instar du double corps du roi, elle protège le pouvoir *au présent*, par la désignation des coupables, par la possibilité de réagir, et elle garantit sa *pérennité*, le respect à travers le temps de la structure politique et sociale toute entière.

Pourtant, si elle accompagne le pouvoir, la surveillance ne se montre pas. Ou si elle se montre, c'est pour rappeler que le pouvoir sait aussi punir. *La surveillance est porteuse, historiquement, d'une connotation négative*. Elle rappelle l'inquisition et la délation. Elle est entrée dans la mythologie collective avec l'œil de Caïn et l'épée de Damoclès. Dans un contexte politique démocratique, être l'institution qui surveille, c'est être la représentation même de la défiance du pouvoir envers le principe de la démocratie : « Le peuple n'est-il pas assez *responsable* pour se gouverner lui-même ? Faut-il qu'on le suspecte ? ». Ce n'est pourtant pas le peuple qui est soupçonné, mais le malfaiteur *potentiel*, celui qui peut *troubler l'ordre public*. Et d'en conclure que la démocratie n'est pas viable sans ordre... Sous cet éclairage historique et politique, la problématique de la surveillance *pour la firme* revêt un tout autre aspect. Surveiller, c'est s'exposer à la critique. La firme qui surveille va être soupçonnée de vouloir agrandir son pouvoir, de prévoir des *punitions*, d'utiliser la *délation*. La firme qui surveille

⁵¹ Michel FOUCAULT, *Surveiller et Punir*, Gallimard, 1975, p. 32.

⁵² Michel FOUCAULT, *Op. Cit.*, p. 33.

entre dans un *schéma historique*, elle adhère *de facto* au principe punitif. Ainsi, le mot « surveillance » ne sera pas employé.



Dimension historique de la surveillance

On le remplace par le mot « veille » qui se rattache, lui, à des connotations fortement positives (la mère « veille » sur son enfant malade et fait preuve de « bienveillance »). La notion de « veilleur » est très éloignée de celle de « surveillant ». Ce qui éloigne ces deux notions, justement, c'est que le veilleur est là pour avertir l'autorité, mais *jamais ne punit*. Le surveillant est chargé d'administrer les coups, de réprimander, pour maintenir l'ordre. Le « veilleur », lui, bien plus « démocrate », a une mission *préventive*.

Ainsi, les conseillers d'entreprises vont progressivement faire du surveillant un manager et adapter la pratique de la surveillance aux contraintes de la modernité{ XE "modernité" } et de la démocratie{ XE "démocratie" } : « Profession naissante, la fonction de veilleur ne peut encore avoir de cadre définitif. (...) Le veilleur est un cadre. Sa mission est d'animer un réseau de communication{ XE "communication" }. (...) Le veilleur est donc un animateur, avec ce que le terme porte en lui de capacité d'écoute⁵³ ». Les auteurs déclarent la profession « *naissante* » et rejettent ainsi tout lien possible avec le surveillant pris dans son contexte historique de « geôlier », ou « d'inquisiteur ». Il « *anime* », donc participe : ce qui l'éloigne encore du surveillant dont la participation se résume souvent, dans la mythologie collective, à l'administration de la réprimande. Il « *communique* », ce qui sous-entend un dialogue et non plus la simple prise de renseignement. Et pourtant, sa mission est la même : il recueille l'information pour l'autorité qui le gouverne.

3.1.2 Ses dimensions sociales et culturelles

On ne surveille plus, on « veille ». Il n'y a plus de surveillant, mais des « veilleurs ». Ils ne font plus du renseignement, mais « recueillent l'information ». Ils ne font plus partie des services d'espionnage{ XE "espionnage" }, ou de contre-espionnage industriels, mais de « l'observatoire de l'environnement⁵⁴ ». La surveillance s'est adaptée à son nouvel *habitat social*. Elle a pris une forme plus douce et n'utilise pas les termes qui rappellent les temps éloignés de l'autoritarisme. La veille est un phénomène social de la firme. Elle est révélatrice d'un comportement qui s'adapte à la fois à des impératifs économiques et à des impératifs sociaux.

D'une façon plus générale, toutes les fonctions de la firme qui l'amènent à mettre en jeu son identité{ XE "identité" }, prennent désormais en compte le facteur social. La firme gère son image en régulant les intrants et les extrants qui peuvent être révélateurs de son identité (son projet, ses publications, jusqu'aux codes vestimentaires et le jargon professionnel de ses employés). Dans ce contexte, la fonction de surveillance externe et interne risque d'être révélatrice de son approche de l'environnement et de sa politique envers ses salariés. C'est pour cela que rien ne doit révéler une approche autoritaire dans la gestion des hommes

⁵³ Bruno MARTINET, Jean-Michel RIBAUT, *La veille technologique, concurrentielle et commerciale*, Editions d'Organisation, 1989. Le passage cité est tiré du chapitre 12, p. 253.

⁵⁴ Bruno MARTINET, Jean-Michel RIBAUT, *Op. Cit.*, pp. 237-255.

et des domaines d'activité stratégiques. La firme vend son image{ XE "image" } avant ses produits{ XE "produits" } et il devient difficile de vendre un produit *pour tout le monde* à un client *démocrate* si on est une organisation *autoritaire*.

Problématique d'autant plus forte que la culture{ XE "culture" } de l'entreprise est un *vecteur* de cette veille. L'exemple japonais est alors inévitable. La performance d'un système de surveillance réside dans la qualité et la quantité de l'information qu'il procure et dans son adaptabilité à la firme. Le système japonais associe histoire de la firme et histoire de l'individu dans la structure groupale. Un homme ne peut être dissocié du groupe auquel il doit tout : savoir, moralité et environnement quotidien.

Dans ce contexte, l'employé qui défend sa firme, défend son histoire et sa culture. Dans ce schéma shintoïste, la surveillance est *naturelle*. Elle fait partie du système de défense du moi. La nation, le groupe, la tradition et l'homme ne font qu'un, et « pourtant il serait erroné de croire que la notion d'intimité ou d'isolement n'existe pas chez les Japonais : elle est seulement très différente de la conception occidentale{ XE "conception occidentale" }⁵⁵ ». Ainsi, le Japonais qui surveille *son espace* ne surveille pas la même chose que l'Occidental qui surveille *son territoire* car « lorsque les Occidentaux parlent ou pensent à l'espace, il s'agit pour eux des distances entre les objets. (...) les Japonais ont au contraire appris à donner une *signification* aux différents espaces⁵⁶ ». Leur espace englobe leur symbolique{ XE "symbolique" } et leur tradition.

Cet espace, si important, ils le structurent, ils en font un outil de gestion, un objet communiquant et « l'analyse des espaces fait apparaître l'habitude japonaise de conduire l'individu à l'endroit précis où il sera en mesure de découvrir quelque chose par lui-même⁵⁷ ». Dans ce contexte, le mot « surveiller » n'a plus la même signification. Il est accompagné d'un grand dessein et d'un réflexe culturel. C'est un outil pédagogique, pour « conduire l'individu » en regardant ce que font ses semblables. La surveillance n'est pas en contradiction avec le mythe{ XE "mythe" }, la tradition et les acquis sociaux.

En Occident, la surveillance n'est pas aussi fortement liée à son contexte culturel. Les combats occidentaux sont frontaux et font appel à la puissance *directe* plutôt qu'au détournement de la puissance de l'adversaire. Que dire des arts martiaux qui apprennent à développer l'*acuité du combattant* pour qu'il puisse deviner l'attaque et l'utiliser aux dépens de l'offenseur ? Quand l'anticipation{ XE "anticipation" } et la flexibilité adaptative{ XE "flexibilité adaptative" } font partie des réflexes culturels, peut-on encore nier l'évidence ?

3.1.3 Ses dimensions économiques et technologiques

⁵⁵ Edward T. HALL, *La dimension cachée*, Editions du Seuil, Paris, 1971, pp. 183-189.

⁵⁶ Edward T. HALL, *Op. Cit.*

⁵⁷ Edward T. HALL, *Op. Cit.*

Le troisième aspect de la problématique de la surveillance est d'ordre économique et technologique. La surveillance doit en effet s'exercer sans menacer la *rentabilité* de l'organisation et même l'améliorer en augmentant sa *performance économique* ou en valorisant ses ressources technologiques.

Mais on ne peut parler de technologie sans en préciser la notion. On différenciera ainsi technique{ XE "technique" } de technologie. La technique est une activité qui consiste à créer des *objets techniques*, c'est-à-dire des *projections* du savoir scientifique sur la pratique, sans que cette pratique soit forcément effective.

L'objet technique{ XE "objet technique" } n'est pas forcément disponible pour une application économique, industrielle et/ou sociale. Il décrit l'exhaustivité des savoirs à mettre en œuvre pour réaliser une opération de production, mais diffère totalement des *technologies* qui seront effectivement mises en œuvre.

Les technologies sont des combinaisons de techniques. Elles résultent de leur étude. Elles nécessitent l'utilisation d'*information* complémentaire pour se réaliser. Les technologies ont pour finalité la production à laquelle elles participent. En d'autres termes, ce qui sépare l'objet technique du bien industriel, c'est la technologie.

Dans cet ouvrage, la surveillance sera abordée comme une *technologie du pouvoir*. Elle combine en effet plusieurs techniques permettant l'écoute, la vision, le contrôle et forme ainsi une technologie dont la finalité est bien de maintenir l'assujettissement. Pour développer une vision totale et permanente de l'aire à surveiller, un objet technique, une forme architecturale par exemple, peut être conçu. C'est l'*idée générique* de Bentham, son panoptique à l'état d'objet technique. La réalisation du panoptique va ensuite mettre en œuvre d'autres ressources génériques permettant d'autres activités renforçant la surveillance. Il s'agit des jalousies, objets techniques dont la construction permet de sélectionner l'information visuelle à son entrée et à sa sortie. Avec elle, un homme peut voir à l'*extérieur*, mais ne sera pas vu de l'*extérieur*. Il s'agit aussi de la cellule qui laisse passer la lumière (*input*) qui se projette sur le prisonnier et découpe sa silhouette (*output*) que distingue le surveillant. Il s'agit aussi d'un tube de fer blanc qui conduit parfaitement le son sur une distance suffisante, entre une cellule et une tour de surveillance par exemple. La *combinaison* de la technique de la jalousie, de la technique du tube transportant le son, de la cellule transformant la lumière en une *information binaire* (prisonnier présent, prisonnier absent) constitue le panoptique en tant que *technologie* de surveillance.

Le panoptique reste un *objet* technique tant qu'il reste une proposition écrite, tant qu'il n'est pas *effectivement* construit. Jeremy Bentham l'a compris. C'est pourquoi il choisit d'éditer son panoptique sous la forme de correspondances entre lui et un bâtisseur de prisons⁵⁸ : il veut en faire une *technologie* et pas seulement une invention séduisante.

⁵⁸ Jeremy BENTHAM, *Panopticon or the inspection house (...) and a series of letters written in the year 1787, from Crecheff in White Russia*, Réédition de Belfond, 1977, page 93.

Ainsi, le panoptique, en tant que technologie, aborde dans sa première parution, les *problèmes sociaux et organisationnels*. La technologie fournit des réponses à des problèmes vastes, tels que ceux de l'information, de la gestion, de l'organisation. Jeremy Bentham va plus loin, son panoptique est pour lui, ce que nous appellerons, une *technologie générique*, c'est-à-dire une technologie qui, par sa combinaison avec d'autres, permet de *générer* des technologies dont les portées sont encore plus vastes. En d'autres termes, le panoptique est une technologie du pouvoir, mais associée aux technologies de la production industrielle, elle deviendra un modèle d'industrie, une technologie qui *induit* les méthodes de gestion des hommes, des matières premières et des processus de production.

Ce que nous avons introduit comme le *néopanoptisme* est fondé sur une même technologie générique. C'est parce que les technologies de l'information, dont Bentham est un précurseur, ont atteint un seuil très élevé de *contenu technologique*, c'est-à-dire d'intensité en recherche et développement, qu'elles peuvent être le support d'un *système* de surveillance. Et ici, le terme surveillance n'a plus d'aspect restrictif. Il englobe tous les aspects de sa problématique. C'est une surveillance qui est comprise comme l'ensemble des activités mises en œuvre pour appréhender les dimensions historiques, juridiques, politiques, sociales, culturelles, économiques et technologiques des espaces de compétition de la firme.

Le *néopanoptisme*, enfin, suscite des nouvelles technologies *génériques* du pouvoir car il s'applique à plusieurs domaines d'activité, couvrant la recherche, le développement, la commercialisation et la communication de la firme, entre autres. Il *modifie* le système de compétitivité. La compétitivité dans la pratique néopanoptique n'est plus parcellisée. On ne peut plus l'appréhender séparément dans chaque domaine de compétition de la firme. Dans le nouveau *paradigme de l'information* que nous avons introduit plus haut, toutes les composantes du système d'information interne et externe de la firme sont liés.

3.2. Aspects théoriques de la firme surveillante

3.2.1. De la théorie de la firme à la théorie de l'information

Si la problématique de la surveillance revêt de multiples aspects, elle est toutefois sous-tendue par un même problème de fond. Surveiller, que ce soit dans un contexte culturel, politique ou économique, a toujours la même finalité : « *Savoir pour prévoir afin de pouvoir* ⁵⁹ ». Les termes « veille », « surveillance » et « intelligence » n'ont pourtant pas la même signification. La veille est une mission naturelle et passive de l'organisation. Les informations obtenues par la veille sont celles qui sont les plus accessibles. Ce sont des informations du

⁵⁹ Auguste COMTE (1798-1857).

domaine public. Il suffit à l'entreprise de mettre en place un scanning continu de l'environnement pour les obtenir. « veille » et « surveillance » sont des synonymes mais on considère, à juste titre, que la surveillance est coercitive. Elle manifeste la volonté de l'entreprise de connaître pour contrôler. Ses champs d'action sont donc plus spécifiques afin que le contrôle et l'intervention de l'entreprise soient rendus possibles. Quant à l'intelligence, elle n'est plus seulement un art d'observation mais une pratique offensive et défensive de l'information. Son objet est de relier entre eux plusieurs domaines pour servir les objectifs tactiques et stratégiques de l'entreprise. Elle est un outil de connexion entre l'action et le savoir de l'entreprise

Mais le savoir de l'entreprise, comme le souligne Donald Teece, est difficilement *transférable* en dehors de l'organisation. Ce savoir est non seulement *spécifique* à la firme, mais également à *chacun de ses salariés* et aux différentes *situations* dans lesquelles il a été acquis⁶⁰. En fait, le savoir et *notamment le savoir-faire*, sont avant tout le résultat d'un long et laborieux *apprentissage*. Toute entreprise doit sa connaissance à la « *routine* » qui lui permet d'acquérir son habileté et « *sa connaissance opérationnelle spécifique* ⁶¹ ».

	VEILLE	SURVEILLANCE	INTELLIGENCE
INFORMATIONS	publiques	privées	toutes sortes
MODE D'ACTION	scanning	benchmarking	interactif
DOMAINES	ouverts	spécifiques	reliés entre eux
CONNOTATION	passivité	coercition	connexité

Différences entre veille, surveillance et intelligence

Pour la surveillance, cela signifie que *l'acquisition d'un savoir-faire externe à la firme* ne pourra en aucun cas se réaliser *de visu*. Il faudra partager avec la firme qui détient le savoir-faire désiré *la situation dans laquelle elle l'acquiert*.

Nous prendrons en considération plusieurs façons *de partager une situation d'acquisition de savoir-faire* : le partenariat stratégique, la filiale commune{ XE "filiale commune" }, les acquisitions{ XE "acquisitions" } et les rachats de firmes

⁶⁰ Donald J. TEECE, « The Market for Know-how and the Efficient International Transfer of Technology », *Annals of The American Academic Journal of Political and Social Science*, November 1981.

⁶¹ Donald J. TEECE, « Towards an Economic Theory of the Multiproduct Firm », *Journal of Economic Behavior and Organization*, Vol. 3, 1982, p. 44.

concurrentes mais surtout, *le réseau d'expertise*. Ce que nous appelons *réseau d'expertise* est l'organisation industrielle qui relie par des liens d'expertise plusieurs firmes dans un réseau favorisant l'échange du *capital gris* { XE "*capital gris*" }. Des *liens d'expertise* sont des *points communs* dans l'orientation des programmes de recherche, ou dans la constitution des combinatoires de technologies génériques, qui ont amenés la firme à *formaliser ses relations avec ses partenaires* au travers de plusieurs contrats de recherche et développement. Le *capital gris* est constitué des savoir-faire organisationnels et intellectuels de la firme.

3.2.2. L'approche de la dynamique des structures

Pour aborder cette question des *structures du transfert d'informations* entre firmes, la *concurrence* sera vue comme une *rivalité d'entrepreneurs*, au sens de Schumpeter⁶², ou comme une *négociation d'acteurs*, au sens de Crozier et Friedberg⁶³. C'est-à-dire que nous partons de l'hypothèse que l'entreprise a de réelles possibilités *d'interaction* avec son environnement. Compétitivité et concurrence ne seront pas prises, dans cet ouvrage, dans leur acception néoclassique⁶⁴. La compétition sera ainsi considérée comme *un phénomène systémique*, c'est-à-dire comme le déroulement *dynamique* d'une confrontation entre plusieurs éléments *organisés en fonction d'un but commun*. Cette finalité commune du système pourra être de différentes natures selon que la compétition se déroule au niveau de la recherche, des combinatoires de technologies, ou du marché. A l'instar de Schumpeter, nous opposons l'analyse dynamique, *qui étudie l'évolution du système dans le temps sous l'influence de son environnement et des éléments qui le composent*, à l'analyse statique, qui établit « des relations entre les éléments du système économique (...) qui ont tous le même indice de temps, c'est-à-dire qui se réfère à la même date⁶⁵ ». Mais comme le précise François Perroux, « statique et dynamique s'impliquent à ce point pour former l'ensemble du système, qu'on ne peut les concevoir l'un sans l'autre⁶⁶ ». C'est dans cette optique que nous nous placerons.

Quant au « *centre moteur* » de cette dynamique, nous serions tentés, comme Schumpeter, d'y placer *l'entrepreneur* qui décide des combinaisons nouvelles des facteurs de production et contribue ainsi à l'évolution du système économique⁶⁷. Mais peut-on considérer cet entrepreneur hors du milieu dans lequel il évolue ? A

⁶² J.A. SCHUMPETER, *Capitalisme, Socialisme, et Démocratie*, Payot, Paris, 1972.

⁶³ M. CROZIER, E. FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977.

⁶⁴ La compétition ne porte plus sur le seul aspect des prix, mais sur des asymétries d'information, des différences de potentiel technologique qui sont tous des intangibles.

⁶⁵ J.A. SCHUMPETER, *Histoire de l'analyse économique*, Gallimard, Paris, 1983 (réédition de l'oeuvre originale de 1954).

⁶⁶ F. PERROUX, *La pensée économique de J.A. Schumpeter : les dynamiques du capitalisme*, Droz, Genève, 1965.

⁶⁷ J.A. SCHUMPETER, *History of economic analysis*, 1954.

quelle « *économie-monde* ⁶⁸ » appartient-il ? Son pouvoir de décision sur son environnement est peut-être fonction du « *schéma de domination* » auquel il appartient. En empruntant cet exemple à Braudel, l'entrepreneur vénitien qui, en 1580, décide d'investir dans l'huile de Pouilles n'a pas réellement fait preuve d'*initiative*. « Venise avait dans la région productrice plus de 500 marchands bergamasques, ses sujets, occupés à collecter, à stocker, à organiser les expéditions⁶⁹. Le milieu influence la décision qui a elle-même besoin de son appui — *c'est-à-dire d'une structure* — pour se réaliser. « La victoire caravanière de l'Islam à travers les déserts relève de l'exploit, un exploit lentement assuré par la *construction d'un réseau* d'oasis et de points d'eau ⁷⁰ ». Cette métaphore est très parlante. Le succès d'une telle entreprise — *l'aménagement d'un désert* — est dû à la combinaison de plusieurs facteurs critiques. Le premier d'entre eux a été la mise en place d'un réseau de communication adapté à l'environnement difficile dans lequel il allait être construit. Le second, c'est peut-être la foi dans un projet sans limites, puisque sa réalisation a nécessité des dizaines de générations. Et le troisième, c'est certainement la gestion de l'espace sans gaspillages des ressources et dans une finalité toujours poursuivie. A l'instar du « modèle » caravanier, l'intelligence d'entreprise nécessite la construction patiente d'un réseau de *sources* dont la sollicitation est mesurée, précisée, dans le cadre d'un réel aménagement des besoins de la firme et des possibilités de recueil d'informations dans l'environnement.

3.2.3. La firme comme réseau d'échanges stabilisés d'information

Plusieurs économistes comme Williamson⁷¹, Thorelli⁷², Johanson et Mattson ⁷³, voient d'ailleurs dans le « *réseau finalisé* » une nouvelle dynamique de l'industrie. Un réseau est un ensemble complexe de firmes liées entre elles par des *interrelations* de toutes natures : programmes communs de R&D, partenariats stratégiques, ou même, plus simplement, *des échanges stabilisés d'informations*. C'est pourtant à l'article de Coase ⁷⁴ que l'on doit l'idée de cette approche en réseau. Coase considère qu'une *transaction* demande beaucoup trop de temps à l'entrepreneur : localiser l'offre de service, négocier un prix, formuler un contrat, définir les obligations de chaque partie, s'assurer que les clauses du contrat sont

⁶⁸ F. BRAUDEL, *Civilisation matérielle, Economie et Capitalisme*, Paris, Colin, 1979.

⁶⁹ F. BRAUDEL, Op. Cit., p. 26.

⁷⁰ F. BRAUDEL, Op. Cit., p. 17.

⁷¹ O. WILLIAMSON, *Markets and Hierarchies: Analysis and Antitrust Implications*, New York, The Free Press, 1975.

⁷² H. THORELLI, « Networks : between markets and hierarchies », *Strategic Management Journal*, Vol. 7, 1986.

⁷³ J. JOHANSON, G. MATTSON, « Interorganizational relations in industrial systems : a network approach compared with the transaction approach », *International Journal of Management and Organization*, 1987.

⁷⁴ R.H. COASE, « The nature of the firm », *Economica*, Vol. 4, Londres, novembre 1937, pages 386-405.

respectées et finalement, réaliser *l'échange*. En *formalisant* l'ensemble de ses échanges dans un nombre de contrats *volontairement limité*, la firme pourrait considérablement réduire les coûts d'utilisation du marché. Sur ce constat, Williamson étudie la firme sous l'aspect *de ses coûts de transaction*. Il voit dans la *capacité limitée de l'individu à traiter l'information* un coût de transaction{ XE "coût de transaction" } supplémentaire⁷⁵. De là provient l'idée du *réseau* qui par la concertation d'individus aux *rationalités limitées*⁷⁶ permet d'obtenir une « quasi-rationalité{ XE "rationalité" } » collective et qui surtout, permet de *réduire le coût global de transaction* supporté par la firme.

Williamson distingue ainsi de multiples *figures relationnelles*, plus ou moins importantes et plus ou moins intégrées selon la complexité et la variété des arrangements contractuels mis en place⁷⁷. Cette complexité contractuelle peut d'ailleurs être rapprochée de *la radicalité*⁷⁸ *des informations transmises dans le cadre de ces réseaux*. C'est ce que suggère Donald J. Teece quand il démontre que plus l'acquéreur est *familier* avec la technologie, moins est important le coût du transfert de celle-ci⁷⁹. En d'autres termes, *l'asymétrie*{ XE "asymétrie" } *des niveaux d'information* des firmes constituant le réseau de transfert de connaissances va *structurer* le canevas contractuel de ce réseau. Plus l'information sera complexe et *étrangère* à la partie réceptrice, et plus le contrat sera précis et détaillé. La genèse de la « firme-réseau{ XE "firme-réseau" } » est donc inséparable de la nature des informations qui font l'objet des échanges avec ses partenaires. Et il faut finalement se résoudre à l'idée que, dans ces réseaux, le créateur d'une connaissance n'est pas forcément « la personne la mieux placée pour exploiter cette connaissance commercialement⁸⁰ ». La *découverte* et la *valorisation* d'une technologie font chacune l'objet de réseaux différents. Les théories de la firme et de l'information trouvent ici leur point de rencontre.

⁷⁵ O. WILLIAMSON, *Markets and Hierarchies: Analysis and Antitrust Implications*, New York, The Free Press, 1975.

⁷⁶ Concept proposé par J.G. March et H.A. Simon, *Organizations*, New York, Wiley, 1958.

⁷⁷ O. WILLIAMSON, Op. Cit.

⁷⁸ La radicalité est le caractère unilatéral de la nouveauté de ces informations.

⁷⁹ DONALD J. TEECE, « Technology Transfer by Multinational Firms : The Resource Cost of International Technology Transfer », *Economic Journal*, Juin 1977, pp. 242—261.

⁸⁰ Donald J. TEECE, « Innovations, Trade and Economic Welfare: contrast between petrochemicals and semiconductors », University of California, Berkeley, Colloque de la North American Economics and Finance Association, 1985, p. 3.

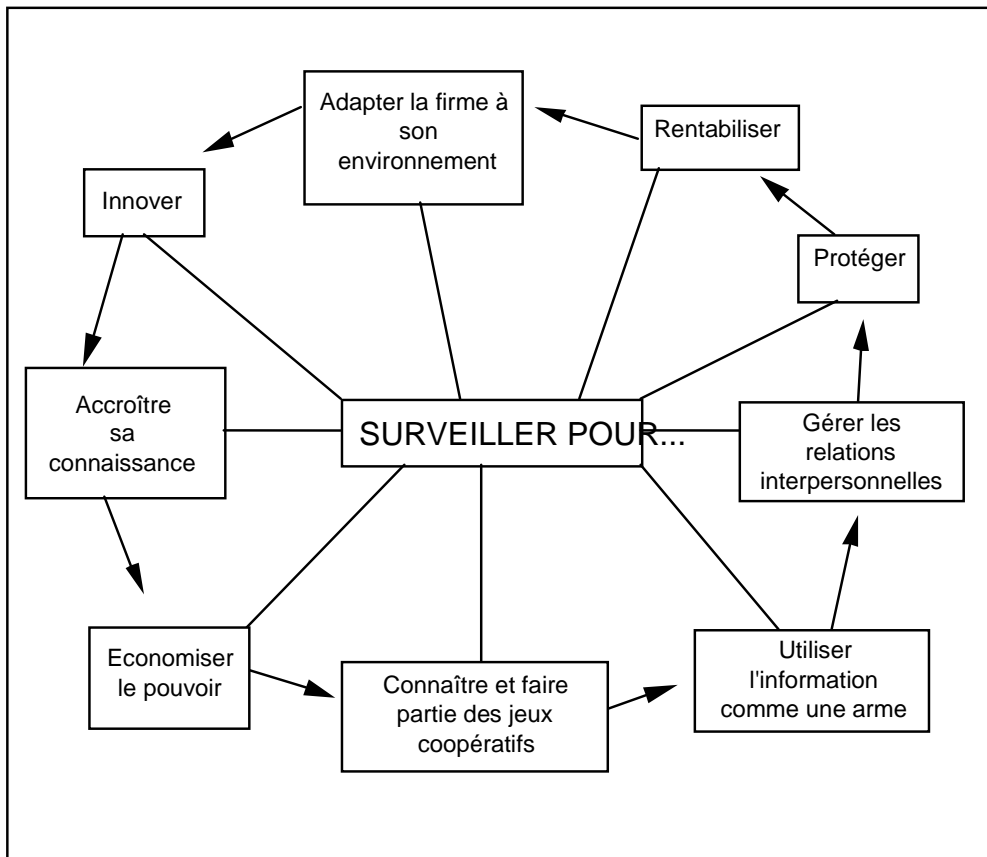
CHAPITRE IV

Surveillants et surveillés

4.1. Le concept de veille stratégique

4.1.1 Les différentes approches mondiales de la surveillance

Les études actuellement menées sur le sujet tendent à montrer que la notion de « veille stratégique » connaît des acceptions fort différentes selon les pays où elle est exercée. Certains observateurs européens ont d'abord vu dans la veille « un besoin de nouveauté méthodologique » qui ne modifiait pas fondamentalement les tenants et les aboutissants de la compétitivité, mais ils font exception et les experts, tout comme les praticiens, considèrent aujourd'hui qu'il s'agit « d'un problème de fond, devant mobiliser toute l'entreprise ». La surveillance est avant tout considérée comme un acte d'information permettant à l'entreprise de s'adapter à son environnement, d'une part pour innover et d'autre part, pour accroître sa connaissance de façon générale. Le lien entre accroissement de connaissance et économie « des forces » de l'entreprise est donc tacitement admis. Mieux connaître, c'est économiser son pouvoir. On vient donc à la surveillance par souci d'information, par déficit de connaissance... Et on en revient avec le désir de participer plus activement à l'environnement. Le besoin de savoir se transforme en besoin d'agir. Dès lors, l'information se présente à l'entreprise sous un autre jour : celui de la tactique{ XE "tactique" } et de l'offensive{ XE "offensive" }. La surveillance devient un outil pour gérer les manœuvres stratégiques{ XE "manœuvres stratégiques" } de l'entreprise. Elle est de plus en plus sollicitée pour gérer les relations quotidiennes de la firme avec les acteurs de l'environnement, pour obtenir et protéger des positions nouvelles ou encore pour rentabiliser des positions déjà acquises par une meilleure connaissance d'un secteur ou d'un segment de marché.



La « spirale » de la vigilance d'entreprise

Il existe donc une « spirale » de vigilances qui entraîne l'entreprise, itération après itération, vers une pratique systématique de la surveillance. Cette spirale d'implications pourrait s'écrire « s'adapter — connaître — utiliser — rentabiliser » pour montrer la progression de la nature de l'enjeu : du cognitif { XE "cognitif" } à l'économique. Dans ce contexte, les grandes entreprises surveillent beaucoup plus leur environnement que les petites et moyennes organisations. « Un effort important doit être réalisé auprès des PMI, dont 15% seulement déclarent avoir une stratégie clairement définie en matière de veille technologique », nous précise M. Bayen, du Centre de prospective et d'évaluation⁸¹. La possibilité d'*écouter son environnement* n'est pourtant pas réservée aux grands groupes. Il existe de nombreuses sources d'information ne nécessitant aucun investissement important : la banque, la presse spécialisée, la participation à des conférences organisées par la recherche, ou plus simplement, *tous les salariés de l'entreprise*. Il suffit parfois de questionner plusieurs fournisseurs pour débiter un *système d'information stratégique*. Même si, au début, il paraîtra modeste vis-à-vis des systèmes de surveillance de

⁸¹ Le Centre de prospective et d'évaluation du ministère de la recherche et de la technologie édite de nombreuses publications destinées à soutenir les firmes dans leur veille environnementale.

l'environnement de firmes comme DSM, Rhône-Poulenc ou Shell, l'état d'esprit sera le même. Car ce qui compte, « c'est avant tout une *prise de conscience collective* de ce que représente la nécessité d'être compétitif », nous confie un praticien.

C'est ce qui fait, pour beaucoup, la différence entre la surveillance japonaise{ XE "surveillance japonaise" } et la surveillance occidentale. Même si certaines entreprises européennes et américaines ont réussi à égaler la performance des systèmes d'information japonais, l'état d'esprit n'y est pas. « Chaque jour, 68 millions d'exemplaires de journaux sont mis en vente au Japon. A titre indicatif, le tirage de ces quotidiens est six fois plus élevé que celui des journaux français alors que la population n'est que deux fois supérieure à celle de la France ⁸² ». A la rigueur, le Japonais peut se défaire de son système d'information pour surveiller. Pour lui, la technologie qui transporte ses messages ne fait qu'accélérer le processus : elle n'est pas primordiale. A l'opposé, l'Occidental n'a pas le réflexe de diffusion de l'information au sein du groupe. Il réagira d'abord par rapport à son intérêt propre, à ce que cette information représente pour lui. Ensuite, il projette l'utilisation *qu'il en ferait* sur le groupe. Il faut, pour l'Occidental, que « la technologie *viennent chercher l'information* auprès des opérationnels », comme nous le confie un responsable du service du marketing stratégique d'une entreprise nationalisée. De son côté, un responsable de Digital Equipment explique : « Nous avons, chez Digital Equipment, *ressenti depuis longtemps le besoin de mettre en place un système intégré d'information* (notre premier système interne de messagerie électronique a démarré il y a quinze ans) et, aujourd'hui, ce réseau est constitué de près de 4 000 ordinateurs et de 50 000 postes de travail dans le monde, soit pratiquement un poste de travail par employé, si nous excluons les unités de production ⁸³ ». De même, il paraît nécessaire à la plupart des praticiens de recourir à la création d'une unité spécialisée dans l'écoute de l'environnement. Mais à l'instar de l'exemple japonais, « une poignée d'hommes ne sauraient avoir la même capacité d'écoute que plusieurs milliers; il y a *complémentarité* entre *l'expérience* de la cellule{ XE "cellule" } stratégique qui connaît bien les problèmes liés au traitement de l'information et l'ensemble du personnel qui est *le mieux placé pour la recueillir* », nous précise ce chef de service d'une grande société informatique française. Dans le contexte actuel d'une mondialisation{ XE "mondialisation" } des stratégies et des entreprises, la difficulté de maintenir leurs positions concurrentielles conduit donc les entreprises à « espionner » leurs concurrents, leurs clients, leurs fournisseurs, l'Etat et les entrants potentiels sur leur secteur. Il ne s'agit pas d'une simple veille technologique et concurrentielle — laquelle est désormais une pratique courante et maîtrisée de l'entreprise — mais d'actions d'intelligence contre ou avec la concurrence et l'ensemble des acteurs de l'environnement. Nous verrons dans ce qui va suivre que tous les pays ne

⁸² Jacques VILLAIN, *L'entreprise aux aguets*, Masson, 1989, p. 66.

⁸³ Cité par Humbert LESCA, *Système d'information pour le management stratégique de l'entreprise*, McGraw Hill, 1986, p. 111.

connaissent pas les mêmes succès dans la conduite de leurs opérations de surveillance. C'est aux conditions sociales, historiques et économiques qui ont produit ces différentes « manières de surveiller » que nous rattacherons ces échecs et ces succès.

L'approche soviétique{ XE "approche soviétique" } : « la résonance »

En URSS, les entreprises sont renseignées par l'Etat⁸⁴. Comme le souligne Hans Graf Huyn⁸⁵, le système d'information stratégique de l'URSS était d'ailleurs légitimé par l'existence de l'ennemi{ XE "existence de l'ennemi" } : les Etats-Unis. Comme il n'y a apparemment plus d'ennemi, tout porte à croire qu'il n'y a plus besoin d'espions ni pour l'Etat, ni pour les entreprises. Si, par contre, on envisage l'URSS comme une entité économique visant à défendre sa place au sein des économies mondiales, les « ennemis » sont alors nombreux et ils se nomment Japon{ XE "Japon" }, Allemagne{ XE "Allemagne" } et Etats-Unis{ XE "Etats-Unis" }, mais sur le plan économique cette fois-ci. Ce changement de mode de domination de l'équilibre précaire des nations — du dissuasif nucléaire au coercitif économique — a amené l'URSS à réviser sa structure de surveillance pour l'Etat et pour ses entreprises. Ainsi, pour attirer les capitaux devant redonner à l'URSS les moyens d'une compétitivité dans le jeu mondial des affrontement{ XE "affrontement" }s et des coopération{ XE "coopération" }s économiques, il fallait faire oublier l'image d'un système bureaucratique fondé sur une surveillance continue et systématique de ses membres. Ceci ne remet nullement en cause le KGB{ XE "KGB" } mais oblige une meilleure « communication » de sa part (jusqu'alors, il y avait très peu de communication de la part de cette organisation).

Contrairement à ce qu'une mauvaise interprétation des signaux{ XE "signaux" } émis par l'URSS peut laisser penser, le système d'information stratégique de l'Union Soviétique n'a jamais été aussi performant qu'à l'heure actuelle car l'URSS, comme le souligne Georgui Arbatov⁸⁶, « a fait à l'égard de l'Occident ce qu'il y a de pire : elle l'a privé d'un ennemi ». Le jeu de l'Union Soviétique est ici double. D'une part, elle gère le changement{ XE "changement" } de sa surveillance par un « dégel » unilatéral de ses lourdes structures, par une réorganisation de ses agents experts en « agents généralistes » et d'autre part, elle prépare le « re-gel » de sa nouvelle organisation surveillante dans une optique plus économique et communicative. Celle-ci sera fondée sur un principe de résonance tel qu'il a pu être observé lorsque des soldats traversent un pont et que le rythme cadencé de leur pas, vibrant en « résonance » avec le pont, conduit à la destruction de celui-ci. L'URSS{ XE "URSS" } s'apprête donc à communiquer à l'unisson avec l'occident, jusqu'à l'effondrement des derniers bastions de suspicion, le temps de former ses bureaucrates du renseignement au management de l'information concurrentielle...

⁸⁴ Voir à ce propos JACQUES VILLAIN, *L'entreprise aux aguets*, Masson, 1990.

⁸⁵ Hans Graf HUYN, « La stratégie de la désinformation », in *Géopolitique*, no 29, Printemps 1990.

⁸⁶ Georgui ARBATOV, cité par H.G. HUYN, *Op. Cit.*, p. 22.

Sans nul doute, l'exemple soviétique montre pertinemment, d'une part, l'évolution de la surveillance de la sphère politique et stratégique à la sphère économique et d'autre part, l'interdépendance grandissante entre nations et entreprises.

L'approche nord-américaine{ XE "*approche nord-américaine*" } : «*business intelligence*»

Les entreprises américaines pratiquent le monitoring{ XE "monitoring" }⁸⁷, c'est-à-dire une action continue de surveillance tous azimuts exercée par l'organisation sur son environnement en privilégiant avant tout des moyens d'investigation comme les bases de données{ XE "bases de données" } et l'enregistrement systématique des données recueillies sur des fichiers informatiques. Le terme provient bien entendu du mot anglais « monitor » qui suggère que les veilleurs passent beaucoup de temps derrière leurs écrans... Selon Leonard Fuld, les prérogatives d'un monitoring efficace sont les suivantes :

- connaître les sources{ XE "sources" } ouvertes et publiées de l'environnement,
- motiver les sources de sa propre organisation, c'est-à-dire le personnel,
- identifier et exploiter les acquis méconnus de l'entreprise en matière d'intelligence,
- établir une typologie de l'information{ XE "typologie de l'information" } désirée et se fixer un rythme d'acquisition,
- développer un réflexe de communication au sein du personnel,
- aménager des canaux de distribution sélective de l'information,
- développer des programmes d'entraînement et de formation au monitoring.

Le monitoring fait appel à des bases de données externes à l'entreprise telles que Dialog, Newsnet ou Nexis. Cette activité de « veille sur écran » est doublée d'une « veille sur papier » ou newsclipping{ XE "newsclipping" }. Cette dernière consiste à classer, synthétiser et indexer des coupures de presse dans des fichiers qui sont, selon le choix de l'entreprise, informatisés ou non. Les sources utilisées lors du newsclipping peuvent être :

- des fichiers{ XE "fichiers" } publics comme les « federal filings », les « Uniform Commercial Code filings » ou encore les « Securities and Exchange Commission annual 10-K reports » qui sont des rapports sur la santé financière et l'endettement des entreprises dans le domaine public aux Etats-Unis,
- des sources d'information privées comme le « Technology Executive Roundtable », lettre d'information publiée par Digital Equipment aux Etats-Unis.

Selon le Stanford Research Institute, le monitoring a pour objectif de « développer et de communiquer une compréhension profonde de la concurrence

⁸⁷ D'après Leonard M. FULD, *Monitoring the Competition*, John Wiley and sons, New-York, 1988

au sein de l'entreprise »⁸⁸ mais dans la plupart des cas, la mise en place d'un système de monitoring se heurte aux obstacles suivants :

- le personnel ne sait pas réellement l'information qui pourrait lui être utile,
- le personnel ne prend pas le temps de rassembler ou de partager l'information.

La mobilisation désirée de tout le personnel n'est donc pas obtenue. C'est pourquoi Leonard Fuld préconise l'identification de « champions » pour mobiliser l'état de veille au sein du personnel mais là encore les échecs sont nombreux. D'une part, la cellule de monitoring a tendance à s'isoler et à perdre du sens vis-à-vis de sa mission de départ, c'est-à-dire informer le plus grand nombre. D'autre part, le monitoring est une veille « tous azimuts » et donc, fréquemment, une veille qui s'égaré faute d'avoir concentré ses efforts sur des zones privilégiées d'observation. Les solutions retenues par les entreprises sont le plus souvent :

- de focaliser le monitoring sur un élément unique de l'environnement, et le plus souvent sur le consommateur (comme l'ont réalisé le groupe Mars, Owens-Corning Fiberglas et Johnson & Johnson),

— de faciliter la circulation de l'information{ XE "circulation de l'information" } au sein de l'entreprise par la création d'une ligne téléphonique permanente d'accueil d'informations, une hot-line{ XE "hot-line" }, ou par la création d'un réseau d'information permanent grâce au courrier électronique, ou encore par le recueil continu de rapports spéciaux sur la concurrence et la nomination d'intelligence représentatives, hommes de liaisons de la cellule de monitoring au sein de l'entreprise. Ce correspondant du monitoring est choisi pour ses qualités d'écoute, de persévérance, de souci du détail, de curiosité insatiable et de pensée claire.

Le cas MIRIS, « the Motorola Intelligence Research Information System », illustre bien les atouts et les limites d'un monitoring formel tel qu'il est pratiqué aux Etats-Unis. MIRIS est un système de monitoring tous azimuts créé par Motorola en 1983. Une équipe de cadres répondant aux profils des « intelligence reps » fut chargée, avec un budget annuel de 300.000 \$, de mettre en place le monitoring général de Motorola. En 1984, l'équipe fait l'acquisition d'un logiciel de gestion de bases de données textuelles. Trois ans plus tard, le système compte 55.000 enregistrements dont 20% seulement proviennent de sources internes. Dès la fin 1987, le problème d'un taux d'utilisation faible du système, en dehors des initiés, est posé. Dès lors, Motorola envisage d'étendre progressivement la diffusion de l'information à 5000 des terminaux informatiques prioritaires que compte le groupe.

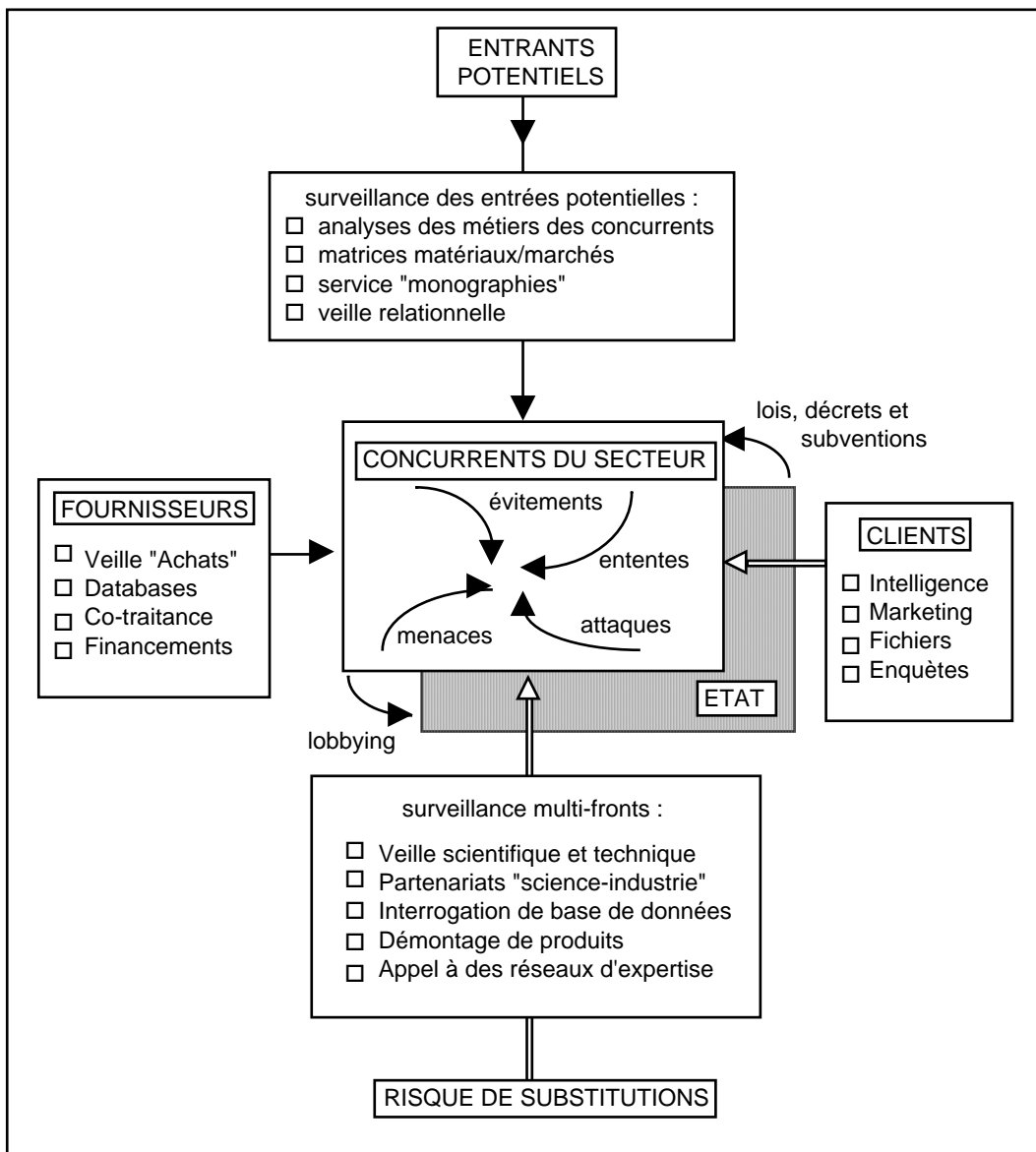
Cet exemple démontre, malgré les avantages d'un accès large et d'un stockage de données compréhensives par tous, puisqu'enregistrées en langage naturel, que le monitoring présente également les défauts d'être :

- coûteux et peu flexible,

⁸⁸ STANFORD RESEARCH INSTITUTE, « Managing competitive intelligence », Business Intelligence Program, Printemps 1985.

- difficile à contrôler au regard de la quantité d'informations traitées,
- difficile à mettre en œuvre car très ambitieux (« *large scale* »),
- plus apte à traiter quantitativement que qualitativement l'information.

Face aux difficultés rencontrées pour mettre en place des activités de monitoring rentables, de nombreux groupes américains se sont lancés avec succès dans le benchmarking. Copiant les organisations étatiques de renseignement, les agents réalisant le benchmarking concentrent leurs efforts sur un seul acteur selon une logique imitée de Michaël Porter dans « Competitive Strategy ».



D'après Michaël Porter, Competitive Strategy, 1980

Il existera donc des activités de benchmarking{ XE "benchmarking" } propres à chaque force du secteur : les fournisseurs, les clients, les substituts, les entrants potentiels et les concurrents (voir schéma ci-dessus).

Le système d'information stratégique des entreprises américaines présente donc l'avantage d'être homogène et orienté vers l'industrie et la compétition. On pourra cependant lui reprocher d'être justement trop préoccupé, à court terme, par les agissements de la concurrence pour pouvoir bâtir, à long terme, une approche globale et stratégique de l'environnement.

L'approche allemande{ XE "approche allemande" } : « le Blitzkrieg de l'information »

Comme le soulignait Henri Hauser⁸⁹ en 1917, le système de renseignement économique allemand est caractérisé par une forte concertation{ XE "concertation" } dans laquelle les banques ont joué et jouent encore aujourd'hui un rôle essentiel. Le modèle allemand d'information concurrentielle pour les entreprises est ainsi fondé sur les principes suivants :

- les banques sont parties prenantes dans les affaires de leurs clients,
- une émulation collective est toujours recherchée par la concertation,
- l'intérêt général allemand subordonne les intérêts particuliers,
- la prise d'information et la communication sont indissociées,
- une trace écrite et un comportement rigoureux dans le recueil de l'information.

L'approche allemande est donc fondée sur un réseau officiel toujours en éveil et au service des entreprises. A l'opposé du système soviétique, ce réseau n'est pas constitué de spécialistes du renseignement mais de spécialistes des affaires : sociétés de commerce, banques, antennes consulaires et forces de vente. Contrairement aux Etats-Unis, l'Allemagne ne recherche pas la démonstration de sa puissance. Elle est en cela restée dans une conception classique du renseignement qui s'inspire de l'utilitarisme anglais du XVIII^e siècle : *voir sans être vu*⁹⁰. Elle n'émet donc aucun signal signifiant son activité de surveillance à ses partenaires commerciaux. Elle est par contre extrêmement efficace.

L'approche française{ XE "approche française" } : « derrière l'Etat »⁹¹

Pour Christian Harbulot, le renseignement est une discipline de la guerre économique. Ce cadre conceptuel posé, l'auteur trace le portrait très contrasté du système d'information stratégique français.

⁸⁹ Henri HAUSER, *Les méthodes allemandes d'expansion économique*, Armand Colin, 1917.

⁹⁰ Voir à ce propos Jeremy BENTHAM, *The Panopticon*, Edition Dumont, Genève, 1791.

⁹¹ D'après Christian HARBULOT, *Techniques offensives et guerre économique*, étude Aditech et Centre de Prospective et d'Evaluation, n° 131, Aditech, Paris, février 1990.

Le système français d'information économique et stratégique n'a pas été conçu comme dans les économies nationales offensives (Japon, Etats-Unis et Allemagne). Il n'est pas fondé sur la recherche de rentabilité réelle des données fournies aux organisations et entreprises nationales.

Le réseau international de collecte d'informations de la France est institutionnel, fondé sur la présence diplomatique française à l'étranger (ambassades), les Postes d'Expansion Economique et les Chambres de Commerce bilatérales. Ce réseau, longtemps dominé par les notions de « service public » et de gratuité ne s'est pas développé dans un souci de rentabilité et d'utilisation tactique ou stratégique de l'information. Le système d'information stratégique français n'est donc pas compétitif avec ceux du Japon ou de l'Allemagne, par exemple. Harbulot propose donc de rationaliser la collecte nationale d'informations dans une perspective d'utilisations tactiques et stratégiques de celles-ci.

Il préconise, aussi bien pour l'Etat que pour tout autre type d'organisation, une *structure matricielle* de recueil et de traitement de l'information dans l'objectif :

— de résorber tout phénomène de rétention d'information{ XE "rétention d'information" },

— et d'augmenter la synergie entre les différents éléments des organisations concernées.

INTERETS MICROECONOMIQUES

	entreprises	particuliers	lobbies	régions	villes	ethnies
Etat	○	○		○		○
Gouvernement			○	○		
Industrie		○				
Assemblée			○			
Recherche	○					
Education	○					○
Culture				○		
Lobbies	○	○				

La matrice de concertation, d'après Harbulot, 1990

Pour Harbulot, le frein essentiel à la diffusion de l'information en France est l'opposition interne qui perdure entre l'Etat et les institutions, d'une part, et les entreprises et les individus, d'autre part. Ce cloisonnement{ XE "cloisonnement"

} français nous éloigne un peu plus d'une conception stratégique de l'information. Il s'exprime par :

— un clivage politique{ XE "clivage politique" } et un sectarisme social importants,

— des antagonismes culturels nombreux et l'absence de consensus national,
— le corporatisme{ XE "corporatisme" } et l'élitisme{ XE "élitisme" }.

En France, le droit d'accès à l'information est encore perçu comme un « privilège de caste ». Au sein des administrations, une information pour le plus grand nombre serait perçue comme une perte très certaine de pouvoir des corps dirigeants au profit des personnels dirigés, mais paradoxalement, donner de l'information ne rapporte rien. Les cloisonnements se nourrissent de ces processus d'exclusion.

Pour Harbulot, il s'agit donc de mettre en œuvre au plus vite une ingénierie macro-économique et micro-économique de l'information en France selon les phases suivantes :

— inciter tout type d'organisation à inclure la veille environnementale dans la formulation de sa stratégie,

— optimiser la rentabilité de l'information en réduisant les écarts de qualité qui séparent l'information publique de l'information privée ou secrète, en augmentant la qualité des informations ouvertes en France (presse, registres publiques, information des ministères...),

— rechercher une taille critique de l'industrie de l'information française permettant à tout un chacun d'obtenir au moindre coût un niveau d'information « honorable »,

— passer de l'information-connaissance à de l'information-action, c'est-à-dire faire de l'information utile et rentable : de l'intelligence.

L'approche japonaise{ XE "*approche japonaise*" } : « *symbiotique*{ XE "*symbiotique*" } »⁹²

« Les Japonais ont constitué le meilleur système d'informations stratégiques d'entreprises de la planète ». A la lecture d'un tel aphorisme, personne n'est étonné. C'est un fait admis. Et c'est d'ailleurs ce que recherchait le Japon. Reprenant à leur compte les théories de Michel Foucault⁹³ — la potentialité de l'inspection{ XE "potentialité de l'inspection" } évite son coûteux déploiement — , les Japonais n'ont cessé de répéter au monde leur goût pour la veille technologique et l'espionnage industriel. Très systématiques et s'affichant dans les salons et expositions avec appareils photographiques et caméras, ils effectuaient des démonstration{ XE "démonstration" }s de force, ce qui leur permettrait, plus

⁹² D'après la thèse de Doctorat en Sciences Economiques de Jacques GRIMALDI, « *Mitsui* », soutenue à Aix-En-Provence en Juin 1986.

⁹³ Michel FOUCAULT, *Surveiller et punir*, Gallimard, 1975.

tard, de masquer leurs faiblesses en réitérant de telles démonstrations mais cette fois-ci, montées de toutes pièces.

La force des Japonais est non seulement un maniement « stratégique » de la désinformation{ XE "désinformation" } mais également la disponibilité d'un réel potentiel de surveillance. Ainsi, le réseau Worldwide Information Network (WIN) de la sogo-shosha Mitsui est un des cinq premiers réseaux privés de communication du monde avec ceux de la CIA et d'Electronic Data Systems (racheté par General Motors...). C'est un réseau en fibres optiques, centralisé sur Tokyo. Il effectue le recueil de toutes les informations dont la Technological Development Division de Mitsui pourrait avoir besoin pour anticiper son renouvellement technologique.

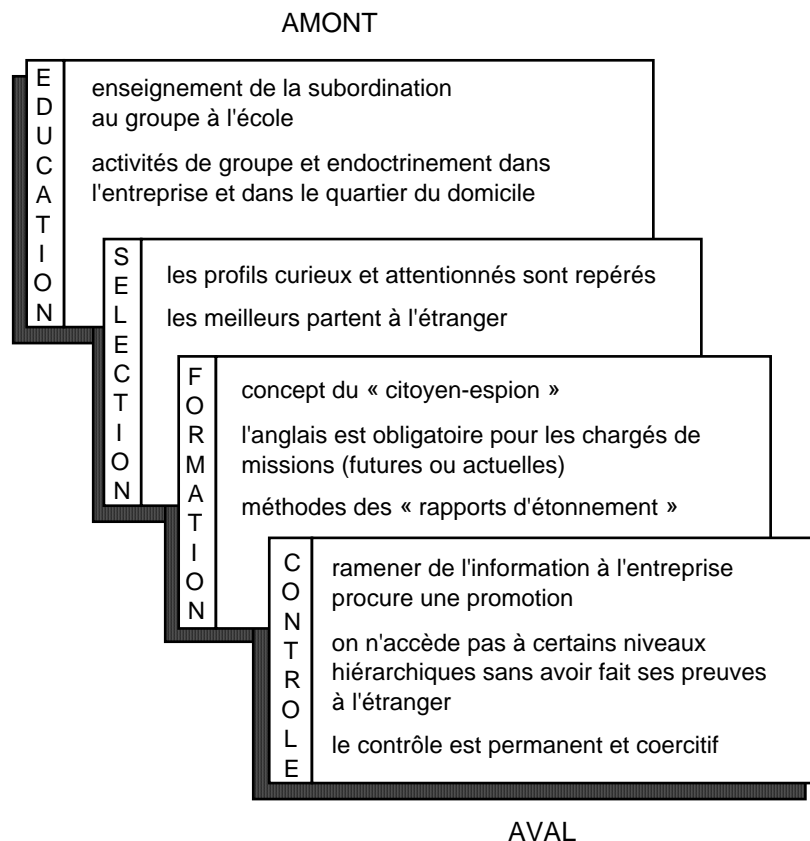
Il existe entre la surveillance et le Japon une histoire commune : un développement symbiotique. D'une part, le Japonais est plus curieux que l'Occidental — il lit en moyenne cinq fois plus de journaux qu'un Français — et d'autre part, le Japon doit beaucoup à la surveillance : elle est à l'origine de leur développement. Il existe donc un consensus national à ce propos qui se traduit pour chaque Japonais :

— par l'acceptation des conditions d'efficacité de leur système, c'est-à-dire la sélection, la formation, le contrôle et la manipulation des symboles ;

— par une subordination des intérêts personnels du Japonais aux intérêts de son groupe d'appartenance. Ainsi, les membres des zaibatsu, ces organisations qui contrôlent les sogo-shoshas, s'engagent-t-ils sur leur vie à défendre les intérêts du groupe ;

— par une subordination des intérêts des groupes (zaibatsu, sogo-shosha{ XE "sogo-shosha" } et entreprises) à l'intérêt du Japon car les Japonais fondent leur stratégie sur des horizons temporels beaucoup plus long que les occidentaux. Il n'est pas rare, dans leurs plans, de lire un historique du groupe de plus de deux cent ans pour justifier une stratégie dont l'échéancier peut avoir plus de cinquante années.

Le Japon développe donc, et entretient, une relation de symbiose avec la surveillance, de l'amont à l'aval de la société.



Cette relation symbiotique, fondée sur un système éducatif et sociétal dédié à la création d'une vigilance nationale, constitue un avantage concurrentiel certain pour la nation japonaise. A l'inverse du libéralisme{ XE "libéralisme" } qui n'a pas su intégrer la question nationale à la compétitivité des entreprises privées, le Japon a adopté une stratégie délibérée de concertation et de non-dissociation de l'intérêt général et des intérêts particuliers.

L'approche suédoise{ XE "approche suédoise" } : « l'intelligence périphérique »⁹⁴

⁹⁴ Entretien du 24 octobre 1990 du Dr Stevan DEDIJER, directeur de recherches sur l'intelligence d'entreprise à l'université de Lund en Suède. En 1934, DEDIJER étudie la physique théorique à Princeton. Journaliste scientifique de Newsweek, il rejoint le Parti Communiste et se porte volontaire pour combattre le fascisme lors de la Guerre d'Espagne. Devinant l'imminence de la Seconde Guerre mondiale, il se porte volontaire pour l'O.S.S. (American Office of Strategic Services). Il défend la Yougoslavie où il est né et le général Tito. Il est exclu de l'O.S.S. et s'engage dans le 101^e Airbone pour les opérations des troupes parachutistes en Hollande et dans les Ardennes françaises. Le général Eisenhower le transfère alors en Yougoslavie en Février 1945 pour aider Tito. Il est déçu par sa découverte de Belgrad et du communisme. En 1949, il participe activement à la guerre froide des deux blocs. En 1990, il est un défenseur de la démocratie et du « socialisme-capitalisme » selon ses propres termes.

L'approche suédoise de la surveillance d'entreprise est issue, d'une part, de sa position géopolitique{ XE "géopolitique" } à la périphérie des pays dominants de l'Europe, et d'autre part, d'une tradition et d'une culture suédoise développant un véritable « réflexe d'information » au sein de la population. La Suède est le seul pays européen à former ses étudiants à « l'intelligence » et non pas simplement à la « veille technologique » comme certaines initiatives françaises. La différence est essentielle. Tandis que la veille technologique est un outil, une technique, l'intelligence est *un système de jugement* favorisant, dans le cas de l'approche suédoise, l'appréhension globale des problèmes de compréhension des hommes, des entreprises et des nations.

Cette vision holiste de la surveillance est défendue par Stevan Dedijer qui conçoit l'intelligence comme :

- la cohabitation du secret et de la transparence,
- l'interdépendance du local et du global,
- l'avènement d'un monde de « souverainetés-dépendances »,
- le troisième élément d'une trilogie de la compétition et de la coopération.

Lors de l'un de ses derniers discours⁹⁵, Dedijer situait dans les années 1920 et dans les écrits de Teilhard de Chardin⁹⁶, Julian Huxley et Wells, l'émergence d'une *intelligence sociale et organisée*. C'est un peu le point fort et l'ambiguïté, recherchée, de cette approche suédoise : les frontières entre l'intelligence comme faculté de comprendre (intelligence de l'homme) et « l'intelligence » comme activité de surveillance de l'environnement sont délibérément imprécises et confondues dans une interrelation dynamique. Le message suédois semble vouloir donner une « conscience sociale » à la surveillance; celle-ci a pour objectif d'apporter des solutions à ce que Dedijer décrit comme les arbitrages décisifs de cette fin du XX^e siècle :

- la défaillance de la bureaucratie{ XE "bureaucratie" } comme système social,
- le développement de l'économie mondiale au détriment des écosystèmes,
- la montée de la violence{ XE "violence" } en temps de paix,
- le rééquilibrage des échanges socio-économiques Nord-Sud,
- le manque de capacité à résoudre des problèmes globaux,
- le manque de perception des limites humaines.

Repoussant l'idée que les sciences sociales puissent apporter des réponses à ces questions clés de notre développement, Dedijer encourage toute organisation humaine à pratiquer « l'intelligence » pour recueillir l'information et les connaissances qui pourront l'aider à trouver des solutions concertées et globales à ces questions préoccupantes. Il en appelle à une *révolution de l'intelligence* qui

⁹⁵ Quarantième lecture de « l'Alumni War Memorial Foundation » à la Milton Academy, le 30 avril 1990 (le troisième lecteur, en 1926, fut Franklin Delano Roosevelt et le dix-huitième, le général George Marshall).

⁹⁶ TEILHARD DE CHARDIN, *Le phénomène humain*, 1955.

permettrait à l'homme de résoudre l'ensemble de ses problèmes sans recourir à l'affrontement ou à la guerre.

L'impasse occidentale en matière d'information stratégique

Il y a en occident une absence chronique de concertation nationale en matière de défense de la nation. D'une part, l'information stratégique ne circule pas entre les concepteurs des politiques économiques et les acteurs de terrain. D'autre part, l'horizon temporel des stratégies est trop court. Le secret{ XE "secret" } est ainsi très mal « géré » dans les cultures occidentales, de façon trop peu nuancée et sans règles communément admises.

La culture américaine confie à des « champions », ou à des « professionnels », le recueil de l'information stratégique. La France tend à développer des réflexes plus institutionnels, préférant l'emploi des structures d'Etat du renseignement plutôt que de créer des structures privées. Les Anglo-saxons, bénéficiant de leur passé d'empire « où le soleil ne se couche jamais » exploite leur habileté britannique et la rigueur de la culture Wasp⁹⁷ pour institutionnaliser de véritables réseaux de correspondants du royaume. Les pays de la périphérie européenne, comme l'Italie, la Suède ou l'Espagne, contraints de compenser des positions concurrentielles défavorables par une meilleure information, ont fondé sur leur tradition commerciale et l'ouverture de leur pays une sorte de « dynamique entrepreneuriale du renseignement ». Autant d'approches qui par leurs différences soulèvent une nouvelle fois, notamment en Europe, la question clé de la concertation entre nations et entreprises.

Alors quel avenir pour la surveillance ? Les réponses sont aussi diverses que les questions sur la définition du terme lui-même. Ce n'est pas un hasard si l'avenir de la veille et sa définition suscitent les mêmes difficultés de réponse aux praticiens : car c'est dans la formulation de la veille qu'est inscrit son avenir. Pour la majorité des experts de la question, la perspective européenne de libre circulation des biens et des personnes annonce une formidable dynamique de l'information et de nouvelles formes de veille. Et quel que soit le niveau d'équipement des firmes en nouvelles technologies de l'information. Seulement un paradoxe ?

4.1.2 Discussion du concept sur réseau : la liste Apogées

Les débats ayant eu lieu dans le cadre du groupe de discussions Apogées sont archivés dans différents fichiers au siège du European Academic Research Network pour la France, à Montpellier. Ces fichiers sont désignés dans ce qui suit par la mention « Archives Apogées ».

Le thème « strategic information and management » s'est révélé très porteur puisqu'en moins d'un mois la liste comptait cent abonnés, dont la majorité

⁹⁷ White Anglo-Saxo Protestant.

provenait des Etats-Unis ⁹⁸. On peut expliquer cela de diverses manières. L'adjectif « stratégique » a la même aura aux Etats-Unis qu'en Europe : il attise la curiosité et l'imagination collective lui attribue un caractère important, secret et réservé. Il faut aussi s'attarder sur la population totale des utilisateurs du réseau BITNET (ou EARN qui n'est qu'une émanation de BITNET en Europe). Ce réseau relie des universités et des centres de recherche publiques et privés. Les utilisateurs sont donc des universitaires dans la plupart des cas. Aux Etats-Unis, beaucoup d'étudiants ont également accès au réseau (alors qu'en Europe, l'informatique{ XE "informatique" } interuniversitaire est plus réservée aux corps professoral et administratif). Dans le cas particulier du groupe de discussion Apogées, la liste était majoritairement composée d'enseignants et de chercheurs.

L'utilisation de l'information est un problème mobilisateur aux Etats-Unis. Le grand nombre de bases de données, privées, industrielles et publiques a développé une réelle économie de l'information avec ses producteurs, ses commerçants et ses utilisateurs. La taille croissante des bases de données américaines inquiète. Les problèmes de confidentialité et de sécurité sont des thèmes très porteurs aux Etats-Unis (deux des forums de discussion les plus importants sur le réseau sont Security Digest et Virus List). De plus, le « networking{ XE "networking" } », c'est-à-dire le travail quotidien sur réseau, est très répandu. Face aux grandes distances, les relations inter-universitaires sur réseau se sont largement développées. Certaines entreprises, comme Digital Equipment Corporation, en ont fait leur philosophie. « Le Networking est la base de la philosophie de D.E.C. Nous favorisons l'initiative des ingénieurs grâce au réseau de communication et à nos satellites. Chez nous, chacun peut se connecter avec n'importe lequel de ses collaborateurs dans le monde pour faire progresser la compagnie », confie David Romano, responsable des Spécificités chez Digital.

Cet engouement des Etats-Unis pour les technologies de l'information est assez bien résumé par un des participants d'Apogées :

« In the context of this global proliferation of information technology, it is important to systematically understand and document the problems, opportunities and management issues. Furthermore, the events unfolding themselves in the international arena — 1: the tidal wave of freedom and democratic reforms sweeping eastern European countries, 2: unprecedented unification of west european countries in 1992, 3: constantly decreasing US dominance in the world markets not only in the industrial sector but also in the service sector, 4: US losing competition not only to Japan, but also to countries like South Korea, Taiïwan, Hong Kong and Singapore — warrant a serious reassessment of how American business use information technology to compete globally ⁹⁹ ».

⁹⁸ Cf liste des participants en encadré.

⁹⁹ Shailendra PALVIA, University of Babson, USA, Archives Apogées, 6 Mars 1990.

LES FACTEURS CONTRIBUANT AU REGAIN DE L'INFORMATION	
1	La vague de réformes démocratiques a l'est
2	L'unification européenne en 1992
3	Le déclin de l'industrie nord-américaine
4	La montée des dragons du sud-est asiatique

Selon S. Palvia, U of Babson

L'Amérique voit donc dans les technologies de l'information le facteur critique de succès de la décennie. Ainsi, l'utilisation des réseaux informatiques de grandes tailles (WAN : Wide Area Networks) est-il un des domaines de recherche les plus explorés du moment. Edward Schmitt, Villanova University, écrit à ce propos :

« Networking in general implies a system of interconnected sources capable of exchanging information and sharing resources. A network consists of information sources such as people, computers, facsimile machines, instruments..., linked by communication media capable of allowing voice, visual or data transmission. (...) To date no specific research has been published on the marketing profession's use of Wide Area Networks. Hiltz (1985), Hiltz and Turoff (1978), and Muffo and Snizek (1987) along with other communication researchers have done research concerning the impact of computer mediated communications on researchers and academics in general ¹⁰⁰ ».

En d'autres termes, le réseau est étudié dans son application quotidienne, celle qui fournit aux chercheurs des possibilités d'expérimenter leurs concepts : la recherche et l'université. Mais le réseau informatique comme moyen d'approcher de nouveaux marchés, comme facteur de compétitivité, n'a pas fait l'objet de recherches approfondies, même si son utilisation est un fait quotidien pour des firmes multinationales comme Digital Equipment, ou IBM. De telles recherches permettaient-elles d'améliorer l'utilisation des réseaux pour le développement économique ?

Dans cette perspective, une véritable économie de l'information est en train de naître aux Etats-Unis. John Muffo, membre du Virginia Polytechnic Institute et auteur de plusieurs ouvrages sur le sujet, écrit à ce propos :

« People in our field do management information work colleges, universities, polytechnics, and other institutions of higher education, as well as governmental and private group that work with such organizations in some capacity. Our primary job is identifying and reporting the key information that is required for the efficient and effective operation of our organizations. This can include information on the exterior environments in which we exist; scientific and political trends are examples of these. Of course internal operational information is critically important as well. An additional interest of some of the people in our field is the issue of technology transfer and the larger question of the proper relationship between higher education

¹⁰⁰ Edward SCHMITT, Villanova University, USA, Archives Apogées, 22 Novembre 1989.

institutions and the national and international economic entities that support them, both governmental and private ¹⁰¹ ».

L'intérêt d'un groupe de discussions comme Apogées est de rendre possible et immédiate la contradiction. C'est un moyen très efficace de progresser dans la réflexion puisqu'il permet, avec chaque intervenant, de découvrir de nouveaux éclairages des problèmes et de leur résolution. Ainsi l'un d'entre eux va-t-il répondre à un autre correspondant, au sujet du rationalisme technologique :

« I couldn't agree more. I know this phenomenon as « technological rationalism ». If we break the word technology into its root components, we find « ology », or the study or science of, combined with « techni » or technique : a focus on the 'means' to ends. Too often we focus on this without due consideration of the 'ends' (organizational mission, goals, objectives, values, etc) to which these means are applied. Moreover, it is often the 'criteria' for effectiveness that is in conflict between management and users ¹⁰² ».

La nécessité de lier « moyens mis en œuvre » et « finalité de l'organisation », s'accompagne, pour ce participant d'une acception dynamique de la gestion de l'information :

« In short, I am interested in the 'movement' of information to whom and where it's needed at the right times. (...) So, for me, strategic information management must include strategic management of the potential users, as well as the implementation processes which introduce the technologies to the organization ¹⁰³ ».

Lier le concept de « gestion stratégique de l'information » au concept même du management global de la firme a souvent été avancé par les participants. Jim Goes, Montana State University, écrit à la liste, le 21 Février 1990 :

« Let me propose a working definition for strategic uses of information, subject to revision at any time. I would suggest that strategic uses of information take place anytime in organization gathers/utilizes information to modify its overall mission or direction, or to compete in a fundamentally different way ¹⁰⁴ ».

Jim Goes accompagne sa définition de l'exemple suivant :

« An example from my own research in acute care hospitals in the state of California. For years many of these hospitals were sitting on an untapped gold mine of information regarding their patients. Particularly hospitals administrated by the Kaiser Foundation had a wealth of data about patients : what medical services they purchased, insurance, mortality statistics, income levels, etc.. This data could all be cross-referenced by city of residence, ethnic background, and other demographic measures ¹⁰⁵ ».

Deux points essentiels apparaissent ici. Tout d'abord, le problème éthique{ XE "éthique" } n'est pas soulevé. L'exploitation de données concernant des malades ne dérange apparemment pas. Ensuite, l'utilisation de méthodologies statistiques

¹⁰¹ John A. MUFFO, Virginia Polytechnic Institute, USA, Archives Apogées, 28 Novembre 1989.

¹⁰² Steve LEVITT, University of Kentucky, répondait à Joe Moore, University of South-Dakota, USA, Archives Apogées, 14 Février 1990.

¹⁰³ Steve LEVITT, Op. Cit., Archives Apogées, 7 Février 1990.

¹⁰⁴ Jim GOES, Montana State University, USA, Archives Apogées, 21 Février 1990.

¹⁰⁵ Jim GOES, Op. Cit., Archives Apogées, 21 Février 1990.

est tout de suite invoqué (tris croisés) avec des données ethniques. Jim Goes poursuit :

« Only recent have the hospitals begun to exploit this data. A cost constraints have increasingly lowered hospitals' margins, they have had good reason to seek out affluent markets, identify neighborhoods or socio-economic classes towards which to tailor their services ¹⁰⁶ ».

La valorisation de l'information stockée par l'hôpital au sujet de ses malades s'accompagne d'objectifs commerciaux. L'information est ici source de diversification. La question de la gestion de l'information stratégique est détaillée en trois phases par Charles J. Wertz, Buffalo State College :

« One : I would be very interested to hear some definitions of strategic information. My dictionnary suggests that it must be information that is used for planning. I have also heard suggestions that it is information of value to an enterprise or information that can be use to gain some advantage. Two : given a good concept of strategic information, I wonder how one might recognize instances, obtain some of it, and manage it. Three : how can we make useful information out of volumes of data ? Is it possible ? ¹⁰⁷ ».

DEFINITION DE L'INFORMATION STRATEGIQUE	
1	Elle est utilisée pour la planification
2	Elle confère à l'entreprise un avantage concurrentiel
3	Elle permet à l'entreprise de modifier sa mission
4	Son aspect stratégique réside dans l'utilisation qu'on en fait

D'après C.J. Wertz et J. Goes

Un bon concept, une méthodologie pour reconnaître l'information stratégique, l'analyser et la rendre exploitable. Tout est dit. Charles J. Wertz accompagne son intervention de l'exemple suivant :

« Here in the US, our President has just presented a proposed budget to Congress. I think I read that it runs 1500 pages. How could anyone possibly evaluate this document and make constructive criticisms ? ¹⁰⁸ ».

Cette *approche en différentes étapes* est commune à de nombreux participants. Le recueil, le traitement et la valorisation des résultats d'analyse sont les trois étapes citées le plus fréquemment. Harper G. Grimm, West Virginia Network for Educational Telecomputing, écrit :

« I am concerned about creating a 'West Virginia Data Base' containing information about West Virginia (as well as tools for accessing, manipulating, and presenting

¹⁰⁶ Jim GOES, *Op. Cit.*, Archives Apogées, 21 Février 1990.

¹⁰⁷ Charles J. WERTZ, Buffalo State College, USA, Archives Apogées, 31 Janvier 1990.

¹⁰⁸ Charles J. WERTZ, *Op. Cit.*, Archives Apogées, 31 Janvier 1990.

that data). It seems to me that much of the data which might be included would be of 'strategic' importance ¹⁰⁹ ».

Dans la suite de son message, Harper G. Grimm soulève quatre problèmes :

« (1) What data might be appropriate; (2) what tools might be appropriate; (3) how that data should be structured; and (4) what problems (technical, political, etc) might be encountered and how these problems might be dealt with ? ¹¹⁰ ».

Comme le souligne M. Grimm, la question des données précède celle des outils. Il ne s'agit pas de multiplier les méthodologies de traitement de l'information sous prétexte de sa quantité croissante. Connaître les données appropriées au problème à résoudre est la première étape. Elle permet d'économiser des coûts importants de traitement et initie une réflexion utile à la suite de l'analyse (conséquences politiques, techniques...).

Les Etats-Unis expérimentent actuellement et payent la « datamania » des années quatre-vingt. Les *capacités* des mémoires des ordinateurs ont connu ces dix dernières années une croissance exceptionnelle, parallèlement à une *baisse des coûts* de production des semi-conducteurs. Une compétition pour la *miniaturisation* des systèmes de stockage de l'information est initiée par la création du micro-ordinateur. La conjonction de ces trois phénomènes (baisse des coûts, croissance des capacités de stockage, miniaturisation) a permis, à *chaque individu*, de posséder les technologies de l'information nécessaires au stockage et au traitement de données de plus en plus nombreuses (paradigme de l'individualisation). Les bases de données publiques et privées se sont multipliées, si bien que furent stockées, systématiquement, toutes sortes de données (la manie de la donnée, ou *datamania*). Barry Newton, du National Institute of Standards and Technology, nous confirme ce phénomène de société :

« Concepts of data administration and data resource management are being taken seriously in the United States; one of these concepts is the idea that data (perhaps any data) generated within an organization has some value as a resource ¹¹¹ ».

L'idée qu'une donnée (*peut-être n'importe laquelle*) générée par un organisation a de la valeur comme une ressource. Entre ces deux parenthèses, on découvre l'entière explication de la prolifération des bases de données aux Etats-Unis : *le doute*.

« *Quelle donnée sera exploitable ?* » : les experts doutent et préfèrent multiplier les données que devoir subir, bien plus tard, la critique : « Comment avez-vous pu décider de ne pas prendre en compte ceci ou cela ? ». Pourtant, l'utilité des bases de données n'est plus à prouver. Barry Newton continue :

« The obvious example for commercial enterprises is the customer list. The use and abuse of mailing lists, theft of them, rental of them, etc..., are familiar themes to

¹⁰⁹ Harper G. GRIMM, West Virginia Network for Educational Telecomputing, USA, Archives Apogées, 12 Février 1990.

¹¹⁰ Harper G. GRIMM, *Op. Cit.*, Archives Apogées, 12 Février 1990.

¹¹¹ Barry NEWTON, du National Institute of Standards and Technology, USA, Archives Apogées, 31 Janvier 1990.

most people who use in any capacity. The company which retains data about every sale to every customer, however, has a resource of some considerable value. Sales personnel, for example, will not waste their time offering customers items which have recently been ordered. The pattern of one customer's purchases, however, may suggest additional items which may be of interest. The statistical patterns of all purchases over one-three years may affect decisions about plant or warehouse capacities, identify items which are becoming uneconomical, or provide the first evidence of competition ¹¹² ».

La veille commerciale, relayée par un réseau de nouvelles technologies de l'information, procure un gain de temps pour la force commerciale, mais aussi, pour la production et la recherche pour lesquels elle préfigure des axes de développement. Ce que M. Newton précise :

« The American garment industry is increasingly relying on early sales figures (often direct from intelligent cash registers) to provide a competitive edge in the production of lines of clothing. This early data prevents the production of items which are not selling, allowing resources to be devoted to those which are. The combination is difficult for overseas competitors with shipping delays to counter ¹¹³ ».

Cette précision contient deux éléments intéressants. Les technologies de l'information sont fortement *diffusées* (comme les « caisses enregistreuses intelligentes ») et leur mission de recueil d'information n'est *pas explicite* (nul n'est censé savoir qu'une caisse enregistreuse comptabilise, analyse et synthétise les achats des clients). Le recueil immédiat de l'information (*early data*) permet au fabricant, non seulement de *voir sans être vu*, mais aussi de *voir avant ses concurrents*. Grâce à l'utilisation avancée des technologies de l'information, les producteurs créent ainsi une barrière à l'entrée de concurrents étrangers (dont les délais de livraison reculent d'autant leur possibilité de réagir). Barry Newton parle « *d'utilisation stratégique de l'information* », notion qui sous-entend que le caractère stratégique d'une information réside dans l'utilisation qu'on en fait.

4.1.3. La notion de « réseau de surveillance »

La notion de surveillance est toujours associée à celle du *réseau d'informateurs*, car pour augmenter les possibilités de recueil de l'information, on augmente d'abord le nombre de personnes impliquées dans ce recueil. On ne peut ainsi cerner le concept de « veille stratégique » sans aborder la question des réseaux.

En comparant l'exemple français à l'exemple américain ¹¹⁴, on s'aperçoit vite que la problématique de la surveillance réside plus dans le *facteur humain* que dans la technologie. En France, l'utilisation des bases de données se développe très rapidement, mais le niveau d'équipement des firmes et des universités en nouvelles technologies de l'information reste inférieur au niveau américain. La France, bien que détenant 10% du stock mondial des données informatisées, ne

¹¹² Barry NEWTON, *Op. Cit.*, Archives Apogées, 30 Janvier 1990.

¹¹³ Barry NEWTON, *Op. Cit.*, Archives Apogées, 30 Janvier 1990.

¹¹⁴ Contenu des entretiens et résultats du groupe de discussion Apogées.

représente que 1% du temps total consacré à la consultation de bases de données dans le monde ¹¹⁵. La technologie aux Etats-Unis n'a pourtant pas résolu le problème : *elle l'a déplacé*. Le fait que l'économie américaine soit dotée de puissantes ressources en technologies de l'information n'a pas empêché *sa perte de compétitivité* et son recul face aux économies asiatiques.

	ORGANISATION D'UN RESEAU DE SURVEILLANCE	
	ROLES	
	DE LA TECHNOLOGIE	DE L'HOMME
RECUEIL	augmenter les quantités	sélectionner les domaines d'intérêts
TRANSPORT	accélérer le retour	préserver l'information (contrôle)
STOCKAGE	augmenter les capacités	structurer l'information stockée
TRAITEMENT	calculer et trier	faire preuve de discernement
DIFFUSION	atteindre toutes les cibles	faire preuve d'une stratégie

La technologie améliore le transport — *plus rapide* — et le stockage — *plus important* — de l'information, mais sa contribution au *traitement des données* est seulement technique (calcul, modélisation, tri...). L'analyse et la valorisation de ses résultats reste une opération *humaine*. Le système expert{ XE "système expert" } lui-même, s'il sait appliquer des règles, ne peut les créer *ex nihilo*, ou les induire d'une impression globale sur les faits. En d'autres termes, *l'aptitude à discerner l'information critique pour le succès de l'organisation reste le véritable facteur de succès d'une opération de surveillance*. Mais pour effectuer ce discernement, il faut pouvoir *séparer* les faits de leur contexte, les considérer sous différents éclairages, et ensuite, se *concerter* pour décider sur des *bases élargies d'information*. Cet effort de réflexion nécessite *un groupe* qui puisse aller à chaque source d'information rechercher une justification nouvelle, un élément novateur pour l'analyse. Ce groupe d'informateurs, qui assure la liaison entre les *émetteurs* d'information (firmes, Etat{ XE "Etat" }, presse, manifestations culturelles, ...) et les *récepteurs* devant l'analyser, constitue le *médium* de la surveillance, c'est-à-dire *son réseau*.

Il subsiste, cependant, même au sein d'un réseau, *un risque de déformation* de l'information. C'est pour y faire face que la surveillance japonaise exige de ses agents la transmission *en l'état* des informations recueillies : « votre mission est de prendre intact tout ce qui se trouve sous le ciel ». Ayant intégré le fait que si le facteur humain conditionne le succès de la surveillance, il peut aussi en

¹¹⁵ Philippe LEMOINE, « Savoir s'informer », Télécoms Magazine, n° 32, Mars 1990, p. 83.

conditionner l'échec, l'industrie japonaise conçoit le réseau d'informateurs dans son *acceptation technologique*. S'il n'existe pas de technologies susceptibles de remplacer l'être humain dans le recueil de l'information sur l'ensemble de la surface planétaire, alors ce recueil sera réalisé par l'homme. On s'étonnera dans le monde occidental de cette pratique de la surveillance qui oblige les japonais à gérer de complexes réseaux d'informateurs dont la seule mission est de rapporter tel quel au Japon chaque information recueillie (le Worldwide Information Network de Mitsui est un réseau centralisé aussi important par sa taille et ses effectifs que celui de la C.I.A.). On retrouve d'ailleurs dans les écrits du stratège chinois Sun Tzu cette conception de l'espionnage : « Celui qui sait tout *par avance* ne l'a pas obtenu des esprits, ni par comparaison avec d'autres faits, ni en faisant des calculs, il doit l'obtenir des *hommes* qui connaissent la situation réelle de l'ennemi ¹¹⁶ ». L'information, *en l'état*, est le bien sacré. Le stratège réfute l'oracle, la spéculation sur les faits et l'extrapolation. Seule l'information recueillie à sa source a de la valeur pour les plans de la guerre.

Chaque firme japonaise a ainsi ses codes formalisés de conduite. Comme l'armée chinoise, cinq siècles avant Jésus Christ, honorait les Treize Articles de Sun Tzu, le personnel de la *sogo-shosha* Mitsui honore ceux de Shotoku Taishi. Ces derniers préconisent « la consultation des autres (...) (car) quand les grandes choses sont en jeu, le danger de l'erreur est lui-même grand. L'affaire doit par conséquent être discutée et mise au point à plusieurs, afin de trouver la bonne solution ¹¹⁷ ». Mais cette *concertation* dans la décision ne peut se réaliser sans *conditions préalables* et c'est seulement « quand le sens de l'harmonie existe au-dessus, et la franchise au-dessous, et quand des deux côtés on emploie les mêmes mots, qu'alors la raison qui est inhérente aux choses, décide ¹¹⁸ ». La sagesse du Prince (*l'harmonie*), qui n'abuse pas de son privilège et la discipline{ XE "discipline" } du sujet (*la franchise*) conditionnent, avec l'utilisation d'un *même langage*, le succès de la prise de décision (*la raison*). Soumission à l'autorité, logique groupale et communication sont bien les trois piliers de la surveillance japonaise.

De l'exemple asiatique, on retiendra l'essentiel : la performance d'un réseau d'informateurs est subordonnée à *la discipline* que l'on y maintient. Sun Tzu, dans son article sur l'utilisation des espions, conseille la règle suivante : « Si un secret n'a pas été divulgué, mais qu'on en entende parler, l'espion qui le connaissait et ceux qui l'avaient informé doivent mourir ¹¹⁹ ». Au regard du stratège, la divulgation d'un message entraîne la destruction de son *émetteur* (les informateurs), et de son *médium* (l'espion, qui est le moyen de transport du

¹¹⁶ SUN TZU, *L'art de la Guerre*, Article XIII, « De l'utilisation des espions », traduction de Niquet-Cabestan, Economica, 1988, p. 93.

¹¹⁷ Dix-septième article de SHOTOKU TAISHI, document Mitsui, in J. GRIMALDI, thèse de Doctorat en Sciences Economiques, Aix-En-Provence, 1986

¹¹⁸ SHOTOKU TAISHI, *Op. Cit*, Article Premier.

¹¹⁹ SUN TZU, *L'art de la Guerre*, Article XIII, « De l'utilisation des espions », traduction de Niquet-Cabestan, Economica, 1988, p. 93.

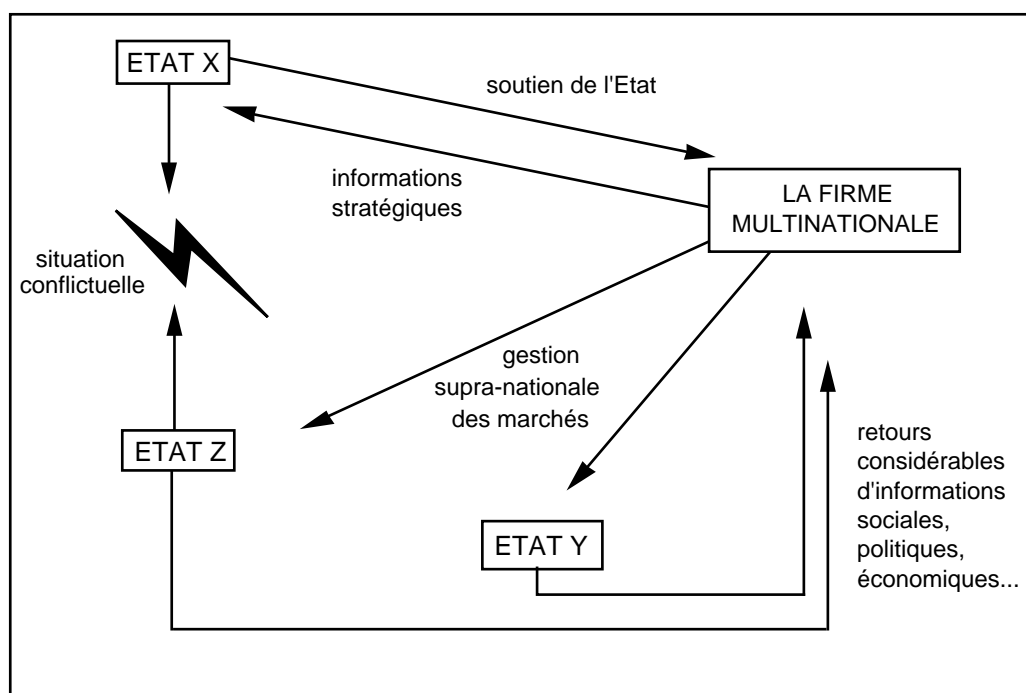
message) afin de sauvegarder son *récepteur* (l'autorité). Ici, le médium est solidaire de chacun de ses messages, jusqu'à sa mort, car pour Sun Tzu, les espions « dont personne ne connaît les agissements, constituent ce que l'on appelle l'*écheveau* des esprits ; c'est le trésor du peuple et du prince ¹²⁰ ». La notion d'*écheveau*, ensemble serré d'éléments liés entre eux de façon complexe, annonce celle de *système* de surveillance : l'information transportée, les hommes qui la transportent, leur méthode, les *inputs* et *outputs* de leur mission sont en complète interdépendance. Que l'on modifie un des éléments de cette « boîte noire » et l'ensemble du système sera modifié : l'objectif initial ne sera pas accompli, mais *approché*. Chaque élément étant régi par le temps, certaines informations seront devenues *obsolètes*, et le système modifié ne pourra plus accomplir sa mission telle qu'elle avait été définie au départ. Ainsi faudra-t-il que la vigilance émane du système lui-même, que chacun s'attache à remplir son rôle, sans retarder la systémique mise en place pour réaliser l'objectif commun. Le facteur *discipline*, dans le système de surveillance organisé en réseau, est la clé de son succès.

4.2. La nécessité disciplinaire

4.2.1 Les problèmes de la circulation de l'information

L'expérience du contrôle de gestion a montré que la maîtrise des flux d'information au sein de la firme passe par une formalisation d'un *système d'information*, par son suivi et sa *surveillance*. Ainsi, le contrôleur de gestion doit *forcer* les opérationnels pour qu'ils consignent sur leurs tableaux de bord la synthèse de leur activité professionnelle.

¹²⁰ SUN TZU, *Op. Cit.*, p. 93.



Pour permettre à l'information de circuler, il faut que chacun remplisse son rôle de *récepteur* et d'*émetteur*. L'étude des flux d'information, *formel* { XE "formel" } s et *informel* { XE "informel" } s, dessine ainsi le canevas des relations de pouvoir dans l'entreprise. Des flux d'information mal maîtrisés constituent donc des facteurs de risque importants pour toute organisation. Lorsqu'une firme multinationale détient plus d'informations qu'un Etat, *ses capacités de prévision* des conjonctures futures, ou d'*évaluation des risques du pays*, dépassent souvent les aptitudes mêmes du pays concerné.

Lorsque de surcroît, cette firme multinationale étend ses réseaux de communication sur l'entière surface de la planète, les Etats ont peut-être des raisons de s'inquiéter pour leur *souveraineté nationale* { XE "souveraineté nationale" }. D'un autre côté, « peut-être la principale incidence des *techniques télématiques* sur la souveraineté nationale a-t-elle été de *transformer ce concept* qui était exprimé en *termes géographiques* pour passer à la notion de *souveraineté en matière d'information*. A mesure que son rôle se développe dans le domaine de la gestion, l'information est de plus en plus considérée comme une *ressource* dont l'Etat doit être maître. La circulation transfrontière de données est cependant pour les Etats un problème difficile à cerner ¹²¹ ».

Les *propriétaires des réseaux de distribution* menacent-ils les pouvoirs en place ? Ou les servent-ils en leur permettant une meilleure connaissance de leur environnement ? Le développement de la télématique est ainsi soumis à « la tension créée par les intérêts *contradictoires* de l'Etat qui, d'une part, cherche à protéger, à conserver et à contrôler l'information et, de l'autre, à importer,

¹²¹ H. MOWLANA, « La circulation internationale de l'information : analyse et bilan », Unesco, 1985, p. 54.

exporter et échanger des idées, à la fois pour poursuivre ses propres buts et pour étayer ses politiques nationales ¹²² ». L'information se révèle donc une matière première bien contradictoire : à la fois *nécessaire* et *dangereuse* pour le maintien de l'autorité. La maîtrise et surtout *l'identification* des flux d'information devient donc prioritaire pour l'Etat comme pour la firme.

Mais un flux d'information n'est pas aussi facilement *identifiable* que dans son acception théorique. Tout d'abord, l'information revêt des formes multiples, plus ou moins formalisées : la gestuelle, les codes culturels font partie du langage au même titre que les mots ¹²³. De plus, à la différence du flux physique{ XE "flux physique" } de marchandise, le flux d'information{ XE "flux d'information" } n'est pas immédiatement *perceptible*. La duplication d'une information, suivie de son déplacement par différents canaux, n'a nullement supprimé l'existence de l'information originale. La copie parfaite existe, et l'on peut multiplier les *doubles*, en créant chaque fois un original. Or devant la multiplication de possibles en tout point identiques, l'esprit s'égaré, la confusion s'installe ¹²⁴. Cette multiplication des doubles, et leur *déformation* incontrôlée, crée ce que l'on peut appeler *des sphères informatives* qui ne doivent leur existence qu'au double phénomène de la propagation et de la déformation de l'information. Une *sphère informative*{ XE "sphère informative" }, c'est-à-dire l'ensemble des informations nées de la duplication et de la déformation d'un groupe d'informations originales, peut elle-même devenir le *cadre de référence* d'un groupe et servir de base de développement de nouvelles sphères, plus limitées, plus éphémères, jusqu'à leur disparition. C'est devenu un *phénomène de rumeur*.

Quand on parle de circulation de l'information, il ne faut donc pas négliger *les transformations du message* dont s'accompagne sa diffusion{ XE "diffusion" }. Les rumeur{ XE "rumeur" }s sont ainsi « mises en circulation parce qu'elles ont la double fonction d'expliquer et de soulager les tensions émotionnelles éprouvées par l'individu ¹²⁵ ». La rumeur qui libère l'individu de toutes formes de pression, « fournit à celui qui la communique une explication à son *anxiété* ¹²⁶ ». Quand on a conscience du phénomène de rumeur, envisager de maîtriser *l'entière* circulation de l'information au sein d'une organisation tient de l'utopie. « A mesure que la rumeur circule, elle tend à devenir plus courte, plus concise, plus facile à comprendre et à raconter. Les versions successives contiennent de moins en moins de mots et de détails ¹²⁷ ». « La mémoire sociale{ XE "mémoire sociale" }

¹²² A. GOTLIEB, C. DALFEN, K. KATZ, « The transborder transfer of information by communications and computer systems : issues and approaches to guiding principles », *American Journal of International Law*, n° 68, 1974, p. 227

¹²³ Voir à ce propos E.T. HALL, *Le langage silencieux*, Editions du Seuil, 1984.

¹²⁴ Voir à ce propos Clément ROSSET, *Le réel et son double, traité de l'Idiotie*, Editions de Minuit, Paris, 1974, « La confusion des chemins », p. 14.

¹²⁵ G.W. ALLPORT, L.J. POSTMAN, *The Psychology of Rumor*, Holt & Co Publishers, New York, 1947, traduction française, pp. 170-185.

¹²⁶ ALLPORT et POSTMAN, *Op. Cit*, mêmes pages.

¹²⁷ ALLPORT et POSTMAN, *Op. Cit*, mêmes pages.

accomplit en quelques minutes une *réduction* { XE "réduction " } équivalente à celle accomplie par la mémoire individuelle { XE "mémoire individuelle" } en quelques semaines ». Une seconde tendance, appelée *accentuation* { XE "accentuation" } se définit « comme la perception, la rétention et la reproduction *sélective* d'un nombre *limité* de détails provenant d'un contexte plus large ». Cette accentuation revêt plusieurs aspects. Elle peut être « *numérique*, les détails accentués étant multipliés dans le récit ». Elle peut être « *temporelle*, (ce) qui consiste à placer le déroulement des événements dans le moment présent » ou même *symbolique* { XE "symbolique" }. Dans tous les cas, les accentuations que subit le message « illustrent la recherche d'une *signification*, nécessaire au sujet se trouvant dans une situation *non structurée* ». Enfin, il y a le phénomène d'*assimilation* { XE "assimilation" } « qui résulte de la force d'attraction exercée sur une rumeur { XE "rumeur" }, par les habitudes, les intérêts et les sentiments de ceux à qui elle s'adresse ». Ce dernier phénomène, par une ultime déformation de la perception et de la mémoire, permet à l'individu de transmettre la rumeur dans une configuration mentale qui lui est plus *cohérente*. Besoin de facilité de transmission et de mémorisation (*réduction*), besoin de signification et de symbolisme (*accentuation*) et besoin de cohérence entre le message et l'individu qui le transporte (*assimilation*), la circulation de l'information est loin d'être un phénomène neutre. L'exemple de la rumeur nous apporte un enseignement pour la surveillance : *la circulation de l'information contient, dans sa nature, une part irréductible d'incertitude*.

4.2.2. Les approches managériale et cybernétique de la surveillance

Lorsque l'on surveille l'environnement, il y a plusieurs façons de se comporter face à l'*incertitude*. On peut ne pas vouloir perturber *la régulation* { XE "régulation" } *du système de surveillance*, c'est-à-dire en aucun cas interpréter de façon fautive ce que l'on peut percevoir selon nos propres critères d'analyse. On va donc *inhiber* notre possibilité d'interpréter l'information, et *transmettre* ce que l'on a acquis à une personne mieux placée pour en comprendre les tenants et les aboutissants. Dans cette première approche, l'informateur se considère comme *l'élément d'un système* qui doit *se réguler* dans l'objectif de *ne pas transformer* l'information lors de sa transmission. Elle constitue *l'approche cybernétique* { XE "approche cybernétique" } *de la surveillance*¹²⁸.

On peut également, face à l'*incertitude*, considérer qu'il ne faut *pas attendre* pour mettre en œuvre toutes nos compétences pour *la réduire*. L'informateur, dans cette seconde approche, s'implique dans *l'interprétation de cette incertitude* : d'où vient-elle ? A quelles *autres sources* puis-je me référer pour mieux en cerner les causes et les conséquences ? La transmission de l'information s'accompagne ici d'une *sélection* — *d'une première analyse* — réalisée par l'informateur lui-même.

¹²⁸ *Cybernétique* : ensemble des théories de l'information relatives aux *communications* et à la *régulation* dans des systèmes (vivants ou non) dont l'activité est orientée vers la réalisation d'une fonction. Cf N. WIENER, *Cybernetics or Control and Communication*, New York, Wiley, 1948, et également W.R. ASHBY, *Introduction to Cybernetics*, Londres, Chaman & Hall, 1956.

Le management de l'information s'effectue dès son recueil. Il s'agit de *l'approche managériale*{ XE "approche managériale" } de la surveillance. Quelle est la meilleure approche ? Et dans quels contextes ?

Il faut se pencher sur la cas de l'informateur{ XE "informateur" } venant d'acquérir une information qu'il considère importante pour la firme. Plusieurs *freins psychologiques* peuvent le dissuader de transmettre cette information à ceux qui en ont besoin. Il peut avoir peur de s'être trompé sur l'importance réelle de cette information. Il *anticipera* une mauvaise réaction de ses supérieurs, ou simplement, il préférera éviter le *discrédit*, aussi minime soit-il. Sa crédibilité{ XE "crédibilité" } est en jeu, et, après-tout, il n'est qu'un *opérationnel*. Il sait bien que ce n'est pas son rôle de s'occuper des orientations stratégiques de la firme, ou de s'inquiéter pour *un signal de l'environnement contraire aux projets corporatifs à long terme*. Et au fur et à mesure que l'on descend dans les échelons hiérarchiques, le *niveau d'information sur l'avenir de la firme diminue*. C'est cette *asymétrie d'information* qui fait la différence entre lui et le dirigeant. Il en est conscient et n'a pas l'intention de bousculer l'ordre des choses.

Ce n'est pas son rôle de prévoir et de toute façon, « ces possibilités de prévision qui constituent un élément si important de la lutte pour le pouvoir (...) dépendent dans une large mesure de la *façon dont les informations sont distribuées* ». Et lors de cette distribution, certains, plus que d'autres, « *disposent d'informations* donc de possibilités de prédiction{ XE "prédiction" } et donc finalement de possibilités de contrôle et de pouvoir, *simplement du fait de leur place dans la pyramide hiérarchique* ¹²⁹ ». Si bien qu'il sait, qu'en diffusant l'information au niveau hiérarchique supérieur, il en renforce le pouvoir, car *au-dessus* est la maîtrise des technologies de prévision ¹³⁰.

Dans la logique de ce petit scénario, la firme perd beaucoup d'informations importantes pour son développement stratégique. Le niveau d'équipement en technologies de l'information n'y pourra rien changer. Ce n'est pas *les possibilités* de transmettre l'information qui manquent, mais *la volonté* de le faire. Deux approches différentes naissent de ce constat : les approches *cybernétique* et *managériale* de la circulation de l'information. Dans l'approche cybernétique, l'informateur est considéré comme une *technologie de recueil et de transport de l'information*, au même titre qu'une fibre optique ou qu'une liaison satellite, associée à une mémoire vive (que l'on peut effacer et réutiliser). En assignant l'informateur à une mission de recueil et de transport, les freins psychologiques disparaissent. Il ne sait pas à qui va servir cette information, ni dans quel objectif elle sera utilisée. Son contrat est de rapporter l'information, sans qu'il soit nécessaire de l'assimiler ou de porter un jugement sur elle. Cela évite notamment tous les problèmes de *distorsion de l'information* que nous avons évoqués au sujet de la rumeur. Cette forme de surveillance est fortement parcellisée dans une sorte de schéma Taylorisé où chacun doit s'en tenir à sa tâche, sans forcément percevoir

¹²⁹ Michel CROZIER, *Le phénomène bureaucratique*, Editions du Seuil, 1963, p. 201.

¹³⁰ *Technologies de prévision* : statistique, analyse financière, systèmes de gestion de bases de données, et méthodologies de planification.

la machine particulière qu'il est en train de construire. L'informateur remplit son *rapport d'étonnement*{ XE "*rapport d'étonnement*" }¹³¹ sans se soucier de la hiérarchie, ou de sa position dans la pyramide sociale. Pour motiver sa mission de *relais neutre*, on va bien sûr user de pressions psychologiques, mais aucune ne se rapportera à l'information. On mettra à profit un fort sentiment nationaliste, initiant parfois des fanatismes, ou simplement l'indivision entre l'avenir de l'individu et l'avenir de la firme (*modèle japonais*).

Dans ce premier schéma, il va sans dire que l'on doit maintenir l'informateur dans un *état agentique*{ XE "*état agentique*" }, « ce par quoi on désigne la condition de l'individu qui se considère comme l'agent exécutif d'une volonté étrangère, par opposition à l'*état autonome* dans lequel il estime être l'auteur de ses actes¹³² ». Cela nécessite avant tout une sélection de l'informateur dont les traits de personnalité doivent limiter naturellement le désir d'initiative personnelle. Ce travail est facilité au Japon, où la structure groupale de la société amène dès leur enfance les sujets dans un schéma de ce type. Il est évident qu'une personnalité de leader demande des *coûts* supplémentaires pour être mise en état agentique. L'approche cybernétique de la surveillance, par son mode *rationnel* de mise en place, s'adapte à des objectifs *économiques* ambitieux, et peut bénéficier du gain lié à l'expérience et aux économies d'échelle. La mise en état agentique demande un fort investissement au départ car elle doit réformer partiellement les systèmes éducatifs, familiaux et salariaux de l'individu, mais la possibilité de répéter *indéfiniment* le même schéma est rapidement une source d'économie importante. Une politique prudente en matière de salaires (*afin de ne pas encourager l'appât personnel du gain*), une contrainte groupale constante (*afin d'éviter à l'individu la possibilité de rentrer dans un schéma personnel*) et une modification profonde (*dès l'enfance*) de sa structure mentale{ XE "*structure mentale*" } contribuent à améliorer la mise en état agentique. Le Japon bénéficie d'un contexte historique favorisant la mise en place d'un tel schéma.

¹³¹ *Rapport d'étonnement* : rapport dans lequel l'informateur mentionne tout ce qui l'a étonné au cours d'un voyage ou d'une mission, même et surtout, ce qui n'est pas en relation directe avec le motif de sa visite ou sa profession.

¹³² Stanley MILGRAM, *Soumission à l'autorité*, Calman-Lévy, 1982, p. 167.

	DEUX APPROCHES DE LA SURVEILLANCE	
	MANAGERIALE	CYBERNETIQUE
RECUEIL DE L'INFORMATION	opportuniste	systématique
TYPE D'INFORMATEUR	décideur infiltré	agents interchangeables
PSYCHOLOGIE	personnelle	de groupe
CULTURES	occidentales	orientales
POINTS FORTS	autonomie et réactivité	fiabilité et ampleur
POINTS FAIBLES	risque de subversion	manque de souplesse

Tout d'abord, comme nous le précise l'auteur, « une organisation sociale stable augmente la capacité du *groupe* à dominer son environnement et diminue son agressivité interne en réglant les relations entre ses membres ». Mais « l'instauration de *l'organisation sociale* suppose nécessairement une potentialité d'obéissance chez ceux qui veulent en bénéficier¹³³ ». Sur ce point, les deux approches se rejoignent. Que l'informateur soit un *relais neutre* ou un *relais actif et participatif* de l'information, il a conscience qu'il doit son pouvoir de domination sur l'environnement à l'appartenance à un groupe. De même, ils savent parfaitement, l'un et l'autre, que les *contrats* qui lient les différents membres du groupe entre eux sont nécessaires à la réduction des tensions internes à l'organisation. Ce en quoi la théorie de l'agence est intéressante : elle peut aussi bien illustrer, *sous des formes contractuelles différentes*, l'approche cybernétique que l'approche managériale de la surveillance. La nécessité de l'obéissance{ XE "obéissance" } est de même très bien acceptée par l'un et par l'autre. Ce n'est pas dans l'acceptation, mais bien dans le partage de l'autorité que réside la différence des deux approches. Le fait que l'autorité soit acceptée constitue en effet la condition nécessaire commune aux deux approches, mais elle n'est pas suffisante. Dans l'étude cybernétique de l'autorité, Stanley Milgram précise que « le contrôle exercé par les mécanismes *inhibiteurs* indispensables au fonctionnement autonome de l'élément individuel doit nécessairement être supplanté par le contrôle de l'agent *coordonnateur*¹³⁴ ». En d'autres termes, si l'inhibition{ XE "inhibition" } individuelle préserve la survie de l'individu, elle s'exerce instinctivement, sans tenir compte des effets négatifs qu'elle peut induire sur le groupe. L'obéissance à un *coordonnateur* permet de préserver le groupe *en même temps* que l'individu, si bien que « les hiérarchies ne peuvent fonctionner que si

¹³³ Stanley MILGRAM, Op. Cit., p. 157.

¹³⁴ Stanley MILGRAM, Op. Cit., p. 162.

une modification interne est apportée aux éléments qui la composent ¹³⁵ ». Pour pouvoir agir à l'encontre de ses inhibiteurs, l'individu doit se modifier, instinctivement, pour se préserver. « A partir de ce stade, son comportement et son équilibre interne subissent des altérations si profondes que l'attitude nouvelle qui en résulte met l'individu dans un état différent de celui qui précédait son intégration dans la hiérarchie ¹³⁶ ».

On peut mettre en évidence cet état agentique dans la pratique de la surveillance japonaise en Europe. Le systématisme de leur questionnement, qui ne s'embarrasse d'aucun détour, a effectivement montré que le Japonais en mission tient absolument à remplir son rôle tel qu'il lui a été défini : le recueil *en l'état* de l'information. Il veut préserver l'intégralité du contenu des réponses. Il ne veut pas introduire, par une éventuelle implication de sa part, un biais dans l'analyse qui sera faite des informations qu'il a recueillies. Aucune initiative ne sera prise de sa part.

La présence du coordonnateur est aussi confirmée. Il s'agit d'un responsable hiérarchique qui vient contrôler, dans les jours suivants, sous prétexte d'une visite de courtoisie, l'effective réalisation de la mission des informateurs. Son intervention est d'abord agentique : avec systématisme, il vérifie un à un les points de passage et les articulations de la mission japonaise. Ensuite, il reprend une certaine autonomie relative pour éventuellement négocier une seconde visite, ou une transaction d'informations¹³⁷.

La même analyse, menée dans le cadre de la théorie de l'agence, va nous permettre d'identifier les *pôles contractuels* ¹³⁸ de la firme et d'en comprendre les multiples transformations. Essayons de décrire, sous cet angle, chacune des approches managériale et cybernétique de la surveillance. Chaque réseau pourra être assimilé *au contrat* que ses membres sont susceptibles de défendre ensemble. Ce « contrat » pourra aussi bien être *formel qu'informel*. Ses objectifs pourront être d'ordres économiques, politiques, sociaux, ou même culturels. Une distinction essentielle pourra cependant être faite entre les deux réseaux. La structure agentique du premier réduira considérablement le nombre de nœuds contractuels. Le réseau managérial, *a contrario*, offre la possibilité d'affecter un *ou plusieurs* contrats, d'ordres différents, à chaque membre du réseau. On pourra ainsi organiser le déploiement d'un réseau managérial de *lobbying* { XE "lobbying" } ¹³⁹ selon la nature des pressions à mettre en œuvre, en différenciant les contrats selon la personnalité de chaque acteur. *En d'autres termes, c'est dans*

¹³⁵ Stanley MILGRAM, Op. Cit., p. 165.

¹³⁶ Stanley MILGRAM, Op. Cit., p. 167.

¹³⁷ Ces faits ont été observés par un cadre supérieur d'une industrie nationale très convoitée par la surveillance japonaise.

¹³⁸ Groupes d'acteurs liés par des mêmes contrats, et constituant ainsi des *sous-systèmes* du pouvoir par leur capacité de structurer leur négociation dans le cadre d'une seule démarche de groupe.

¹³⁹ Groupes de pression représentant la firme auprès des différents acteurs de son environnement.

la possibilité de multiplier et d'adapter les contrats des acteurs du réseau managérial que réside l'intérêt d'une telle structure. Alors quels types de réseaux selon quels types de mission ? Leurs finalités et leurs performances sont-elles comparables, voire complémentaires ?

4.2.3. La voie du management participatif

Il paraît évident qu'un réseau agentique{ XE "réseau agentique" } est moins ouvert au *management participatif* qu'un réseau managérial{ XE "réseau managérial" } de surveillance. Le *processus d'adaptation* des modalités de la surveillance à son contexte requiert en effet une certaine *autonomie décisionnelle* au niveau de chaque informateur. Quand l'individu entre dans un réseau agentique, « il ne s'estime plus responsable. Il voit en lui un simple instrument destiné à exécuter les volontés d'autrui ¹⁴⁰ ». Comment, dans un tel contexte, pourrait-on espérer d'un réseau agentique *la participation* de l'informateur dans le management de la surveillance ? Nous allons montrer qu'un certain nombre de « *réactions réflexes* » peuvent être enseignées à l'informateur du réseau agentique lors de la phase de préparation de la surveillance. Comme Milgram, nous devons pour ce faire « examiner les forces qui ont agi sur l'individu avant qu'il devienne notre sujet, ces forces qui ont modelé son orientation fondamentale vis-à-vis de la société et préparé le terrain de l'obéissance ¹⁴¹ ». Le passage à l'état agentique requiert certaines *prédispositions* dont on peut retrouver les racines dans l'enfance et la formation de la personnalité. Le progrès, plus ou moins rapide, de la personnalité de l'individu au sein de sa famille et de son cadre social et culturel conditionne de même sa *prédisposition agentique*{ XE "prédisposition agentique" }. C'est ainsi que nous pouvons mettre en relief dans les conditions préalables de l'état agentique, et dans ses facteurs de maintenance, les contraintes qui limitent les possibilités d'un réseau d'informateurs pris dans son acception cybernétique (de relais neutre). « Le sujet a grandi au milieu de structures d'autorité. Depuis son plus jeune âge, il a été soumis à la discipline imposée par ses parents, ce qui lui a inculqué un sentiment de respect envers l'autorité des adultes ¹⁴² ». « Dès que l'enfant émerge du cocon familial, il est transféré dans un *système d'autorité institutionnel*, l'école ¹⁴³ ». Par l'instauration de règles et de codes visuels, vestimentaires, notre société « présente la caractéristique supplémentaire d'inculquer à ses membres l'habitude de se soumettre à des autorités *impersonnelles*, (...) à une autorité abstraite symbolisée...¹⁴⁴ ». La promotion sociale, récompense de l'obéissance, a « pour principal mérite d'assurer la *continuité* de la hiérarchie. Le résultat net de ce mode d'organisation est *l'intériorisation de l'ordre social* ». Et c'est pourquoi « la première condition

¹⁴⁰ Stanley MILGRAM, *Op. Cit.*, p. 167.

¹⁴¹ Stanley MILGRAM, *Op. Cit.*, p. 169.

¹⁴² Stanley MILGRAM, *Op. Cit.*, p. 170.

¹⁴³ Stanley MILGRAM, *Op. Cit.*, p. 171.

¹⁴⁴ Stanley MILGRAM, *Op. Cit.*, p. 172.

nécessaire à la conversion à l'état agentique est la *perception* d'une autorité légitime ¹⁴⁵ ». Le réseau agentique est maintenu dans son état de soumission aux objectifs par le sentiment permanent de l'autorité qui le surveille. En d'autres termes, c'est la *visibilité* de l'autorité qui conditionne cette soumission. L'auteur emploie la notion de *proximité de la figure d'autorité* : le sujet aborde la situation d'obéissance « avec la conviction *a priori* que *quelqu'un le dirige* ¹⁴⁶ ». Pour maintenir cette conviction, il faut non seulement avoir recours aux symboles autoritaires ¹⁴⁷, mais aussi à une *présence effective* de l'autorité. Ce qui signifie qu'un réseau agentique est forcément accompagné d'un supérieur hiérarchique, un coordonnateur du fonctionnement quasi-cybernétique du réseau. Et c'est bien là la première faiblesse de ces réseaux : leur chef est leur cerveau commun, celui qui sait *pourquoi* et *comment* le réseau agira ! Dans l'approche cybernétique de la surveillance, cette autorité qui coordonne n'en tolère aucune autre car la faculté de s'autodéterminer est retirée aux informateurs. L'autorité leur est imposée, par une manipulation symbolique doublée d'un processus hiérarchique. A contrario, l'approche managériale laisse au groupe le soin de choisir son leader. C'est là la seconde différence entre les deux approches. Et troisième différence, ce leader doit posséder des qualités pour le commandement{ XE "commandement" }, un certain charisme, tandis qu'en situation agentique, « c'est à l'apparence de l'autorité et non à sa qualité intrinsèque que le sujet répond ¹⁴⁸ ».

Enfin, ce qui différencie fondamentalement ces deux réseaux, c'est la façon par laquelle leurs sujets respectifs *entrent dans le système d'autorité*. Dans les deux cas, il s'agit d'un choix volontaire, et leur « obéissance répond à une motivation intériorisée et non à une cause externe ¹⁴⁹ » *mais la nature de cette motivation est différente*. Comme nous l'avons vu, le réseau agentique est « motivé » (au sens premier de simple mise en mouvement) par sa soumission à la symbolique autoritaire (l'ensemble des symboles qu'il intériorise) et à *son schéma culturel* (par exemple, le shintoïsme). Cette motivation, si elle est intériorisée, a malgré tout une origine extérieure à l'individu. Son « choix volontaire », il l'a appris lors de son enfance, lors de sa formation ou dans le cadre de sa firme. C'est un choix qu'il a répété mille fois : un choix qu'il connaît, qu'il *assimile*. De façon analogue à la rumeur, ce choix, qui était au début justifié par une croyance *étayée et argumentée*, a vu son argumentation se *réduire* au fur et à mesure qu'il se répétait, remplacée par une conviction presque *machinale*. Ce choix, qui au début naissait des *conflits* entre sa conviction personnelle, ses valeurs morales et les symboles permanents de l'autorité, s'est « rationalisé » dans le temps. Il s'est aussi *accentué* dans la mesure où l'informateur agentique lui a conféré une *signification*

¹⁴⁵ Stanley MILGRAM, *Op. Cit.*, p. 173.

¹⁴⁶ Stanley MILGRAM, *Op. Cit.*, p. 174.

¹⁴⁷ Devoir de l'enfant envers son père, codes vestimentaires, rituels, et tradition; on notera les similitudes avec ce que l'on a pu appeler le « management » japonais.

¹⁴⁸ Stanley MILGRAM, *Op. Cit.*, p. 174.

¹⁴⁹ Stanley MILGRAM, *Op. Cit.*, p. 176.

*arrangeante*¹⁵⁰, soutenue par une *symbolique cohérente*, avec sa position de délateur{ XE "délateur" }¹⁵¹. Ce choix est finalement totalement *assimilé*, en dehors de tout principe moral¹⁵². *Réduction, accentuation et assimilation* : ce « choix » d'obéir à l'autorité, qui se propage au sein du réseau agentique, n'est rien d'autre *qu'un phénomène dérivé de la rumeur*. Il en est dérivé, en ce sens qu'il se perpétue alors que la rumeur ne résiste pas à sa réduction. Et à chaque fois que la question de l'obéissance se pose (*dilemme du délateur*), le phénomène du « choix » se réitère et se consolide. Le réseau agentique est *très rapidement* solidaire dans la soumission, aussi rapidement qu'une rumeur peut se propager dans un groupe de petite taille. Est ce que cela fait sa force ou sa faiblesse ? De quel point de vue doit-on aborder cette question ? De celui de l'informateur ou de celui de l'autorité ?

« La justification idéologique se révèle essentielle quand on veut obtenir l'obéissance *spontanée*. Elle permet au sujet docile de voir son comportement en relation avec un objectif souhaitable¹⁵³ ». C'est le point fort du réseau agentique d'informateurs : *la spontanéité*, c'est-à-dire un gain de temps appréciable dans la recherche de l'information, et par conséquent, dans la course pour la compétitivité. Du point de vue de l'autorité, le réseau agentique, qui se soumet aux objectifs aussi vite qu'une rumeur se propage dans un petit groupe, offre ainsi l'avantage de la *rapidité de réponse aux signaux de l'environnement*. Mais la gamme d'actions offerte à l'autorité par un réseau agentique s'avère vite limitée. Le stratège Sun Tzu, il y a vingt-cinq siècles, nous offrait la définition la plus complète de l'espion : « On utilise cinq types d'espions : les agents d'influence{ XE "agents d'influence" }, les agents de l'intérieur{ XE "agents de l'intérieur" }, les agents retournés, les agents sacrifiés{ XE "agents sacrifiés" }, les agents qui doivent vivre. (...) Les agents d'influence influencent leurs compatriotes pour les utiliser; les agents de l'intérieur influencent les gens du palais pour les utiliser; les agents retournés influencent les espions de l'ennemi pour les utiliser. Pour transmettre de fausses informations à l'extérieur, je fais en sorte que mes propres espions les connaissent et les transmettent aux ennemis, ce sont les agents sacrifiés; les agents qui doivent vivre reviennent pour *transmettre* leurs informations¹⁵⁴ ». Dans la conception de Sun Tzu, un réseau agentique d'informateurs présente d'excellentes caractéristiques pour devenir un réseau qui doit mourir...

¹⁵⁰ Par exemple : « J'informe ma nation pour qu'elle triomphe des idéologies mauvaises ».

¹⁵¹ Multiplication de symboles à connotations positives, « la lutte pour le bien », ou « la lutte pour le mérite ».

¹⁵² De toute façon, « le sens moral est bien moins contraignant que ne voudrait nous le faire croire le mythe social. Bien que des prescriptions aussi impératives que « *tu ne tueras pas* » occupent une place prédominante dans les règles de l'éthique universelle, elles sont loin d'avoir la même position privilégiée dans la structure psychique de l'homme », Stanley MILGRAM, *Op. Cit.*, page 23.

¹⁵³ Stanley MILGRAM, *Op. Cit.*, p. 178.

¹⁵⁴ SUN TZU, *L'art de la Guerre*, Article XIII, « De l'utilisation des espions », traduction de Niquet-Cabestan, Economica, 1988, p. 93.

En effet, les informateurs du réseau agentique ne savent ni le « *vers quoi* » de leur contribution, ni même son réel « *pourquoi* » (remplacé par des motifs idéologiques, ou par une manipulation{ XE "manipulation" } symbolique). Aspect positif, ils ne risquent pas d'informer leur cible des réels motifs de leur mission et leur rapide soumission permet de leur apprendre très facilement de faux motifs, ou de faux secrets technologiques. S'ils ont été choisis pour intégrer un réseau agentique, c'est bien pour remplir, à l'occasion, ce genre de mission de *désinformation*. Agents qui doivent vivre, ils le sont aussi dans la mesure où le principe agentique garantit une bonne fiabilité dans la *transmission* de l'information. Mais un réseau agentique n'a pas de grande capacité d'adaptation. Or, pour pouvoir *influencer*, il faut pouvoir *s'adapter*, se *confondre* aux contextes culturels et corriger éventuellement sa mission en fonction des contraintes imprévues que présente l'environnement surveillé. Le réseau agentique ne peut se séparer de son autorité : il doit toujours être en contact avec elle, c'est son « cerveau ». La *spontanéité* acquise dans le recueil et la transmission de l'information est alors peine perdue. D'où provient cette faiblesse du réseau agentique ?

« Le changement agentique a pour conséquence la plus grave que l'individu estime être engagé vis-à-vis de l'autorité dirigeante, mais ne se sent pas responsable du contenu de ses actes que celle-ci lui prescrit. Le sens moral ne disparaît pas, c'est son point de mire qui est différent : le subordonné éprouve humiliation ou fierté selon la façon dont il a accompli la tâche exigée de lui ¹⁵⁵ ». Et c'est là l'explication de cette faiblesse : si la rapidité de réponse groupale est améliorée dans des mesures inégalées par tout autre type de réseau, la capacité de réponse de chaque individu est soumise à l'autorité dirigeante du réseau; ce en quoi le réseau agentique peut vraiment être appelé un réseau d'ordre cybernétique, car c'est la performance de la technologie de l'information qui transporte la question de l'informateur embarrassé et la réponse de l'autorité qui lui ordonne la correction, qui conditionne la rapidité de réponse « individuelle » de l'informateur agentique. A titre d'élément de réflexion, la société Mitsui n'a eu de cesse d'améliorer ses technologies de l'information pour son réseau international d'informateurs. La plus récente amélioration prévue à ce jour est l'équipement des liaisons entre l'autorité japonaise de Tokyo et les centres informateurs du monde entier par des fibres optiques et des liaisons satellites. Le principe des fibres optiques est de transporter de la lumière non transformée (et non des impulsions électriques) : les messages lumineux circulent donc, à la vitesse de la lumière. On s'approche peu à peu de la perfection d'un système nerveux : chaque informateur peut transmettre très rapidement le « stimulus » de l'environnement au « cerveau » de Tokyo, le siège de la Technological Development Division.

L'informateur « agentique » ne met donc en œuvre qu'une partie très restreinte de facteurs de motivation personnelle¹⁵⁶. La motivation du personnel pour qu'il

¹⁵⁵ Stanley MILGRAM, *Op. Cit.*, p. 182.

¹⁵⁶ Sinon aucun dans une mission de simple recueil, la motivation étant de toute façon reportée sur la perfection des moyens : il désire accomplir sa tâche de la *meilleure façon*.

puisse *impliquer sa personnalité* dans sa mission, qu'il coïncide à ce qu'il souhaite être et à ce qu'il fait, constitue le principe de base du management participatif qui renouvelle le concept de surveillance. La participation et la capacité à s'adapter peuvent ainsi concurrencer le systématisme et les effectifs importants employés par les réseaux agentiques. Dans le cadre du management participatif, chaque informateur, engageant sa personnalité, tire de ses ressources culturelles les moyens de mener sa mission au succès. L'informateur du réseau managérial bénéficie donc d'une *totalité non chronologique de facteurs de motivation*. Il n'y a plus dissociation entre son désir de réalisation personnelle et son besoin d'appartenance à un groupe¹⁵⁷. L'ensemble des facteurs de motivation ne se succèdent plus, ils se justifient les uns les autres au même moment; ce qui les renforce et crée une synergie. Le réseau managérial peut conduire des missions difficiles, s'infiltrer au sein des réseaux de recherche des concurrents, investir leurs combinatoires de production. C'est dans ces situations *complexes*, où la simple détermination à réussir ne suffit plus, que le réseau managérial trouve toute sa justification : là où le réseau agentique n'a pas la capacité d'adaptation suffisante pour agir sans être mis à jour. C'est l'avantage de la personnalité sur le réflexe cybernétique.

Pratiquer une surveillance à travers un réseau managérial introduit cependant un risque plus grand. La grande force du réseau agentique était de minimiser le risque de désobéissance¹⁵⁸, en contraignant les individus à suivre une voie prédéfinie. L'approche managériale, quant à elle, se situe plus dans une perspective d'optimisation des résultats par rapport aux risques encourus. Elle augmente de la même manière la possibilité de réussite¹⁵⁹ que la possibilité d'échec¹⁶⁰. L'autorité doit donc apprendre à gérer l'incertitude inhérente au réseau managérial, c'est-à-dire apprendre à l'évaluer et à mettre en place des indicateurs des dangers possibles. L'autorité doit développer une *expertise de l'incertain*. Mais dès que cette possibilité sera envisagée, « deux types de pouvoir auront toujours tendance à se développer. D'abord le pouvoir que nous pourrions appeler *le pouvoir de l'expert*, c'est-à-dire le pouvoir dont un individu dispose du fait de sa *capacité personnelle* à contrôler une certaine source d'incertitude affectant l'organisation, et en second lieu le pouvoir hiérarchique fonctionnel, c'est-à-dire le pouvoir dont certains individus disposent, du fait de leur fonction dans

¹⁵⁷ A.H. MASLOW, *Motivation and Personality*, New York, Harper, 1954. MASLOW hiérarchise les besoins psychologiques de l'homme dans une pyramide dont la base représente les besoins physiologiques, et dont le sommet est partagée entre le besoin d'appartenance à un groupe, et, plus haut placé, le besoin de se réaliser.

¹⁵⁸ Bien qu'il soit toujours présent comme l'a montré STANLEY MILGRAM dans ses expériences, menées cependant sur des sujets pris au hasard, sans tenir compte de leur terrain propice à l'obéissance, c'est à dire sans les former des années durant à l'intégration dans un réseau agentique.

¹⁵⁹ Des résultats plus *qualitatifs*, c'est à dire intégrant une plus grande possibilité de modulation par rapport aux aléas du contexte de la mission.

¹⁶⁰ Désobéissance, née du conflit moral entre la personnalité de l'informateur et l'objectif de sa mission.

l'organisation, pour contrôler le pouvoir de l'expert et à la limite y suppléer ¹⁶¹ ». Et ces deux pouvoirs, au sein du même réseau, vont entrer en *conflit*. Pouvoir hiérarchique et pouvoir d'expertise doivent donc, autant que faire se peut, être réunis dans les mêmes acteurs.

La pérennité du réseau managérial est donc fonction de l'aptitude de ses membres à renouveler leur expertise, en conservant leur pouvoir social. Le réseau doit lui-même contrôler les sources d'incertitude, afin de préserver *son pouvoir social*, car « les experts n'ont de pouvoir social, que sur la ligne de front du progrès, ce qui signifie que ce pouvoir est changeant et fragile ¹⁶² ». Mais apprendre à maîtriser l'incertitude, c'est avant tout bien connaître les contextes de la surveillance.

4.3. Les contextes de la surveillance

4.3.1. La nouvelle économie industrielle

Nous venons de voir que la surveillance s'organise en *réseaux* ayant des *modalités de fonctionnement différentes* selon plusieurs facteurs, parmi lesquels les problèmes inhérents à la circulation de l'information, les aspects culturels et la maîtrise des technologies de communication. Nous avons pu conclure qu'un élément commun, *l'incertitude*, restait inhérent à chacune des approches envisagées, dans une proportion plus ou moins grande selon les objectifs à atteindre (du simple recueil, à l'infiltration des réseaux de recherche et de production des concurrents). Nous allons voir maintenant comment le monde industriel a changé et comment *l'information en est devenue un élément fondateur*. Ce que nous avons pu dire plus haut, va évidemment être envisagé sous un tout autre aspect. Ce qui *était* une différence *formelle* entre deux modalités d'acquisition de l'information, va devenir, sous ce nouvel éclairage, un *élément clé de la compétitivité industrielle*.

Ce qui caractérise, avant tout, la nouvelle industrie, c'est sa *dématérialisation*. Elle se manifeste sous plusieurs formes : un plus fort taux d'investissements immatériels, une autorité plus grande du scientifique au sein des réseaux de commandement, et la progression des systèmes de production automatisés, dont le fonctionnement est assuré par un centre de traitement de l'information. La production se dégage peu à peu de ses contraintes matérielles : « aujourd'hui, c'est au niveau de la *reproduction* — mode, média, publicité, réseaux d'information et de communications — au niveau de ce que Marx appelait négligemment les faux frais du capital (on peut mesurer l'ironie de l'histoire), c'est-à-dire *dans la sphère des simulacres et du code*, que se noue *l'unité du processus d'ensemble du*

¹⁶¹ Michel CROZIER, *Le phénomène bureaucratique*, Editions du Seuil, 1963, p. 202.

¹⁶² Michel CROZIER, *Op. Cit.*, p. 204.

*capital*¹⁶³ ». Ce « simulacre{ XE "simulacre" } » dont parle Baudrillard, c'est simplement la possibilité de produire *en série des objets identiques*, à partir d'un modèle qui en 1976, à l'époque où l'auteur écrit, n'était encore qu'un plan, ou un moule, mais qui aujourd'hui est devenu *un ensemble d'informations directement entrées dans l'ordinateur de pilotage de la production*. Produire, c'est organiser les « signes génériques » de la production. Parallèlement à cette dématérialisation, la standardisation des processus s'est accentuée, puis s'est *modifiée*, ne s'intéressant plus qu'à la production de technologies génériques, bases de départ de l'innovation. Ce noyau de technologies de base va permettre à la firme de *se positionner* en termes de savoir et de savoir-faire. Il lui suffira ensuite de diffuser dans de nombreux domaines d'application cette connaissance pour entériner sa démarche stratégique. Une question vient tout de suite à l'esprit : comment la firme se différencie-t-elle ?

En fait, la firme industrielle mène parallèlement deux démarches, qui ne sont pas dénuées d'influences l'une sur l'autre. En amont, la première démarche tend à mettre en place des combinatoires{ XE "combinatoires" } originales et performantes de technologies génériques. L'originalité ne réside donc plus dans la complexité inhabituelle d'une technologie, ou dans son contenu scientifique intrinsèque; elle se situe en fait dans la capacité à connaître en profondeur plusieurs domaines de compétences permettant la genèse de multiples combinaisons de technologies. La seconde démarche, en aval, consiste à ne plus considérer des produits comme des objets industriels destinés à être consommés, puis jetés, mais comme des produits-systèmes qui vont évoluer avec le consommateur. Autour du produit industriel constitué de composants standards (nés d'une combinatoire de technologies génériques), on va organiser des services et d'autres possibilités d'évolution du système commercialisé. Le produit-système va ainsi s'adapter à l'évolution de l'environnement de sa commercialisation. Dans ces deux approches, deux combinatoires entrent donc en œuvre : une combinatoire de structuration{ XE "combinatoire de structuration" } des technologies génériques et une combinatoire de différenciation{ XE "combinatoire de différenciation" } des composants de finition.

Il manque assurément une étape à ce cheminement. Comment organise-t-on la combinatoire des technologies génériques si l'on ne connaît pas l'évolution de la demande ? Ou comment organise-t-on les combinatoires de différenciation si l'on ne connaît pas les possibilités offertes par les technologies génériques ? *La circulation de l'information* entre l'aval et l'amont devient un facteur de compétitivité de la firme. Il manquait dans notre approche un *relais d'information* entre la recherche qui améliore le *potentiel technologique*¹⁶⁴ de la firme et le marché qui en conditionne les axes d'évolution.

¹⁶³ Jean BAUDRILLARD, *L'échange symbolique et la mort*, Gallimard, 1976, p. 86.

¹⁶⁴ *Potentiel technologique* : ensemble des technologies génériques parfaitement maîtrisées par la firme, et qui constituent sa « bibliothèque vivante ». On peut comparer ce potentiel de la firme à une « culture générale » qui permet d'explorer certains domaines de connaissance dont la *proximité* facilite l'investigation.

Cette double articulation va être assurée par une interface complexe, mettant en œuvre de multiples petites unités stratégiques¹⁶⁵.

Les missions de ces petites unités vont être, d'une part, de recueillir l'information ¹⁶⁶ et de la transmettre aux centres de recherches et à aux différentes directions afin qu'ils réfléchissent à de nouvelles combinatoires ¹⁶⁷, et d'autre part, de produire une grande partie de la valeur ajoutée ¹⁶⁸.

La compétition s'organise aujourd'hui autour de *pôles de savoir*, plutôt qu'autour de *pôles de marché*. Un produit en devient, non plus une somme de caractéristiques, mais une *gamme de performances*. La compétitivité des firmes réside désormais dans leur capacité de se mouvoir de plus en plus loin en amont et en aval de la fabrication (de la recherche fondamentale à la psycho-sociologie des consommateurs).

Si la firme doit étendre dans une telle mesure son pouvoir d'investigation pour être compétitive, on peut soupçonner les technologies de l'information d'être elles même un nouveau facteur de compétitivité, voire de *structuration* de l'industrie. Selon une étude récente de la Communauté européenne, dans 69% des cas, la coopération en matière de technologies de l'information est considérée « comme un moyen d'accroître la connaissance de la firme », voire « d'atteindre des résultats de recherche plus ambitieux qu'ils n'auraient été sans ces coopérations ¹⁶⁹ ». La maîtrise commune des technologies de l'information a également aidé beaucoup « d'entreprises européennes à passer d'une position de *suiveur* à une position de *leader* dans l'évolution des *standards*, parmi une gamme de technologies incluant l'automatisation de la production, le design assisté par ordinateur (C.A.D.), l'architecture documentaire, les outils de programmation, les systèmes de communication et la compression de données ¹⁷⁰ ». On se rend compte de l'importance de ces technologies de l'information qui investissent aussi bien les fonctions productives ¹⁷¹, la valorisation de la recherche et le traitement

¹⁶⁵ *Strategic Business Unit* : unité réunissant plusieurs compétences pour poursuivre un seul objectif stratégique, parfois même *tactique*. La firme devient un *assemblage horizontal de fonctions stratégiques*, dont les compétences sont *essaimées* dans de petites structures délocalisées et responsables de leurs évolutions.

¹⁶⁶ *Business Scanning* : activité consistant à surveiller l'environnement de la firme.

¹⁶⁷ *Networking* : utilisation des réseaux informatiques pour faire circuler l'information de l'amont vers l'aval, puis de l'aval vers l'amont, mais aussi, horizontalement, entre combinatoires.

¹⁶⁸ *Value Added Resellers* : revendeurs produisant de la valeur ajoutée en proposant des *systèmes* comprenant le produit, le conseil, les services leur étant associés, le suivi dans le temps et l'amélioration du système vendu.

¹⁶⁹ COMMISSION OF EUROPEAN COMMUNITIES, *The Review of Esprit 1984-1988*, European Strategic Programme for Research and development in Information Technologies, C.E.C., May 1989, p. 27.

¹⁷⁰ COMMISSION OF EUROPEAN COMMUNITIES, *The Review of Esprit 1984-1988*, *Op. Cit.*, page 28.

¹⁷¹ *Computer Integrated Manufacturing* : production intégrée par l'utilisation de l'informatique comme coordonnatrice de systèmes optoélectroniques et mécaniques (*la mécatronique*); ce sont désormais les technologies de l'information qui contrôlent les processus de production.

de l'ensemble de l'information de la firme. C'est en cela qu'elles peuvent *structurer* la firme autour de l'idée générique de maîtrise de l'information. Mais ce bilan encourageant cache une réalité aux disparités cruelles pour la compétitivité des entreprises.

En fin de compte, quelles firmes ont eu les premières la possibilité d'expérimenter des systèmes d'information intégrés ? Quelles firmes ont pu, avant toutes les autres, créer des standards, puis les diffuser pour asseoir leur domination{ XE "domination" } sectorielle ? Cette domination ne peut être défendue qu'au prix d'une rente technologique{ XE "rente technologique" } confortable, c'est-à-dire un niveau d'expérience dans la maîtrise des combinatoires génériques *qu'aucune petite ou moyenne industrie ne peut s'offrir*. La petite industrie n'a plus qu'une seule défense face à cette situation : *négocier de façon serrée les informations qu'elle détient*. La grande firme a en effet besoin de concilier la nécessité du secret technologique, pour protéger sa rente, et le besoin constant d'informations nouvelles pour stimuler son innovation. Il faut en effet tenir compte de ce qu'on pourrait appeler la nouvelle temporalité industrielle. Plus vite se diffuse l'information scientifique, plus diminue la marge de manœuvre totale des firmes. La supériorité technologique devient éphémère. Le rythme d'acquisition de nouvelles informations doit s'accélérer, si la firme désire conserver les éventuels leaderships qu'elle détient dans la maîtrise de quelques combinatoires. Pour gagner du temps et pour maîtriser l'information, on n'hésite plus à modifier les structures. C'est pourquoi, pour être les premières à savoir et pour recueillir à leur source des messages de plus en plus complexes, les firmes se rapprochent de leurs consommateurs. Car s'implanter à la porte des consommateurs, cela permet, malgré un coût d'investissement de départ élevé, de bénéficier d'un effet de feed-back immédiat. De même, tendre entre le consommateur et le producteur une fibre optique ou une liaison satellite, c'est bénéficier d'un effet de flexibilité d'initiative{ XE "flexibilité d'initiative" }¹⁷². La compagnie IBM grâce à des réseaux inter-universitaires mondiaux, mis en place à des conditions de prix très compétitives, a su tirer parti de cette réflexion, bien avant qu'elle ait même été conçue par ses concurrents. Le premier pilier de la nouvelle norme productive est donc la maîtrise des technologies de l'information.

Mais sur un seul pilier, cette nouvelle norme ne tiendrait pas longtemps. Mettre en place des technologies dans l'objectif de faciliter la circulation de l'information, c'était, pour ainsi dire, le minimum qu'il fallait faire pour s'adapter à la mondialisation de la compétition. Des technologies, sans un apprentissage{ XE "apprentissage" } collectif de leur utilisation, sans un « remodelage » des principes de base du management, c'est pourtant un coup d'épée dans l'eau. La nouvelle économie industrielle va donc s'intéresser autant aux hommes qui utilisent l'information, qu'aux technologies qui soutiennent cette utilisation. C'est à ce niveau qu'entre en jeu la notion de *partenariat*. Pour dominer, il faut détenir;

¹⁷² *Flexibilité d'initiative* : les firmes, par prévention, augmentent la flexibilité de leur environnement spécifique pour pouvoir répondre dans les meilleures conditions de temps et de qualité aux signaux, ou aux questions, de l'environnement général.

mais pour détenir, il faut commencer par partager. Acquérir un brevet, dans le cadre de l'accélération de la compétition, c'est poser un jalon bien fragile si ce brevet n'est pas accompagné d'un contrat de partenariat avec son inventeur. La progression très rapide du nombre de filiales communes¹⁷³ témoigne de cette nécessité. Mais comme, finalement, la mise en place de combinatoires de technologies génériques{ XE "technologies génériques" } conditionne le déploiement des combinatoires de commercialisation, ces joint-ventures vont aussi se focaliser sur des objectifs plus directement liés aux marchés. Il en résulte que, là encore, la question du partage ou de la rétention d'information devient un facteur critique de succès de ces partenariats. Et l'arbitrage entre ce qui est donné et ce qui est gardé est avant tout le propos des hommes¹⁷⁴.

Cet arbitrage, pourtant, n'est réalisable que dans une relation de pouvoir raisonnablement *déséquilibrée*... Et ce n'est que très rarement le cas. On s'aperçoit alors que l'information, « si surveillée et rigoureuse qu'elle soit (...) n'est pas indépendante des moyens organisationnels qui la produisent¹⁷⁵ ». La lutte pour le *standard* dans le domaine des technologies de l'information n'est qu'une *lutte pour le pouvoir*. C'est le *médium* qui devient aujourd'hui la caractéristique principale du *message*. La technologie qui transporte les messages va bientôt exiger des *formats*, des *normes de compression de l'information*, un *langage*, comme celui qui permet à un système expert de diriger une production automatisée. Le producteur de la technologie de l'information devient, *par cette stratégie*, le « *propriétaire du discours* », au sens où l'entend Michel Foucault¹⁷⁶. La maîtrise des combinatoires de technologies génériques de l'information, comme celles de la fibre optique, ou de l'optoélectronique, confère donc « droit à parler, compétence à comprendre (...) et est réservée en fait (...) à un groupe déterminé d'individus¹⁷⁷ ». Mieux encore, on va prétexter une quasi-intégralité verticale{ XE "quasi-intégralité verticale" }¹⁷⁸ pour équiper de ces technologies du pouvoir l'ensemble des PME et des PMI qui fonctionnent dans le sillage de la grande firme. Finalement, à quoi servira la surveillance ? On pourra jusqu'à oublier sa pratique puisque la technologie, omniprésente, supprime la nécessité de

¹⁷³ Le terme anglais de « *joint-venture* » suggère d'une manière plus dynamique ce type de partenariat. Est-ce seulement une différence de langage ?

¹⁷⁴ Toutes choses égales par ailleurs. Nous prenons pour hypothèse qu'il n'y a pas, d'une part, de systèmes experts assez performants pour mener à bien une réflexion stratégique, et d'autre part, qu'il n'y a pas d'hommes assez fous pour laisser à une machine le soin de définir leur cadre d'évolution à long terme.

¹⁷⁵ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, page 332.

¹⁷⁶ Michel FOUCAULT, *L'archéologie du savoir*, Gallimard, 1969.

¹⁷⁷ Michel FOUCAULT, *Op. Cit.*, p. 90.

¹⁷⁸ *Quasi-intégralité verticale* : relations interactives stabilisées entre une grande firme et des petites et moyennes industries qui font de cet ensemble un groupement *intégré verticalement* par des *échanges d'informations*, et des relations de sous-traitant à donneur d'ordres.

son déploiement. C'est ce que nous appellerons plus loin le *néopanoptisme*¹⁷⁹, mais pour l'instant, continuons d'explorer ces nouvelles formes organisationnelles. L'information, dans cette parodie de « co-traitance¹⁸⁰ », joue donc un double rôle. Elle est, par sa rétention, un facteur temporaire de richesse, et par sa diffusion{ XE "diffusion" }, un facteur dynamique d'innovation{ XE "innovation" }. Or, une richesse sans novation est une richesse qui subit l'usure, puis se meurt (la fin d'une rente technologique, par exemple). Il faudra donc innover, et pour ce faire concéder une partie de son savoir en échange de données complémentaires, voire de créativité. Deux nouveaux facteurs de succès apparaissent ici. D'une part, il faudra stimuler la créativité au sein de la firme si l'on ne veut pas avoir à l'acheter ailleurs. D'autre part, il faudra apprendre à évaluer son besoin d'information, dans le cadre d'une approche économique visant à optimiser son coût d'obtention. En fait, ces deux facteurs peuvent très bien être maximisés ensemble, en mettant à profit la situation de crise. Nous allons montrer que la crise, économique ou scientifique, est paradoxalement un moment privilégié pour la créativité et l'échange d'information. Tout commence très simplement. La recherche se remet en cause. L'incertitude se répand comme une rumeur dans les esprits rationnels. Partout, on s'inquiète, on cherche...

4.3.2. La situation de crise et le besoin d'information

Le comportement des agents économiques vis-à-vis de l'information est fortement lié à la situation économique dans laquelle ils se situent. Ainsi, lorsque la crise s'est installée, elle s'est accompagnée de doutes et de remises en causes des fondements théoriques. Pour tous, la tentation fut « grande de chercher ailleurs ce que les problématiques traditionnelles et consacrées semblaient incapables d'offrir. (...) On alla quérir dans d'autres champs de la connaissance (théorie des systèmes, théorie de l'information, théorie des catastrophes, ...) de nouveaux paradigmes. Ce qui, bien entendu, ne régla rien de façon immédiate¹⁸¹ ».

La peur de ne pouvoir plus expliquer, de ne pouvoir plus se référer à un cadre théorique rassurant, motive chercheurs, théoriciens, praticiens, à renouveler leur approche et élargir leur champ de connaissance. Dans l'évolution la plus récente des comportements face à la crise, on a même affirmé que « les systèmes sociaux ont une histoire et que cette histoire est signifiante, c'est-à-dire qu'elle rend compte non seulement des modes de cohésion sociale existant dans les sociétés

¹⁷⁹ Dérivé du principe panoptique, *voir sans être vu grâce à une technologie du pouvoir qui structure l'environnement*, le néo-panoptisme va jusqu'à supprimer la nécessité de voir en poussant la structuration de l'environnement jusqu'à former, à partir du médium, les tenants, et les aboutissants du langage de la production.

¹⁸⁰ La co-traitance : terme utilisé par les donneurs d'ordres pour faire croire à leur sous-traitant qu'une véritable coopération se met en place dans le traitement des projets industriels, et preuve de leur bonne foi, les grandes firmes iront même jusqu'à aider les petites à s'équiper en technologies... de l'information (sic).

¹⁸¹ Christian BARRERE, Gérard KEBABDJIAN, Olivier WEINSTEIN, *Lire la crise*, Paris, Presses Universitaires de France, Paris, 1983, page 14.

présentes, mais aussi de leur relativité et de leur fragilité ¹⁸² ». Cela veut dire que la crise a une dimension culturelle essentielle, et qu'elle affecte aussi bien le marché, la production, que l'inconscient collectif{ XE "inconscient collectif" } et les systèmes de connaissance{ XE "systèmes de connaissance" } propres à chaque culture.

La réaction des agents économiques face à une information perturbatrice de leur environnement se modifie également : « C'est ainsi que la *spéculation*, qui joue un rôle essentiel dans une économie capitaliste pour réduire l'incertitude et qui est le principe de fonctionnement des marchés financiers et des marchés des changes, devient en situation de crise le siège des comportements collectifs puissamment déséquilibrants, où n'importe quelle information captée par les marchés donne lieu à des mouvements immédiatement imités et vertigineusement amplifiés ¹⁸³ ». La crise s'accompagne donc, pour ce qui est de l'information, d'un processus de fragilisation des comportements rationnels et d'amplification des mimétismes. Ce qui devait réduire l'incertitude l'augmente. On réagit de façon mimétique{ XE "mimétique" } pour « n'importe quelle information » : l'inconscient collectif est fragilisé. Le comportement de masse, n'obéissant qu'à des pulsions émotionnelles, est incapable d'opérer un *discernement* sur la nature de l'information captée. Cette fragilisation des comportements rationnels vis-à-vis de l'information serait-elle *irréversible* ¹⁸⁴ ? ».

Contrairement aux apparences, la notion d'irréversibilité est une notion rassurante, même lorsqu'elle s'applique à une crise. En annonçant qu'un phénomène est irréversible, on le consolide, on lui confère par ce biais une *crédibilité* dont on a fortement besoin pour réduire la tension émotionnelle collective. Les environnements turbulents{ XE "environnements turbulents" } auxquels ont été confrontés toutes les grandes théories économiques ont déstabilisé la recherche scientifique. D'un point de vue psychologique, l'irréversibilité va être cette « certitude » qui réduira la tension qui pèse sur le chercheur ou l'économiste. En d'autres termes, le besoin de se rattacher à des notions nouvelles, d'élaborer, encore et toujours, des explications pour chaque élément perturbateur de notre environnement cognitif, est révélateur d'une modification dans la *perception* de l'information. Et quand les économistes s'interrogent, l'entrepreneur s'inquiète : puisque l'on ne peut plus se fier à la théorie, à l'approche rationnelle des problèmes économiques, aux grands principes censés réguler l'offre, la demande, les marchés et le capital, l'entrepreneur se crée des « principes de refuge{ XE "principes de refuge" } ». Dans un climat général d'incertitude, qui s'étend des milieux scientifiques aux milieux financiers,

¹⁸² Michel AGLIETTA, « Crises et transformations sociales », in *Problèmes économiques*, n° 1723, 13 mai 1981, p. 17.

¹⁸³ Michel AGLIETTA, *OP. Cit.*, p. 18.

¹⁸⁴ Michel AGLIETTA, dans le même article, considère que « les phénomènes d'irréversibilité concernent l'ensemble du monde où nous vivons », en argumentant que la description d'un système « n'est intelligible que par la connaissance du passé ».

commerciaux et juridiques, l'intuition retrouve ses heures de gloire ¹⁸⁵. Est-ce à juste titre ?

On peut effectivement considérer qu'il « n'y a de connaissance vraie que par l'intuition{ XE "intuition" }, c'est-à-dire par un acte singulier de l'intelligence pure et attentive, et par la déduction, qui lie entre elle les évidences ¹⁸⁶ ». Comme le montre Berkeley : « Le feu que l'on voit n'est pas la cause de la douleur dont je souffre si j'en approche : il en est l'*indice* qui me prévient de cette douleur ¹⁸⁷ ». L'appréhension peut ainsi motiver l'état d'alerte dans lequel je suis fortement stimulé pour repérer ces indices de la connaissance. De façon analogue, la crainte de la crise stimule l'éveil de la vigilance. Dès qu'un indice de « douleur » est repéré, une connexion s'opère entre ce que signifie *potentiellement* cet indice (la douleur de l'échec) et cet indice lui-même. Cette « connexion des idées implique non pas la relation de cause à effet, mais seulement celle d'un indice et d'un signe à la chose signifiée ¹⁸⁸ ». La crise provoque le doute et les remises en cause, mais elle met aussi l'esprit en éveil. Pour Thomas Kuhn, les « crises sont une condition préalable et nécessaire de l'apparition de nouvelles théories ¹⁸⁹ ». Elles permettent de stimuler la réflexion, de reformuler les besoins en information, afin que cette acuité, née de l'échec, permette l'innovation. Les crises sont donc propices à la découverte scientifique, mais à une condition : l'aptitude du chercheur à *reformuler son besoin d'information*.

Cette reformulation du besoin d'information est d'abord apparue dans les milieux scientifiques car la science, dans la conduite de ses expériences, est grande consommatrice d'informations pour soutenir ses avancées dans la théorie. Reformuler son besoin en information, c'est d'abord prendre « conscience d'une anomalie dans la cohérence entre la théorie et la nature ¹⁹⁰ ». C'est reconnaître une incompatibilité entre l'information que l'on détient et l'usage qu'on en fait. Cette lutte incessante pour faire reculer l'incohérence crée une tension essentielle{ XE "tension essentielle" } ¹⁹¹ à la créativité scientifique. C'est par *reformulations successives* que la science progresse.

Mais quand la référence commune est un même paradigme, quand la crise n'est pas encore concevable, l'environnement entier du chercheur s'est *stabilisé*. Son

¹⁸⁵ *Le Planning Without Facts*, issu de la nécessité de planifier pour fonctionner quelque soit l'information disponible, n'est pas très éloigné d'une pratique intuitive du management.

¹⁸⁶ Michel FOUCAULT, *Les mots et les choses*, Gallimard, 1966, p. 66.

¹⁸⁷ George BERKELEY, *Principes de la connaissance humaine*, Oeuvres Choiesies, Tome I, page 267

¹⁸⁸ George BERKELEY, *Op. Cit.*, même page.

¹⁸⁹ Thomas KUHN, *La structure des révolutions scientifiques*, Flammarion, 1983, « Réponse à la crise », pages 115 à 132.

¹⁹⁰ Thomas KUHN, *Op. Cit.*, p. 119.

¹⁹¹ Le terme de « tension essentielle » est emprunté à Thomas KUHN, dans « The Essential Tension : tradition and innovation in scientific research », in *The third university of Utah Research Conference on the identification of creative scientific talent*, édition Calvin W. Taylor, 1959, pages 162 à 177.

langage s'est modifié : il a pris les travers du sentiment de sécurité, c'est-à-dire qu'il a adopté des formes verbales, un jargon, qui signifie à qui veut l'entendre que le paradigme auquel se réfère ses recherches est imprenable. Le *jargon* très spécialisé que le chercheur pratique est là pour prouver que si « on ne peut pas comprendre », il n'a pas à vous détailler l'explication de chacun des termes qu'il emploie ¹⁹² : nous n'avons plus qu'à étudier, comme lui, tout ce qui fait la richesse de ce paradigme. Ce chercheur, si sûr de lui, et si sûr du paradigme sur lequel repose son assurance personnelle, est victime de la tradition qu'encourage ce paradigme « intouchable ». « Son imagination est entravée, et même son langage cesse de lui appartenir. Et cela se reflète encore dans la nature des faits scientifiques, qui sont vécus comme étant indépendants des opinions, des croyances et des appartenances culturelles. Il est donc possible de créer une tradition et de la maintenir par des règles strictes ; cela, dans une certaine mesure, permet des succès. Mais est-il souhaitable de soutenir une telle tradition en rejetant tout autre possibilité ? Doit-on lui attribuer le droit exclusif de traiter la connaissance, avec pour conséquence que tout résultat obtenu par d'autres méthodes est éliminé sans appel ¹⁹³ ? ».

Cette tradition si sécurisante est la source même de *l'inaptitude* du chercheur à reformuler son besoin d'information en situation de crise. Il ne sait plus formuler un besoin en dehors des cadres théoriques dans lesquels il l'a toujours formulé. Les schémas qu'il utilisait pour mettre en place ses expériences n'ont plus aucune utilité quand *la connaissance tacite* qui les soutenait vient de s'effondrer sous l'ultime attaque d'une nouvelle réalité scientifique. Par abus de langage, on pourrait dire que le chercheur se confond avec son « paradigme ». C'est-à-dire que ses méthodes pour concevoir les problèmes et poser des solutions ¹⁹⁴ qui lui proviennent de son paradigme, ont modifié sa personnalité au point de faire de lui-même un « modèle accepté ». Si le besoin d'information est « reformulé » sous l'égide de la connaissance tacite propre au paradigme du chercheur, il y a de fortes chances que cette « reformulation » soit inadéquate aux nouvelles conditions de recherche suscitées par la crise.

Ce que le chercheur a l'habitude de faire, ce n'est pas « reformuler » mais bien « formuler » ses besoins d'information dans la logique rassurante des centaines de modèles que lui propose son paradigme, pour résoudre des problèmes qui ne sont que de « légers obstacles » au maintien de la toute puissante certitude à laquelle il a consacré sa personnalité. En fin de compte, c'est la répétition de ces résolutions quotidiennes de petits problèmes qui réduisent, avec le temps, l'intuition personnelle en bagage technique de « solutions types » applicables à des

¹⁹² Voir à propos de la détérioration du langage qui fait suite à un accroissement du professionnalisme, l'essai de Paul FEYERABEND, « Experts in a Free Society », *The Critic*, novembre-décembre 1970.

¹⁹³ Paul FEYERABEND, *Contre la méthode, esquisse d'une théorie anarchiste de la connaissance*, Editions du Seuil, 1979, p. 16.

¹⁹⁴ Selon la définition de Thomas KUHN, dans *La structure des révolutions scientifiques*, Flammarion, 1983, p. 45.

« problèmes types ». L'individu qui, au contraire, pourra tirer de « tout ce qui est remarquable dans sa nature ¹⁹⁵ » une faculté personnelle de traitement de problèmes nouveaux, saura définir ses besoins. C'est pourquoi il faut « cultiver l'individualisme{ XE "individualisme" } qui seul produit, ou peut produire, des êtres humains développés ¹⁹⁶ » capables d'investir leur propre personnalité dans l'effort de résolution de problèmes fondamentalement modifiés par la situation de crise. Reformuler son besoin d'information, cela signifie pouvoir adapter aux conditions nouvelles de sa recherche, la nature et la forme d'information susceptibles d'apporter des éléments nouveaux dans le cadre d'une résolution ne reposant sur aucun paradigme connu à ce jour. La crise suscite donc « une conception du monde entièrement nouvelle, y compris une nouvelle conception de l'homme *et de ses capacités à connaître* ¹⁹⁷ ». La fréquence toujours grandissante selon laquelle les paradigmes se renouvellent, et même se créent (dans des domaines différents de la science) suggère une capacité plus grande à trouver l'information, à la traiter, à l'organiser dans des contextes nouveaux, pour en retirer les enseignements nécessaires au sortir de la crise. Il faut pour cela développer la personnalité et l'attention de chacun, afin de refuser cette « nécessité d'attendre et d'ignorer d'énormes masses d'observations et de mesures critiques, (qui) n'est presque jamais discutée dans nos méthodologies ¹⁹⁸ ».

4.3.3. Technologie, violence et compétitivité

Cette nécessité de « ne pas attendre », d'apporter encore plus d'attention à ce qui est en dehors de la norme scientifique, ou de ses paradigmes, suggère-t-elle une nouvelle rationalité ? Entrons-nous dans l'ère de la vigilance rationnelle ? Comme le suggère Paul Feyerabend dans son exposé « *Contre la méthode* », « nous ne devons pas tomber dans l'erreur de croire, comme beaucoup de rationalistes{ XE "rationalistes" } sont enclins à le faire, que les hommes en général, ou des groupes particuliers comme celui des scientifiques, sont poussés à la rationalité et qu'ils font avancer leur profession, et en vérité la totalité de l'histoire, dans la direction prescrite par ses règles ¹⁹⁹ ». En vérité, la nécessité d'augmenter sa *capacité à écouter les silences* ne relève pas d'une approche rationnelle de l'information, mais plutôt d'une prise de conscience de sa *rationalité limitée* ²⁰⁰. Il faut donc redoubler d'attention à l'égard des « silences »,

¹⁹⁵ John Stuart MILL, *On Liberty*, The Philosophy of John Stuart Mill, New York, Editions Marshall Cohen, 1961, p. 265.

¹⁹⁶ John Stuart MILL, *Op. Cit.*, p. 251.

¹⁹⁷ Expression empruntée à Paul FEYERABEND, *Contre la méthode, esquisse d'une théorie anarchiste de la connaissance*, Editions du Seuil, 1979, p. 164.

¹⁹⁸ Paul FEYERABEND, *Contre la méthode, esquisse d'une théorie anarchiste de la connaissance*, Editions du Seuil, 1979, p. 164.

¹⁹⁹ Paul FEYERABEND, *Op. Cit.*, p. 168.

²⁰⁰ Terme emprunté à J.G. MARCH, H.A. SIMON, *Organizations*, New York, Wiley, 1958. MARCH et SIMON montrent que de nombreuses contraintes, affectives, cognitives et organisationnelles, limitent la rationalité des individus qui ne seront plus en mesure de rechercher

ces domaines de la connaissance oubliés du « bruit » de l'industrialisation, du rationalisme qui voudrait les ignorer, ou les classer, de façon rédhibitoire, dans le vaste dossier des « problèmes à résoudre ». L'objectif de cette attention redoublée *envers le moins signifiant*, est de maintenir l'intérêt pour un domaine menacé par l'oubli. C'est pour cela qu'il faut faire circuler l'information, diffuser la connaissance mais aussi *ses silences*, c'est-à-dire le descriptif des domaines dans lequel il nous faut avancer. Il faut propager l'information et mettre à jour nos déficits informationnels ²⁰¹.

« Cette propagande{ XE "propagande" } est essentielle », aurait pu dire Paul Feyerabend. « Elle est essentielle parce qu'il faut créer l'intérêt à un moment où les prescriptions méthodologiques habituelles ne trouvent pas de points d'attaque; et parce que cet intérêt doit être maintenu, peut-être pendant des siècles, jusqu'à ce que de nouvelles raisons surviennent ²⁰² ». Ce qui est vrai pour la science, l'est parfois pour la firme. Ce qui explique la nécessité de développer l'utilisation des nouvelles technologies de l'information, non seulement au bénéfice de la science, mais encore au bénéfice de la compétitivité de l'entreprise. Parce que les nouvelles technologies de l'information vont permettre d'explorer des champs méconnus de la connaissance, il faut encourager leur utilisation dans le cadre d'une stratégie de veille économique et technologique, mais aussi, lorsque c'est possible, avec des objectifs sociaux et culturels. L'entreprise, dans cette perspective, va-t-elle se peupler de *propagandistes* ? Nous le sommes tous un peu, comme le disait Harold Lasswell ²⁰³, car l'activité humaine n'est faite que de relations de pouvoir et de persuasion{ XE "persuasion" }. Ainsi, il ne faut pas systématiquement voir dans la propagande cette désinformation à grande échelle que l'on a pratiquée au service de la guerre. Certains auteurs ont même pu écrire que la propagande est au service de la démocratie ²⁰⁴. L'erreur à ne pas commettre, c'est celle qu'engendre trop souvent *la violence*, c'est-à-dire la mise en place d'une *communication biaisée* ²⁰⁵. Ce type de propagande, qui s'appuie sur la

une solution optimale, mais juste la solution ménageant au mieux ces différentes contraintes: un seuil minimal de satisfaction. L'information étant un produit de l'homme, cette rationalité limitée se reporte, selon nous, sur sa structure, sa diffusion et son contenu.

²⁰¹ Terme emprunté à François WEYERGAUS qui y voit l'explication de l'angoisse.

²⁰² Paul FEYERABEND, Op. Cit., p. 172.

²⁰³ Harold D. LASSWELL, « The function of propagandists », p. 258-268, The International Journal of Ethics, Vol. 38, University of Chicago Press, 1927. LASSWELL précise que nous sommes tous des sujets, puis des objets de la propagande. Ainsi, le pédagogue, ou l'enseignant, qui défend sa matière et tente de persuader ses élèves d'en faire de même, est lui aussi un propagandiste.

²⁰⁴ Voir à ce propos B.L. SMITH, « Propaganda Analysis and The Science of Democracy », Public Opinion Quarterly, Vol. 5, n° 2, Juin 1941. Voir également, C.I. HOVLAND et co-auteurs, *Communication and Persuasion : Psychological Studies of Opinion Changes*, Yale University Press, New Haven, 1953. Ceci est tout de même fortement discuté dans la mesure où la propagande opère une sélection de l'information, qu'elle accompagne d'une méthode de propagation, qui ne donnent pas au peuple tous les éléments de la décision.

²⁰⁵ Karin DORVIN, *Road of Propaganda : The Semantics of Biased Communication*, Philosophical Library, New-York, 1959, pp. 124 et suivantes.

manipulation des valeurs du groupe, conduit, un jour ou l'autre, au totalitarisme. Il ne tolère pas la contradiction et fonde toute sa dynamique sur des phénomènes de masse : il est en contradiction avec notre projet de laisser libre cours, dans une structure adéquate, à la personnalité des acteurs. Comme Crozier et Friedberg²⁰⁶, il nous faudra « affirmer avec force que la conduite humaine ne saurait être assimilée en aucun cas au produit mécanique de l'obéissance ou de la pression des données structurelles. Elle est toujours *l'expression et la mise en œuvre d'une liberté, si minime soit-elle* ».

Stanley Milgram était d'ailleurs fortement critiqué sur ce point. L'état « agentique » dans lequel étaient plongés les participants de sa célèbre expérience, a été, tour à tour, qualifié de « trucage expérimental », ou d'interprétation « dangereusement simpliste ». Ses détracteurs justifiaient l'obéissance des sujets aux ordres de l'expérimentateur par une tendance destructrice propre à la nature humaine. Donner la possibilité d'agresser, dans un objectif scientifique, avec l'aura de la blouse blanche, et sans brandir la menace d'une réprimande, libérait tout naturellement cette agression. Milgram répond à ses détracteurs à la fin de son ouvrage : « Bien que les tendances agressives fassent partie inhérente de la nature humaine, elles n'ont en réalité pratiquement aucun rapport avec le comportement des sujets dans l'expérience (...) Nous avons pu constater qu'à de rares exceptions près, ils trouvaient déplaisante, voire odieuse, l'action qui leur était prescrite, mais ils s'estimaient tenus de l'accomplir²⁰⁷ ». La réalité se situe certainement à mi-chemin entre la thèse cybernétique et la thèse psychanalytique²⁰⁸. Il est bien dommage que Milgram n'ait pas envisagé cette hypothèse lors de la conduite de ses expériences. On saurait peut-être aujourd'hui quelles sont les implications de l'une dans l'autre. L'expérience de Milgram a cependant le mérite de montrer la violence comme une donnée courante de la vie sociale, et nous montrerons, à notre tour, qu'elle est une donnée structurante de la compétitivité.

Peu importe l'origine de la destruction accomplie par les sujets expérimentaux de Milgram, peu importe qu'elle soit inscrite dans le psychique hors de tout contexte d'obéissance, ou qu'elle ne soit que « *violence transmise* » par le donneur d'ordre : cette destruction a bien eu lieu, à l'encontre de tout sens moral. Milgram écrit : « Après avoir constaté au cours de mes propres expériences la soumission inconditionnelle de centaines d'individus ordinaires, force m'est de conclure que la conception de la banalité du mal formulée par Hannah Arendt²⁰⁹ est plus

²⁰⁶ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, page 45.

²⁰⁷ Stanley MILGRAM, *Soumission à l'autorité*, Calman-Lévy, 1982, Chapitre XIII, « Une autre théorie : l'agression est-elle la clé ? », pp. 205-208.

²⁰⁸ C'est à Sigmund FREUD que revient cette théorie de la force destructrice, profondément ancrée en nous, et dont l'expression est inhibée par le surmoi ou la conscience.

²⁰⁹ Hannah ARENDT : philosophe américaine d'origine allemande (Hanovre 1906 - New York 1975). Elle a étudié les fondements des systèmes totalitaires (*Les Origines du Totalitarisme*, 1951).

proche de la vérité que nous n'aurions jamais osé l'imaginer ²¹⁰ ». Chaque grande université américaine a d'ailleurs aujourd'hui son programme de cours d'éthique et de management, ou d'éthique et de communication de masse ²¹¹. Ce débat autour de la question éthique n'est pas fortuit. Il correspond à une inquiétude réelle face à une compétition de plus en plus sévère, qui a amené les entreprises à mettre en œuvre tous les moyens à leur disposition pour maintenir leur niveau de compétitivité. Parmi ces moyens, l'espionnage, la corruption du personnel d'encadrement de l'adversaire, et l'introduction d'un virus dans le système expert du concurrent, se sont avérés cruellement efficaces ²¹².

Lamère, Leroux et Tourly, dans leur ouvrage « La sécurité des réseaux informatiques ²¹³ », citent pas moins de 90 cas de criminalité informatique dans les rubriques des détournements de fond, des détournements de biens, des sabotages immatériels et des détournements d'informations²¹⁴. Il ne s'agit pas là d'erreurs de saisie, ou de catastrophes naturelles, mais bien de crimes, c'est-à-dire du détournement d'une compétence professionnelle dans le domaine de l'information, au détriment de l'organisation, ou au profit des intéressés. Les auteurs citent, parmi bien d'autres, l'exemple suivant : « Un cadre ayant autrefois travaillé au service informatique, entre sur écran une série d'écritures dont le compte d'origine est « Réserves » et le compte d'aboutissement est un numéro de compte personnel dans une banque étrangère. Les opérations sur réserves sont rejetées en anomalies dans un fichier d'attente afin d'être ultérieurement recyclées. Le fraudeur utilise alors une chaîne de recyclage *batch* ²¹⁵, normalement employée en mode dégradé dans le cadre d'un plan de secours. Cette chaîne ²¹⁶, ancienne, n'est pas à jour et les écritures passent. Ce n'est que le lendemain que l'anomalie est identifiée. Les mouvements de fonds ont déjà été réalisés pour 7,5 millions de francs ²¹⁷ ». On peut tirer deux enseignements de cette anecdote : d'une part, le système était non entretenu, et d'autre part, c'est vis-à-vis de l'homme qu'on a manqué de vigilance : il avait déjà travaillé dans le département informatique de cette banque.

²¹⁰ Stanley MILGRAM, *Op. Cit.*, p. 22.

²¹¹ COLE, « Ethics and Mass Communication », cours de l'Université de Californie de Los Angeles (UCLA).

²¹² En 1986, les pertes dues à la fraude et au sabotage informatiques sont estimées à plus d'un milliard de dollars pour les seuls Etats-Unis (chiffre cité par J. VILLAIN, *L'entreprise aux aguets*, Masson, 1989, p. 119).

²¹³ Jean-Marc LAMÈRE, Yves LEROUX, Jacques TOURLY, *La sécurité des réseaux informatiques*, Dunod, Paris, 1989, pp. 86-102.

²¹⁴ Le registre des cas de sinistres informatiques présentent au total 145 cas ayant eu lieu entre 1984 et 1986, et en France pour 75 % d'entre eux.

²¹⁵ BATCH : programme permettant à tout utilisateur d'un réseau de faire exécuter des travaux (JOBS) à distance sur un autre site, à condition qu'il ait l'autorisation nécessaire de la part du site (*numéro de compte et mot de passe*).

²¹⁶ Suite d'instructions permettant le traitement de l'information.

²¹⁷ J.M. LAMÈRE, Y. LEROUX, J. TOURLY, *Op. Cit.*, p. 89.

Les auteurs de l'ouvrage proposent ensuite de minimiser le risque de criminalité informatique par une méthode qui connaît beaucoup de succès en France : la méthode Marion.

En analysant de plus près cette méthode, on s'aperçoit que seulement 16 questions sont consacrées au personnel informatique, représentant une pondération de 5% dans le total des critères retenus (voir tableau ci-joint). Comme on peut le constater, l'approche Marion s'attaque donc majoritairement à la sécurité de la technologie et à son environnement. Excellente sur ce point, elle prend trop peu en compte le *facteur humain* : seulement 5 % des facteurs s'intéressent au personnel et d'une façon normative²¹⁸. Aucun des facteurs pris en compte ne s'attaque à la *stratégie d'acteur* de l'informaticien ou du cadre, aux éventuels troubles psychiques qu'il a pu subir et aux fondements de sa motivation personnelle à exercer son métier. Pourtant, dans les nombreux exemples cités au début de l'ouvrage, la part du risque humain est largement majoritaire sur la défaillance technologique : 62% des cas cités sont des cas de criminalité, 20% sont des cas d'erreurs de conception, d'exploitation et de transmission, 5% des sinistres informatiques cités sont issus directement de problèmes humains dans l'entreprise, et seulement 13% des cas cités relatent des sinistres liés à des défaillances de la technologie.

En fait, le déterminisme technologique des méthodes généralement utilisées pour la sécurité des systèmes d'information peut s'expliquer, d'une part, par le coût plus important des sinistres causés par une défaillance technique (panne générale) ou par une catastrophe naturelle (incendie, inondation), et d'autre part, par le manque de moyens dont nous disposons pour lutter contre la « défaillance humaine ». Il nous faut pourtant insister sur l'aspect *statique* de ce choix.

²¹⁸ Normes de rémunération sectorielle, normes de turn-over, normes de qualité d'environnement de travail, règlements, clauses contractuelles...

Organisation générale	2,5 %
Les contrôles permanents	3 %
La réglementation et l'audit	4 %
Les facteurs socio-économiques	1 %
L'environnement de base	3 %
Le contrôle des accès	3,5 %
La pollution	1,5 %
Les consignes de sécurité	1 %
La sécurité spécifique incendie	5 %
La sécurité spécifique dégâts des eaux	1 %
L'amélioration de fiabilité de fonctionnement	3 %
Les systèmes de procédures de secours	7 %
Les protocoles utilisateurs-informaticiens	1,5 %
Le personnel informatique	5 %
Le plan informatique	4 %
La fiabilité du matériel	4 %
La sécurité des télécommunications et des données	6 %
La protection des bases de données	1,5 %
L'archivage et le désarchivage	2 %
La saisie et le transfert des données	1 %
La sauvegarde des données	6,5 %
Le suivi de l'exploitation	5 %
La maintenance	7 %
Les procédures de révision	5 %
Les méthodes d'analyse programmation	3,5 %
Les contrôles programmés	7,5 %
Sécurité du logiciel	5 %
Total des Facteurs de Sécurité	100 %

Si les catastrophes naturelles ou les pannes générales sont plus coûteuses que la criminalité informatique, et parfois dans des rapports de 400 contre 1, cela n'est que temporaire. L'informaticien était, jusqu'à une période très récente, un expert dans l'entreprise. Une très faible partie du personnel maîtrisait parfaitement l'informatique et a fortiori l'informatique complexe des réseaux. Mais cet état des choses évolue très rapidement. N'importe quel cadre, informaticien ou non, maîtrisera bientôt suffisamment de procédés de communication pour effectuer un sabotage de base : la bombe logique { XE "bombe logique" } ²¹⁹.

Lamère, Leroux et Tourly donnent, à ce propos, l'exemple suivant : « Pose de bombes logiques dans la chaîne de paye d'une entreprise nationalisée sensible, puis mise en action en période de troubles sociaux. Les difficultés de paiement des salaires ont précipité et durci la grève. Le coût est estimé à 8 millions de

²¹⁹ Une bombe logique est un sous-programme caché dans la mémoire de l'ordinateur qui répète indéfiniment une opération très simple, comme la recopie d'une donnée. Ce petit programme, d'une dizaine d'instructions, fonctionne parfois sous le principe d'une *boucle*. Avec les fabuleux progrès que l'industrie informatique a pu réaliser dans l'augmentation de la rapidité des microprocesseurs, cette *bombe logique* va très rapidement inonder le système de données, et le bloquer complètement. Mais comment repérer 10 instructions parmi 10 000 ?

francs ²²⁰ ». Cette bombe logique n'est pas forcément le fait d'un expert. Il suffit de créer deux instructions pour modifier un des paramètres de la paye (par exemple, décaler de quelques données l'accès au fichier comptabilisant les heures effectuées si le programme de paye est mise en route) pour que cette paye soit entièrement à refaire ²²¹. Un cadre, sensibilisé par une formation continue, ou par des cours du soir, saura réaliser un tel piège en moins d'une heure ²²². Quels enseignements peut-on en tirer pour l'économie industrielle et la surveillance ?

D'une part, si l'information est devenue une des pièces maîtresses de la stratégie industrielle, autant pour le contrôle des firmes sous-traitantes que pour le contrôle des hommes, elle est aussi porteuse de risques nouveaux pour la compétitivité des firmes. La maîtrise de ces risques ne doit pas être envisagée avec un déterminisme technologique inapproprié aux véritables enjeux de cette méta-industrie informationnelle ²²³. Pour être compétitive, comme nous l'avons montré en comparant un réseau agentique et un réseau managérial de surveillance, il ne suffit plus d'assujettir : il faut motiver. Mieux encore, il ne faut pas faire de la technologie une forteresse contre l'agression, mais plutôt s'attaquer aux causes de cette agression. La surveillance doit donc jouer un rôle de médiation entre l'agresseur et sa cible, l'autorité capitaliste. « Cette fonction de surveillance, de direction, et de médiation{ XE "médiation" } devient la fonction du capital dès que le travail qui lui est subordonné devient coopératif, et comme fonction capitaliste elle acquiert des caractères spéciaux ²²⁴ ». Cette définition de Marx est intéressante à plusieurs titres. D'une part, la surveillance, la direction et la médiation sont confondues dans *une seule et même fonction*. Et cela ne peut que soutenir notre détermination à ne pas séparer la vision stratégique (la direction), de la surveillance et de la gestion des technologies de l'information (la médiation). D'autre part, il s'agit d'une fonction du capital, et à ce titre, comme le précise Michel Foucault, « la surveillance devient un *opérateur économique décisif* ²²⁵ ». Dans cette perspective, le pouvoir n'a plus besoin de l'éclat des supplices ²²⁶ car « il fonctionne en permanence et pour une bonne part en silence.

²²⁰ J.M. LAMERE, Y. LEROUX, J. TOURLY, *Op. Cit.*, p. 96.

²²¹ Faire tourner un programme de paye dans une entreprise de très grande taille peut prendre plusieurs jours, auxquels il faut ajouter le temps nécessaire pour localiser la « bombe logique » parmi des milliers d'instructions, et parfois, parmi de fausses bombes logiques écrites pour dérouter le réparateur du sinistre.

²²² Toutes conditions objectives égales par ailleurs, il faut supposer qu'il ait eu accès à l'ordinateur, par sa fonction ou *fortuitement*, et que le système soit peu ou pas du tout protégé.

²²³ *La méta-industrie informationnelle* : une industrie dont les processus productifs sont parfaitement maîtrisés, et dont la compétitivité repose désormais sur son aptitude à mettre en place des *réseaux d'information* pour « nourrir » sa recherche, ses procédés automatisés, sa force commerciale, jusqu'à sa planification stratégique à long terme.

²²⁴ Karl MARX, *Le Capital*, Livre I, Section Quatrième, Chap. XIII.

²²⁵ Michel FOUCAULT, *Surveiller et Punir*, Gallimard, 1975, p. 177.

²²⁶ *L'éclat des supplices* : cérémonial qui « produit, en plein jour, la vérité du crime », mêlant « un acte d'instruction et un élément de punition » afin de « reconstituer la souveraineté un instant

La discipline fait « marcher » un pouvoir relationnel qui se soutient lui-même par ses propres mécanismes et qui, à l'éclat des manifestations, substitue le jeu ininterrompu des regards calculés. Grâce aux techniques de la surveillance, la « physique » du pouvoir, la prise sur le corps s'effectue selon les lois de l'optique et de la mécanique, selon tout un jeu d'espaces, de lignes, d'écrans, de faisceaux, de degrés, et sans recours, en principe au moins, à l'excès, à la force, à la violence²²⁷ ». Le pouvoir ainsi constitué crée, en empruntant le terme à Crozier et Friedberg, une interstructuration{ XE "interstructuration" } de l'environnement du surveillé, avec la position relationnelle du surveillé lui-même²²⁸. Parallèlement, la nouvelle compétition s'accompagne de violences, envers les concurrents, et dans la pratique du management qui emprunte de plus en plus fréquemment ses tactiques à l'art de la guerre{ XE "guerre" }. Dans ce contexte, le pouvoir s'organise de manière à désorienter l'agression, soit en la dirigeant vers la technologie, soit en la dirigeant vers les concurrents. Ces technologies qui nous surveillent devraient idéalement « absorber » l'agressivité du personnel, comme la chambre capitonnée réceptionne la violence du dément. La technologie est passée du stade de la camisole de force au stade de l'environnement capitonné.

Cet environnement surprotégé devient l'enfant gâté de l'autorité. Des investissements importants sont consacrés à la perfection de la sécurité informatique{ XE "sécurité informatique" } et à la qualité de la technologie. Le système d'information devient une forteresse qui brave les cadres. « Nous avons tout prévu et je ne vois pas ce que pourrait inventer un cadre pour défier nos protections, peut-être un ouvre-boîte », confie un responsable de la sécurité informatique d'une grande société. Mais compliquer le jeu, c'est ignorer la personnalité des acteurs qui introduisent des virus dans les systèmes ou des « bombes logiques » dans les chaînes de traitement.

C'est justement la perspective du jeu qui les motive : et plus ce jeu est complexe, plus il met au défi leur capacité à libérer leur violence; et plus celle-ci sera encouragée. Que cette violence spécifique soit contenue, et ce sera une victime émissaire qui en subira les conséquences, c'est-à-dire une victime anodine, peut-être un collaborateur, ou le traitement d'un « dossier sans conséquence ». Mais comme l'écrit René Girard, « la violence longtemps comprimée finit toujours par se répandre aux alentours ; malheur, dès lors, à celui qui passe à sa portée²²⁹ ». Et la somme de ces « dossiers sans conséquences » qui seront mal traités, et la somme de ces « conflits dénués d'importance » qui naîtront de cette violence inexprimée, vont diminuer la compétitivité de la firme

blessée », « en la manifestant dans tout son éclat », Michel FOUCAULT, *Op. Cit.*, pages 39, 45 et 52.

²²⁷ Michel FOUCAULT, *Op. Cit.*, p. 179.

²²⁸ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, « L'organisation devant les contraintes de sa situation : adaptation unilatérale ou interstructuration ? », Editions du Seuil, 1977, pages 156-162.

²²⁹ René GIRARD, *La violence et le sacré*, Editions Grasset, Collection Pluriel, 1972, p. 50.

dans un domaine clé : la cohésion sociale²³⁰. La violence est « une chose éminemment communicable. Sa tendance à se précipiter sur un objet de rechange, à défaut de l'objet originellement visé, peut se décrire comme une espèce de contamination²³¹ ». Celui qui crée un virus²³² procède à un rituel{ XE "rituel" } : il va créer la technologie qui servira de réponse injuste, aléatoire et imprévisible à une autre technologie, celle du pouvoir. Les créateurs de virus vont ainsi se donner des « noms de guerre », pour revendiquer leur différence.

Ainsi, un des groupes de piratage des plus célèbres s'appelle-t-il le Chaos Computer Club, « société forte de 90 membres en R.F.A., et dont les statuts légalement déposés indiquent que son but est de *démontrer* que dans le monde informatique *règne le chaos*²³³ ». La violence que déploie ce groupement est une réponse au rationalisme technologique. Ils ne prétendent pas introduire le désordre au sein d'une organisation technologique bien structurée. Ils prétendent au contraire démontrer que le chaos règne sur cette organisation, sans qu'ils aient à le provoquer. Cette réaction naît d'un dilemme entre la fierté de détenir une expertise propre à un groupe restreint, et la façon dont ils ont obtenu cette expertise, dans un environnement capitonné{ XE "environnement capitonné" }²³⁴. La technologie qu'ils utilisent « nourrit » à la fois leur personnalité, et le malaise qu'ils ressentent. S'ils se réalisent grâce à la technologie, leur groupe d'appartenance n'est pas celui dans lequel ils évoluent dans le cadre professionnel²³⁵. Pour laisser libre cours à la violence qui va apaiser cette contradiction, ils vont créer un groupe de « pirates ». Il vont se créer un discours qui sera le leur, « car dans nos sociétés, la propriété du discours — entendue à la

²³⁰ Remarquons, à ce propos, que les Japonais ont su mettre en place des structures pour canaliser la violence de leurs cadres, comme ces « mannequins de défoulement », remplis de mousse compressible et à l'effigie de leurs supérieurs, qui permettent aux cadres de se « défouler » en libérant leur violence sur des symboles de l'autorité, plutôt que sur l'autorité elle-même.

²³¹ René GIRARD, *Op. Cit.*, p. 50.

²³² *Virus* : ensemble d'instructions constituant un programme dont la finalité est de perturber, par tous les moyens, le fonctionnement d'un système, ou de plusieurs systèmes mis en réseau. Ses moyens peuvent être des « bombes logiques », mais aussi simplement la destruction systématisée de données, de logiciels, voire de fichiers d'identité d'utilisateurs de réseau.

²³³ Jacques VILLAIN, *L'entreprise aux aguets*, Masson, 1989, p. 117. Les activités du C.C.C. furent interrompues par la police allemande le 28 Septembre 1987. Le groupe détenait un listing de 400 pages délivrant les codes d'accès et les mots de passe relatifs à des centaines d'ordinateurs, dont plusieurs de la NASA, du Space Physics Analysis Network, et par voie détournée, des Centres de Recherches Nucléaires de Genève en Europe et d'Alamos aux États-Unis.

²³⁴ Métaphore d'un environnement protégé, où la technologie est censée guider l'évolution de son utilisateur, par des niveaux d'accès à l'information, par les limites intrinsèques des programmes dont les instructions, par leur nature, limitent les possibilités, et par *un discours que s'est appropriée la technologie*.

²³⁵ Ceci vient directement contredire ce qu'affirmait MASLOW à propos d'une *hiérarchie* des besoins de l'homme, et notamment le fait qu'il fallait d'abord satisfaire son besoin d'appartenance à un groupe, avant de satisfaire son besoin de *self-realization* (A.H. MASLOW, *Motivation and Personality*, Harper, New York, 1954). Ici, le pirate « se réalise » dans la pratique de son expertise, bien que cette pratique s'effectue dans le cadre d'un groupe dans lequel il ne se reconnaît pas.

fois comme droit à parler, compétence à comprendre, accès licite et immédiat au corpus des énoncés déjà formulés, capacité enfin à investir ce discours dans des décisions, des institutions ou des pratiques — est réservée en fait (parfois même sur le mode réglementaire) à un groupe déterminé d'individus²³⁶ ». Dans le discours technologique, ils étaient des produits de l'ordre, des utilisateurs de l'élément structurant tout le système. Dans leur discours, ils deviennent les symboles de l'énoncé contraire du discours technologique : « C'est le chaos qui règne. Il n'y a pas de centre technologique et de périphérie humaine d'utilisateurs. Il n'y a qu'un désordre généralisé que la technologie ne sait pas maîtriser. Nous le prouvons : nous sommes partout, même au cœur des systèmes stratégiques de défense qui font la fierté des propriétaires du discours technologique²³⁷ ».

Replaçons nous, désormais, dans le contexte d'une grande firme négociant avec les multiples PMI œuvrant dans son sillage. Là aussi, la propriété du discours est à celui qui détient, a priori, le savoir technologique et l'information que nécessite la mise en œuvre de la production. En d'autres termes, « si l'organisation a réussi à se constituer en interlocuteur obligatoire, car elle est seule à pouvoir répondre à la demande que le relais exprime, le relais se trouve en fait intégré par l'organisation, donc dépendant, donc en situation d'infériorité²³⁸ ». En fin de compte, le comportement de la grande firme est aussi violent que le comportement du pirate. Michel Crozier et Erhard Friedberg en parlent comme d'une « colonisation des relais²³⁹ ». Le cadre va donc procéder à la destruction de cette technologie qui symbolise son désaccord avec sa situation d'infériorité. Cette destruction, immatérielle, « a pour fonction d'apaiser les violences intestines, d'empêcher les conflits d'éclater²⁴⁰ ». La standardisation du traitement de l'information tend à aplanir les différences qui font les personnalités des acteurs, voire des petites firmes qui agissent dans le sillage de la grande organisation. « Or, ce qu'annonce pour un groupe social la perte des différences, c'est l'escalade de la violence{ XE "violence" }; car, si tous les hommes ont les mêmes désirs, ils deviennent des rivaux mimétiques, voués à des vengeances symétriques, affrontés dans des conflits sans fin. La seule façon d'échapper à l'enfer des représailles en chaîne, c'est de répondre à la question : qui a commencé²⁴¹ ? » Réponse : c'est la « technologie ». La violence, trop longtemps

²³⁶ Michel FOUCAULT, *L'archéologie du savoir*, Chapitre VI, La formation des stratégies, Gallimard, 1969, p. 90. Déjà cité à propos des technologies d'information de la firme dont la production est, elle aussi, une forme d'appropriation du discours.

²³⁷ Nous empruntons ce discours à l'imaginaire; l'arrestation d'une partie des membres du C.C.C. n'ayant pas été prolongée par une étude approfondie de leur mouvement, et de ce qu'ils avaient à dire.

²³⁸ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, page 171.

²³⁹ Michel CROZIER, Erhard FRIEDBERG, *Op. Cit.*, p. 171.

²⁴⁰ René GIRARD, *La violence et le sacré*, Editions Grasset, Collection Pluriel, 1972, p. 27, « la fonction du sacrifice ».

²⁴¹ Mona OZOUF, Article à propos de *La violence et le sacré*, paru dans *Le Nouvel Observateur*, le 12 Février 1973.

contenue, est transférée sur une victime émissaire qui a plus une fonction de symbole, que de réelles raisons d'être détruite. « Que toute société humaine ne puisse donc survivre qu'au prix d'un mécanisme d'expulsion de la violence{ XE "mécanisme d'expulsion de la violence" }, et que ce mécanisme fonctionne sous nos yeux, voilà ce qu'il devrait être interdit d'ignorer plus longtemps ²⁴² ». Faire du système d'information de la firme une « forteresse » contre l'agression, c'est réagir beaucoup trop violemment; a fortiori, si la position d'infériorité de l'agresseur est augmentée par une rétention d'information naturelle à toute hiérarchie. René Girard donne l'avertissement suivant : « Persuadés comme nous le sommes que le savoir est toujours une bonne chose, nous n'accordons qu'une importance minime, ou même aucune importance à un mécanisme, celui de la victime émissaire{ XE "victime émissaire" }, qui dissimule aux hommes la vérité de leur violence. Cet optimisme pourrait bien constituer la pire des méconnaissances. Si l'efficacité du transfert collectif est littéralement formidable, c'est justement parce qu'il prive les hommes d'un savoir, celui de leur violence avec laquelle ils n'ont jamais su coexister ²⁴³ ».

²⁴² Pierre MANENT, Article consacré à *La violence et le sacré*, paru dans *Contrepoint*, n° 14, Juin 1974.

²⁴³ René GIRARD, Op. Cit., p. 125.

CHAPITRE V

La stratégie de l'entreprise en état de veille

5.1. Voir sans être vu

5.1.1. La « prison » des paradigmes

Pour cette seconde partie, nous allons nous placer essentiellement du côté du surveillant, c'est-à-dire du côté de la firme face à son environnement, ou face aux « rébellions » de son personnel. Nous verrons, d'une part, que la stratégie du surveillant n'est de toute façon pas concevable sans une sérieuse prise en compte de la stratégie des surveillés. Et nous montrerons, d'autre part, que c'est à la firme de prendre l'initiative « d'adapter » sa surveillance à l'évolution de son environnement, tout en conservant à l'esprit l'idée que « le rapport à l'environnement ne saurait être réduit à une simple influence extérieure suivie d'adaptation unilatérale ²⁴⁴ ». Nous avons pu remarquer, dans le chapitre précédent, que la compétition industrielle se réalise dans un climat de plus en plus violent. Pour y faire face, les technologies de l'information se sont multipliées dans l'environnement quotidien de l'entreprise. Dans un premier temps, il s'agissait d'être à l'écoute d'un environnement de plus en plus rapide, et ensuite, il fallait, par le biais des normes de transport, de stockage et de traitement de l'information, maîtriser la violence environnante par l'assujettissement des utilisateurs de la technologie. A la fin de ce chapitre, nous avons pu constater que la technologie, à force de contraindre si « innocemment » ses utilisateurs, devenait parfois leur

²⁴⁴ « Il s'agit, en fait, d'un *processus permanent d'échange* à travers lequel une organisation s'ouvre, pour ainsi dire *sélectivement*, au système de pouvoir plus large auquel elle participe, et par lequel elle *intègre* des parties de façon plus ou moins permanente dans *son propre système d'action* pour ainsi pouvoir « l'adapter » à son tour à ses exigences propres », Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, p. 179.

victime *émissaire*, au sens où l'entend René Girard. Nous allons voir maintenant que cette pratique qui consiste à faire d'une technologie l'architecture permettant le transport de l'autorité dans tous les lieux où elle doit s'exercer, correspond à un seul concept, tiré des écrits de Jeremy Bentham²⁴⁵, et que nous appellerons le néopanoptisme. Pour mener à terme l'approche de cette notion, nous commencerons par analyser en quoi un discours dont le déploiement s'effectue dans le cadre d'une norme bien déterminée, appartient autant aux fondateurs de cette norme qu'à l'individu qui s'exprime en s'y référant.

Entre le discours — entendu comme un droit d'expertise et d'initiative dans le jugement — et la pratique, il y a une relation de cohabitation. La pratique est « l'habitat » du discours. Ce qui nous permet de « montrer qu'un changement, dans l'ordre du discours, ne suppose pas des « idées neuves », un peu d'invention et de créativité, une mentalité autre, mais des transformations dans une pratique, éventuellement dans celles qui l'avoisinent et dans leur articulation commune²⁴⁶ ». Ainsi, la maîtrise de la production d'une technologie de l'information, doublée d'un leadership dans l'élaboration du langage qu'utilise cette technologie pour « interagir » avec ses utilisateurs, permet à une grande firme de « bâtir son discours », puis de « l'enseigner » aux firmes auxquelles elle soustraite les modules de sa production. Les manuels d'utilisation d'une machine de production intégrée par l'informatique²⁴⁷, le service de formation qui est inclut dans l'offre technologique, le contrat de maintenance, sont autant de *vecteurs* pour la diffusion de ce discours. Le cadre de référence que suggère la technologie de l'information est-il ainsi soutenu, dans le temps, par une combinatoire de prestations indissociables du partenariat entre les firmes. Si bien qu'un gestionnaire, devant préparer la mise en place d'un nouveau système d'information, pourrait très bien s'écrier, en empruntant ces termes à Michel Foucault²⁴⁸ : « *Qui parle ?* Qui, dans l'ensemble des individus parlants, est fondé à tenir cette sorte de langage ? *Qui en est titulaire ?* (...) Quel est le statut des individus qui ont — et eux seuls — le droit réglementaire ou traditionnel, juridiquement défini ou *spontanément accepté*, de proférer un pareil discours ? ». C'est à partir de ce moment là, c'est-à-dire à partir du moment où l'on assimile dangereusement la qualité du discours à celui qui le prononce, que le système commence à affaiblir sa position transactionnelle{ XE "position transactionnelle" }. S'il n'y a pas, au sein de la firme, la compétence nécessaire pour évaluer quels sont les enjeux dissimulés par une offre technologique, il vaut mieux, dans un premier temps, acquérir cette compétence plutôt que cette technologie. Ce que Michel Foucault décrit pour la médecine du XIX^e siècle²⁴⁹ est tout à fait

²⁴⁵ Jeremy BENTHAM, *Le panoptique*, Réédition de Belfond, 1977.

²⁴⁶ Michel FOUCAULT, *L'archéologie du savoir*, Gallimard, 1969, p. 272.

²⁴⁷ Computer Integrated Manufacturing.

²⁴⁸ Michel FOUCAULT, Op. Cit., p. 68.

²⁴⁹ Dans le Chapitre IV de *L'archéologie du savoir*, Michel FOUCAULT démontre que tout ce que l'on peut trouver dans les discours des médecins du XIX^{ème} siècle, est fonction de diverses modalités énonciatives, comme le statut du médecin, par exemple.

transposable, de nos jours, à l'expertise technologique dans l'industrie. Les diverses situations que peut occuper le sujet du discours vont ainsi se redéfinir « avec *l'organisation d'un champ perceptif tout autre (...)*, et avec la mise en place de nouveaux systèmes d'enregistrement, de notation, de description, de classement, d'intégration dans des séries numériques et dans des statistiques, avec l'institution de nouvelles formes d'enseignement, de mise en circuit des informations, de rapport avec les autres domaines théoriques (sciences et philosophie) et avec les autres institutions (qu'elles soient d'ordre administratif, politique ou économique) ²⁵⁰ ». A l'image de la médecine décrite par Foucault, la technologie ne peut revendiquer un « pouvoir thérapeutique » pour les organisations qu'à travers son statut, son établissement dans la norme statutaire de la collectivité.

Pour accéder à cette « crédibilité statutaire », on se réclama souvent de la démarche scientifique. C'est ainsi qu'à travers différents paradigmes, les technologies de l'information de la firme ont réussi à *unifier leur discours*, à créer un seul et même paradigme que différentes approches du pouvoir avaient, pendant près de trente ans, essayé de morceler ²⁵¹. Entre l'invention de l'IBM 1401 en 1959, et les réseaux complexes liant machines-outils et systèmes experts dans des systèmes à tâches réparties, le nombre d'informations élémentaires (*bits*) est parfois passé de 1000 à 100 000 000 au cm². Dans le même temps, la vitesse de traitement de l'information augmentait dans un rapport de 1 à 500. Ceci a offert *deux possibilités* aux détenteurs de la technologie. D'une part, une possibilité physique de pouvoir déplacer, puis multiplier les centres de traitement de l'information, et de le faire dans des temps de plus en plus courts. D'autre part, une possibilité politique d'accroître leur pouvoir par la quantité d'information détenue et traitée.

Le premier paradigme des technologies de l'information fut par conséquent celui de la centralisation{ XE "centralisation" }. D'une part, la technologie ne permettait pas de décentraliser efficacement, et d'autre part, la croissance économique des années 1960 a renforcé la compétition, *mais aussi la suspicion*. La structuration des systèmes d'information n'est pas non plus étrangère aux formes d'organisations sociales. L'industrie vit encore, en 1960, dans la « nostalgie » de « l'analyse rationaliste étroite, presque mécaniste, des Taylor et des Fayol, qui dominait les années 1920 ²⁵² ». Elle aimerait encore appliquer ces règles disciplinaires qui valorisent l'autorité, comme celle de « la force centrifuge (qui) l'emporte quand la force centrale s'affaiblit ²⁵³ ». Pourtant, dès l'après-guerre, « la réaction anti-taylorienne qui s'est manifestée aussi bien sur le plan

²⁵⁰ Michel FOUCAULT, Op. Cit., P; 71.

²⁵¹ Pour une définition du paradigme, et une description détaillée de ce morcellement, puis de cette unification du paradigme de l'information, se reporter Partie I, Chapitre II, Hypothèses de travail : « Le nouveau paradigme de l'information ».

²⁵² Michel CROZIER, *Le phénomène bureaucratique*, Editions du Seuil, 1963, p. 177.

²⁵³ Henri FAYOL, *Administration industrielle et générale*, Dunod, 1916, p. 81.

littéraire que sur le plan politique et social ²⁵⁴ » annonçait déjà la menace qui pesait sur le pouvoir centralisateur, et sur son paradigme des technologies de l'information. En fin de compte, la technologie n'aura contrecarré que très temporairement, « l'effort scientifique des psychologues, des sociologues, des pédagogues et des expérimentateurs sociaux ²⁵⁵ » à renouveler l'approche du management.

Deux facteurs essentiels vont suggérer, voire provoquer, pendant plus de vingt ans, les remises en cause successives des trois paradigmes des technologies de l'information. Il s'agit d'une part, de l'acceptation de l'autorité, et d'autre part, de son partage. Moins le pouvoir centralisateur sera accepté, et plus il devra se partager. En 1970, IBM crée la série 370. Le paradigme de l'interactivité — encore très partielle, il est vrai — construit son développement autour de la mini-informatique. La possibilité physique d'accéder aux informations, encore centralisées, en secondes plutôt qu'en heures, permet d'en partager le traitement. C'est la première concession de l'autorité. Ce sera le début d'une série d'ajustements successifs qui vont bientôt remettre en cause le *concept même de « centralisation »*. L'après 1968 n'a pas encore ôté leur pouvoir aux experts, notamment aux analystes qui développent, à cette époque, des applications totalement hermétiques à l'utilisateur final. L'autorité qui se partage désire garder le dernier mot, celui d'un propriétaire du discours, au sens de Foucault. La psychologie sociale avait pressentie, avec dix années d'avance, ce tournant de l'organisation industrielle. Dès 1960, « les problèmes du pouvoir tendent de plus en plus à passer au premier plan des études sur les organisations ²⁵⁶ ».

Avec la crise économique qui débute en 1973, l'ensemble des ressources de la firme doivent être optimisées. Il n'est plus question de protéger le pouvoir par une centralisation coûteuse, ou par une interactivité qui veut bien concéder le traitement, ou l'utilisation des données, sans en céder la propriété. Parallèlement, en 1972, IBM vient de généraliser l'utilisation des mémoires virtuelles, et annonce d'autres innovations dans ce même domaine. Pour renforcer leur compétitivité, les firmes commencent à partager l'autorité, d'abord d'une façon fonctionnelle, puis bientôt au niveau de chaque individu. Les notions de participation et de motivation entrent dans la pratique courante du management. La société de consommation, depuis la fin des années 1960, avait achevé de « glorifier » l'individu. Tous les éléments étaient en place pour une seconde remise en cause. Entre le premier et le second des paradigmes des technologies de l'information, la transition avait été douce, car, finalement, l'interactivité nécessitait toujours, pour le moment, l'utilisation d'ordinateurs centraux. Si bien que les deux paradigmes avaient coexisté, avec leurs défenseurs respectifs. Mais la révolution qui se préparait allait connaître une remise en question plus profonde, voire une crise. La multiplication des centres de traitement avait fait « exploser » le marché du logiciel. La matière grise commençait déjà à reprendre le dessus sur le micro-

²⁵⁴ Michel CROZIER, *Op. Cit.*, p. 178.

²⁵⁵ Michel CROZIER, *Op. Cit.*, p. 178.

²⁵⁶ Michel CROZIER, *Op. Cit.*, p. 183.

processeur, quand le micro-ordinateur, symbole de l'individualisation, fait son apparition. Le Japon — qui avait bien suivi la leçon du standard{ XE "standard" } donnée par les Etats-Unis, quand ils dominaient les deux premiers paradigmes — décide de devenir les propriétaires de ce nouveau discours. Or, qu'est-ce que l'individualisation sinon la possibilité d'avoir, chez soi, la capacité de traitement d'informations que l'on avait auparavant au sein de la firme ? Pour transporter la technologie sur les lieux d'activité de l'individu, il fallait la miniaturiser. C'était là l'enjeu de ce nouveau paradigme. La force du Japon est de l'avoir compris avant les autres, peut-être, justement, parce que son fonctionnement groupal si différent de notre individualisme, lui permettait d'en saisir toute la particularité.

Les trois paradigmes coexistent avec difficulté pendant la décennie 1980. L'individualisation{ XE "individualisation" } a gagné l'informatique de gestion. Le paradigme centralisateur a encore ses défenseurs, notamment auprès des pouvoirs politiques, ou des institutions financières, pour lesquels le *contrôle* de l'information est une question de *suprématie*. De plus, toute une génération de cadres, les baby-boomers, ont été formés dans le cadre de ce paradigme. Les langages qu'ils ont appris, le Fortran, mais surtout le Cobol, sont utilisés à grande échelle. Vingt ans après, on ne peut plus envisager de réécrire l'ensemble des chaînes de traitement de l'information qu'utilisent les multinationales. On s'aperçoit alors que l'on devient vite « prisonnier » d'un paradigme. L'école Cobol va défendre ses outils. L'interactivité partielle qu'offre les mini-ordinateurs — car il y a toujours, entre l'utilisateur final et la technologie, le pouvoir de l'expert — créera aussi ses adeptes, puis ses « prisonniers ». D'une part, il est difficile, financièrement, d'envisager la refonte complète d'un système. D'autre part et surtout, il faut changer les formations, les mentalités, voire la pratique même de la gestion et le comportement vis-à-vis de l'information. L'autorité, qui a concédé le traitement décentralisé de l'information, encourage, bien malgré elle, la créativité. D'autres langages sont créés. Avec l'individualisation, l'environnement est encore plus hétérogène, plus atomisé, de moins en moins ouvert à une régulation unilatérale. Et « plus le système de relations de pouvoir et de négociation est complexe et dynamique et plus le contrôle social tend à être opéré consciemment par la direction au lieu de l'être par la pression du milieu ²⁵⁷ ». Au fur et à mesure que les paradigmes se font moins « prisons », c'est-à-dire plus ouverts au partage de l'autorité, le pouvoir tend à renforcer d'autres pressions pour contrôler des sources d'incertitude de plus en plus nombreuses. Le jeu de la violence est entamé. Les belles années de la sécurité informatique commencent. Nous sommes au début de la décennie 1990. En fait, tous les domaines de l'économie industrielle et du management ont été, peu ou prou, influencés par l'évolution de ces trois paradigmes. La notion de « quasi-intégralité verticale » en témoigne. Le pouvoir industriel ne s'embarrassait pas de compromis dans l'après-guerre. Il en avait les moyens. Il maîtrisait l'information au sein d'un paradigme centralisateur tout à son avantage. Le fait que ce même pouvoir préfère, aujourd'hui ménager les sensibilités — et parler de « co-traitance » plutôt que de

²⁵⁷ Michel CROZIER, *Op. Cit.*, p. 212.

« sous-traitance » — tend à prouver, qu'au travers des derniers paradigmes, l'information mieux répartie a rééquilibré les relations de pouvoir. C'est la fin du paradigme qui « emprisonne » ses chercheurs et ses praticiens, dans des relations de pouvoir stabilisées. La bataille actuelle pour les standards dans le domaine des technologies de l'information de production — les Computer Integrated Machines et autres Office Systems — témoigne, quant à elle, d'une prise de conscience de cette situation. On voudrait appliquer la « recette » qui fonctionnait si bien dans le cadre d'un paradigme centralisateur, ou être au moins propriétaire des « micros » si l'on est obligé de partager la propriété du discours.

5.1.2. Atouts et méfaits d'un paradigme unique

Trois paradigmes qui, nous l'avions annoncé, n'en feraient bientôt plus qu'un. Car, enfin, quel était la contrainte essentielle à leur unification ? Tout d'abord, il y avait, bien sûr, leurs défenseurs respectifs. Mais, surtout, il était techniquement impossible de faire communiquer entre eux des gros systèmes, des micro-ordinateurs, des mini-systèmes, voire des « machines-outils ». Il y avait la stratégie des constructeurs, et la lutte pour le standard universel, qui faisaient qu'une machine DEC s'entendait plus ou moins bien, voire pas du tout, avec des machines IBM ou Apple. Dans l'entreprise, on supportait de plus en plus mal cette situation. L'ancien patron préférait IBM, et le nouveau, c'était DEC. Et comme à ce moment-là, on réorganisait la gestion financière, ce serait DEC. Pourtant, la compétition rend aujourd'hui interdépendants la finance et la gestion de la production, la recherche et le marketing. Comment profiter de cette interdépendance si chacune de ces fonctions a son propre système d'information ?

Il y a eu, bien sûr, les firmes entièrement équipées par IBM, et les firmes entièrement équipées par DEC. Mais, la nouvelle compétition, ce sont aussi les partenariats{ XE "partenariats" }, et la création de filiales communes{ XE "filiales communes" }. Et le jour où il faut réunir deux équipes de deux firmes différentes : comment brancher un IBM sur un DEC ? Des spécialistes ont vu le jour. Et à force de traiter toujours les mêmes problèmes, — eu égard au nombre croissant d'absorptions, de fusions, d'acquisitions, de partenariats, de joint-ventures — ces spécialistes ont réussi à mettre au point des combinatoires de technologies génériques permettant l'interconnexion de machines totalement différentes. Des sociétés comme Novell, ou 3Com, commercialisent de telles combinatoires tant au niveau du software, que de l'hardware. Cette dernière, 3Com, sûr de ce nouveau paradigme, affiche clairement ses ambitions : être le leader mondial²⁵⁸ du réseau d'entreprise avec un chiffre d'affaires d'un milliard de dollars en 1992. Mais ce paradigme unique ne s'étend pas qu'à l'informatique d'entreprise. L'information prend une place de plus en plus importante à tous les niveaux de la firme : ce sont les *niveaux d'information*{ XE "*niveaux d'information*" } qui hiérarchisent les positions des

²⁵⁸ Selon la société d'étude DATAQUEST, ce marché devrait connaître une croissance annuelle mondiale de 40% dans les cinq prochaines années, et atteindra 8,8 milliards de dollars en 1992.

firmes dans des quasi-intégrations verticales. C'est encore la qualité du traitement de l'information qui conditionne la performance d'une machine à commande numérique, et bientôt d'une C.I.M. C'est la « désinformation » qui détruit l'image de marque du concurrent et lui fait perdre 2 à 3 points de parts de marché. C'est la qualité de la gestion de l'information scientifique et technique qui conditionne, sinon la créativité{ XE "créativité" }, au moins la performance d'un bureau d'études. Le recours à la conception assistée par ordinateur est même parfois le « ticket d'entrée » d'un secteur, comme celui de l'aéronautique. Si bien que l'information est devenue un élément structurant de la firme. L'interstructuration de la firme et de son environnement, que décrivent Crozier et Friedberg ²⁵⁹, c'est avant tout une modification simultanée de la quantité d'informations à appréhender, et du comportement des acteurs vis-à-vis d'elles. Leur comportement va désormais s'articuler autour de leur niveau d'information, de leur aptitude à les traiter, de leur capacité à les stocker, et de leur rapidité à les diffuser. Le gestionnaire, l'ingénieur ou le financier ne pourront plus se réfugier derrière leurs statuts. Ils devront prouver leur compétence dans le traitement de l'information, et lors de sa valorisation. A un échelon au-dessus, la firme toute entière devra intégrer à sa stratégie une politique générale de l'information.

L'atout d'un paradigme unique est donc de favoriser l'amélioration des comportements professionnels vis-à-vis de l'information. En remettant en cause la propriété statutaire du discours ²⁶⁰, ce paradigme va tous nous contraindre à nous positionner vis-à-vis de l'information, puis à agir en dehors de toute protection statutaire. Mais son méfait est sans aucun doute d'offrir à chacun *la possibilité de libérer sa violence dans des proportions encore inégalées*. Les exemples cités par Lamère, Leroux et Tourly en témoignent ²⁶¹. Un seul homme, dans un tel paradigme, peut, par exemple, effectuer la « copie de la nomenclature de tarification d'un grand contrat à l'export au profit d'un concurrent qui emporte le marché ²⁶² (la perte est de l'ordre de 15 MF) ». Ou encore, il peut, mettant à profit l'omniprésence des systèmes d'information dans le fonctionnement de la firme, « dans une entreprise spécialisée en recherche minière », modifier un programme « de telle sorte qu'il produise un rapport à forte probabilité de gisement permettant ensuite une série d'opérations mobilières dont l'ampleur est estimée à 80 MF ²⁶³ ». Et ce qui prouve encore l'étendue de ce paradigme, c'est ce cas effrayant de détournement de l'information : « Modification criminelle des seuils d'alarme d'une centrale informatique de surveillance de malades gravement atteints dans un hôpital, entraînant deux décès ²⁶⁴ ». La manipulation{ XE

²⁵⁹ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, pages 156-162.

²⁶⁰ Voir à ce propos Michel FOUCAULT, *L'archéologie du savoir*, Gallimard, 1969, pp. 55-84.

²⁶¹ Jean-Marc LAMÈRE, Yves LEROUX, Jacques TOURLY, *La sécurité des réseaux informatiques*, Bordas, 1989.

²⁶² J.M. LAMÈRE, Y. LEROUX, J. TOURLY, *Op. Cit.*, p. 97.

²⁶³ J.M. LAMÈRE, Y. LEROUX, J. TOURLY, *Op. Cit.*, p. 92.

²⁶⁴ J.M. LAMÈRE, Y. LEROUX, J. TOURLY, *Op. Cit.*, p. 95.

"manipulation" } de l'information, dans un environnement où tout est structuré pour la favoriser — jusqu'aux mentalités — constitue le plus grand danger d'un tel paradigme. Il pourrait devenir, si la vigilance et la responsabilité de chacun se relâchaient, un « paradigme de la violence libérée ». La pratique de l'intelligence d'entreprise, dans un tel contexte, nécessite une gestion rigoureuse des systèmes d'information, mais également une réelle éthique professionnelle des équipes qui recueillent l'information et une vigilance accrue des instances coordinatrices de la veille.

5.1.3. Le néopanoptisme

C'est justement de vigilance dont parlent les « nostalgiques » de la technocratie omnipotente²⁶⁵. Ils voudraient surveiller, protéger le discours technologique, et même renforcer la discipline. Afin de d'atteindre ces trois objectifs simultanément, ils vont mettre en œuvre un ensemble de nouvelles technologies de l'information, dites *panoptiques*, pour appréhender leur environnement dans l'unique perspective de « voir sans être vu ». C'est une idée technocrate, non pas au sens péjoratif, mais au sens premier du mot : une technologie, ou une combinatoire de technologies, va permettre à un groupe déterminé d'individus — ceux qui maîtrisent ces combinaisons — d'atteindre le pouvoir. Leur préoccupation est souveraine : « L'ordre est le père de toute prospérité ²⁶⁶ ». A l'instar des Bentham, Bergery, et autres Fayol, il ne saurait y avoir pour eux d'enjeux économiques sans aucune précaution disciplinaire, c'est-à-dire *sans sujétion*{ XE "*sujétion*" }. Et si l'assujettissement{ XE "*assujettissement*" } peut être obtenu autrement qu'à la suite d'un « face à face » pénible, on utilisera un intermédiaire suffisamment « précis, scientifique et impersonnel ²⁶⁷ » pour dissimuler dans l'utilisation de la technologie son véritable enjeu. « Tout moyen d'atténuer la signification implicite d'une action en facilite l'accomplissement », écrivait Milgram à propos de sa machine à donner des chocs électriques qui servit toutes ses expériences ²⁶⁸. Là encore, le rôle joué par la technologie n'a pas été assez souligné. La technologie, en fournissant des formats standardisés de résolution de problèmes, à l'instar d'un paradigme, est source de réconfort psychologique pour un individu aux prises avec un conflit moral. Le jeu mécanique, presque nerveux, de la manipulation des touches d'un clavier canalise

²⁶⁵ Telle qu'on a pu la pratiquer sous l'égide d'un machinisme régulateur de toutes les instances humaines qui l'environnaient. Voir à ce propos W. TAYLOR, *La Direction des Ateliers*, Dunod, 1919, et également H. FAYOL, *Administration industrielle et générale*, Dunod, 1920.

²⁶⁶ C.L. BERGERY, *Economie industrielle*, Tome III, « La conduite d'une fabrique », Metz, 1831, p. 51.

²⁶⁷ Stanley MILGRAM, *Soumission à l'autorité*, Calman-Lévy, 1982, « Tension et désobéissance, les amortisseurs de tension », p. 195.

²⁶⁸ « Le stimulateur de chocs lui-même joue un rôle très important. Appareil précis et impressionnant, il crée une discontinuité très nette entre la facilité de manipulation de ses trente leviers de commande et la force des décharges qu'il administre à la victime », Stanley MILGRAM, *Op. Cit.*, p. 195.

la violence, évite le doute intérieur, et son extériorisation. Seul celui qui est assez familier avec la technologie de l'information qu'il utilise, ne sera pas effrayé par cet « environnement formaté » dans lequel doit évoluer sa pensée, car les formats, justement, il sait les modifier. Il détient là le seul moyen de se libérer de cette tension normalisatrice : détruire le format, voire le détourner. Son expertise sera pour lui le moyen d'exprimer sa désapprobation, « peut-être le premier stade d'un conflit progressif (avec le pouvoir), et un moyen de sonder ce dernier ²⁶⁹ ». Le stade suivant, c'est la désobéissance, le piratage, le détournement d'informations. Face à une telle menace, on a envie de tout voir. Mais on voudrait aussi que la technologie nous remplace dans cette inspection fort peu démocratique. On n'aimerait pas être vu dans une telle situation. De là naît l'idée d'un *nouveau panoptisme*.

Rappelons brièvement le principe du panoptique de Bentham : « à la périphérie, un bâtiment en anneau; au centre, une tour; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau. Le bâtiment périphérique est divisé en cellules, dont chacune traverse toute l'épaisseur du bâtiment. Ces cellules ont deux fenêtres : l'une ouverte vers l'intérieur, correspondant aux fenêtres de la tour; l'autre, donnant sur l'extérieur permet à la lumière de traverser la cellule de part en part. Il suffit alors de placer un surveillant dans la tour centrale, et dans chaque cellule d'enfermer un fou, un malade, un condamné, un ouvrier ou un écolier. Par l'effet de contre-jour, on peut saisir de la tour, se découpant dans la lumière, les petites silhouettes captives dans les cellules de la périphérie. En somme, on inverse le principe du cachot; la pleine lumière et le regard d'un surveillant captent mieux que l'ombre, qui finalement protégeait ²⁷⁰ ». Transposé à l'usine, le modèle panoptique devient plus simplement celui de *l'enfermement*, et du regard constant de l'autorité sur les ouvriers. Un modèle qui, pour être « hautement symbolique aux débuts de l'industrialisation, devient, plus que jamais, par les contradictions qu'il engendre, *une contrainte*. L'enfermement, significatif au départ d'un coup de force de la mise au travail ²⁷¹, devient significatif de l'existence de *forteresses ouvrières* ²⁷² ». Et si chacun des individus surveillés prend conscience, que, finalement, dans cette tour, il n'y a qu'un seul regard, alors, tous se soulèveront. Le surveillant, derrière ses jalousies, pourra bien regarder où il voudra. Il pourra surveiller qui il veut. Peu importe, puisqu'ils viennent *tous ensemble* de se soulever. La possibilité d'être identifiés par ce regard omniprésent n'a plus

²⁶⁹ Stanley MILGRAM, *Op. Cit.*, p. 200.

²⁷⁰ Michel FOUCAULT, *L'oeil du pouvoir*, in *Le Panoptique*, Réédition de Belfond, 1977, page 10.

²⁷¹ « Discipliner par et pour le travail, par et pour la production : tel est le discours obsessionnel de Bentham, apôtre et témoin de ce gigantesque effort de mise au travail - au pas, à l'heure, à la cadence - qui accompagne, ou même sans doute précède et permet l'industrialisation », Michelle PERROT, *L'inspecteur Bentham*, in *Le Panoptique*, Réédition de Belfond, 1977, p. 216.

²⁷² J.P. DE GAUDEMAR, *Usines et Ouvriers, figures d'un nouvel ordre productif*, Maspéro, 1980, p. 17.

beaucoup d'importance : ils sont *tous* coupables. Le lecteur, ici, va s'inquiéter. Le panoptisme n'est même pas présenté, qu'il est déjà réfuté.

Cette réfutation n'est que le contrepoint de notre développement. Ce soulèvement général, qui rend inopérant le panoptique, n'a qu'une seule cause : la prise de conscience collective. Ce qui fait l'échec de la prison benthamienne, c'est que son principe est *évident*, tout autant pour le surveillant que pour les prisonniers. Chacun sait, enfermé dans cette machine du pouvoir, qu'elle fonctionne sous le joug de l'aléa et de la visibilité. Chaque prisonnier sait, qu'à tout moment, il est visible. Chacun d'eux sait également que l'aléa de n'être pas surveillé, s'il existe, est très faible eu égard à l'architecture. Et pourquoi le savent-ils ? Ils le savent, parce qu'à l'instar du surveillant, les surveillés, eux aussi, voient la machine qui les emprisonnent. Et plus ils la voient, et plus ils prennent conscience : ils ne sont pas seuls à être emprisonnés. Le surveillant est prisonnier de son regard, de sa position centrale. Si tous se soulèvent, cette architecture ronde fera l'écho de leur colère. L'économie du coût de la surveillance — c'est-à-dire l'utilisation d'un seul homme là où il en fallait cent — diminue de plus belle le pouvoir de la répression{ XE "répression" }. Moins de surveillants, certes, mais autant d'hommes en moins pour punir la rébellion.

Poussons plus loin encore l'utopie : imaginons que le panoptique tout entier, ait été invisible. Les prisonniers auraient été enfermés dans des cercles tracés à la craie sur le sol. Rien n'aurait pu leur faire penser que l'autorité était là, tout près, en train de les surveiller. Mais, chaque fois que l'un d'eux ferait un pas en dehors du cercle, il tomberait, foudroyé²⁷³. Bien qu'elle fasse partie de l'imaginaire, voilà une invention qui est bien plus mystérieuse et terrifiante que celle de Bentham. Pourtant, là aussi, il ne s'agit que « d'une simple idée d'architecture ²⁷⁴ ». Seulement, cette architecture n'est pas visible. Les surveillés n'ont pas à subir la tension liée à sa présence. Rappelons nous : « tout élément susceptible de réduire le rapport psychologique entre l'action du sujet et sa conséquence diminue également le degré de tension ²⁷⁵ », et par là même, le risque de désobéissance. Selon Milgram, pour maintenir l'individu dans la sujétion, il suffirait donc d'identifier la source des tensions qu'il subit. Si l'architecture du pouvoir est trop pesante, trop visible, il faut la « gommer ». Plus d'architecture, plus de malaise. Sortir du cercle, c'est simplement sortir de la norme. La punition se justifie d'elle même. « Le Normal s'établit comme principe de coercition (...) Aux marques qui traduisaient des statuts, des privilèges, des appartenances, on tend à substituer ou du moins à ajouter tout un jeu de degrés de normalité{ XE "normalité" }, (...) qui ont eux-mêmes un rôle de classification, de hiérarchisation et de distribution des rangs ²⁷⁶ ». Il s'agit ici d'encourager la *dérobade du surveillé, ou le refus de*

²⁷³ Les références tacites au mythe d'Abel et Caïn ne sont pas fortuites.

²⁷⁴ Jeremy BENTHAM, *Le Panoptique, mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maisons de force*, Imprimé par Ordre de l'Assemblée Nationale, à Paris, Imprimerie Nationale, 1791, p. 5.

²⁷⁵ Stanley MILGRAM, *Soumission à l'autorité*, Calman-Lévy, 1982, p. 195.

²⁷⁶ Michel FOUCAULT, *Surveiller et punir*, Gallimard, 1975, p. 186.

l'évidence, qui « réduit la tension du sujet (...) en lui fournissant une interprétation plus consolante des faits ²⁷⁷ ». Ce n'est plus à l'autorité qu'il se soumet, mais à la norme de fonctionnement d'une machine. La consolation est immédiate puisque cette norme est, de toute façon, *nécessaire* pour pouvoir travailler en utilisant tous le même langage. Finalement, une architecture invisible du pouvoir, est-ce vraiment une utopie ?

Ne parle-t-on pas « d'architecture » d'un système d'information ? Et cette architecture est-elle visible aux yeux de ses utilisateurs ? Si le bien le plus échangé de la décennie est l'information, l'intéressant est avant tout « de comprendre que *ce qui est ainsi véhiculé*, et par là même *transformé* dans ses formes d'existence, c'est le rapport social ²⁷⁸ ». En empruntant le vocabulaire de Crozier et de Friedberg ²⁷⁹, on pourrait dire que l'interstructuration de la firme et de son environnement — de la technologie surveillante et de ses surveillés — n'est pas du tout innocente. Elle est certes le résultat d'une négociation entre les deux parties, mais d'une « négociation » pendant laquelle l'information est distribuée aux surveillés, avec la technologie du surveillant. C'est cela le néopanoptisme : supprimer la visibilité de l'architecture, pour voir sans être vu, en poussant cette expression à son paroxysme, tant dans son principe que dans l'utilisation de technologies de plus en plus complexes. Il est pourtant « encore assez rare de rencontrer des dirigeants d'entreprise qui voient dans l'informatique autre chose qu'un outil pour la gestion des opérations administratives courantes ²⁸⁰ ». Ce que nous allons présenter n'est donc pas lié à l'observation d'une pratique très répandue. Il s'agit plutôt d'une prospective, à l'instar du panoptique, pour montrer que ce qui est dans le domaine du possible n'est pas forcément souhaitable sans une sérieuse réflexion au préalable.

Organisons une entreprise en réseau. A chaque nœud de ce réseau, un individu, ou un contrat à remplir. Pour lier tous ces individus entre eux, des connexions informatiques, et même parfois des liaisons satellites. Ce réseau pourra avoir deux architectures. La première sera apparente, et même montrée volontairement. Tel pourrait être le discours officiel : « Chez nous, tous les ordinateurs sont connectés les uns aux autres. Nous voulons encourager l'initiative et faire circuler l'information ». Une seconde architecture serait, quant à elle, totalement *centralisée*, et *invisible*. Il s'agirait en fait d'un réseau de programmes assurant le guidage des informations vers un seul nœud. Individualisation et « libre arbitre » peuvent très bien cohabiter, grâce à l'anonymat de la technologie, avec centralisation et contrôle systématique. Nous avons montré qu'une pression psychologique trop voyante constitue l'expression d'une violence. Et que celle-ci ne fait que provoquer la rébellion des prisons benthamiennes, ou encore,

²⁷⁷ Stanley MILGRAM, *Op. Cit.*, p. 197.

²⁷⁸ J.P. DE GAUDEMAR, *Op. Cit.*, p. 19.

²⁷⁹ Michel CROZIER, Erhard FRIEDBERG, *L'acteur et le système*, Editions du Seuil, 1977, pages 156-162.

²⁸⁰ Humbert LESCA, *Système d'information pour le management stratégique de l'entreprise*, McGraw Hill, 1986, p. 111.

encourager la « crise sacrificielle{ XE "crise sacrificielle" }²⁸¹ » de la criminalité informatique. C'est pourquoi ces programmes délateurs sont des programmes cachés. On pourrait même envisager de construire les machines en prévoyant, dans leur mémoire permanente, ce genre de sophistication. Nous sommes loin ici du principe de Beccaria : « Que l'idée du supplice soit toujours présente au cœur de l'homme faible et domine le sentiment qui le pousse au crime²⁸² ». On ne met plus en face de l'idée du crime, l'image terrifiante de la punition. On essaye plutôt d'éloigner de l'esprit du criminel potentiel *le mobile* de ses crimes éventuels. Le réseau de communication de la firme, détourné de son utilisation originale, devient « une technologie du pouvoir propre à résoudre les problèmes de surveillance²⁸³ ».

Mais on peut également sortir du cadre interne de la firme, et envisager une même architecture pour un système d'information liant entre eux les partenaires d'une quasi-intégration verticale. La surveillance serait d'une toute autre nature. Il ne s'agirait plus de programmes cachés dans un système d'information, mais simplement d'un déséquilibre dans les niveaux d'information qui forcerait l'ensemble des relais à participer, bon gré mal gré, à la centralisation de l'information. Et pour les y aider, les technologies de l'information — déployées en étoile autour de la grande firme — vont transporter, synthétiser, analyser et valoriser l'information à leur place. Sous le prétexte d'une meilleure information, la surveillance va se déployer dans tous les espaces d'activités des firmes ainsi intégrées. Dans cette perspective, le néopanoptisme n'est-il pas un moyen de réduire les coûts opératoires du pouvoir ? « Le pouvoir, en effet, ne s'exerce pas sans qu'il en coûte quelque chose. Il y a évidemment le coût économique, et Bentham en parle : combien faudra-t-il de surveillants ? Combien, par conséquent la machine coûtera-t-elle ? Mais il y aussi le coût proprement politique. Si on est très violent, on risque de susciter des révoltes; ou bien, si on intervient de façon trop discontinue, on risque de laisser se développer dans les intervalles des phénomènes de résistance et de désobéissance d'un coût politique{ XE "coût politique" } élevé²⁸⁴ ».

Quelle leçon pour l'économie industrielle ! La stratégie du surveillant commence à se dessiner. La grande firme ne doit, en aucun cas, *rompre la discontinuité* de ses relations avec ses sous-traitants et ses partenaires. Elle doit toujours paraître la plus conciliante possible, c'est-à-dire que sa présence, si elle est permanente, doit être des plus discrètes. La démarche est intrinsèquement panoptique. C'est un « regard qui surveille et que chacun, en le sentant peser sur lui, finira par intérioriser au point de s'observer lui-même²⁸⁵ ». La seule

²⁸¹ Selon une terminologie empruntée à René GIRARD, *La violence et le sacré*, Editions Grasset, Collection Pluriel, 1972.

²⁸² BECCARIA, *Des délits et des peines*, édition de 1856, p. 119.

²⁸³ Michel FOUCAULT, *L'oeil du pouvoir*, in *Le Panoptique*, Réédition de Belfond, 1977, page 11.

²⁸⁴ Michel FOUCAULT, *Op. Cit.*, p. 19.

²⁸⁵ Michel FOUCAULT, *Op. Cit.*, p. 19.

différence est que le néopanoptisme industriel multiplie les écrans entre le surveillant et les surveillés, au point d'en faire oublier le surveillant lui-même, avantageusement remplacé par une technologie dont les *connotations positives* — compétitivité, réduction des coûts, fierté pour le sous-traitant d'être reconnu pour le niveau de qualité de sa production — font oublier la dépendance. Le « regard » que le surveillé intériorise n'est pas directement celui de la grande firme — loin de nous cette idée — mais plutôt celui de la compétitivité. Si bien, qu'effectivement, le discours{ XE "discours" } de la grande firme sur la technologie et la compétitivité peut devenir très vite un discours motivé par des ambitions panoptiques.

Le contrôle de la qualité{ XE "qualité" }, la concertation dans l'approche des marchés, ou même, la conduite commune d'un programme de recherche et développement, peuvent devenir des média de ce néopanoptisme. Poussé à son paroxysme, l'environnement immédiat de la firme pourrait devenir « cet espace clos, découpé, surveillé en tous ses points, où les individus sont insérés à une place fixe, où les moindres mouvements sont contrôlés, où tous les événements sont enregistrés, où un travail ininterrompu d'écriture relie le centre et la périphérie²⁸⁶ ». C'est sur ce dernier point, *l'écriture systématisée, ou la bureaucratie*, que le néopanoptisme transfère la possibilité de contrôle qu'il avait perdu du fait de l'absence de surveillance directe. Mais le principe est sauvegardé au niveau du relais : « Il est vu, mais il ne voit pas; objet d'une information, jamais sujet dans la communication²⁸⁷ ».

²⁸⁶ Michel FOUCAULT, *Surveiller et Punir*, Gallimard, 1975, p. 199.

²⁸⁷ Michel FOUCAULT, *Op. Cit.*, p. 202.

PRINCIPES	La machine panoptique	Le comportement néopanoptique
Mode d'action	forces réelles	forces virtuelles
Coercition	par la possibilité directe de punition	contrainte exercée par l'impression uniquement
Visibilité	centralité de l'inspection	délocalisation de l'inspection
Dissociation du couple «voir / être vu »	écrans autour du poste d'observation	désinformation pour persuader l'adversaire qu'il est vu sans voir
Présence de la menace	« la tour » comme signe de connaissance des agissements des surveillés	« la démonstration » qui consiste à émettre un signal de connaissance du concurrent
La potentialité de l'inspection remplace son déploiement	emprisonnement réel dans un environnement où la potentialité d'être surveillé est vraie	emprisonnement virtuel dans un schéma relationnel où la potentialité d'être surveillé n'est qu'une conviction

Du panoptique au néopanoptisme...

Le pouvoir, dont la visibilité est transmise par l'omniprésence de la technologie de l'information, reste invérifiable... Mais ne serait-on pas taxé de paranoïa si l'on commençait à soupçonner tout réseau informatique d'être un surveillant potentiel ?

Il y a pourtant une certaine analogie entre l'automatisation du processus productif — *intégré par l'information* — et cet « état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir ²⁸⁸ ». En effet, la production est réduite à une série d'instructions, — une suite d'informations — qui va « nourrir » les automates. Cette chaîne d'instructions est conservée dans la mémoire de la machine. Qu'une erreur soit commise, et elle sera découverte. Celui qui pilote la production en est conscient, et il est, pour ainsi dire, lui aussi « dans un état permanent de visibilité », même si celle-ci se réalise a posteriori. Dans d'autres domaines de l'activité économique, on retrouve ce principe du panoptique. Le disque qui contrôle la vitesse des poids lourds en est un exemple. La boîte noire des avions de ligne, un autre. La nouveauté ne réside pas dans le phénomène en lui-même, mais *dans l'ampleur* qu'il prend dans l'économie : « Faire que la surveillance soit permanente dans ses effets, même si elle est discontinuée dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice ; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce; bref que les détenus soient pris dans une situation de pouvoir dont ils sont eux mêmes les

²⁸⁸ Michel FOUCAULT, *Op. Cit.*, p. 202.

porteurs²⁸⁹ ». La montée des incertitudes à tous les niveaux de l'économie encourage cette attitude. Les *réseaux*, de relations, de production, de commercialisation, ne sont en fait que des réactions panoptiques face à l'incertitude. Ils ne sont rien d'autre que les résultats d'une approche spatiale de l'économie{ XE "approche spatiale de l'économie" }, « un type d'implantation des corps dans l'espace, de distribution des individus les uns par rapport aux autres, d'organisation hiérarchique, de disposition de centres et de canaux du pouvoir²⁹⁰ ». Le réseau est une structure qui donne à ses membres l'illusion de la visibilité, la croyance d'appartenir, eux seuls, dans un monde bouleversé par l'aléa, à une « maison de certitude », selon les termes de Foucault pour qualifier le panoptique.

Comprendre la réalité du fonctionnement d'un réseau est essentiel à l'approche du néopanoptisme. Car lorsque Bentham rédige son panoptique, il « rêve d'en faire *un réseau* de dispositifs qui seraient partout et toujours en éveil, parcourant la société sans lacune ni interruption²⁹¹ ». Il voit dans son panoptique « une nouvelle manière de donner à l'esprit du pouvoir sur l'esprit²⁹² ». Il pense que « la généalogie de chaque idée observable pourrait être retracée dans chacune des étapes avec la plus extrême minutie, les souches originelles étant connues et dénombrées²⁹³ ». Le néopanoptisme, c'est un réseau qui se souvient. Un réseau dont chacun des membres est individualisé, et dont chacun des mouvements est enregistré. Un réseau qui sera d'autant plus puissant que son fonctionnement exploitera toutes les possibilités offertes par un paradigme unique de l'information.

Finalement, la mise en œuvre des nouvelles technologies de l'information dans le cadre d'une *architecture virtuelle*{ XE "architecture virtuelle" } qui rappelle le panopticon de Bentham, c'est le plus beau cadeau posthume qu'on ait pu lui faire. N'a-t-on pas réalisé ses rêves les plus fous ? « Qu'en diriez-vous si, par l'adoption graduelle et l'application diversifiée de cet unique principe, vous voyiez un nouvel état des choses se répandre dans la société civilisée (...), tout cela par une simple idée d'architecture²⁹⁴ ? ». Il manquait à Bentham ce paradigme unique de l'information pour réaliser ses vœux. Bentham, en effet, était fortement attaché à une différence essentielle qui sépare son panoptique de tout autre système de surveillance : « Vous voudrez bien noter que si le point le plus important dans ce plan est que les individus sous surveillance *se sentent constamment surveillés*, ou, à tout le moins, qu'ils pensent qu'il y a des chances qu'ils le soient, il n'est aucunement *le seul*. Le serait-il que le même avantage pourrait être dérivé de bâtiments de toutes formes ou presque. Ce qui, ici, n'est pas moins important, c'est

²⁸⁹ Michel FOUCAULT, *Op. Cit.*, p. 203.

²⁹⁰ Michel FOUCAULT, *Op. Cit.*, p. 207.

²⁹¹ Michel FOUCAULT, *Op. Cit.*, p. 210.

²⁹² Jeremy BENTHAM, *Le panoptique (1791)*, réédition de Belfond, 1977, p. 95.

²⁹³ Jeremy BENTHAM, *Op. Cit.*, p. 164.

²⁹⁴ Jeremy BENTHAM, *Op. Cit.*, p. 168.

que, pendant la plus grande proportion de temps possible, chaque individu soit en fait sous surveillance²⁹⁵ ». C'est là que le génie de Bentham se heurte à une limite physique aujourd'hui supprimée. Le regard de l'autorité ne peut voir plus loin que l'œil d'un homme comme les autres. Car si la visibilité n'est pas la seule condition de succès du panoptique, elle en est au moins une condition nécessaire pour que les yeux du surveillant puissent distinguer les silhouettes des prisonniers. Ainsi, Bentham conseille-t-il : « Le lieu le plus éloigné de l'endroit par où pénètre la lumière, c'est-à-dire le centre commun au bâtiment et au pavillon (du surveillant), ne sera pas distant de cet endroit de plus de 50 pieds; distance qui, je pense, n'est pas plus grande que ce que l'on constate dans les églises, mêmes dans celles qui ne sont pas, comme cet édifice, percées de baies sur tout leur pourtour²⁹⁶ ». A cette limite physique, Jeremy Bentham va opposer toute son ingéniosité. Et il va devenir le précurseur de l'utilisation des technologies de l'information au service du pouvoir. « Pour épargner à l'inspecteur l'effort de hausser la voix pour être entendu, et pour parer au fait que les prisonniers sauraient ainsi qu'il est occupé, plus loin, avec un des leurs, un petit tube de fer-blanc pourrait être installé de chaque cellule jusqu'au pavillon central, en passant par le vide intermédiaire, et en remontant par la fenêtre correspondante du pavillon. Ce dispositif permettrait d'entendre le plus léger murmure à l'une ou l'autre extrémité, surtout en appliquant l'oreille au tube²⁹⁷ ». Mais la perfection des technologies n'est pas, en 1787, au même niveau qu'aujourd'hui. Bentham abandonne, dans le « Postscript to the panopticon », publié en Angleterre en 1791, l'idée de cette surveillance acoustique, « peut-être parce qu'il ne pouvait pas introduire de dissymétrie{ XE "dissymétrie" } et empêcher les prisonniers d'entendre le surveillant aussi bien que le surveillant les entendait²⁹⁸ ».

Sur le constat de cet échec, on découvre un concept essentiel, autant pour la surveillance que pour la compétitivité : la dissymétrie.

5.2. La genèse du regard stratégique

5.2.1. L'information secrète dans la compétition

Le panoptique, nous l'avons vu, est une fabuleuse « machine à dissocier le couple voir-être vu²⁹⁹ ». Quant au néopanoptisme, il est une pratique qui consiste à mettre à profit une différence importante de niveaux d'information pour faire

²⁹⁵ Jeremy BENTHAM, *Op. Cit.*, p. 109.

²⁹⁶ Jeremy BENTHAM, *Op. Cit.*, p. 105.

²⁹⁷ Jeremy BENTHAM, *Op. Cit.*, p. 101.

²⁹⁸ Michel FOUCAULT, *Surveiller et Punir*, Gallimard, 1975, p. 203.

²⁹⁹ « Dans l'anneau périphérique, on est totalement vu, sans jamais voir; dans la tour centrale, on voit, sans jamais être vu », Michel FOUCAULT, *Op. Cit.*, p. 203.

basculer le pouvoir aux mains de ceux qui détiennent la connaissance. La concurrence parfaite — celle qui n'existe plus qu'en théorie —, c'est a contrario l'égalité des champs de bataille; c'est la symétrie des besoins et des contraintes de la compétition. Le concept qui sous-tend — et rapproche — compétitivité et surveillance, c'est la dissymétrie. C'est selon ce même principe que l'information secrète modifie les données de la compétition. Plaçons-nous dans une situation compétitive. Par définition, elle fait intervenir plusieurs centres de décision ayant chacun une perception de l'environnement différente de celles des autres. D'une part, chaque centre — ou chaque firme — ne « négocie » pas avec son environnement de la même façon et avec les mêmes pouvoirs. D'autre part, les informations obtenues de l'environnement n'ont *pas la même valeur* selon les contextes dans lesquels elles sont acquises. En d'autres termes, une information n'a pas de valeur intrinsèque.

On peut donc construire sur le secret le fondement du comportement stratégique de la firme, et nous verrons en quoi les enseignements du panoptisme vont servir cette approche. La première étape consistera à dégager, a priori, les possibles, et parmi ceux-ci, d'affecter différentes probabilités selon les objectifs particuliers à atteindre. Ensuite, pour chacun de ces objectifs, et pour chacune de ces décisions envisageables, on identifiera les sources d'incertitude qui peuvent contrarier nos projets. Pour chacune de ces sources, on listera les réducteurs d'incertitude dont nous disposons : quels relais d'information ? Quels historiques des comportements détenons-nous à propos de ces relais ? Compte tenu de l'ensemble des possibles, et du sous-ensemble des probables, avons-nous des chances de réussir en atteignant le seuil minimal de satisfaction que nous nous sommes fixés ?

Ce raisonnement, à première vue, paraît cohérent. Il cache cependant un piège qui remet complètement en cause ce type d'approche rationnelle : il est fondé sur une hypothèse tacite de stabilité des conditions d'acquisition de l'information. Les concurrents « sont-ils également informés (information publique{ XE "information publique" }) ou bien sauront-ils seulement que des informations sont acquises sans plus de précision (information privée{ XE "information privée" }) ou bien encore cette acquisition se fera-t-elle à leur insu complet (information secrète{ XE "information secrète" }) ? (...) La résolution de situations de ce genre peut être délicate (...) ; si la situation se répète ou simplement si elle se déroule de façon dynamique, le joueur non informé ne pourra manquer de constater que le comportement de l'autre joueur est celui d'un joueur très avisé, donc certainement informé ³⁰⁰ ». Ce qui n'était pas probable le devient, et ce qui était possible ne l'est plus. A quel niveau faut-il alors reprendre le raisonnement ? A celui des probables en modifiant les coefficients affectés aux différents scénarios ? Ou à celui des possibles en supprimant ou en ajoutant des alternatives ? Le joueur « ayant acquis l'information secrètement se trouve finalement devant le dilemme suivant : ou bien il fait usage de son information en adaptant son comportement à

³⁰⁰ Jean-Pierre PONSSARD, Logique de la négociation et théorie des jeux, L'usage de l'information en situations compétitives, Editions d'Organisation, 1977, p. 103.

ce qu'il sait et son comportement risque de tellement surprendre les autres joueurs qu'ils en déduiront qu'il est informé, ou bien il ne modifie pas son comportement mais alors, son information secrète ne lui sert plus à rien ³⁰¹ ». C'est ce qu'on peut appeler le dilemme du néopanoptisme{ XE "dilemme du néopanoptisme" }. En d'autres termes, en admettant qu'une combinatoire de technologies puisse transposer à la compétition le principe du panoptique, cela ne résout pas le problème essentiel : à savoir qu'une information n'a de valeur que dans l'utilisation qu'on en fait.

Il n'empêche que détenir une quantité importante d'informations secrètes ouvrent de nombreuses possibilités d'utilisations pour surprendre la concurrence. On ne saurait concevoir d'approche stratégique sans secret : « La guerre, c'est l'art de duper. C'est pourquoi celui qui est capable doit faire croire qu'il est incapable; celui qui est prêt au combat doit faire croire qu'il ne l'est pas; celui qui est proche doit faire croire qu'il est loin; celui qui est loin doit faire croire qu'il est proche ³⁰² ». C'est pourquoi, sommes-nous tentés d'ajouter, celui qui détient un potentiel technologique ne doit pas le divulguer. Car ce potentiel — cet ensemble de technologies génériques — va conditionner les plans de développement de la firme. Elle ne pourra investir que les domaines d'application *proches* de ce noyau générique. La connaissance fondamentale de la firme doit être protégée. Cette connaissance fera le caractère des innovations de la firme. Si le potentiel est fortement concentré dans des domaines peu maîtrisés par la science, au carrefour de la biotechnologie et de l'informatique par exemple, les innovations risquent d'être « révolutionnaires », voire « architecturales », concernant de ce fait l'ensemble du secteur ³⁰³. Ce noyau de connaissances porte en lui la préfiguration des stratégies de grappes technologiques{ XE "grappes technologiques" } de la firme ³⁰⁴. Il détermine l'architecture de l'outil de production, et l'ensemble des combinaisons de valorisation des technologies générées dans les espaces de leurs utilisations.

L'usage de l'information secrète dans la compétition peut aussi porter sur des enjeux de moins longs termes. Il permet notamment des avancées tactiques sur des marchés sans avoir à déployer un arsenal compétitif coûteux. « C'est pourquoi, remporter cent victoires en cent combats n'est pas ce qu'il y a de mieux ; *soumettre l'ennemi sans combattre* est ce qu'il y a de mieux ³⁰⁵ ». N'était-ce pas l'idée de Jeremy Bentham ? La potentialité{ XE "potentialité" } de la surveillance remplace son déploiement. « Etre incessamment sous les yeux d'un inspecteur, c'est perdre en effet la puissance de faire le mal, et presque la pensée

³⁰¹ Jean-Pierre PONSSARD, Op. Cit., p. 104.

³⁰² SUN TZU, *L'Art de la Guerre*, traduction de Niquet-Cabestan, Economica, 1988, p. 64.

³⁰³ Termes empruntés à W.J. ABERNATHY et K.B. CLARK, *Innovation : mapping the winds of creative destruction*, in W.J. KANTROW, *Industrial renaissance : productive a competitive future for America*, Basic Books, 1983.

³⁰⁴ Voir à ce propos GEST-EUROCONSULT, *Grappes technologiques et stratégies industrielles*, Centre de prospective et d'évaluation, n° 57, mai 1985.

³⁰⁵ SUN TZU, *L'Art de la Guerre*, traduction de Niquet-Cabestan, Economica, 1988, p. 67.

de le vouloir³⁰⁶ ». Ainsi, avoir un pouvoir d'inspection des marchés supérieur à la concurrence, présage d'une connaissance plus grande de leur composition, et d'un temps de réponse plus court à leur évolution. Si l'information sur les marchés est publique, le temps de réponse ne dépendra plus du niveau d'information des concurrents — qui sera quasiment le même pour tous — mais de leur aptitude à mettre en place la logistique de la réponse. L'information secrète nivelle donc la compétitivité des acteurs en modulant leur connaissance du « champ de bataille », et en réduisant leur temps de réponse à un éventuel mouvement concurrent. En d'autres termes, l'information secrète confère à la firme un niveau de flexibilité méconnu des concurrents, et conditionne ainsi sa capacité de réponse. « La flexibilité traduit la possibilité pour un décideur de pouvoir à tout moment reconsidérer ses choix de manière à maintenir l'optimalité de sa décision{ XE "décision" }³⁰⁷ ». Plus le décideur détient d'informations sur son environnement, plus nombreuses pourront être les alternatives qui se présentent à lui. Si de surcroît, ces informations ont été acquises secrètement, le décideur aura, face à ses concurrents, l'avantage de pouvoir ajouter à sa flexibilité une *capacité à surprendre*. Mais il ne s'agit, dans notre exemple, que « de la manière dont le décideur peut gérer les informations en provenance de son environnement pour s'adapter aux modifications de ce dernier³⁰⁸ ». Ce que les auteurs appellent *flexibilité décisionnelle*{ XE "*flexibilité décisionnelle*" }. Elle est inopérante, si après cette prise de décision, l'outil de production n'est pas lui-même capable de s'adapter aux mouvements de l'environnement. C'est ce qu'on appelle *flexibilité organisationnelle*{ XE "*flexibilité organisationnelle*" }. Cela suppose l'adoption de quelques hypothèses. D'une part, « l'unité de décision disposera d'un degré de contrôle élevé sur sa structure productive³⁰⁹ », et d'autre part, elle devra être elle-même *suffisamment flexible* par rapport à son environnement. Cela nécessite bien sûr une très grande aptitude de la firme à gérer, de façon interne, l'information : de nombreux relais actifs entre l'unité de décision et de production, un mode d'organisation ouvert à la prise en compte d'informations nouvelles pouvant le modifier. La figure ci-après montre quel peut être le rôle d'une cellule de veille en tant qu'interface entre une flexibilité décisionnelle dédiée à l'écoute externe et une flexibilité organisationnelle située au niveau du traitement interne de l'information.

En tenant pour acquis cette capacité d'adaptation de la firme, nous allons voir maintenant comment l'information secrète peut bouleverser le jeu de la compétition. Il nous faut cependant utiliser deux autres concepts : l'effet de

³⁰⁶ Jeremy BENTHAM, *Le Panoptique*, mémoire sur un nouveau principe de construire des maisons d'inspection, (1791), réédition de Belfond, 1977, p. 8.

³⁰⁷ Patrick COHENDET, Patrick LLERENA, *Flexibilité, information et décision*, ouvrage collectif, Recherches du BETA de l'Université de Strasbourg, Economica, 1989, p. 7.

³⁰⁸ Patrick COHENDET, Patrick LLERENA, *Op. Cit.*, p. 8.

³⁰⁹ Patrick COHENDET, Patrick LLERENA, *Op. Cit.*, p. 11.

démonstration³¹⁰ et l'effet de réputation{ XE "réputation" }³¹¹. Une firme peut ainsi démontrer sa capacité de réponse en s'essayant, sur différents marchés, à exercer son pouvoir. Cette démonstration est déployée dans l'objectif de dissuader les concurrents. Mais cette démonstration n'aurait aucun effet si les concurrents savaient parfaitement de quoi il en retourne. En d'autres termes, c'est l'incertitude, ou plutôt, l'asymétrie d'information qui permet la démonstration. C'est parce que les concurrents vont réputer possible l'exécution de la menace que cette démonstration aura l'effet escompté. C'est ce qu'on appelle l'effet de réputation³¹². Ce que nous venons de décrire « devrait montrer clairement qu'une bataille entre concurrents peut être complètement menée par l'intermédiaire d'annonces{ XE "annonces" }, avant qu'un seul dollar de ressources ait été dépensé³¹³ ».

POTENTIEL DE SURVEILLANCE	non communiqué à l'adversaire	communiqué à l'adversaire
utilisé	L'entreprise accumule secrètement de nombreuses informations ACQUISITION	Une agression est réalisée contre le patrimoine de l'adversaire DEMONSTRATION
non utilisé	Le potentiel « sommeille » dans l'attente de son utilisation INFILTRATION	La potentialité de l'inspection remplace son déploiement. Economie des forces par l'impression et la persuasion INTOXICATION

Le cycle de l'économie de la dissuasion

Le rôle de l'information secrète commence à se dessiner dans la stratégie de la firme. Il n'y a plus désormais qu'un seul objectif : augmenter l'asymétrie pour pouvoir déployer des dissuasions de plus en plus nombreuses et efficaces. Car il y a effet de cumul. Un nombre de plus en plus grand de dissuasions ayant réussi, augmente la réputation de la firme à les réussir. C'est là qu'entre en jeu la notion de flexibilité : plus la firme peut prouver des flexibilités décisionnelle et

³¹⁰ F.M. SCHERER, *Industrial Market Structure and Economic Performance*, Rand McNally, Chicago, 1980, p. 338.

³¹¹ Bernard BELLOC, « Dissuasion et réputation », in *Dynamique, information incomplète et stratégies industrielles*, ouvrage collectif dirigé par Antoine-Augustin Gremaq, Economica, 1988, page 201.

³¹² D.M. KREPS, R. WILSON, « Reputation and Imperfect Information », *Journal of Economic Theory*, 1982, n° 27, pp. 253-279.

³¹³ Michaël E. PORTER, *Choix stratégiques et concurrence*, Economica, 1982, page 87.

organisationnelle importantes, plus sa crédibilité sera grande. Connaissant sa capacité de s'adapter à son environnement, les concurrents prendront beaucoup plus au sérieux ses menaces. La boucle est bouclée. Flexibilité, démonstration, réputation, puis dissuasion : l'information fait le jeu de la compétition. Et c'est pourquoi la vérité quant aux réelles aptitudes de la firme à s'adapter doit être au mieux protégée. L'information secrète est la clef de voûte de l'économie de la dissuasion.

Encore une fois, Jeremy Bentham l'avait compris. D'une part, l'information acquise sur les prisonniers l'est tout à fait secrètement. « La tour d'inspection est aussi environnée d'une galerie couverte d'une jalousie transparente, qui permet aux regards de l'inspecteur de plonger dans les cellules, et qui l'empêche d'être vu ³¹⁴ ». D'autre part, aucun prisonnier n'est en mesure de savoir s'il est effectivement sous le regard de l'inspecteur. Le panoptique est une technologie de la dissuasion. « On ne forme point de desseins quand on voit l'impossibilité de les exécuter; les hommes se rangent naturellement dans leur situation, et une soumission forcée amène peu à peu une obéissance machinale ³¹⁵ ». Cet aspect technologique est représenté, dans la compétition moderne, par les formes prises par la dissuasion. Dissuader, ce peut être proférer une menace...

CAPACITE D'INTELLIGENCE	non effective (pas de force réelle)	effective (force réelle)
perçue comme effective (force virtuelle)	la désinformation A court terme, une utilité tactique. A moyen terme, l'échec probable.	la puissance affichée L'intimidation mais également l'appel à l'agression.
perçue comme non effective (pas de force virtuelle)	la vulnérabilité Situations réelles et virtuelles confondues dans l'échec.	l'avantage tactique Avantage conféré par le secret aux opérations d'intelligence.

Néopanoptisme, entre effectivité et virtualité

Mais cette pratique, brutale, ne fait qu'engendrer le processus destructeur de la violence que nous avons décrit plus haut. La meilleure dissuasion est celle d'une capacité d'intelligence réelle, celle qui permet à l'entreprise d'avoir le choix entre une approche couverte ou découverte de la concurrence. La « zone de flou » quant à la réalité de la capacité à surveiller, et à connaître l'adversaire, constitue le fondement des tactiques néopanoptiques. L'entreprise, pour gérer au mieux ce

³¹⁴ Jeremy BENTHAM, *Le Panoptique, mémoire sur un nouveau principe de contruire des maisons d'inspection*, (1791), réédition de Belfond, 1977, p. 7.

³¹⁵ Jeremy BENTHAM, *Op. Cit.*, p. 12.

type d'approches, doit cependant bien connaître ses capacités (leur effectivité{ XE "effectivité" }) et la perception qu'en ont les concurrents (leur virtualité{ XE "virtualité" }).

Quatre alternatives stratégiques se présentent donc à l'entreprise souhaitant bâtir sa politique d'intelligence :

— ne pas développer de potentiels particuliers mais communiquer aux entreprises concurrentes « l'existence » de ce potentiel. Cet emploi uniquement virtuel de capacités de surveillance inexistantes constitue une désinformation ;

— développer une réelle capacité d'intelligence{ XE "capacité d'intelligence" } et le faire savoir; ce qui correspond à la puissance affichée, avec tous les risques que cela peut impliquer ;

— construire dans le secret sa puissance d'intelligence, perçue comme non effective, et mettre à profit cette situation de façon tactique en surprenant la concurrence{ XE "concurrence" } ;

— ne développer aucune force réelle{ XE "force réelle" } et ne communiquer aucune force virtuelle{ XE "force virtuelle" }, mais ceci correspond à une situation très vulnérable.

En réalité, le néopanoptisme prend tout son sens dans la gestion dynamique de ces quatre alternatives, entre effectivité et virtualité. Chaque situation de connaissance (ou d'ignorance) à laquelle est confrontée l'entreprise nécessite tout autant l'emploi de forces réelles et de forces virtuelles. Tout l'intérêt de la machine de Bentham résidait en cela. Les firmes, entre elles, comme l'inspecteur et les prisonniers du panoptique, ont le choix entre l'affrontement{ XE "affrontement" } et l'illusion{ XE "illusion" }. Le panoptique est un système d'illusions pour l'économie des forces.

5.2.2. De la maintenance du pouvoir à la cohésion sociale

Quel est le coût que la machine de Bentham a permis de supprimer ? A quoi sert le déploiement des regards et de la répression ? Ils servent à maintenir le pouvoir. La dissuasion est la forme la plus économique de maintenance pour l'autorité. Son coût politique est moindre, car moins fréquent est le recours à la punition, et plus stables sont les relations de pouvoir dans l'organisation. Son coût économique{ XE "coût économique" } est moindre, car, nous l'avons déjà dit, la potentialité est moins coûteuse que le déploiement. Mais la dissuasion porte en elle un risque important pour l'organisation. A chaque fois qu'il est nécessaire que la firme s'implique pour dissuader en proférant des menaces, elle met en jeu sa crédibilité. Si elle dénonce, par exemple, une concurrence déloyale, ou la nocivité d'un produit d'un concurrent pour l'environnement, il faut que ses déclarations soient justes. Sinon, la croyance des concurrents et de l'opinion dans les déclarations de la firme va considérablement diminuer. Et là aussi, il y a effet de cumul.

C'est pourquoi la firme ne doit pas voir dans la surveillance une simple fonction de maintenance du pouvoir. Il ne faut pas la considérer comme un simple

outil dont la maîtrise serait proportionnelle à l'expérience. Il faut, au contraire, que la surveillance accompagne le pouvoir : elle évoluera en fonction de sa forme et de son étendue ; et le pouvoir, lui-même, devra à la surveillance sa nature et sa force. « La scrutation prospective de l'environnement s'apparente davantage à un *processus d'apprentissage dynamique* qu'à une tâche répétitive qu'il suffirait d'apprendre une fois pour toutes ³¹⁶ ». On peut différencier ici deux conceptions de la surveillance. « L'objet de l'une est la détection, l'objet de l'autre est la prévention{ XE "prévention" }. Dans le premier cas, l'individu qui détient l'autorité est un espion ; dans le second, un moniteur ³¹⁷ ». Dans le premier cas, son mode de fonctionnement est la suspicion ; dans le second, c'est l'éducation. Il faut éduquer le « regard » de la firme afin qu'il apprenne à prévenir le danger. La surveillance ne doit pas être comprise comme l'arme du pouvoir, comme le symbole permanent de la répression. Cette acception engendre la violence. Elle conduit au conflit interne parce que l'autorité s'oppose au personnel de la firme dans une confrontation des regards, de bas en haut, puis de haut en bas. Si l'autorité choisit ce chemin, elle sera, tôt ou tard, contrainte à faire recours à l'état agentique pour pouvoir diriger ses hommes. Il n'y aura plus qu'un seul regard : celui de la consigne, celui qui vient d'en haut et qui se transmet à travers un réseau agentique de surveillants non impliqués dans la vigilance qu'ils exercent. Au contraire, la surveillance doit être acceptée par tous les membres de la firme comme un moyen de se protéger de la menace extérieure, comme un stimulateur de la cohésion sociale vis-à-vis de la turbulence des marchés. La maintenance du pouvoir ne s'effectue plus par le haut, mais simultanément, et à tous les niveaux de la firme. Le morcellement de l'industrie en plusieurs petites unités stratégiques va dans ce sens. Le panoptisme est déraisonnable quand il dit : « Dénoncez le mal, ou souffrez comme complice ³¹⁸ ». Il est encore déraisonnable quand il conseille : « autant de camarades, autant d'inspecteurs ; les personnes mêmes qu'il faut garder se gardent mutuellement ³¹⁹ ». Il emprunte la voie de la suspicion, quand il pourrait mettre à profit la fabuleuse ingéniosité de son architecture pour s'engager sur le chemin de l'éducation. Le néopanoptisme, dans sa version technocratique, n'est pas viable au sein de l'organisation. Il méprise trop l'individu au profit d'une norme technologique censée le canaliser, voire l'appivoiser.

5.2.3. Vers une dynamique nouvelle de la compétition

Refuser « d'appivoiser » par la norme technologique, c'est faire le premier pas vers une dynamique nouvelle de la compétition. La conception d'une « firme-

³¹⁶ Humbert LESCA, *Système d'information pour le management stratégique de l'entreprise*, McGraw Hill, 1986, p. 138.

³¹⁷ Jeremy BENTHAM, Op. Cit., p. 167.

³¹⁸ Jeremy BENTHAM, Op. Cit., p. 49.

³¹⁹ Jeremy BENTHAM, Op. Cit., p. 50.

réseau » comme celle de Thorelli³²⁰, est intéressante à condition que la cohésion sociale{ XE "cohésion sociale" } en soit l'élément fondateur. A l'instar du chemin de fer de Chandler, qui fluidifie l'espace mercatique de la firme et fait de *la vitesse* l'élément catalyseur de toute la genèse organisationnelle ³²¹, l'intérêt d'un réseau de surveillance réside dans sa capacité à motiver chacun de ses relais dans les gains de temps et d'efficacité. Le réseau que nous encourageons est une formulation d'un espace finalisé, dont chaque connexion, chaque relais, est motivé par son rôle spécifique dans la compétition. C'est un réseau qui a le libre choix de sa formulation, qui correspond plus à un état d'esprit qu'à un dispositif normatif ou réglementaire. Le « discours » que développe ce réseau lui est propre. C'est ce qui fait toute sa dynamique, c'est-à-dire sa capacité à évoluer de lui-même vis-à-vis de son environnement. Tout acteur de la surveillance « tend ainsi à apparaître comme un nœud d'un réseau fluide, nœud de connexions ou de ruptures temporaires des flux, mais qui ne peut être analysé que relativement à son appartenance à ce réseau ³²² ». Cette grande connectivité, qui se développe autant au niveau des systèmes d'information ³²³ que des réseaux de compétences, annonce une dynamique de la compétition dont le fondement est le partenariat stratégique entre firmes ³²⁴.

Ce que le néopanoptisme aurait pu concevoir, c'est *une structure* favorisant une participation volontaire au progrès collectif. Si la centralisation des données est, tôt ou tard, nécessaire au regard stratégique, pourquoi devrait-elle toujours s'effectuer à l'insu de tous ? L'information ne circulerait-elle pas mieux si chacun en avait la préoccupation à l'esprit ? Il n'est pas question, ici, de dévoiler les secrets dans lesquels se fondent toute stratégie. Il s'agit de réaliser un arbitrage dans la finalité de mobiliser l'éveil au sein de la firme. Il s'agit d'impliquer le personnel dans un projet de gestion de la connaissance se développant dans le cadre de réseaux adaptés à la personnalité de chacun. L'acquisition de l'information doit se réaliser dans le cadre exclusif de ce projet commun, faute de quoi, chacun pourrait « avoir intérêt à fausser la procédure de communication pour ne pas révéler intégralement les informations qu'il détient de façon privée ³²⁵ ». Il faut à tout prix éviter qu'il soit « de l'intérêt de chaque personne de

³²⁰ H. THORELLI, « Networks : between markets and hierarchies », *Strategic Management Journal*, Vol. 7, 1986.

³²¹ A. CHANDLER, *The Visible Hand*, Harvard University Press, 1977, pp. 253 et s.

³²² J.P. DE GAUDEMAR, *Usines et ouvriers : figures d'un nouvel ordre productif*, Maspéro, 1980, p. 24.

³²³ A. TINGAUD, *Les systèmes Client-Serveur, le quatrième millénaire de l'informatique*, 3Com, 1989.

³²⁴ J.B. ZIMMERMANN, M. DELAPIERRE, *Towards a new europeanism strategic partnership*, Document de Travail Grege 89B02, 1989.

³²⁵ G. D'ASPREMONT, L.A. GERARD-VARET, *Concurrence et contraintes d'incitation*, Document de Travail Grege 8802, 1988, p. 3.

donner de faux signaux{ XE "faux signaux" }, de prétendre retirer moins d'une consommation collective qu'il en retire réellement ³²⁶ ».

C'est dans cet objectif qu'il faut structurer le système de veille stratégique de la firme. Mais mettons-nous à la place de celui qui détient l'information : quelle sera la structure la plus adéquate à l'encourager à la transférer ? Nous pourrions envisager une sorte d'enchère anglaise{ XE "enchère anglaise" }, c'est-à-dire une incessante confrontation des offres à la hausse, tout à l'avantage du « vendeur », mais ce dernier ne peut s'annoncer, au grand jour, possesseur de l'information que ses partenaires recherchent. Il se mettrait vis-à-vis d'eux dans la position inconfortable de « maître-chanteur ». En fait, la réalité des relations intra-industrie correspond plus à une enchère hollandaise{ XE "enchère hollandaise" }, c'est-à-dire que chacun sait ce qu'il pourra retirer de la divulgation de l'information, ou du transfert de sa connaissance. Il perçoit très bien dans quelles mesures il pourrait ainsi améliorer, ou affaiblir, sa position transactionnelle. Par ailleurs, il n'est pas en position dominante ³²⁷ et sait très bien que la seule façon qu'il a de « vendre » son information est d'en diminuer le « prix » jusqu'à ce qu'il y ait preneur ³²⁸. Ce « prix » auquel nous faisons référence, c'est la détérioration ou l'amélioration de sa position transactionnelle. Et il existe un seuil minimal d'amélioration de cette position transactionnelle, sans quoi cette information ne sera jamais transférée. L'objectif de tout système de veille{ XE "système de veille" } stratégique est de découvrir ces seuils minimaux pour chacune des firmes prises en considération. Il s'agit ensuite de structurer le système transactionnel qui relie les firmes entre elles afin de diminuer ces minima exigés pour le transfert de l'information.

Le fait d'être le partenaire d'un réseau de veille technologique peut déjà diminuer ce seuil minimal d'exigence du fait de l'aura « statutaire » d'un groupe formalisé. Mais beaucoup d'autres éléments entrent en compte dans ce « prix » : ce sont les coûts psychologiques{ XE "coûts psychologiques" } que doit supporter la transmission de l'information, et le sentiment de concéder à ses partenaires une base de valorisation acquise par un long apprentissage, coûteux et laborieux. C'est la problématique des barrières à l'entrée{ XE "barrières à l'entrée" } créées par des asymétries d'informations ³²⁹. Les projets de

³²⁶ P.A. SAMUELSON, « The pure theory of public expenditure », *The Review of Economics and Statistics*, Vol. 36, pp. 387-389.

³²⁷ Conformément à nos hypothèses de travail, nous ne prenons en considération que les concurrences imparfaites, avec fortes asymétries de niveaux d'information dans le cadre d'une organisation industrielle oligopolistique.

³²⁸ L'enchère hollandaise se présente d'ailleurs comme la solution médiane pour l'enchériste. Si l'on devait classer les types d'enchères les mieux adaptées à une situation de confidentialité des annonces d'offre et de demande, elle serait certainement au premier plan. Cf P.A. MILGROM, R. WEBER, « A theory of Auctions and Competitive Bidding », *Econometrica*, Vol. 50, 1982, pages 1089-1122.

³²⁹ P.J. BUCKLEY, « New theories of international business : some unresolved problems », Chap. II dans M. CASSON, (éd.), *The growth of international business*, George Allen & Unwin, Londres, 1983, p. 49 et s.

combinatoires de technologies génériques{ XE "technologies génériques" } constituent la base de développement de la firme. Ils sont l'essence même de ces asymétries fondamentales d'informations et ne peuvent être divulgués, parfois même au sein d'une joint-venture{ XE "joint-venture" }³³⁰. Une dynamique nouvelle de la compétition se dessine alors au niveau de ces partages très mesurés de l'information : une dynamique du transfert des connaissances dont le fondement est un réseau liant le principe de vitesse de Chandler³³¹ et les gains en coûts de transaction de Williamson³³². Un réseau qui s'énonce comme « une nouvelle structure d'information et de communication (...) favorisant des échanges nombreux dans un nouvel espace de dialogue convivial et permanent³³³ ».

5.3. La stratégie autrement

5.3.1 La nécessité de nouvelles règles du jeu

Pour mettre en place un réseau favorisant le transfert des connaissances, il faut avant tout « renouveler le jeu ». Ce qui était appréhendé en termes de concurrence d'intérêts entre les acteurs de la compétition industrielle doit être révisé dans un objectif de convergence stratégique. La notion de « convergence stratégique » se situe à un niveau au-dessus de la divergence d'intérêts. Elle appréhende le jeu des acteurs dans une perspective à long terme, c'est-à-dire très simplement à l'échelle de la connaissance. A ce stade de réflexion, il faut pouvoir dépasser le déni de la compétition{ XE "déli de la compétition" } absolutiste³³⁴. Il faut se dégager de ce réflexe de défense qui consiste à refuser la réalité d'une perception traumatisante de la compétition. Si la compétition tolère la relativité, le profit réalisé par une firme grâce à une combinatoire unique de technologies et de services n'en sera pas moins réalisé par aucune autre. Un partenariat stratégique entre deux firmes ne va pas les confondre l'une dans l'autre. Elles seront toujours, à un moment donné, dans des positions contraires vis-à-vis de l'acquisition, ou du partage, d'une connaissance. La nouvelle règle du jeu, c'est rejeter « le mécanisme psychotique, le déni, (...) ce refus de la réalité d'autant plus catégorique que

³³⁰ Exception faite de la fusion-acquisition où le transfert intégral de la connaissance générique est la condition *sine qua non* du rachat.

³³¹ A. CHANDLER, *The Visible Hand*, Harvard University Press, 1977, pp. 253 et s.

³³² O. WILLIAMSON, *Markets and Hierarchies : Analysis and Antitrust Implications*, The Free Press, New-York, 1975.

³³³ M. MOUYSSINAT, *Recherche et industrie, une volonté de coopérer*, dans « De nouveaux enjeux pour la recherche et ses applications », Publication Greco Programmation, 1988, pages 89 à 91.

³³⁴ Le terme « déni » est emprunté à J. LAPLANCHE, J.B. PONTALIS, *Vocabulaire de la Psychanalyse*, Paris, 1973.

l'angoisse est plus importante ³³⁵ ». C'est considérer qu'après tout la compétition n'a rien de traumatisant, et qu'il n'est pas nécessaire de projeter ses adversaires économiques dans la faillite pour justifier son aptitude à rester dans le jeu. La nouvelle règle du jeu, enfin, c'est éviter de rentrer dans le processus de la « violence symbolique partout inscrite dans les signes ³³⁶ » ; c'est sortir des schémas de domination, comme ceux de Taylor ³³⁷, ou de Bergery ³³⁸, pour maîtriser l'espace et le temps autrement.

Un important travail de recherche est donc requis au niveau de l'étude et de la préparation de ces partenariats stratégiques de partage et d'acquisition de la connaissance. C'est une recherche qui doit non seulement mobiliser l'économiste industriel, mais aussi, de façon coopérative, le sociologue des organisations et l'expert en technologies de l'information. Autant dire que ces trois expertises n'existent pas dans un seul homme. Une fois encore, la maîtrise de l'information stratégique passe par la concertation.

5.3.2. A la recherche de structures adéquates

Des structures adéquates au transfert et au partage facilités des connaissances, c'est finalement ce que toute entreprise soucieuse d'améliorer ses performances en intelligence devrait essayer de mettre en place. Il est nécessaire, dans cet objectif, de respecter les critères d'efficacité que nous venons d'introduire. D'une part, il doit exister au moins un canal d'échange d'informations formalisé et finalisé. D'autre part, cette formalisation de l'échange doit être adaptée aux personnalités des acteurs entrant dans le jeu de la coopération. Elle leur est adaptée car elle choisit comme supports de communication des média faisant partie, à la fois, de l'environnement quotidien de l'émetteur et du récepteur de l'information, comme par exemple un réseau informatique, ou des publications internes ou externes lues des deux partenaires. Ce système de partage des connaissances { XE "partage des connaissances" } doit aussi proposer des règles du jeu clarifiées. Qu'elles soient écrites ou tacites, formelles ou informelles, elles doivent être connues et acceptées de tous les participants à ce système de partage. Cela permet à chacun de se représenter « mentalement » le système de partage dans lequel il a fait le choix délibéré de rentrer. Cela permet également à chacun de discerner les possibilités de ce système : ses atouts et ses limites. Le réseau peut ainsi être optimisé par ses utilisateurs, parce qu'identifié. Ainsi, on se rapproche à la fois de la firme comme

³³⁵ Ruth MENAHEM, *La mort apprivoisée*, Editions Universitaires, Paris, 1973, p. 59. Le propos de MENAHEM se rapporte à l'appréhension mythique de la mort dans notre société. Il peut servir de métaphore à un refus de la compétition au sein de la firme.

³³⁶ Jean BAUDRILLARD, *L'Echange Symbolique et la Mort*, « La fin de la production », Gallimard, 1976, p. 23.

³³⁷ W. TAYLOR, *La Direction des Ateliers*, Dunod, 1919.

³³⁸ C.L. BERGERY, *Economie industrielle*, Tome III, « La conduite d'une fabrique », Metz, 1831.

« nœud » de contrats de Coase³³⁹ et de la théorie de la vitesse de communication comme fondement de la genèse capitaliste de Chandler³⁴⁰. Nous sommes également très proche du réseau de Donald Teece qui permet de réduire les coûts de transaction entre partenaires d'un transfert de connaissances³⁴¹.

Ce « réseau », c'est aussi l'opportunité de mettre à l'épreuve quelques autres hypothèses sur le secret et l'information, que le système de partage de connaissances doit gérer, ou sur les asymétries de niveaux d'information comme facteur essentiel de la compétitivité. En effet, l'adaptation des structures à la veille stratégique, c'est avant tout avoir le respect du jeu de la compétition. Par exemple, un réseau de R&D ne peut s'envisager autrement qu'en garantissant la confidentialité^{ XE "confidentialité" } des transactions entre laboratoires et industries. Le partage des connaissances génériques doit avoir ses propres moyens de communication, ses lieux de rencontre, ses rituels, comme peuvent l'être des conférences sur un sujet de pointe, ou des colloques réguliers réunissant plusieurs institutions du réseau autour d'un thème clairement annoncé au départ. C'est pourquoi, nous devons développer des recherches quant à des partenariats plus stratégiques de partage et d'acquisition d'information. Ce seront, au sein du réseau général, des pôles contractuels^{ XE "pôles contractuels" } de petites tailles, des contrats stabilisés et confidentiels de recherche et de développement. Nous aurons ici deux niveaux de dialogue : la dynamique d'ensemble, c'est-à-dire le rituel collectif qui rapproche les deux communautés scientifiques et industrielles, et la dynamique différenciée, sur la ligne de front du progrès, qui oriente par de nombreuses investigations d'équipes de tailles restreintes, les axes du développement futur du réseau. Nous avons là une dynamique des structures, en interrelations, dans un système formalisé, finalisé et cohérent.

5.3.3 Les réseaux du transfert de la connaissance

Pour que le concept d'une firme organisée en réseaux finalisés ait toute sa valeur, il faut supposer que le transfert d'information soit possible entre chacun de ses membres. Ce qui n'est pas sans difficultés. L'échange de biens intangibles comme l'information connaît en effet de multiples obstacles. D'une part, par son aspect intangible ou stratégique, l'information est difficile à vendre, puisque

³³⁹ R.H. COASE, *The nature of the firm*, *Economica*, Vol. 4, Londres, novembre 1937, pages 386-405.

³⁴⁰ A. CHANDLER, *The Visible Hand*, Harvard University Press, 1977, pp. 253 et s.

³⁴¹ Donald J. TEECE, « The Market for Knowhow and the Efficient International Transfer of Technology », *Annals of The American Academic Journal of Political and Social Science*, novembre 1981, p. 83.

difficile à montrer. D'autre part, la possibilité de reconnaître des opportunités d'échange dépend bien souvent de facteurs stochastiques ³⁴².

Et même lorsque l'opportunité d'échange est clairement identifiée, le paradoxe fondamental de l'information ³⁴³ se manifeste : pour connaître la valeur de l'information, il faut *la recevoir et l'utiliser*, ce qui est irréalisable, puisqu'une fois divulguée, cette information n'a plus de propriétaire spécifique. L'acheteur se trouve dans le dilemme d'acquérir et de risquer de se tromper, ou de ne pas acquérir, et perdre l'opportunité qu'il avait identifiée. Dilemme d'autant plus fort que l'information est supposée avoir un contenu technologique important. La menace de l'obsolescence s'ajoute à l'incertitude de l'acquisition. C'est pourquoi le transfert d'information s'accompagne souvent d'un cadre contractuel prévoyant la possibilité de compter sur un flux de connaissances à venir.

Supposons que l'information soit effectivement transférée, elle n'en sera pas pour autant immédiatement utilisable par son acquéreur. L'information, pour être échangée, doit s'accompagner d'une codification comprise par le vendeur et l'acquéreur. La codification { XE "codification" } est l'abstraction de l'expérience et de l'information du vendeur en des formes symboliques compréhensibles par l'acquéreur. « Ses coûts de transmission et de réception seront d'autant plus bas que les similitudes dans l'expérience de l'unité qui transfère et de l'unité qui reçoit seront grandes ³⁴⁴ ». La standardisation joue ici un rôle essentiel : maîtriser un standard, c'est avoir la possibilité de réduire le coût du transfert technologique. Des standards différents dans le domaine des technologies de l'information sont des freins à la circulation de l'information entre firmes. Les standards de codification représentent un enjeu important pour la recherche.

En effet, un savoir non codifié sera complexe et laborieux à transmettre. Il nécessitera une « traduction » pour l'adapter aux codes de la firme qui l'acquiert. Des relations stabilisées, et formalisées, entre firmes peuvent là encore encourager une codification commune de la connaissance, et réduire ainsi les coûts de transfert de la technologie. Le réseau de ces firmes pourrait être idéalement intégré par une information aux codifications nouvelles.

C'est autour de ces trois idées — nouvelles règles du jeu, structures adéquates, et nouvelles codifications de la connaissance — que peut désormais se développer notre système d'intelligence d'entreprise. Pour en décrire le fonctionnement, nos objectifs seront les suivants :

(1) Dans un premier temps, analyser le « jeu des acteurs » lors d'un transfert de connaissances d'une même industrie, ou d'un secteur « très concurrentiel comme

³⁴² KIRZNER, *Competition and Entrepreneurship*, University of Chicago Press, Chicago, 1973, pages 215-216.

³⁴³ Donald J. TEECE, « The Market for Knowhow and the Efficient International Transfer of Technology », *Annals of The American Academic Journal of Political and Social Science*, novembre 1981.

³⁴⁴ Donald J. TEECE, « The Market for Knowhow and the Efficient International Transfer of Technology », *Annals of The American Academic Journal of Political and Social Science*, novembre 1981.

celui de l'informatique, marqué de sauts technologiques importants et rapides ³⁴⁵ ».

(2) Dans un second temps, en déduire une formulation des « règles du jeu » d'un transfert de connaissances réalisé dans le cadre d'un partenariat stratégique entre deux firmes et étudier l'impact de la mise en place d'une structure de transfert de connaissances telle que nous l'avons énoncée plus haut : en quoi les concepts avancés par Teece et Williamson peuvent-ils éclairer les stratégies de rapprochement des entreprises ?

(3) Quelle codification de la connaissance est la mieux adaptée à cette dynamique du transfert des connaissances fondée sur l'approche « réseau » de Teece, Thorelli et Williamson ?

³⁴⁵ M. MOUYSSINAT, *Recherche et industrie, une volonté de coopérer*, dans « De nouveaux enjeux pour la recherche et ses applications », Publication Greco Programmation, 1988, pages 89-91.

CHAPITRE VI

Intelligence d'entreprise et compétitivité

6.1. Nature et spécificité des activités d'intelligence

6.1.1. Les enseignements tirés de l'histoire

L'entreprise est-elle en train d'accorder un sursis au panoptisme ? Pour être compétitif, on est prêt à tout... Et si cela s'avère nécessaire, on est prêt également à adopter des méthodes et des pratiques que toute organisation, dotée d'un peu d'éthique, considérerait jusqu'alors avec effroi. De l'intelligence-service à l'intelligence d'entreprise, nous assistons à une métamorphose des métiers qui peut prêter à confusion.

L'intelligence d'entreprise{ XE "intelligence d'entreprise" } réveille, chez les européens, des « consciences vigilantes »... Lecteurs de Beccaria (Des délits et des peines...), de Bentham (The panopticon), puis de Foucault (Surveiller et punir...), on peut être plus ou moins séduits par ces démonstrations pertinentes qui firent de la surveillance une « technologie du pouvoir », un moyen de conférer aux surveillés l'utilité{ XE "utilité" } et la profitabilité attendues des surveillants. Seulement, Foucault a-t-il respecté la déontologie de l'historien ? Sa lecture des énoncés reflète-t-elle la pratique de la surveillance telle qu'elle fût vécue, à la fin du XVIII^e siècle ?

Autrement dit, on peut lire Jeremy Bentham et ne pas y percevoir la « société surveillante » de Foucault... Les règlements qui ont servi d'appuis à Michel Foucault ont d'ailleurs été cassés lors d'un jugement qui eût lieu avant même leur application, mais ceci n'est finalement pas très important. L'important est qu'ils aient été écrits, que des conditions sociales et industrielles aient amenés une entreprise à énoncer un tel règlement. Il n'y a peut être pas eu une pratique effective de la surveillance telle qu'elle a été énoncée dans ces règlements, mais il

y a eu une projection de l'entreprise dans cette forme de surveillance interne et disciplinaire. Le panoptique n'était d'ailleurs qu'un modèle d'emprisonnement. Mais on peut le considérer autrement si l'on supprime la prison et qu'on analyse le panoptique en termes de flux d'informations, d'aménagement de l'espace pour pratiquer la coercition{ XE "coercition" } et pour dégager des espaces de visibilité. Le panoptique peut ainsi être traduit comme une approche spatiale et économique de la surveillance d'un environnement au sens strict : une méthodologie. Au moment où les firmes européennes désirent elles aussi « voir, sans être vues », il n'est pas inutile de retracer les grandes lignes d'un débat que nous avons cru éteint et que de nouvelles formes de concurrence sont en train de « réanimer ». Le panoptique est donc ce modèle de pénitencier imaginé par Bentham suite, nous dit-on, à la visite par son frère de la Ménagerie royale de Versailles. Les cages y étaient disposés en demi-cercle à la fois pour faciliter le travail du gardien (nourriture et surveillance), et pour offrir aux visiteurs un « panoramique » animalier plaisant. De là est née très facilement l'idée d'aménager dans un bâtiment circulaire un pénitencier offrant lui aussi ce formidable panorama pour surveiller chacun d'un seul coup d'œil. Bentham perfectionne son modèle en perçant les cellules de part et d'autre afin que la lumière découpe dans chacune d'elles les silhouettes des prisonniers. Et pour économiser le nombre de surveillants, le pavillon central de l'inspecteur est entouré de jalousies permettant à ce dernier de voir, sans être vu.

Comme nous l'avons montré, le panoptique est « une machine à dissocier le couple voir-être vu : dans l'anneau périphérique, on est totalement vu, sans jamais voir; dans la tour centrale, on voit tout sans jamais être vu³⁴⁶ ». La tentation est grande d'introduire un tel principe dans le champ de la concurrence entre grandes firmes, et le panoptique semble ouvrir de nombreux champs d'application, pour veiller, surveiller, dérouter et dissuader...

La tour centrale de ce pénitencier n'émet pourtant qu'un seul message, celui de sa présence. Elle donne au prisonnier la certitude d'être visible. Elle est un signe de menace... D'autant plus efficace que la concrétisation de cette menace est certaine ! Pour Bentham, la force de son projet, c'est son « plan » panoptique, mais aussi, la possibilité réelle de punition. Dès lors, nous sortons cruellement du champ de la concurrence d'entreprises pour retrouver l'univers pénitencier. Le panoptisme est soutenu, dans les faits, par une asymétrie{ XE "asymétrie" } dans la position du surveillant et du surveillé. L'un domine l'autre. Tandis que l'entreprise, Michel Crozier n'a pas manqué de le souligner, est un lieu de luttes, de négociations, de « jeu d'acteurs{ XE "jeu d'acteurs" } », d'intérêts personnels où les asymétries, aussi bien internes qu'externes, se font et se défont au gré d'interactions et d'interstructurations complexes. Ceux qui feront l'objet d'une démarche panoptique ne manqueront pas de mobiliser toutes leurs ressources pour inverser le jeu, pour rendre la surveillance inopérante en appuyant leur marchandage sur d'autres terrains que celui de la vigilance. Ainsi, les

³⁴⁶ M. FOUCAULT, *Surveiller et punir*, Gallimard, Paris, 1975, p. 203.

surveillances internes et externes des organisations ne peuvent-elles être elles aussi, à première vue, qu'un « jeu d'acteurs ».

Un système d'intelligence d'entreprise qui fournit à chacun la potentialité d'améliorer la connaissance de son environnement, et le traitement de l'information acquise, sera dans ce schéma lui aussi la proie des jeux, des influences et des conflits. Et l'arme redoutable destinée à surveiller l'environnement sera bientôt un outil au service d'un acteur et au détriment d'un autre. La même information peut en effet signifier le succès d'un projet et l'échec de celui d'un collaborateur. Dès lors, la diffusion interne de l'information n'est pas innocente. Elle fait l'objet d'un jeu « d'éclairages » destiné à médiatiser la réalité sous un aspect qui profite à celui qui maîtrise le mieux le canevas de la diffusion de l'information. Faut-il dans ce contexte accorder un sursis au panoptisme ? Faut-il encourager la centralisation de l'information, au risque de détruire les jeux qui trament l'organisation, en suggérant à chacun d'être l'investigateur d'autrui ?

6.1.2. Forces et faiblesses des organisations centralisées

Le débat, rassurons-nous, ne saurait être bloqué par la métaphore du jeu, ni par celle de la scène où s'affrontent dans une spirale de rivalités des groupes sociaux présumés opposés les uns aux autres... Le détour semblera facile, mais on démontrera que l'intelligence n'a pas d'autre objet que *l'intelligence*, au sens propre du terme cette fois-ci. La capacité d'être en intelligence avec son environnement, et avec soi-même, n'est-elle pas la clé du succès de toute démarche stratégique ? Pour mener à bien cette double articulation de la connaissance de soi et de la connaissance de son environnement, l'école de la centralisation rappellera à chacun que le toucher, l'odorat, l'ouïe, la vue et le goût se développent harmonieusement grâce à la constante présence de notre cerveau. Ainsi, pour regarder loin, faut-il encore regarder « avec sa tête », nous préciserait-on. Le discernement, cela s'apprend, au fil des années. Ne pas centraliser, c'est se priver de cet enrichissement du regard. Tel pourrait être le premier énoncé sur lequel nous pourrions travailler.

Prenons en considération cette métaphore neuronale de l'entreprise. La connaissance se nourrit de turbulences au cœur du « cerveau » et dans l'ensemble du « corps » de l'entreprise. Chaque connaissance partagée crée un lien, une passerelle d'un langage à un autre. Le manque de connaissance provoque une sensation de « faim » de connaître, qui peut d'ailleurs être déclenchée par un simple rappel « gustatif » : en présence d'une information qu'il a l'habitude de consommer, l'acteur va s'en saisir. La métaphore est riche d'exemples assez parlants, peut-être trop parlants d'ailleurs. Lorsque nos yeux s'ouvrent, leur connexion à notre cerveau ne relève pas d'un choix de leur part. C'est un élément de physiologie. Tandis que les yeux de l'entreprise, chacun de ses acteurs, sont d'abord ouverts pour les personnes à qui ils appartiennent. Libres sont ces personnes de transmettre ensuite au nœud central du système ce qu'elles ont bien pu voir. Le schéma centralisateur n'est pas pour autant remis en cause. L'objet de l'intelligence d'entreprise est de considérer l'information comme une ressource

(pour innover, pour entrer en compétition, pour dissuader...) qui doit être remise entre les mains des personnes qui en expriment le besoin. Dans cette gigantesque allocation des ressources informatives, la centralisation est bien le schéma idéal, à condition de connaître les besoins de chacun, et de pouvoir les satisfaire. Ensuite, la centralisation n'a pas les défauts de la fonctionnalité. Une intelligence dédiée à une fonction (l'innovation, la distribution, la commercialisation, la production...) ou à un secteur, présente l'inconvénient de ne pas pouvoir saisir les stratégies globales des concurrents. En centralisant l'acquisition et le traitement (donc les recoupements, intelligence oblige...), on perçoit ces stratégies transversales, ces systèmes d'offres globales réunissant plusieurs métiers dans la satisfaction d'un seul client.

Là où l'école de la centralisation souffre, c'est au niveau de la personne. Premièrement, si elle savait quelle information lui manque, elle ne lui manquerait pas. Tout au plus, elle pourra donc définir un profil d'information, un champ d'investigation, une « question », visant à trouver cette information. Mais là n'est pas le problème majeur. On peut très bien fonctionner à partir d'un système de questions. En fait, le problème est qu'à l'instar de l'entreprise toute entière, la connaissance de ce qu'elle cherche à savoir en dit long sur l'acteur, sa stratégie et sa performance. Avouer que l'on manque d'information au cœur de son domaine de compétence, dans le métier{ XE "métier" } pour lequel on est rémunéré, est perçu comme l'aveu d'un échec. Et puis, toutes ces questions sont fichées... Personne ne peut garantir qu'elles ne soient pas un jour les pièces maîtresses d'un dossier prouvant un « défaut de résultats ». Ou encore, qui va garantir que ces questions ne sont pas elles-mêmes évaluées afin de corriger les « potentiels » accordés à chacun des cadres ?

Là où l'école de la centralisation souffre encore, ce n'est plus au niveau des questions, mais à celui des réponses. Pour pouvoir répondre aux questions qui lui sont posées, cette instance d'intelligence centrale ne peut pas se permettre d'acheter toutes ses réponses à des consultants externes. L'idéal est pour elle de trouver la réponse en interne. Tout l'intérêt d'une telle structure réside dans son aptitude à déplacer des informations afin d'allouer les ressources à ceux qui en ont exprimé le besoin. A ce niveau, les freins personnels sont les plus forts. Donner une information à son organisation, c'est faire progresser très certainement l'entreprise et beaucoup plus hypothétiquement sa carrière. Chacun sait qu'il n'est pas évalué sur sa « cueillette » d'informations rares pour le groupe, mais sur ses résultats, comparativement à ses pairs. Et pour faire mieux que ses pairs, chacun sait également qu'il doit connaître beaucoup plus de choses qu'eux, au niveau du métier, des réseaux relationnels, des points d'appui chez les fournisseurs, chez les distributeurs... Son réseau relationnel fait partie de son « mystère » : on dira de lui que c'est un « homme du métier ». Il tient à préserver cet avantage potentiel dans la possible négociation de sa progression dans l'entreprise, ou hors de l'entreprise. La centralisation souffre de l'humain...

6.1.3. Les appâts de l'autonomie et de la responsabilisation

Si les modèles centralisateurs souffrent des réticences « humaines, trop humaines » des salariés, nous pouvons donc poser les conditions critiques du succès de l'intelligence comme suit :

1. Le système d'intelligence proposé aux salariés contribue directement à l'amélioration de leur métier, en augmentant ses performances, et en s'intégrant à ce métier comme l'une de ses composantes.

2. Le système d'intelligence est un humanisme. Au service de la compétition, il n'en respecte pas moins la personne humaine en permettant son épanouissement dans le cadre d'un métier et d'une éthique qu'il vient renforcer.

3. Le système d'intelligence, enfin, sait se faire oublier. L'idée de contrôle ne lui est pas d'emblée associée. Il est un outil convivial, d'accès facile, simple, qui rend service à son utilisateur.

De prime abord, la mise en œuvre de telles conditions semble difficilement réalisable. Quel système d'information peut prétendre à tant de qualités ? Un « non-système » peut-être... Nous connaissons le principe de ses bases de données partagées par un groupe restreint d'acteurs ayant les mêmes intérêts : chacun y contribue selon ses possibilités et bénéficie d'un ensemble de connaissances partagées. Chacun sait également que ce type de système s'éteint de lui-même au fil du temps alors que les participants donnent de moins en moins d'informations tout en espérant en obtenir de plus en plus.

En fait, un tel système ne remplit pas la condition d'humanisme. Il dépouille l'individu de son savoir spécifique{ XE "savoir spécifique" } pour nourrir un savoir collectif{ XE "savoir collectif" } qui lui échappe, qui perd du sens. Il améliore les performances d'un utilisateur mieux informé mais ne respecte pas son désir de différence, son besoin de stratégies personnelles. Il existe pourtant un moyen de décentraliser les responsabilités en préservant la centralisation d'une vision stratégique : une « intelligence intelligente ». La finesse d'esprit en matière d'intelligence consiste à quitter le champ de la manipulation des sources d'information pour entrer dans celui de la motivation des talents spécifiques. C'est ce que nous appelons une « intelligence intelligente ».

Pour quitter l'optique « renseignement » et entrer dans l'ère de l'intelligence, on cessera d'abord de considérer les salariés comme des « sources » dont la « sollicitation » permet le « retour » des informations. Chacun a des talents personnels qu'on se doit de valoriser. Pour ce faire, la constitution d'un système expert dédié à l'intelligence est une première étape. Au lieu de demander à chacun de se démunir des informations rares qui le différencient, un tel système associera à des objets de connaissance les noms de plusieurs salariés ayant une expérience connue ou déclarée de l'objet. Le système expert permet à l'utilisateur du système de « naviguer à vue » dans le champ de connaissance de l'entreprise par jeux de questions/réponses. En final, il obtient soit le nom et les coordonnées de la personne si celle-ci accepte d'être jointe directement, soit le nom du coordinateur

local à contacter avec une référence codée, soit en dernier recours, si elles existent, les références et les lieux de stockage des documents pouvant l'intéresser (en interne ou en externe). L'avantage de ce système est qu'il peut s'adapter à tout type de réseau centralisé ou cannelé, ou même « absent », si l'on opte pour l'équipement de l'entreprise en bornes interactives dont l'accès est contrôlé par une carte à mémoire. Il ne nécessite pas la création d'un énorme fond documentaire car les documents restent dans les placards et les coffres de leurs acquéreurs locaux. Seules les références de ceux-ci sont centralisées, permettant ainsi de mener une réelle politique d'intelligence : à partir de ces données, le coordinateur pourra « cartographier » les connaissances stockées dans les divisions. De plus, lorsque le système expert ne parvient pas à donner satisfaction à l'utilisateur, il peut automatiquement enregistrer le « profil » de cette information rare. Ce profil est communiqué par le système au coordinateur qui peut dresser des plans d'acquisitions d'informations à partir de ces données immédiates. On peut donc voir ce que les acteurs réclament en matière d'informations, sans être vu. Heurtons-nous, à cet instant, une limite éthique{ XE "éthique" } ?

6.2. Ethique ou performance, la fin d'un faux débat

6.2.1. Enjeux et contraintes de l'écoute de l'environnement

Enregistrer les questions d'un utilisateur à son insu n'est a priori pas très moral. Cela ressemble, pour ainsi dire, à une surveillance rapprochée de son travail et de son champ de connaissance. Nous pouvons toutefois considérer cela autrement. Chacun est conscient dans l'entreprise de la complexité grandissante de l'environnement et du décroisement intensif qui rapproche les mondes politiques, scientifiques, économiques, culturels, sociaux et technologiques en un canevas d'interrelations déroutantes. Gagner des appels d'offres, définir un cahier des charges, un nouveau produit ou un développement commercial demandent de plus en plus de capacité de synthèse et de rapprochement de domaines trop longtemps considérés comme disjoints. Chacun ressent le besoin d'être assisté face à cette complexité. Cette capacité à appréhender un tout mal défini, une globalité où l'intuition seule ne suffit plus à s'orienter, est une « renaissance » du management. L'ouverture d'esprit qu'elle requiert s'accompagnera certainement de heurts, de résistances au changement. Mais, sans nul doute, la révolution tranquille de l'information aura lieu, tandis que la question de son utilisation optimale restera encore ouverte. C'est pourquoi la question éthique doit être ramenée à sa juste mesure. Il ne s'agit pas de faire le procès d'une intelligence qui épie l'évolution de chacun en matière d'information, mais bien de se questionner sur les possibilités d'évolution de la communauté toute entière dans ce domaine.

Et s'il n'existe pas d'autres moyens de rapprocher les hommes qui savent de ceux qui veulent apprendre que l'intelligence d'un système de communication, alors il semble moral d'accompagner ainsi l'évolution des mœurs.

Dans la mesure où l'enregistrement des questions n'a pas une finalité de contrôle des individus, elle sera bien perçue. Il ne tient qu'à l'entreprise à tenir cet engagement moral de ne pas se retourner contre les personnes et se concentrer sur des problèmes d'information uniquement. L'intelligence est réellement performante lorsqu'elle se pratique en toute honnêteté. Réussir dans ce domaine n'est pas à proprement parler une question de structures, mais plutôt une question de confiance envers l'organisation. Un système rudimentaire bénéficiant d'un investissement personnel important de la part de ses utilisateurs peut se révéler bien plus efficace que nombre de systèmes dont la sophistication et le coût n'ont d'égal que l'austérité. Rompre de façon régulière le cloisonnement des métiers en est l'un des exemples. Un environnement convivial et un esprit de conciliation de la part de l'animateur de la réunion peuvent très bien suffire, dans un premier temps, à « globaliser » l'approche de l'environnement, à concevoir et détecter des menaces transversales, des entrées de concurrents sur un marché. Ce type de projections collectives sur ce que l'entreprise et ses métiers veulent être et ne veulent pas être a un fort pouvoir d'implication. Il valorise l'individu à qui on a demandé une participation effective et interactive à la vie de l'entreprise. Les environnements concurrentiels tels qu'ils évoluent actuellement demandent non seulement une maîtrise de plus en plus grande des outils d'analyse quantitative de l'information, mais également une aptitude qualitative à discerner dans un flux grandissant d'informations les liens et les volumes.

6.2.2. Gérer les volumes et les liens

L'aptitude à extraire d'un volume d'informations une donnée épurée et pertinente pour l'organisation relève du métier de chacun. C'est pourquoi la veille technologique est confiée aux hommes de l'entreprise qui sont des experts dans le domaine où ils exercent leurs veilles. Seules leurs expériences, leurs formations et leurs goûts pour les technologies qu'ils veillent nous permettent d'attendre de ces hommes cette aptitude spécifique à traduire pour l'entreprise l'avènement d'une technique en termes de modification de métier, de validité des choix réalisés ou de remise en cause. Nous sommes là dans le domaine des volumes{ XE "volumes" }.

Lorsque des volumes d'informations sont épurés, travaillés, par des hommes qui confrontent leur connaissance du métier aux données qu'ils recueillent dans l'environnement, il arrive parfois qu'une interprétation leur échappe. Elle leur échappe parce qu'elle fait appel à des connaissances liées à un autre métier, formulées dans un autre langage technique, appartenant à une spécificité qui leur est étrangère. L'attitude « classique » en la matière consiste à laisser de côté ce qui n'est pas du domaine de compétences de ce professionnel. L'étonnement existe, mais ne donne pas lieu à une stratégie de connaissance. Aucun lien n'est

construit faute d'un réflexe de communication interne, faute de décloisonnement. C'est là le domaine insuffisamment exploité des liens{ XE "liens" }.

L'intelligence est l'art de discerner des liens tout en perfectionnant le traitement des volumes. L'un ne va pas sans l'autre. L'aptitude à réduire une grande quantité d'informations en un ensemble restreint de faits pertinents, dans un temps limité, est le passage obligé d'une étude de liens. Pour gérer le renouvellement, il faut devancer l'événement, prévoir quelles « liaisons » l'entreprise peut projeter dans des domaines qui lui sont accessibles. Le lien est omniprésent. A l'instar de l'idée, il précède le plan. L'intelligence discerne les liens, identifie les chemins possibles et suscite des idées. C'est ensuite à la stratégie de bâtir des plans, en développant ces idées, en conceptualisant des signaux{ XE "signaux" } en démarches stratégiques, en traduisant en termes de positionnement{ XE "positionnement" } ce que l'environnement lui enseigne en termes de menaces{ XE "menaces" } et d'opportunités. Veiller n'a de sens que dans la perspective de l'action, et c'est dans cette perspective que la veille doit se structurer, en « intelligence » avec un environnement toujours en mouvance, très rapide, très surprenant.

6.2.3. L'intelligence : un investissement stratégique

L'excès de cloisonnement, l'appréhension de problèmes transversaux dans l'entreprise, la résolution de problèmes globaux, réclament une approche réfléchie de l'information. Celle-ci ne peut pas se bâtir à partir de rien. Elle doit être la formulation d'une stratégie délibérée de l'entreprise et de ses acteurs vis-à-vis de leur environnement. Il faut donc se constituer un « appareil d'observation » de cette intelligence. Il faut chercher dans le passé ce qui a motivé des évolutions décisives de l'entreprise. Il faut revivre les actes d'intelligence passés pour mieux comprendre l'histoire des choix, pour mieux préparer les choix futurs. L'objectif d'une analyse historique{ XE "analyse historique" } comme celle-ci n'est pas d'attribuer des causes à des échecs ou des succès. L'objectif est de comprendre et d'améliorer la relation du décideur et de l'environnement : améliorer l'usage de l'information. Beaucoup d'entreprises débordent d'informations, de comptes-rendus sur la concurrence{ XE "concurrence" }, sur les technologies et les marchés. Là encore, nous n'avons pas fondamentalement de problèmes de volumes. Nous avons un problème de complexité, de comportement malhabile vis-à-vis de l'information.

Un ou plusieurs signes précèdent toujours l'émergence d'une réalité nouvelle. La « turbulence » d'un environnement n'est en fait qu'une combinaison méconnue de ses composantes habituelles : des liens inattendus. Ces moments rares marquent des étapes décisives pour les organisations. Ils forcent le changement. Aucun plan ne peut se substituer dans ces moments-là à une compréhension rapide et pertinente de l'environnement, de « ce qui se passe ». Comprendre avant d'agir, tel est le mot d'ordre. Ce sont des moments « d'intelligence », aux sens propre et figuré du terme. Ecrire l'histoire de ses ruptures avec la logique de programmation permet à l'entreprise de « penser » son comportement vis-à-vis de l'information en termes d'erreurs à ne pas renouveler ou en termes de succès à

réitérer. L'objectif est ici de susciter une pratique réfléchie de l'information, créer un « habitat » de l'intelligence au sein du groupe, ce que Stevan Dedijer de l'Université de Lund appelle une « science de l'intelligence ».

Car il existe réellement, dans notre histoire, les bases d'une telle science. Les progrès des technologies d'archivages grâce à la gestion simultanée de l'image, du son et du texte et les progrès des sciences de la cognition peuvent trouver dans cette discipline leur point de rencontre. Le seul obstacle est d'ordre psychologique et social. La surveillance de l'environnement est encore perçue comme une activité peu digne d'être étudiée comme un objet scientifique. Et pourtant, elle fait partie des éléments de la société ayant contribué à son progrès comme la médecine, la biologie ou la physique. Certes, sa contribution au progrès de la société n'est pas toujours évidente à percevoir mais n'oublions pas, par exemple, que les vers à soie furent ramenés de Chine en Europe grâce à une opération d'intelligence et de surveillance. Les transferts de connaissance d'une civilisation à une autre sont pour la plupart initiés par des précurseurs ayant longuement « veillé » sur ses évolutions de la connaissance d'autrui. Quant au frein psychologique, ou même moral, bien qu'il ne soit pas évident que la morale joue un rôle déterminant à ce niveau, il suffit d'observer notre propre histoire pour se persuader de l'omniprésence de la surveillance dans notre quotidien depuis plusieurs siècles. C'est au travers de l'évolution de notre langage qu'il est le plus aisé de s'en apercevoir car les mots ont une histoire et leurs significations évoluent parallèlement à l'évolution même de l'homme et de la société. Pour retracer ces évolutions, l'Institut National de la Langue Française a conçu une base de données textuelle, FRANTEXT, dont le corpus réunit près de 2800 textes dans leur intégralité qui rendent accessibles en interactif 180 millions de citations. Ce sont des œuvres littéraires, traités et ouvrages d'économie, de philosophie, d'histoire..., répartis sur quatre siècles, du XVII^e au XX^e.

C'est à titre d'expérience que la base fut interrogée. L'opportunité de travailler sur 180 millions d'énoncés réunis en un seul champ de connaissance a motivé cet essai. Il s'avère que le mot « surveillance » a une histoire qui aurait certainement séduit Michel Foucault. Le mot a tout d'abord une incroyable présence. 1 514 ouvrages parmi les 2 067 sélectionnés sur la période 1780-1980 le contiennent au moins une fois. Des « propos » d'Alain (13 fois), au « crime » de Bernanos (4 fois), en passant par « les Dieux ont soif » d'Anatole France (10 fois), le mot est là, dans des contextes différents, avec des sens et des portées tout aussi différentes. Il investit aussi bien les sciences, que le roman, le théâtre, l'administration ou la médecine. Michel Foucault n'a pas eu besoin d'une telle base pour le montrer, la surveillance affiche la plus grande présence dans les textes relatifs à l'administration, à l'éducation et à la médecine. Dans l'Encyclopédie de l'éducation en France³⁴⁷, le mot apparaît 137 fois. Dans l'Encyclopédie médicale de Quillet³⁴⁸, le mot apparaît 19 fois. Dans

³⁴⁷ IPN et SEDE, Paris, 1960.

³⁴⁸ QUILLET (éditeur), *Encyclopédie Médicale*, Paris, 1965.

« L'organisation d'une préfecture » de Baradat ³⁴⁹, le mot affiche 20 occurrences. Et ainsi de suite...

C'est un mot persistant. Il suit des auteurs, comme Gide pour lequel on décèle pas moins de vingt-trois fois le mot dans douze ouvrages différents, comme Martin du Gard dans « Confiance Africaine », « Devenir », « Jean Barois », « Les Thibaud » et « Vieille France » ou encore Victor Hugo dans nombre de ses œuvres dont « Les chansons des rues », « Les misérables » et « Les travailleurs de la mer ». C'est un mot discret. Dans la très grande majorité des cas, le mot n'apparaît qu'une ou deux fois dans l'œuvre sélectionnée. C'est un mot inévitable, présent quatre fois dans le décret d'organisation de l'armée de l'air ³⁵⁰ de 1938, cinq fois dans le Code Civil ³⁵¹, cinq fois également dans « L'économie du XX^e Siècle » de François Perroux ³⁵². Le chercheur en quête de variété n'est pas déçu. Le mot « surveillance » est un mot multiple qui s'énonce aussi clairement dans le langage de l'économiste, que dans celui du romancier ou de l'homme d'Etat. C'est un mot, enfin, dont le voyage à travers le temps n'est pas dépourvu de sens. Le panoptique de Jeremy Bentham, publié en France en 1791 par l'Imprimerie Nationale, laisse des traces et l'usage du mot semble s'amplifier dans les écrits du moment. Fait significatif, il n'y a que très peu de ruptures chronologiques : le mot accompagne les réflexions des Goncourt, comme celles de Gobineau, de Giraudoux, de Proudhon ou de Gurvitch ³⁵³.

Finalement, il faudra bien se l'avouer : la « surveillance » n'est pas étrangère à notre culture et à notre évolution. Pourquoi ferions-nous un « interdit » d'un élément si présent dans la pensée des XIX^e et XX^e siècles ? Nous pouvons donc nous interroger, avec le professeur Dedijer, sur notre attitude vis-à-vis de la surveillance. N'est il pas temps de bâtir une « science de l'intelligence », à la croisée des deux sens du terme ?

Quant à d'éventuelles « solutions », laissons donc à chacun le choix de ses moyens et l'initiative de sa propre réflexion. Le propos n'est pas de métamorphoser d'une façon plus malhabile les métiers qu'ils ne peuvent le faire d'eux-mêmes. Renégocier ses relations avec l'environnement, ce n'est pas une affaire « d'intelligence service », mais « d'intelligence », tout simplement.

6.3. Organisation et systèmes d'intelligence

³⁴⁹ BARADAT, *L'organisation d'une préfecture*, Imprimerie Coopérative Toulousaine, Toulouse, 1907.

³⁵⁰ Journal Officiel n° 70, 1938.

³⁵¹ Code Civil, Imprimerie de la République, An XII, 1804.

³⁵² François PERROUX, *L'économie du XX^{ème} siècle*, Presses Universitaires de France, Paris, 1964, pages 475, 489, 525, 537 et 634.

³⁵³ GURVITCH, *Traité de Sociologie*, Presses Universitaires de France, Paris, 1967, pages 451, 455, 456, 457, 458 et 472 du Tome I.

6.3.1. Les limites des solutions uniquement structurelles

De nombreuses critiques peuvent être formulées sur la signification du terme « surveillance » selon les différentes étapes de notre analyse. L'approche a cependant pour objectif de susciter la réflexion et la prise de décision. Ainsi, nous ne ferons pas d'autre distinction entre « surveillance » et « intelligence » de l'environnement que celle qui sépare l'observation passive et l'interaction{ XE "interaction" }. La lecture de Foucault sert à éclairer cette réflexion et l'utilisation du travail de Foucault dans ce contexte reste intéressante. Il est vrai qu'une partie seulement des règlements est utilisée par Foucault pour les développements de « Surveiller et punir » et qu'au niveau historique à proprement parler, une critique peut être formulée. Les règlements pris comme témoins de la naissance d'une « société surveillante » ont été cassés par les tribunaux peu de temps après leur écriture. Cela n'empêche pas, comme nous l'avions déjà indiqué, qu'ils ont été énoncés et désirés par leurs rédacteurs. Pour ce qui est des systèmes actuels de veille, il ne peut y avoir adhésion que s'il y a conceptualisation de ce système de la part du personnel. Cette dernière peut être obtenue si chaque question sur le « dehors », s'accompagne d'une question sur le « dedans »; c'est-à-dire qu'il y ait création d'un *système de pertinence*{ XE "*système de pertinence*" } au niveau des relations internes. Pour veiller, il faut donc s'étonner. « S'étonner » est le terme adéquat, car il ne fait pas tacitement référence à une quelconque norme collective. L'étonnement{ XE "étonnement" } exprime plutôt une contradiction cognitive, un défaut d'harmonie. Il s'agit ici de bien détailler le phénomène de structuration qu'opère un acteur face à une information incertaine. On ne peut séparer ce phénomène de l'histoire de cet acteur. Prospective et rétrospective sont ainsi liées. Notre métier, notre projet et notre histoire sont nos instruments de connaissance. La communauté historique est ainsi à prendre en considération comme l'illustre la devise « Mitsui Wa Nippon » : Mitsui est en harmonie avec le Japon. Il y a donc une double harmonie, dans l'instant (cognitive) et dans l'histoire (groupe d'appartenance, culture). Le traitement de la connaissance doit donc toujours s'effectuer vis-à-vis d'un projet, et toujours comme une régulation{ XE "régulation" }. C'est pourquoi isoler la fonction de surveillance dans une « cellule de veille » peut entraîner une perte de sens de la fonction si cette cellule est trop éloignée des opérationnels, c'est-à-dire trop loin de la frontière du développement de l'entreprise. Car l'information est sophistiquée et requiert pour son traitement l'interrogation d'un métier. Entre l'approche de Chandler et celle de Williamson, pour formuler une orientation, on pourra s'appuyer sur cet aspect historique requis par toute activité de veille. Si on choisit, à l'instar de Williamson de mettre en place, d'en haut, les structures pour approcher l'intégration, on risque de s'opposer aux stratégies personnelles des acteurs.

Il ne serait donc pas inutile de concevoir les structures à partir d'une problématique de terrain : — Que veut-on produire ? — Que veut-on relier ? Par conséquent, l'approche proposée « acteurs => réseaux => codes » gagnerait peut-être à être inversée : « codes => réseaux => acteurs ». Autrement dit, comment peut-on parler de réseaux et d'acteurs sans maîtriser les formes d'échanges de

savoirs ? Il faut connaître un peu mieux ce sur quoi sont bâtis structures et acteurs³⁵⁴. La solution seulement structurelle, c'est la solution pauvre. La solution de valeur, c'est celle qui part de la situation pour effectuer un découpage entre connaissances et pouvoirs, et qui aboutit à la reconstitution du drame. Le terme « drame » offre un bon cadre d'analyse car il suggère une construction (comme au théâtre), tandis que les jeux se réfèrent à des normes collectives : des règles. La notion de jeu modélise une absence de métamorphose des acteurs et l'étonnement conduit soit à la métamorphose, soit au blocage. La capacité d'étonnement traduit la capacité de métamorphose des individus. Or, on ne peut trouver des fortes capacités de métamorphose qu'au cœur de l'évolution de l'entreprise, à la frontière du progrès, et donc « en bas » : au niveau de ceux qui voient évoluer les frontières. Il faut « descendre » dans les organisations au plus près des métiers et des stratégies d'acteurs.

6.3.2. La finalité recherchée d'un système de veille

L'intelligence est donc paradoxalement très pratiquée et rarement structurée. Un minimum de structures et une stratégie délibérée en la matière sont pourtant essentielles au développement de l'entreprise. C'est donc pour répondre à ce besoin de rationalité que nous définirons l'intelligence comme « l'art de l'utilisation de l'information environnementale dans une perspective de gestion tactique et stratégique de l'entreprise ». Cette définition, suffisamment large, nous permet de considérer l'intelligence non seulement comme la collecte, l'évaluation et la diffusion de l'information, mais également comme une approche globale de l'environnement mêlant des stratégies relationnelles à la gestion des ressources technologiques et humaines de la firme.

L'intelligence est très pratiquée. Aucun gestionnaire ne s'aventure dans un projet sans s'être « renseigné » sur ses possibilités d'aboutissement. Quand il perçoit un échantillon satisfaisant de « sorties » positives du projet (succès global, succès partiel, échec avec une solution acceptable de sortie...), il quitte la phase informationnelle pour entrer en phase décisionnelle : il s'implique, il s'engage. Il a effectué un acte d'intelligence. Comme « Monsieur Jourdain », chacun peut se surprendre à effectuer de l'intelligence sans pour cela avoir conçu un système de surveillance au préalable. La pratique a depuis fort longtemps devancé le concept. Un exercice simple permet de s'en persuader. Prenez comme cas d'analyse un projet dans lequel vous vous êtes investi récemment et posez vous les questions suivantes : « quel a été mon premier réflexe d'information ? A quels amis ou collaborateurs ai-je demandé des avis sur la question, des soutiens techniques ou affectifs ? » Vous dessinerez bientôt un « réseau » de contacts ayant chacun contribué au succès de votre projet, plus ou moins modestement, plus ou moins formellement. Vous aviez instinctivement constitué un réseau d'intelligence spécialement (mais instinctivement) conçu pour régler votre problème personnel. Quand ce dernier fut résolu, le « réseau » est mis en sommeil ou en

³⁵⁴ Cf « le jeu de la vérité » de l'Ecole de Palo Alto.

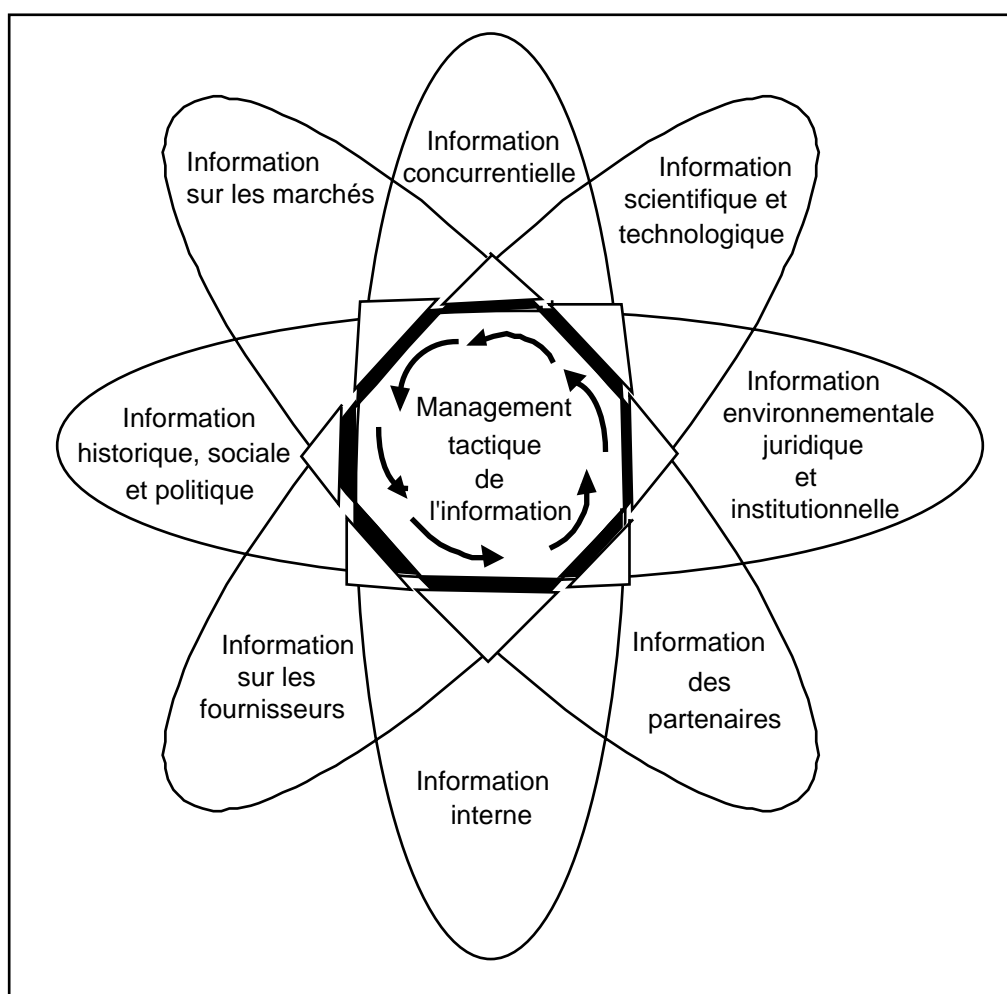
« maintenance » selon le degré de sollicitation des individus, selon les relations que vous avez avec ceux-ci. Des amis de toujours peuvent « sommeiller » assez longuement. Ils ont confiance en vous. Ils seront toujours là pour vous soutenir, tandis que vous avez certainement utilisé les compétences de personnes moins proches de vous mais qui détenaient l'information essentielle au succès de votre projet. Il n'y avait pas de lien affectif entre vous et eux, pas de connaissance interpersonnelle, pas d'histoire partagée. Intuitivement, vous avez « négocié » leur participation à votre projet. Vous n'avez jamais fait partie d'un service de renseignements mais vous en appliquez les méthodes : catégorisation des sources selon la profondeur de l'information pouvant être fournie, degré de confiance et possibilités de sollicitation. Chacun a dans son histoire des expériences d'intelligence.

Le désir de savoir est bien un élément de la nature humaine. Il ne faut pourtant pas commettre l'erreur de vouloir développer un système d'intelligence sur la seule base de cette « spécificité » humaine. L'homme a une capacité de renouvellement et de redressement après l'échec assez exceptionnelle. Cela permet des « à peu près » qu'une organisation soumise à des contraintes économiques ne peut se permettre. Le système d'intelligence soutient l'entreprise dans la formulation et la mise en œuvre de sa stratégie à long terme par une incessante action à court terme, tactique, qui vient réorienter la « vision » de l'entreprise. Si ce système est défaillant, les réorientations formulées conduiront l'entreprise à un échec dont elle risque fort de ne pas se relever.

6.3.3. Le champ de vision d'une organisation de vigilance

Chaque système d'intelligence, à côté de sa vision globale de l'environnement, possède un champ de vision spécifique. Un système d'intelligence se conçoit dans le cadre d'une ou plusieurs « visions » à long terme de l'entreprise. Cette définition du champ de vision du système d'intelligence est à relier à la nature de l'activité de l'entreprise. Une entreprise de taille internationale, devant gérer un important portefeuille d'activités, pourra concevoir une activité de surveillance dédiée au renouvellement de ce portefeuille, subdivisée en autant de systèmes « locaux » qu'il y a d'activités dans son portefeuille. Elle mettra en œuvre des « champs de vision spécifiques » à chacune de ses activités sans omettre, parallèlement, de se constituer une cellule de « vision globale » qui travaillera à l'amélioration de la vision stratégique de l'entreprise et à la détection de nouveaux métiers pour le groupe. Définir ses champs de vision prioritaires est donc la première étape de la conception d'un système d'intelligence d'entreprise. Ne nous leurrions pas : l'information coûte cher. Vouloir être présent sur tous les lieux où le devenir de l'entreprise est en jeu relève de l'utopie. En ce moment même, un acteur inconnu, un chercheur isolé, est peut-être en train de découvrir un procédé ou en train de mettre au point une technologie qui viendra « déranger » les technologies d'assise de l'entreprise. La veille « tous azimuts » ne peut être performante que dans un cadre d'action donné. Ainsi, il est possible de veiller tous azimuts autour d'un objet : par exemple, le téléphone. Une équipe très

créative, voire « subversive », peut être mise en place pour lister dans les temps les plus courts tout ce qui peut remettre en cause le téléphone, tout ce qui peut le remplacer, mais aussi ce qui peut l'améliorer. Il est rare que l'on puisse planifier les activités d'une telle équipe. Il s'agit là d'un « pari » pour l'entreprise. De ce désordre et de cet acharnement, l'entreprise découvre parfois des menaces essentielles sur son devenir, mais les coûts sont importants. De plus, une telle équipe est souvent « hors jeu » dans la mesure où son activité consiste justement à pénétrer le maximum de « jeux » existants, à s'infiltrer partout, à provoquer, pour s'informer. Cette situation de « hors jeu permanent » dérange beaucoup.



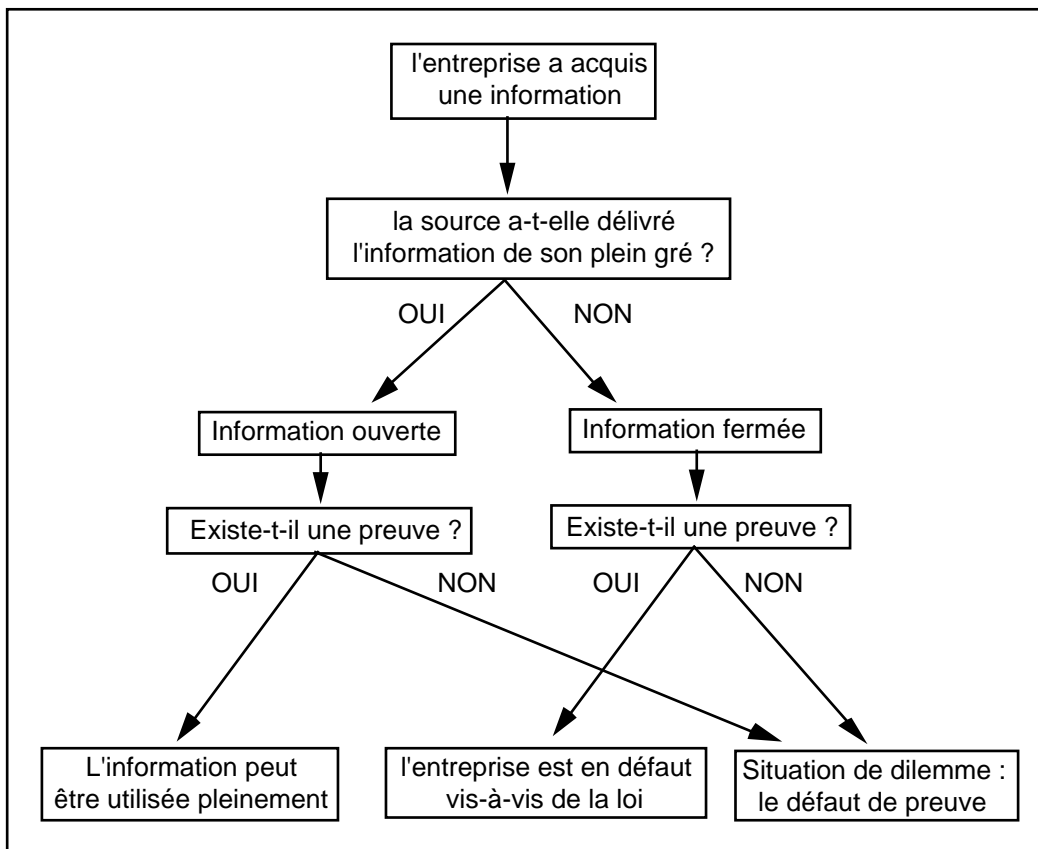
Le champ de vision d'une organisation de vigilance

Une telle équipe ne doit pas, si possible, porter le nom de l'entreprise pour ne pas nuire à son image de marque. La nature et la diversité de ce champ de vision peuvent également varier selon les groupes. Une firme multinationale aura tout intérêt à se constituer une « cellule politique » dont les activités recouvriront l'analyse des risques/pays, l'évaluation des stratégies par paires de pays (relations

bilatérales) et par organisations supra-nationales (CEE, OTAN,...) mais également le « lobbying », c'est-à-dire la délégation auprès des organisations modifiant son environnement d'une équipe défendant les intérêts de l'entreprise. Là encore, à chaque champ de vision doit correspondre un réseau spécifique. On comprend aisément qu'une entreprise ne puisse avoir qu'une seule cellule de veille centralisée et généraliste. Il lui faut une instance de coordination suffisamment créative et motivée pour insuffler la volonté de surveiller à des équipes opérationnelles, spécifiques et expérimentées.

Quand on parle de champ de vision, il s'agit bien sûr des domaines de l'activité d'intelligence, mais également des limites éthiques attachées à chacun de ces domaines. Avant de mettre en place une telle activité, un code d'éthique doit être réalisé. L'entreprise connaît et fait connaître à ses équipes de recherche d'informations les limites qu'elle s'est fixées. D'une manière générale, l'information ouverte { XE "information ouverte" } est l'information délivrée volontairement par la source. Les équipes de recherche d'informations doivent toujours pouvoir prouver le caractère ouvert de l'information qu'elles détiennent, sinon choisir de ne pas la détenir mais simplement de « s'en souvenir ».

L'information peut être utilisée de différentes manières : effectives ou virtuelles. Une utilisation effective consiste, par exemple, à révéler une information (dont on détient la preuve de son acquisition ouverte) pour contraindre un acteur soit à avouer la finalité réelle de ses manœuvres, soit son absence de moyens pour les réaliser. Il s'agit ici d'utiliser une vérité déstabilisante pour corriger des prises de position ou pour pousser cet acteur à l'erreur. L'objectif du détenteur de cette « information forte » est de modifier le langage de négociation jusqu'alors utilisé en dévoilant sa connaissance parfaite du jeu (et des enjeux réels) de l'acteur qui lui fait face. Ceci est un exemple, mais il existe de nombreuses façons d'utiliser une information validée. On peut également la garder secrète et attendre d'avoir accumulé suffisamment d'avantages pour jouer de l'effet de surprise et de l'effet de démonstration en même temps.



Informations ouvertes et informations fermées...

Quand, au contraire, l'entreprise est en défaut vis-à-vis de la loi, elle ne doit pas utiliser l'information en tant qu'émetteur. Elle se protégera en choisissant une voie détournée d'émission de cette information tout en faisant disparaître toutes preuves (documents et fichiers) de la détention de l'information. Elle choisira un tiers, qu'elle informera par provocation d'une rumeur, ou par diffusion d'un document dont on ne pourra pas désigner la provenance. On s'aperçoit aisément que ce genre de situation est d'une gestion délicate. C'est pourquoi il faut, tout en conservant le souci de performance et d'impression sur l'environnement, éviter un recours trop fréquent à l'utilisation d'une information tandis que l'on se trouve en défaut de preuves de son acquisition ouverte.

Nous retrouvons ici les liens étroits qu'entretiennent éthique, stabilité et performance d'un système d'intelligence d'entreprise. Aucun système ne peut prétendre servir l'entreprise s'il autorise ce que l'entreprise interdit. Ainsi, les codes éthiques de l'organisation d'intelligence doivent être au moins équivalents à ceux de l'entreprise toute entière. L'expérience montre que des codes plus stricts permettent un meilleur contrôle des équipes de recueil d'informations. D'une part, l'incitation au recueil ne peut se réaliser que dans un cadre motivant, donc régulier. D'autre part, les organisations d'intelligence ne diffèrent pas des autres. Leur performance nécessite un leadership qui ne tolère pas d'écarts aux règles éthiques.

6.4. Mise en place d'une cellule d'intelligence

6.4.1. Déontologie d'un exercice professionnel de l'intelligence

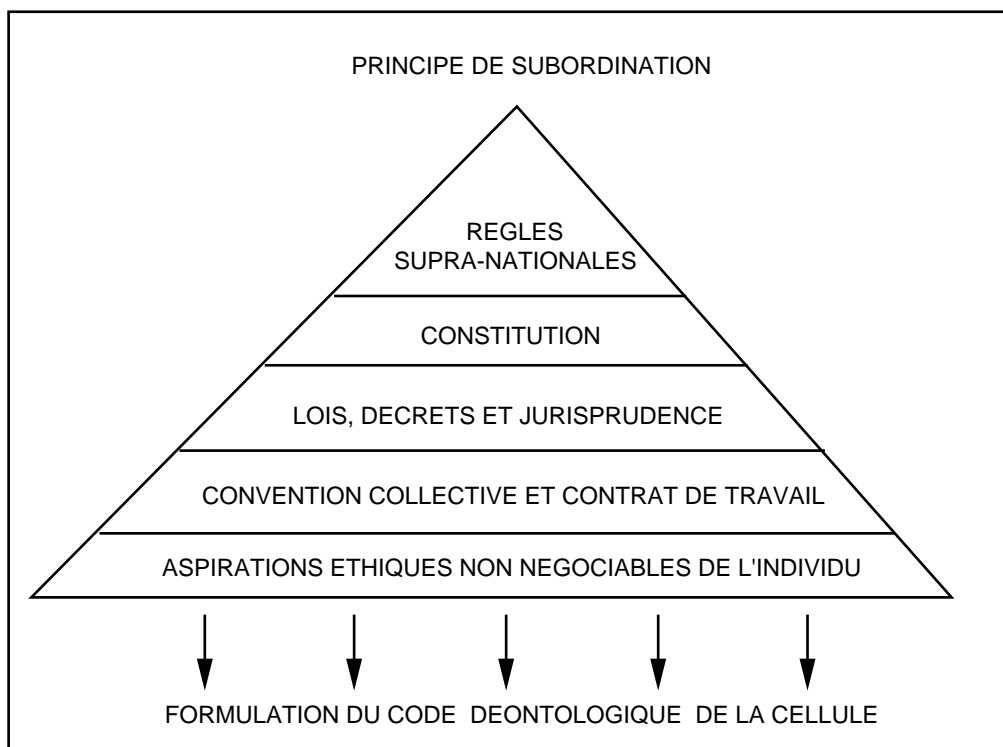
Comme l'ensemble des métiers d'information, l'intelligence nécessite des codes moraux afin que sa pratique ne dérive pas dans des domaines réprimandables par la loi. En France, la loi en matière d'espionnage est sévère³⁵⁵ mais d'une application difficile. Le seul recours indéniablement efficace reste encore la prise des coupables sur le fait. C'est pourquoi l'intelligence d'entreprise et l'intelligence d'Etat ne peuvent avoir que des actions complémentaires. L'une ayant besoin de l'autre dans les domaines où elle ne peut assurer une présence. Les termes de l'échange sont assez simples. L'intelligence d'Etat est investie d'une mission de protection des intérêts de la nation sur son territoire et sur les territoires extérieurs. Ses moyens sont adaptés à une coercition fondée sur le respect des lois. Elle dispose d'une organisation policière permettant les prises de coupables sur le fait. Elle a des marges de manœuvre dans ce domaine beaucoup plus étendues que l'entreprise. L'intelligence d'entreprise, quant à elle, défend les intérêts du groupe pour lequel elle agit. Ses moyens sont adaptés à cette activité. Les équipes de la cellule d'intelligence{ XE "cellule d'intelligence" } de la société sont rompues aux méthodologies de recueil et de validation de l'information dans une perspective économique. Leur métier mêle des compétences techniques (de gestion, de finance, de recherche, de marketing...) à une grande expertise du terrain. Ils peuvent assurer une protection efficace des intérêts économiques et technologiques de leur groupe. Ce qui ne manque pas de retombées positives pour l'Etat. Des complémentarités existent et sont d'ailleurs exploitées. Il n'en reste pas moins que l'entreprise, dans la pratique de l'intelligence, met en jeu son image de marque. C'est pourquoi cette pratique doit être encadrée par un jeu de codes déontologiques réalistes et applicables.

Il faut différencier un code dont la finalité est la censure par l'entreprise d'un membre de la cellule d'intelligence, d'un code dont la finalité est d'éduquer la pratique de l'intelligence pour la contribution la meilleure à l'entreprise. Un code de déontologie de l'information a par conséquent trois objectifs prioritaires :

- protéger l'entreprise contre les effets de la propagande ou de la désinformation réalisées par des acteurs de son environnement à son encontre,
- protéger les membres de la cellule d'intelligence contre les pressions{ XE "pressions" } internes et externes qui voudraient les faire agir dans une voie différente de celle de leur mission,

³⁵⁵ Se reporter aux articles 70 et suivants du Code pénal. On pourra noter que la loi couvre assez bien les questions liées à la protection de la souveraineté nationale, ou les délits vis-à-vis de la défense nationale, tandis que l'espionnage industriel est quelque peu délaissé par le Code. On évolue pourtant de plus en plus, dans ce domaine de l'espionnage, d'un affrontement d'Etats à Etats vers un affrontement entre entreprises... ayant des conséquences économiques graves pour les Etats qui les ont accueillies.

— garantir l'intégrité de l'information recueillie par la cellule et, par là-même, la pérennité de cette cellule.



L'élaboration d'un code déontologique{ XE "code déontologique" } de l'information pour une cellule d'intelligence est difficile à réaliser. Ce code doit respecter le droit du travail. On ne pourra déroger à la convention collective, au règlement intérieur et au contrat de travail qu'en la faveur du salarié. Ce code doit également respecter les dispositions pénales en vigueur. Mais aussi, pour être accepté et pratiqué, les aspirations éthiques non négociables des salariés auxquels on souhaite l'appliquer.

Il n'y a d'ailleurs pas de « standard » en matière d'aspirations éthiques{ XE "aspirations éthiques" } non négociables. Le premier travail du rédacteur du code déontologique de la cellule va donc être d'essayer de définir quelles sont les limites éthiques que l'entreprise et ses dirigeants se fixent de façon générale, et quelles sont les « limites personnelles » des individus qui ont été choisis ou pressentis pour constituer la cellule d'intelligence. Certaines de ces limites sont négociables. Il est prudent de les identifier. C'est souvent par mépris des « limites floues » que les organisations de ce type échouent. Il ne doit y avoir de « flou » que celui strictement nécessaire à la bonne marche d'une organisation, c'est-à-dire la zone d'incertitude nécessaire qui protège les individus les uns des autres : leur espace de compétences personnelles, le territoire opérationnel auquel ils se rattachent et s'identifient. Pour chacune des limites négociables identifiées, le rédacteur du code déontologique doit mettre en place un « encadrement » de

l'individu qui fait face au choix de transgresser ou de ne pas transgresser la limite éthique. L'objectif est ici d'éviter que l'individu négocie sa transgression selon des critères trop personnels, c'est à dire trop éloignés de son engagement vis-à-vis de l'entreprise. Le code permet au membre de la cellule d'intelligence qui est en mission d'avoir une référence de comportement « sous la main ». Ceci a de nombreux avantages. Un chargé de mission doit être totalement immergé dans le milieu sur lequel il veille. Il doit absolument minimiser ses contacts avec la direction de la cellule pour ne pas dévoiler sa mission de veille. Sa connaissance parfaite des codes d'attitudes lui permet de décider de lui-même sa façon de réagir face aux retournements de situation. Il gagne du temps car il n'attend pas la réponse de la direction de la cellule. Il suit, et ajuste selon la situation, les codes d'éthique qui lui ont été indiqués. Il n'est pas pour autant en état agentique. En effet, ces codes lui recommandent justement un investissement personnel dans l'analyse et la résolution des problèmes d'éthique qu'il rencontre, dans le cadre de butoirs lui laissant une marge de liberté suffisante pour garantir la performance de son immersion dans le milieu surveillé. C'est ce qui fait la différence entre un règlement arbitrairement imposé et un code professionnel librement consenti. Ceci n'empêche pas l'organisation de préparer et d'éduquer l'individu au consentement de ce code. On aura donc ainsi différencié des codes d'éthique issus du commun accord entre la direction de la cellule, les dirigeants de l'entreprise et les chargés de mission, et des codes d'éthique imposés par l'environnement (lois, opinion et protection de l'image de marque de l'entreprise).

Cette première distinction faite, l'élaboration des règles de fonctionnement de la cellule doit viser la protection des droits de la personne physique ou morale qui endossera la pleine responsabilité juridique de l'utilisation de l'information recueillie par les équipes de la cellule d'intelligence. Il serait inconsideré de faire systématiquement porter la responsabilité d'une utilisation illicite de l'information à la cellule d'intelligence. Ceci condamnerait la stabilité de l'intelligence dans l'entreprise. L'expérience compte beaucoup dans le recueil de l'information. Les informations les plus rares sont recueillies par les chargés de mission les mieux introduits, les plus expérimentés d'un point de vue technique et les plus « contrastés »³⁵⁶ du point de vue de la personnalité. Si le code doit avoir une fonction de dissuasion ou de coercition sur les chargés de mission, il doit être également un soutien pour le bon fonctionnement de la cellule. Le rédacteur d'un tel code pourra, s'il le désire, s'inspirer des règles déontologiques proposées ci-après :

1) un chargé de mission ne doit pas recourir à des méthodes incompatibles avec sa morale professionnelle pour se procurer de l'information,

³⁵⁶ On entend par « contrastes » de la personnalité l'aptitude de l'individu en mission de s'adapter à des interlocuteurs de tous niveaux, de toutes origines culturelles et de toutes aspirations. Ceci exige une forte capacité d'écoute et d'imprégnation, ainsi qu'une culture générale développée au fil des missions.

2) il n'utilisera pas le chantage ou l'extorsion{ XE "extorsion" }, la violence ou l'intimidation{ XE "intimidation" }, l'outrage aux mœurs établies dans le pays où il mène sa mission,

3) il ne s'introduira pas dans la vie privée d'informateurs potentiels pour dérober les informations qu'il pourrait désirer,

4) il n'aura pas de comportement susceptible d'attirer le discrédit sur l'entreprise, soit en dévoilant le nom de celle-ci lors de missions confidentielles, soit en tenant des propos dévalorisants ou ambigus à son propos lors de missions officielles,

5) il ne rejettera pas sa responsabilité vis-à-vis des informations recueillies lors d'une mission en niant avoir participé au recueil de ces informations,

6) il ne révélera pas l'identité de ses sources à d'autres personnes que celles dont les noms lui ont été notifiés lors de la préparation de sa mission,

7) il ne fera pas de plagiat d'informations, ni de désinformation, et ne validera aucune information sans pouvoir fournir une preuve, ou à défaut de preuve, une démonstration de sa validité (recoupement),

8) il ne fera aucune entorse à la solidarité professionnelle lors de la conduite de missions en équipe, il ne causera aucun préjudice moral ou matériel à ses collaborateurs et n'utilisera ni la dissuasion, ni la coercition, pour influencer la formulation d'un résultat de mission dans un sens plus proche de ses convictions personnelles,

9) il ne modifiera en aucun cas l'information qui n'a pas été écrite de sa main, dont il n'a pas assuré le recueil, et chacune des modifications qu'il apportera à ses propres informations seront datées, notifiées et motivées,

10) il ne se soumettra pas à la contrainte d'un chef de projet de surveillance dont l'objectif serait d'altérer sa liberté d'expression vis-à-vis de la direction de la cellule d'intelligence et informera celle-ci dans les délais les plus brefs,

11) il n'acceptera aucune rémunération effective ou subjective (services rendus, gestes d'amitié, « coup de pouce » professionnel) d'une personne physique ou morale pour quelque motif que ce soit car il pourrait s'agir d'une manœuvre de mise en confiance ou de création de dette (affective ou financière) à des fins d'influence{ XE "influence" }, de détournement ou d'étouffement d'information;

12) il est lié à l'organisation par le secret jusqu'aux limites extrêmes de la légalité et de la conscience,

13) il ne fondera pas son jugement sur des critères non approuvés par la direction de la cellule tels que l'impression, l'intuition, la conviction, la superstition ou l'appréhension. S'il a un avis à exprimer sur une situation qu'il ne peut justifier autrement que par l'intuition, il s'engage à notifier à la direction de la cellule que cet avis est « intuitif » et discute avec elle des modalités de validation du scénario qu'il a pu ainsi concevoir,

14) il ne passera jamais sous silence des données essentielles à l'entreprise même si celles-ci sont de nature à contrarier de façon fondamentale les projets de développement de l'organisation commanditaire,

Ce code n'est pas exhaustif. Il est donné à titre indicatif et toutes ressemblances avec la totalité ou une partie des codes utilisés par certaines organisations d'intelligence ne seraient que pures coïncidences.

6.4.2. L'audit d'intelligence d'entreprise

L'audit d'intelligence{ XE "audit d'intelligence" } précède et définit l'organisation d'une activité de veille stratégique au sein de l'entreprise. Il permet à l'entreprise d'améliorer les structures de veille existantes et d'en créer de nouvelles. Les méthodologies d'audit présentées ci-après ont été mises au point avec le soutien d'hommes de terrain de l'intelligence d'entreprise.

Ce dernier aspect est essentiel. Il confère aux méthodologies présentées l'applicabilité attendue des opérationnels. Une société spécialisée dans la réalisation de missions de veille technologique et concurrentielle dispose dans chacun des pays où elle est installée d'une « cellule d'intelligence ». Cette cellule est autonome pour la conduite de ses opérations. Elle travaille selon un cahier des charges que lui remet le centre coordinateur, situé au siège de la division concernée. Ces cellules peuvent être constituées d'équipes de quatre à dix consultants. Elles assurent le recueil de l'information en mettant en œuvre de nombreuses méthodologies : communication persuasive, techniques d'enquête et d'interview, développement de réseaux relationnels, observations de terrain, interrogation de bases de données, « épiluchage » documentaire et recoupements pour réorientation des missions. C'est donc avec l'expérience de la coordination et de la bonne marche d'une activité d'intelligence que fut réalisée la méthodologie générale de cet audit. Les objectifs de ce dernier sont les suivants :

1. Définir l'intelligence dont les utilisateurs ont besoin.
2. Etablir des profils d'intérêts et des recommandations pour chacun d'eux.
3. Lister les sources d'information disponibles et prévoir leur exploitation.
4. Définir les réseaux et les circuits de collecte de l'information.
5. Définir les réseaux d'expertise et d'analyse (internes/externes).
6. Formuler des recommandations pour la mise en place d'un système.

Définir l'intelligence dont les utilisateurs ont besoin

A chaque métier correspond une intelligence spécifique, avec ses propres réseaux et ses propres méthodes. Il n'y a pas de solution standard dans le domaine de l'intelligence d'entreprise. Il faut, cas par cas, mener des interviews, évaluer les besoins opérationnels d'information et définir, en fonction de ces derniers, des circuits de collecte et d'expertise de cette information.

Etablir des profils d'intérêt pour chacun des utilisateurs

Un programme d'interviews recouvrant les différents domaines d'intérêt de l'entreprise est donc mené. A la suite d'une réunion avec l'équipe chargée de

veiller au bon déroulement de l'audit au sein de l'entreprise, une liste de priorités est dressée. Elle définit les fonctions (R&D, marketing, production, ventes...) et/ou les divisions (par secteurs d'activités, par métiers, par pays...) où sera mené l'audit. Une liste de personnes devant être interviewées est dressée. L'audit d'intelligence a pour mission d'établir, pour chacune de ces personnes, des profils d'intérêt{ XE "profils d'intérêt" } leur étant spécifiques.

Lister les sources d'information disponibles

Pour chacune des personnes interviewées, une liste de sources d'information est produite lors d'un travail commun de réflexion. Ce travail est subdivisé en deux parties. La première partie consiste à établir une liste des sources citées spontanément en enregistrant la chronologie dans laquelle elles sont citées. La seconde partie de ce travail de réflexion consiste à augmenter cette liste en fournissant une assistance à la personne interviewée. On peut ensuite comparer les sources citées spontanément et celles dont la citation a été assistée. Dans le rapport d'enquête que réalise l'interviewer, la distinction est toujours faite entre les sources internes et les sources externes. L'ordre dans lequel se succèdent les citations des sources internes et des sources externes est également relevé.

Pour chacune des sources citées, le degré de sollicitation, la nature et la profondeur des informations estimés par l'interviewé sont analysés par le chargé d'enquête. Les circuits de collecte de l'information qui existent déjà dans l'entreprise sont ainsi mis à plat pour chacune des personnes interviewées, ceci pour permettre la réalisation de recommandations pour améliorer, réduire (en cas de trop grande dispersion) ou augmenter ces réseaux existants.

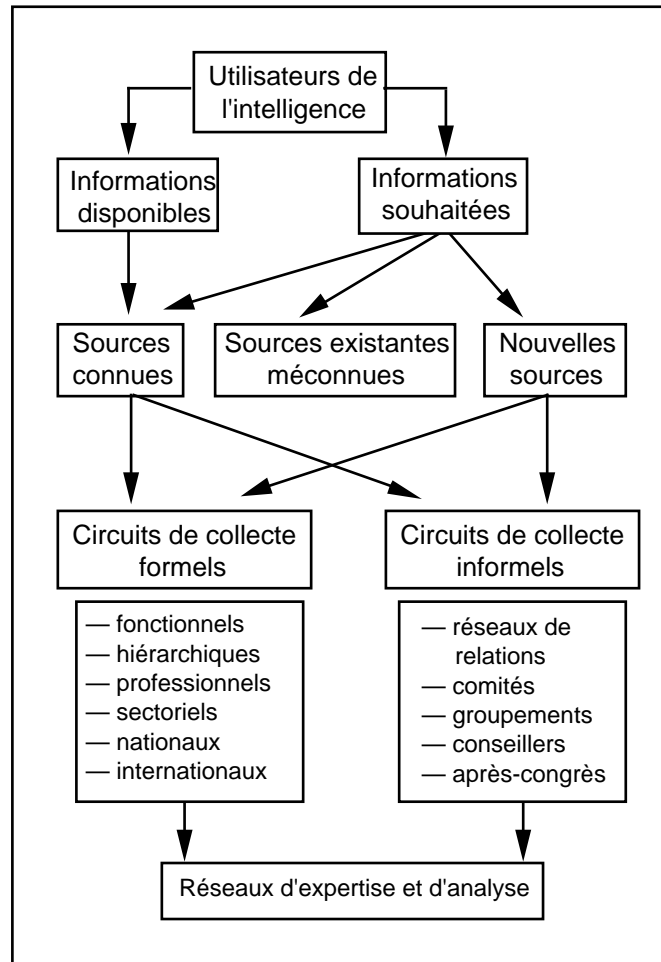
Définir les circuits de collecte de l'information

A partir des résultats des interviews, une liste de sources peu ou pas exploitées est dressée pour chaque interviewé. D'une part, ce sont des sources internes qui nécessitent la mise en place d'un circuit interne de circulation de l'information. Ce circuit est défini en coopération avec les personnes interviewées. Il est décliné en plusieurs « sous-circuits » ou « circuits spécifiques » qui peuvent être formels et informels. D'autre part, le même travail est réalisé quant aux sources externes. Un tableau de bord de gestion de ces sources est proposé dans le rapport d'enquête. Il appartient ensuite à l'entreprise de choisir si elle souhaite ou non la mise en œuvre de ces tableaux de bord au niveau de ses personnels.

Définir les réseaux d'expertise et d'analyse

Sur la base d'une typologie de besoins d'information par département ou activité de l'entreprise, une liste d'experts pouvant être consultée sur différents sujets est établie. Cette liste fait l'objet d'une informatisation qui permet une gestion dynamique des ressources informationnelles de l'entreprise. Cet outil informatique d'aide à la consultation d'experts internes et externes peut soit être placé sous la tutelle de la cellule de veille, soit être mis à la disposition de

l'ensemble du personnel en aménageant différents niveaux d'accès à l'information selon les qualités et position de l'émetteur de l'appel à expertise.



L'identification des besoins d'intelligence

Formuler des recommandations pour un système d'intelligence

L'entreprise dispose de ressources en matière de collecte et de diffusion d'informations. L'optimisation de ces ressources est l'une des missions d'une cellule d'intelligence. Le rapport d'audit fait correspondre une recommandation à chaque besoin identifié lors de la conduite des interviews. Cette recommandation comprend une proposition de plusieurs solutions pertinentes et accessibles parmi lesquelles l'entreprise peut effectuer des choix selon des critères de coût et de faisabilité.

Le déroulement de l'audit

Dans le cadre de la conduite de cet audit, des questions essentielles doivent toujours être présentes à l'esprit du chargé de mission. Tout d'abord, son langage d'intervention doit être compris de tous. Par exemple, la notion de « réseau relationnel », bien que largement diffusée par la presse, n'est pas toujours bien comprise des opérationnels. Dans la définition de ces réseaux relationnels

professionnels, l'entreprise doit écarter tout risque de confusion avec des réseaux personnels³⁵⁷, trop fondés sur l'affectif et par là même très difficilement contrôlables. Ainsi, chacun pourra faire le bilan de ses contacts selon la nature, la qualité et la quantité des informations fournies pour chacun de ses contacts professionnels.

Les questions d'un tel audit doivent donc couvrir le cycle complet de l'information et de la décision dans l'entreprise. L'audit s'attardera notamment sur les chemins que suit l'information pour atteindre les sujets interviewés. Il sera évalué, parmi l'ensemble de ces chemins, la part de ceux qui étaient ignorés de l'entreprise (canaux informels d'information, canaux formels ignorés). Cette « dimension cachée » de l'information de l'entreprise est essentielle à la construction d'un système d'intelligence performant. Il est ainsi recommandé de différencier l'information courante de l'information rare. Sont-elles obtenues auprès des mêmes sources ? Avec la même fréquence ? Dès que l'audit s'intéressera à la question de la rareté et de sa perception par l'interviewé, l'entreprise sera à même d'identifier ses carences en matière d'intelligence et de dresser la liste de ses objectifs d'informations prioritaires. Nombre d'entreprises s'étant exercées à cette forme d'audit ont été surprises de découvrir que l'information concurrentielle de base figurait en première place dans la liste des priorités...

La personne chargée de l'audit doit considérer les interviewés de deux manières. D'une part, ils sont aujourd'hui des décideurs devant accomplir le rôle que leur a affecté contractuellement l'entreprise. D'autre part, ils seront demain des « prestataires d'intelligence » quand le système sera mis en place. De ce second point de vue, ils seront délibérément de grands producteurs ou de grands consommateurs d'informations. Il est très rare qu'une personne ait matériellement le temps de produire et de consommer de l'information en grande quantité. C'est pourquoi l'audit doit identifier les « noyaux » du futur réseau d'intelligence qui seront les véritables moteurs du système : les acteurs-relais du système. Au sein de l'entreprise, l'audit est en quelque sorte un second recrutement, une « chasse de têtes » pour l'intelligence. Il faut d'ailleurs combattre l'idée selon laquelle il existe, au sein de l'entreprise, des *fonctions productrices* et des *fonctions consommatrices* d'information. On ne peut pas conduire un audit dans une telle perspective. D'une part, il est très malhabile de catégoriser les personnes en producteurs et consommateurs avant de mener l'audit. D'autre part, le système d'intelligence doit tout autant être au service des opérationnels (forces de vente, ingénieurs, équipes administratives...) qu'au service de la direction générale, du plan stratégique, du marketing ou de la R&D. Les questions clés auxquelles le rapport d'audit devra répondre sont donc les suivantes :

³⁵⁷ Chaque entreprise est libre d'inciter son personnel à développer des réseaux d'intelligence en dehors des limites strictes des contacts professionnels, mais il s'agit là d'un franchissement d'une frontière éthique dont la résultante est la création d'une zone de flou supplémentaire dans le système d'intelligence.

1) La notion de réseau relationnel{ XE "réseau relationnel" } est-elle bien comprise de tous ?

2) Chacun a-t-il fait le bilan de ses contacts selon la nature, la qualité et la quantité des informations fournies par chacun d'entre eux ?

3) Existe-t-il un moyen, au sein de l'entreprise, de connaître rapidement les compétences distinctives de chacun ?

4) La direction générale montre-t-elle la volonté de mobiliser le personnel dans le recueil d'informations pour l'entreprise ?

5) Chacun sait-il *qui* il peut informer utilement ? *Qui* peut l'informer ?

6) Chacun connaît-il ce qui différencie une information ouverte d'une information qu'il ne doit pas divulguer ?

Plusieurs méthodologies d'audit d'intelligence sont actuellement pratiquées par les entreprises. Les questions suivantes permettront à chacun de bâtir un questionnaire adapté à l'entreprise dans lequel il compte mener l'audit.

La mission de l'auditeur

L'auditeur a pour mission de tracer les circuits d'information de l'entreprise et de détecter leurs faiblesses et leurs forces. Pour chaque personne interviewée, il s'efforcera donc de déceler les « points d'attaches » de celle-ci à l'intérieur et à l'extérieur de l'organisation. Il pourra s'aider des questions suivantes :

1) Quelles sont vos responsabilités au sein de votre entreprise ?

2) Avec qui travaillez-vous régulièrement ?

3) Quels types de décisions prenez-vous ? Avec quelles fréquences ?

4) Quels types de rapports écrivez-vous ? Avec quelles fréquences ?

5) A qui communiquez-vous vos résultats ?

6) Quelles informations utilisez-vous pour vos décisions et rapports ?

7) Qui vous fournit l'information la plus intéressante ? Est-ce régulier ?

8) Comment l'information vous parvient-elle ?

9) Pourriez-vous décrire les contacts les plus utiles à votre information dans l'industrie ?

10) Comment jugez-vous l'information dont vous disposez d'une façon générale : fiable ? adéquate ? en quantité suffisante ? obtenue à temps ?

11) Etes-vous vous-même fournisseur d'informations pour vos collaborateurs ? Lesquels ? De quelle manière ?

12) Quelles améliorations souhaiteriez-vous obtenir en matière d'information ?

13) Souhaitez-vous mentionner autre chose ?

6.4.3. Cellules opérationnelles et cellules de coordination

Pour mettre en œuvre un système d'intelligence efficient, l'entreprise a recours à deux formes de cellules placées à différents niveaux de la hiérarchie et remplissant des missions différentes.

Les cellules de coordination{ XE "cellules de coordination" } ont pour mission de rapprocher des besoins et des sources d'information. Elles coordonnent l'acquisition et l'utilisation de l'information par l'entreprise. De telles cellules ne peuvent être efficaces qu'à condition de leur confier, en supplément, un rôle d'arbitrage quant aux priorités de l'entreprise en matière d'informations à acquérir. C'est pourquoi ces cellules sont à l'interface des directions locales (laboratoires, forces de vente régionales, département marketing d'une division...) et des opérationnels (commerciaux, chercheurs, ingénieurs...).

Les cellules opérationnelles{ XE "cellules opérationnelles" }, quant à elles, n'ont pas de rôle d'arbitrage vis-à-vis des priorités de l'entreprise. Leur mission est le recueil de l'information selon les cahiers des charges que leur ont confiés les cellules de coordination. L'entreprise ne peut évidemment pas disposer de la totalité des cellules opérationnelles dont elle aurait besoin. C'est pourquoi ces cellules sont avantageusement remplacées par des cellules opérationnelles privées, externes à l'entreprise et ayant développé de fortes expertises dans leurs domaines de spécialités. Sous-traiter des activités de veille peut s'avérer très utile. D'une part, l'entreprise est protégée par l'écran que constitue cette société spécialisée dans la veille technologique et concurrentielle. D'autre part, elle bénéficie de l'expérience de cette société dans les pays, ou au niveau des secteurs, où elle exerce son expertise. Bâtir de solides réseaux relationnels est en effet laborieux et coûteux. Afin de développer une capacité de réaction plus vive, l'entreprise a dans de nombreux cas tout intérêt à bénéficier des réseaux existants (même si leur accès est payant).

Pour débiter son système d'intelligence, l'entreprise pourra consacrer ses efforts dans le domaine de la veille concurrentielle. Cela semble contredire les propos en faveur d'une approche globale de l'environnement tenus jusqu'ici, mais d'un point de vue tout à fait pratique, la mise en œuvre d'une cellule est si délicate qu'il est préférable de commencer par l'information purement concurrentielle. D'une part, le système apportera ainsi des résultats plus rapides et se trouvera justifié vis-à-vis d'une direction générale souvent réticente à ce genre de projets. D'autre part, les méthodologies de la veille concurrentielle sont les plus simples et les plus accessibles. Ceci ne signifie pas que l'information concurrentielle soit une information simple, bien au contraire. Elle est cependant entourée d'enjeux à court terme si importants pour l'entreprise qu'il existe une sorte de « paradigme » de l'analyse concurrentielle dont l'entreprise pourra tirer profit en se replongeant dans ses classiques : Ansoff, Aguilar, Porter, Ohmae... En dernier lieu, l'information concurrentielle est parmi les informations les plus tangibles³⁵⁸. L'information culturelle, sociale ou politique est beaucoup plus proche du domaine de « l'intangible ». Leur appréhension soulève la plupart du temps des conflits d'opinions et d'intérêts qui menaceraient très rapidement la pérennité du système d'intelligence. Ceci ne signifie pas, encore une fois, que l'entreprise ne parviendra pas un jour à disposer d'un dispositif d'intelligence couvrant tous les

³⁵⁸ Au sens où elle est souvent accompagnée d'un déploiement réel d'actions concurrentielles (investissements, lancements de produits, retraits).

champs d'information. Ces précautions ne sont pas vaines. De nombreuses entreprises, en cédant à une tentation quasi néopanoptique, ont placé des « figures d'argile » à la tête de leur service d'intelligence. Méconnaissant totalement l'intérêt, et la nécessité, d'une réelle capacité d'intelligence, ces entreprises ont choisi l'usage de forces uniquement virtuelles, non accompagnées de forces réelles. On retrouve à la tête de leur service d'intelligence des hommes peu entourés, peu équipés et sans budget, remplissant une fonction d'impression dont l'efficacité peut être mise rapidement en doute par la concurrence. De même, les entreprises qui annoncent qu'elles fondent leur connaissance des environnements concurrentiels sur la consultation de base de données commettent l'erreur de communiquer à leurs concurrents la faiblesse de leur dispositif. Les bases de données, rappelons-le, ne sont pas des dispositifs d'information suffisants. Rien ne remplace l'information « de terrain ». Une réelle capacité d'intelligence est atteinte quand l'organisation est capable d'aller chercher sur place l'information dont elle a besoin pour orienter sa stratégie. L'intelligence n'est donc pas un exercice de prospective.

les 7 questions-clés de la veille concurrentielle

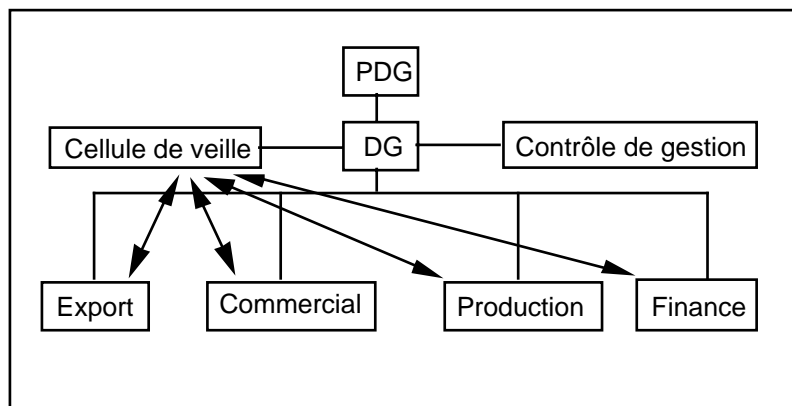
1. Quels sont les métiers de nos concurrents ?
2. Atteignent-ils aujourd'hui leurs objectifs ?
3. De quoi seront-ils capables dans le futur ?
4. Qu'est-ce qu'ils ne pourront jamais faire ?
5. Comment voient-ils leur futur ?
6. Leur futur et le nôtre sont-ils appelés à se croiser ?
7. Cela conduira-t-il à l'évitement, l'entente ou l'affrontement ?

Son objet n'est pas d'imaginer des futurs lointains et incertains, mais plutôt de contribuer à une meilleure appréhension du futur proche de l'entreprise. Une cellule de veille performante est une cellule reconnue comme utile par ses utilisateurs. L'information qu'elle leur fournit doit être immédiatement applicable à la conduite de leurs affaires. Pour atteindre cet objectif, la cellule de veille pourra organiser son recueil d'informations en essayant de répondre aux sept questions clés ci-dessus.

On le constate sur ce tableau, l'intelligence est un outil tactique de l'entreprise. Sa finalité, comme nous l'avions précédemment montré, est d'aider l'entreprise dans la conduite de ses manœuvres d'approche de son environnement, que ce soit dans des perspectives d'affrontement, d'alliance ou d'évitement avec la concurrence. La nécessité de son existence dans l'organisation n'est donc plus à démontrer, mais quelle sera sa place ?

Les expertises à ce sujet sont nombreuses et contradictoires. Pour que la cellule de veille soit efficiente, elle doit acquérir un degré d'autonomie minimum

vis-à-vis du fonctionnement interne de l'entreprise. Si la cellule est placée sous une direction technique, elle sera sans aucun doute au service de cette direction et risque de défendre des points de vue plutôt que de décrire des faits. D'un autre côté, si cette cellule de veille est trop proche de la présidence de l'entreprise, elle sera perçue comme une instance de contrôle de la performance fonctionnelle ou divisionnelle. En conflit permanent avec les opérationnels, elle perdra du sens à leurs yeux et ne sera plus sollicitée. Cela conduira la cellule de veille à devenir une « fonction d'argile », comme nous l'avions précédemment qualifiée. A ce niveau de l'analyse, il faut distinguer les cellules au service de petites et moyennes organisations et les cellules des grandes entreprises. Dans les PME, la cellule de veille{ XE "cellule de veille" } est constituée d'une petite équipe dont le contact avec les opérationnels et les fonctionnels de l'entreprise est facilité par la taille restreinte de l'organisation. Si le climat social est bon, il n'y a alors aucun inconvénient à placer cette cellule auprès de la direction générale de l'entreprise. Elle remplira d'autant mieux son rôle d'interface entre la vision stratégique de l'entreprise et ses manœuvres tactiques que sa crédibilité sera assise au sein de l'entreprise.

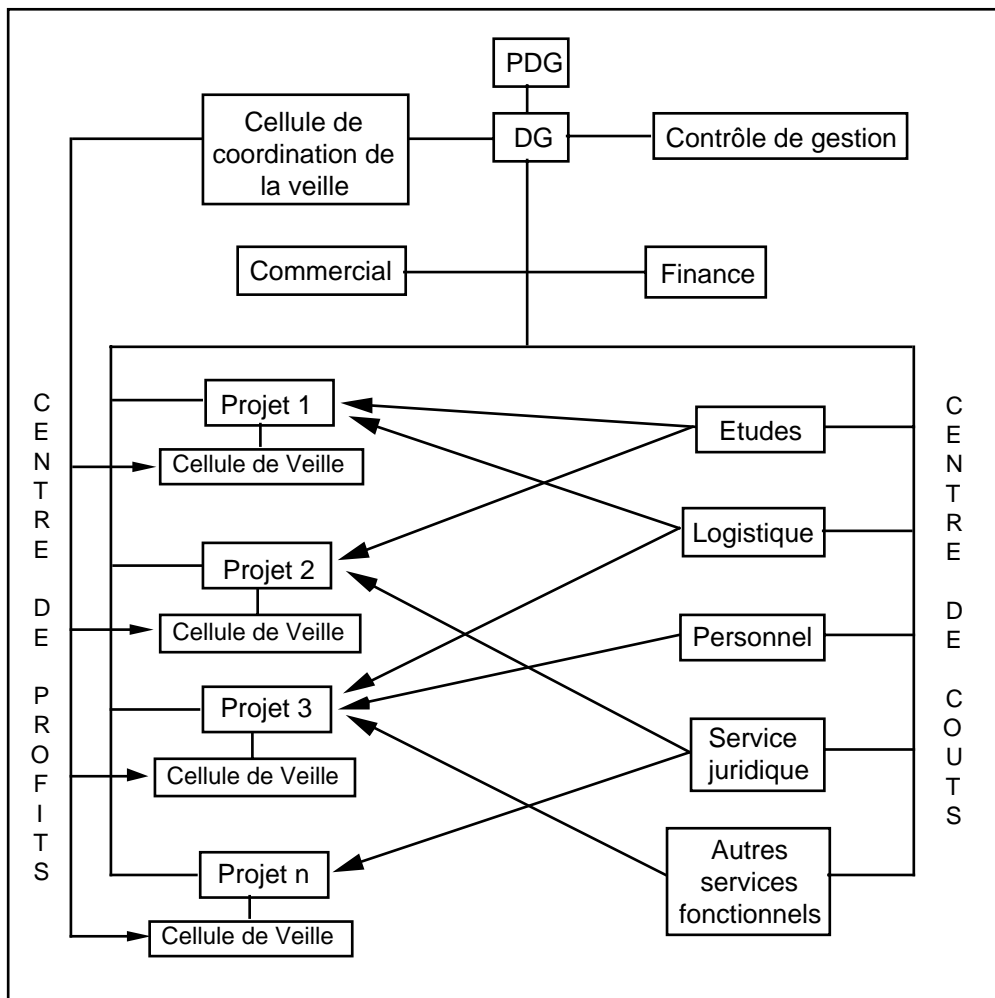


Cellule de veille dans une petite ou moyenne organisation

Dans une entreprise de taille médiane, c'est-à-dire possédant une technostrucure{ XE "technostrucure" } conséquente, il est sage de ne pas noyer la cellule de coordination au sein de cette technostrucure en dispersant les cellules opérationnelles au sein des différents services. Cela contribuerait à renforcer inutilement le pouvoir de la technostrucure en lui confiant l'accueil de la cellule de veille, c'est-à-dire le contrôle d'une partie de l'information de l'entreprise. On ne peut cependant pas placer cette cellule de coordination au-dessous de la technostrucure, sinon son pouvoir en serait limité et elle perdrait toute autonomie d'action pour ses opérations d'intelligence. On ne peut pas non plus placer cette cellule entre la direction et la technostrucure, car elle serait sans cesse la proie de conflits entre les dirigeants et les fonctionnels. Chacun y verrait un moyen d'influence sur l'autre. La cellule de coordination ne trouve apparemment pas sa place dans les organisations de tailles médianes. Le

problème est important car la filialisation des activités des grandes entreprises a multiplié le nombre de ces organisations médianes. Il y a deux solutions pour ce type d'organisation. La direction générale peut choisir de coordonner elle-même l'intelligence de la société. Elle nommera au sein de l'équipe de direction un conseil permanent chargé des questions d'intelligence et coordonnera ainsi toutes les activités de veille. Ce faisant, elle isolera la fonction de veille au sein de l'entreprise et devra faire appel à des consultants extérieurs pour mener ses opérations d'intelligence. Elle gagnera en sécurité{ XE "sécurité" } ce qu'elle aura perdu en implication du personnel dans la vigilance globale de l'entreprise. Cette solution, comme on peut le constater est assez peu nuancée. Elle peut être retenue quand l'entreprise ne comporte aucun système de veille et ressent le besoin de recourir à l'intelligence de façon exceptionnelle, pour se protéger de l'entrée imminente d'un concurrent dans son secteur, par exemple.

Il existe cependant une autre solution qui consiste à ignorer les clivages fonctionnels et divisionnels de l'entreprise pour ne plus prendre en considération que des projets et leurs logistiques. Les divisions continuent d'exister. Il ne s'agit pas ici de réorganiser l'entreprise. Pour ne pas subir les conséquences possibles des stratégies spécifiques d'une division ou d'une fonction, l'activité de veille est simplement organisée sous la forme de projets. A chaque projet est associée une cellule de veille. Cette cellule est soit constituée au sein de l'entreprise, soit privée et sollicitée au moyen d'un contrat de veille ponctuelle avec une organisation spécialisée dans ce type d'opérations. Les différentes fonctions de l'entreprise seront alors considérées comme des prestataires de service vis-à-vis des projets. Cette conception de la veille dans l'organisation permet de mettre en œuvre un contrôle de gestion{ XE "contrôle de gestion" } efficace des opérations d'intelligence. La contribution de l'intelligence au succès de l'entreprise est d'autant plus mesurable que celle-ci est spécifique à un seul projet. Le coordinateur des opérations de veille pourra ainsi dresser un tableau de bord de l'avancement des opérations d'intelligence par projets. Un tel système d'intelligence procure en outre l'avantage de crédibiliser la fonction de vigilance économique et technologique au sein de l'organisation, à condition toutefois que les cellules opérationnelles attachées aux projets remplissent bien leur rôle : faire de l'information pour l'action. Si une telle structure est adéquate pour des entreprises de taille médiane, elle l'est moins pour des entreprises de taille internationale. L'entreprise peut alors choisir de dupliquer une structure de veille par projets au niveau de chacune de ses divisions.



Approche « projets » et intelligence d'entreprise

Et on revient au cas de figure précédent, à la différence près que l'entreprise de taille internationale aura certainement du mal à coordonner l'ensemble des projets de toutes les divisions pour obtenir une vision globale de son environnement. A ce niveau de l'analyse, il faut différencier les industries multi-domestiques (ou multi-divisionnelles) des industries globales. Dans le cas d'une activité multi-domestique, l'interdépendance des différents marchés peut être relativement moindre. Le besoin d'une vision globale de l'environnement international de la firme ne figure dans la liste des facteurs critiques de pérennité de l'entreprise. Il en est de même lorsque l'entreprise voit son activité divisée en des métiers fondamentalement différents. Mais, d'une part, ce cas de figure est assez peu fréquent, et d'autre part, l'histoire a montré que des métiers que l'on pensait foncièrement distincts se sont rejoints dans une relation de forte interdépendance (optique et électronique, électricité et métaux, usinage et numérisation, mathématique et biologie...). On constate ainsi que le cadre d'analyse des entreprises ne saurait plus être la totalité non chronologique de ses marchés locaux mais son *industrie mondiale*. Cette interdépendance grandissante des

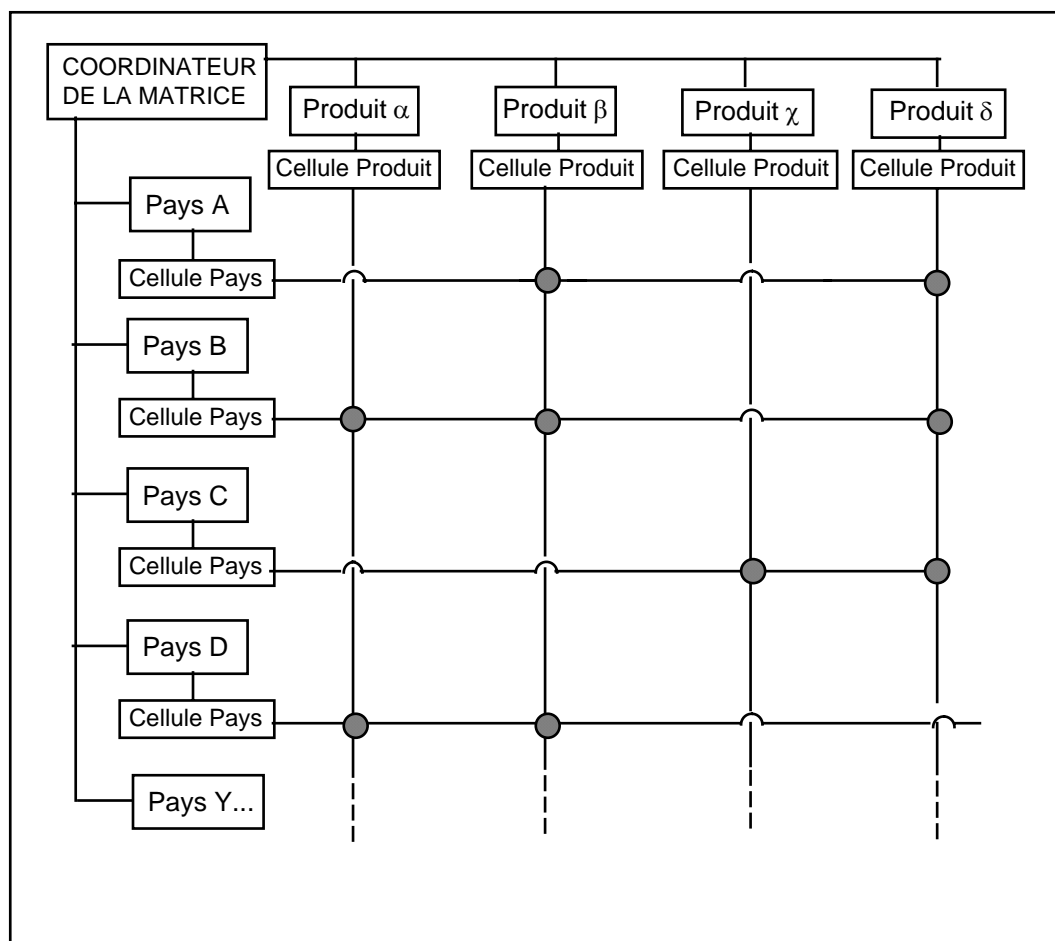
nations et des industries mondiales nécessite la mise en place d'une intelligence globale pour percevoir des menaces qui parfois naissent au Japon, au Brésil, à Singapour, pour contrarier des entreprises qui n'appartiennent plus à un secteur d'un pays particulier, mais à « l'industrie » visée d'une façon générale. Dans un tel contexte, la menace la plus grande est peut-être le risque d'ethnocentrisme des approches occidentales de l'intelligence et du marketing international³⁵⁹. Les enjeux d'une industrie globale sont cependant économiques et il n'est pas certain qu'il y ait une réelle alternative entre le multi-domestique et la globalité. La persistance et l'acharnement de la concurrence encouragent le plus souvent l'entreprise à globaliser son approche avant même qu'elle en ait formulé le choix. De plus, que l'entreprise ait choisi une politique de standardisation de ses produits, ou d'adaptation systématique aux exigences locales, le besoin d'intelligence est identique. Dans le premier cas, c'est-à-dire la standardisation, l'intelligence aidera l'entreprise à lutter contre le syndrome du « S.R.C »³⁶⁰ en améliorant les visions locales pour créer un produit global accepté par chaque culture. Dans le second cas, l'intelligence permet à l'entreprise d'améliorer sans cesse l'adaptation optimale qu'elle recherche. De plus, les alternatives entre approche standardisée ou adaptative des marchés sont de plus en plus nuancées. Grâce à une organisation modulaire de la production et au partage commun des ressources de l'entreprise (R&D, unité de production de produits semi-transformés, services juridiques...), il est désormais possible d'obtenir des combinatoires standardisées de production, et différenciées de finition et d'adaptation des produits en fin de chaîne.

C'est pourquoi les entreprises de tailles internationales peuvent opter pour une organisation matricielle de leur intelligence. L'atout d'un tel choix est très certainement qu'il n'oblige pas l'entreprise à opter elle-même pour une réorganisation matricielle de ses activités. C'est simplement la cellule mondiale de coordination des opérations de veille qui « crée », sur le papier, cette matrice comme un outil de coordination. Cela nécessite bien sûr la présence d'un correspondant local dans les pays et à la direction des produits, mais l'entreprise peut très bien être organisée « par produits » ou « par pays » sans que cela constitue un obstacle au système matriciel d'intelligence.

Le fonctionnement d'une telle matrice{ XE "matrice" } est assez simple. Une direction produit, celle du produit α sur notre schéma par exemple, sera chargée d'établir une vision « verticale » du produit, de sa conception à sa commercialisation dans l'ensemble des pays où il est présent. De leur côté, les directions de chaque pays fourniront au coordinateur une vision « pays » en tenant compte dans leurs analyses de l'ensemble des produits présents dans leur zone géographique. Les deux visions, géographiques et produits, sont constamment confrontées par le coordinateur de la matrice.

³⁵⁹ Voir à ce propos les travaux de J.A. LEE, « Cultural analysis in overseas operations », *Harvard Business Review*, n° 3, mai-juin 1966, pp. 106-114.

³⁶⁰ « Self Reference Criterion », terme que l'on doit à J.A. LEE (Op. Cit., 1966) qui consiste à une propension incontournable à se référer à ses propres critères et schémas culturels.



Une organisation matricielle de l'intelligence

Quand ce dernier relève une incohérence, ou un signal d'opportunité ou de risque, il peut mettre en place une concertation d'urgence afin de préparer au plus vite *la réponse globale* de la part de l'entreprise aux signaux détectés.

La réussite d'une organisation matricielle{ XE "organisation matricielle" } de ce type repose cependant sur une gestion rigoureuse des cellules de coordination et des cellules opérationnelles de l'entreprise. Le schéma ci-dessus présente l'organisation d'une cellule opérationnelle et son encadrement par une instance coordinatrice et une instance de contrôle et de sûreté. Le coordinateur, qui est en fait constitué d'une équipe de coordination dans le cas d'une organisation matricielle, assure les liaisons fonctionnelles de l'ensemble des cellules de terrain avec d'éventuels services regroupés de l'entreprise (R&D, direction financière...). Il planifie l'ensemble de l'activité des cellules organisationnelles en leur fournissant des cahiers des charges de recueil d'informations qu'il a produits grâce à sa position centralisée, à l'écoute de la direction générale et des opérationnels. Ces cahiers des charges, « pays » et « produits », ne constituent pas l'ensemble du travail des cellules opérationnelles. Celles-ci ont bien entendu un rôle de détection des signaux d'opportunités et de menaces en supplément de leurs

activités dirigées (benchmarking). En dernier ressort, le coordinateur de la matrice est responsable des bons ou mauvais résultats de l'intelligence de l'organisation.

Sur le terrain, il existe également une coordination, mais elle est essentiellement opérationnelle. Il s'agit d'une connaissance des besoins locaux en information et d'une gestion du temps de l'équipe de recueil de l'information. Un responsable de la coordination des opérations recueil a donc pour mission de détecter au niveau de sa filiale dans le pays, ou au niveau de la direction du produit, les besoins d'information de ses collaborateurs. Il ajoute au cahier des charges que lui a confié le responsable de la matrice d'intelligence l'ensemble des missions qu'il considère comme importantes localement.

Afin qu'une fonction « mémoire » soit remplie localement, les analystes spécialisés, qui sont chargés de réaliser des critiques et des synthèses des informations recueillies, communiquent au coordinateur des opérations l'ensemble des sujets qu'ils souhaitent voir approfondir.

Ces analystes spécialisés sont importants pour les cellules opérationnelles. Ils rédigent en effet les rapports d'étonnement qui permettront, après recoupements, de détecter des signaux de menaces ou d'opportunités pour l'entreprise. On peut noter que ces spécialistes ne sont pas forcément des permanents de la cellule opérationnelle. Il peut très bien s'agir d'un cadre supérieur ou d'un expert appartenant à l'entreprise auquel on a confié, temporairement, cette mission d'analyse. Dans tous les cas de figure, le nom de l'analyste est attaché à la synthèse réalisée. Afin que les travaux d'analyse ne soient pas influencés par l'émetteur de l'information, les sources ne sont pas systématiquement mentionnées sur les textes à étudier. Un analyste peut en effet être influencé, positivement ou négativement, par la provenance de l'information. De plus, cela réduit le risque d'entente entre une « source » et un analyste afin de faire passer une idée auprès des instances de coordination du groupe. Pour assurer l'indépendance de l'analyse des contenus et de l'évaluation des émetteurs, ce « masquage » des sources est d'ailleurs très utile. Un contrôleur local de la qualité des sources d'information a pour mission de tenir à jour une base de données, non connectée, de l'évolution de la qualité des sources. Il leur attribue un degré de fiabilité qui pourra être consulté, le cas échéant, lors d'un doute quant à la véracité d'une information. Le contrôleur de la qualité des sources participe donc au recoupement des informations en attribuant des scores de validité à chaque étape de la confrontation des informations connues et nouvellement acquises.

Ce travail de recoupement peut être utilement réalisé au moyen d'une base de données. Si le besoin de ce recoupement n'est pas ressenti dans les huit ou dix premiers mois de fonctionnement de la cellule, il est impossible, passé ce délai, de réaliser des recoupements de grande qualité eu égard au volume croissant d'informations traitées par la cellule. L'administrateur de la base de données est le technicien de ce recoupement. Il saisit les analyses et les synthèses, et les

archive selon une typologie de critères qui pourra être utilement identique dans chacune des cellules du groupe.

Selon l'importance des besoins de la filiale ou de la direction produits, cette base de données peut approcher la perfection d'un système informatique d'aide à la décision en comprenant un disque optique numérique (D.O.N) sur lequel sont archivés l'ensemble des images digitalisées des documents ayant servis aux recoupements et à la rédaction des synthèses. Cet archivage peut être accompagné d'une liste de mots clés permettant, si le besoin s'en ressentait, d'imprimer un ensemble de documents-sources relatifs à un même sujet pour effectuer des recoupements complémentaires.

Les méthodes de traitement des données doivent être étroitement surveillées. Une personne, au sein de cette cellule, prendra la responsabilité de ces méthodes. Il est facile d'imaginer quelle pourrait être la conséquence d'une modification de critères de recoupement sur le fonctionnement d'une cellule. La veille informatisée présente l'intérêt d'une plus grande efficacité d'importants volumes d'informations, mais comporte en elle le risque de systématisation d'une erreur. C'est pourquoi un responsable sûreté doit sans cesse protéger la cellule opérationnelle de toutes influences externes, et même internes, à l'entreprise. Il veille également à la sécurité des systèmes d'information et à la protection du stockage des données.

Tel peut être le fonctionnement d'une cellule opérationnelle. Il faut cependant noter que de telles cellules sont peu fréquentes, sans que cela empêche certaines entreprises qui surveillent d'être performantes. Une organisation ayant compris la logique de fonctionnement de la veille active peut très bien, si elle possède des cadres motivés, mettre en place une cellule de taille inférieure. Dans tous les cas, l'entreprise ne doit plus penser à l'information avec une logique d'amateur, poussée par la curiosité « d'essayer elle aussi » ces fameuses opérations d'intelligence qui ont fait le succès d'entreprises concurrentes, qu'elles soient japonaises, allemandes, américaines et même parfois françaises. La veille, et *a fortiori* l'intelligence, sont des métiers. Ils nécessitent, comme nous l'avons montré, des méthodes, de la réflexion et de l'implication. Peu importe, finalement, si l'entreprise n'a pas les moyens, dans un premier temps, de se doter d'une vision globale de son environnement. L'important est la justification économique du montage d'une cellule d'intelligence. Veiller par mimétisme, veiller pour justifier a posteriori des décisions prises là où entreprise « ne voyait goutte ³⁶¹ », veiller pour occuper un cadre supérieur que l'on ne souhaite pas voir être occupé ailleurs... Tels sont les dangers pour la compétitivité de l'entreprise à l'aube d'une période économique où l'on pourra, sans aucun doute, clairement distinguer les veilleurs des suiveurs.

³⁶¹ Selon l'expression consacrée de PIRON, « La Métromanie », manuscrit du XIV^e siècle, Paris, Bibliothèque Nationale.

Conclusion

Nous avons pu montrer, au cours de cet ouvrage, que la surveillance s'exprime dans sa genèse au travers d'une structure en réseaux. Par sa dimension historique, elle rappelle l'éclat des supplices du XVIII^e siècle³⁶², ou encore la direction des ateliers industriels telle que la préconisait Taylor³⁶³, avec un quadrillage précis des espaces et une mesure cadencée du temps. Par sa dimension politique, elle suggère que toute organisation sociale est un tissu de relations interpersonnelles, un canevas de relations de pouvoir pour lesquelles la surveillance, à l'instar du double corps du roi de Kantorowitz, est un outil tactique aussi bien qu'une garantie de pérennité. Avec l'utilitarisme de Jeremy Bentham³⁶⁴, elle devient une pratique économique, et s'inscrit déjà, en 1791, dans une perspective de compétitivité, par les coûts, d'une organisation productive.

C'est la prison benthamienne, dont le surveillant qui voit sans être vu maintient à lui seul dans la sujétion des centaines de prisonniers par la seule force de l'omniprésence supposée de son regard. Mais Bentham, qui voudrait faire de son *panoptique* un principe universel d'économie de temps et d'espace³⁶⁵, se heurte à la *limite physiologique* de l'homme. Au-delà d'une centaine de mètres, le surveillant, malgré la visibilité que procure l'architecture du panoptique, ne distingue plus les silhouettes des prisonniers. Il lui manque *une instrumentation* qui puisse encore majorer son pouvoir d'inspection au-delà des limites humaines du regard et de l'écoute.

Jeremy Bentham n'abandonne pas. Il fait preuve d'une ingéniosité sans limites, utilisant les *techniques optiques* pour voir plus loin — *la longue vue* — et les *techniques acoustiques* pour mieux entendre (*les tubes de fer blanc qui relient le pavillon du surveillant à chaque cellule*). Il est le précurseur de l'utilisation des *technologies de l'information* au service de la surveillance. Sur le chemin tracé par Bentham, un *néopanoptisme* va se cristalliser autour du développement des

³⁶² M. FOUCAULT, *Surveiller et punir*, Gallimard, 1975, pp. 37-72.

³⁶³ W. TAYLOR, *La Direction des Ateliers*, Dunod, 1919.

³⁶⁴ Jeremy BENTHAM, *Le Panoptique, mémoire sur un nouveau principe de construire des maisons d'inspection*, (1791), réédition de Belfond, 1977.

³⁶⁵ Dans la structure circulaire du Panoptique, on surveille, d'un seul regard rapide et efficace, à moindre coût et dans un moindre espace, autant de prisonniers que de cellules dans l'anneau de murs. L'espace et le temps sont regroupés en une seule fraction, en un seul regard.

technologies de l'information. Comme nous l'avons montré, un discours *centralisateur* sur la compétitivité et la technologie dissimule parfois des ambitions panoptiques. La norme, elle-même n'est-elle pas, d'une certaine façon, le moyen d'imposer un regard ?

Mais ce paradigme de la centralisation sera vite remis en cause. Le traitement de l'information sera bientôt concédé à des unités décentralisées et délocalisées par le jeu de la mondialisation de l'économie et des progrès fulgurants des technologies de transport et de stockage de l'information. Ce sera bientôt le *paradigme de l'individualisation* qui verra le jour, et avec lui, des remises en cause de plus en plus nombreuses, de plus en plus fréquentes. Dans le même temps, la crise économique s'installe et s'amplifie³⁶⁶. La violence devient une donnée courante de la vie sociale comme de la compétition entre firmes. Dans ce contexte, la stratégie du surveillant se fait plus précise, adoptant parfois les figures d'un *néopanoptisme* aux allures technocratiques. L'information secrète est appréhendée dans une perspective stratégique. Les firmes se menacent, usent de leur réputation et de démonstrations pour dissuader les concurrents d'entreprendre l'approche de leurs marchés. La surveillance a définitivement changé d'enjeu : elle devient un facteur de compétitivité pour la firme au même titre que sa capacité à innover.

C'est un changement de rôle pour la surveillance : elle passe d'une fonction de maintenance du pouvoir à celle de dynamique de la compétitivité. De nouvelles règles du jeu seront bientôt nécessaires pour esquisser une dynamique nouvelle de la compétition dont les fondements sont le partage et le transfert des connaissances, et dont la structure est celle d'un réseau. Quand l'information joue un rôle si important dans les succès et les échecs des stratégies d'entreprises, la connaissance ne peut plus être abordée comme le patrimoine que l'on a derrière soi. Elle devient un outil de positionnement, d'image et de tactique de l'entreprise. A ce titre, la pensée stratégique doit intégrer dans sa formulation des stratégies de connaissance. Dans ce contexte, le néopanoptisme est avant tout pour le stratège une grille de lecture des pratiques concurrentielles de la connaissance. Un discours moralisateur n'aurait pas sa place ici. Cet ouvrage n'a pas été écrit pour encourager ni la pratique de la désinformation, ni celle de l'impression ou de l'influence. Il en décrit et en montre l'existence. Il en explique les rouages. Il serait certainement dangereux d'en généraliser l'application à tout type de situations concurrentielles.

L'information concurrentielle est une « information subtile ». La crainte d'une manœuvre néopanoptique de la concurrence aidera peut-être l'entreprise à développer au sein de ses équipes managériales le réflexe de la « double-lecture ». Lire entre les lignes et prendre du recul : c'est simplement cela qu'il faut retenir de l'intelligence. L'information est là, mais doit faire l'objet d'un apprentissage méthodique de sa lecture dans le cadre d'une vision tactique et stratégique de l'entreprise.

³⁶⁶ Est-ce une coïncidence ou un corollaire à l'individualisation ? Pourrait-on mettre à jour un lien entre la montée des individualismes et l'installation de la dépression économique ?

Bibliographie

1. Vers un nouveau concept de firme industrielle

- COASE R.H.**, « The nature of the firm », *Revue Economica*, Vol. 4, pp. 386-405, Londres, novembre 1937.
- CHANDLER A.D.**, *Scale and scope, the dynamics of industrial capitalism*, Harvard-Belknap, 1990.
- CROZIER M., FRIEDBERG E.**, *L'acteur et le système*, Le Seuil, Paris, 1977.
- JOHANSON J., MATTSON G.**, « Interorganizational relations in industrial systems : a network approach compared with the transaction cost approach », *International Journal of Management and Organization*, 1987.
- MINTZBERG H.**, *The nature of managerial work*, Harper & Row, New York, 1973.
- NAYLOR THOMAS, VERNON JOHNNAN, WERTZ KENNETH L.**, *Managerial Economics*, Englewood Cliffs Eds, Prentice Hall, 1983.
- PERROUX F.**, *La pensée économique de J. Schumpeter: les dynamiques du capitalisme*, Droz, Genève, 1965.
- SCHERER F.M.**, *Industrial Market Structure and Economic Performance, (second edition)*, Houghton Mifflin, Boston, 1980.
- SCHUMPETER J.A.**, *Histoire de l'analyse économique*, Paris, Gallimard, 1983, édition française de *History of Economic Analysis*, 1954.
- STERLING R.W, SCOTT W.C.**, *The Republic of Plato : A New Translation*, Norton, New York, 1985.
- THOMPSON ARTHUR A.**, *Economics of the Firm*, 4th ed. Englewood Cliffs, N.J., Prentice Hall, 1985.
- THORELLI H.**, « Networks : between markets and hierarchies », *Strategic Management Journal*, Vol. 7, 1986.
- TIMMONS J.A.** et al., *New Venture Creation*, 2nd ed., Dow-Jones Irwin. Editors, Homewood, Illinois, 1985.
- WILLIAMSON O.**, *Markets and Hierarchies: Analysis and Antitrust Implications*, The Free Press, New York, 1975.
- WILLIAMSON O.**, *The economic institution of capitalism*, The Free Press, New York, 1985.
- WILLIAMSON O.**, *The firm as a nexus of treaties*, Sage Publications, Londres, 1990.
- WOODWARD J.**, *Industrial organization : theory and practice*, Oxford University Press, 1965.

2. La construction de la connaissance

- ACOCK A.C., MARTIN J.D.**, « The undermeasurement controversy : should ordinal data be treated as interval ? », *Sociology and Social Research*, No 28, pages 427-433, 1974.
- CALLON MICHEL** (sous la direction de), *La science et ses réseaux*, Editions de La Découverte, Conseil de l'Europe et UNESCO, Paris, 1989.

- FEYERABEND P.**, *Contre la méthode, esquisse d'une théorie anarchiste de la connaissance*, Collection Points, Editions du Seuil, 1979.
- FOUCAULT M.**, *L'archéologie du savoir*, Gallimard, 1969, et notamment le passage intitulé « La formation des stratégies », pages 85 à 101.
- FOUCAULT M.**, *Les mots et les choses*, Gallimard, 1966.
- GUSDORF GEORGES**, « Réflexions sur l'interdisciplinarité », in *Bulletin de Psychologie*, Tome XLII, No 397, Novembre 1990.
- KNORR-CETINA K.D.**, « *The Manufacture of Knowledge : An Essay on the Constructivist of Knowledge and Contextual Nature of Science* », Pergamon Eds, Oxford, 1984.
- KUHN T.**, *La structure des révolutions scientifiques*, Flammarion, 1983 (édition augmentée de la post-face de 1969).
- LATOUR BERNARD**, « *Science in Action* », Milton Keynes, Open University Press (Traduction française : *La Découverte* 1989), 1987.
- POLANYI M.**, *Personal Knowledge: Towards a post-critical philosophy*, University of Chicago Press, 1958.
- POPPER K.R.**, *The Logic of Scientific Discovery*, Hutchinson. (trad. française: *La logique de la découverte scientifique*, Payot, 1973), Londres, 1959.
- POPPER K.R.**, *Conjectures and Refutations*, Routledge and Kegan Paul (traduction française : *Conjectures et réfutations*, Payot, 1985), Londres, 1963.
- STENGERS ISABELLE, ILYA PRIGOGINE**, *La nouvelle alliance*, Gallimard, Paris, 1979.
- STENGERS ISABELLE, SCHLANGER JUDITH**, *Les Concepts scientifiques*, Edition de La Découverte / Conseil de l'Europe / UNESCO, Paris, 1989.

3. Surveillance et discipline de l'organisation

- BECCARIA**, *Des délits et des peines*, édition de 1856, pages 87 à 119, de l'idée de supplice et de la pression qu'elle exerce sur l'homme.
- BENTHAM J.**, *Le panoptique, mémoire sur un nouveau principe pour construire des maisons d'inspection*, imprimé par ordre de l'Assemblée Nationale, Paris, Imprimerie nationale, Secours Publics n° 1, 56 p.
- BERGERY C.L.**, *Economie industrielle*, 3 tomes, Metz, 1831.
- CARTER ROY**, « *Can Your Company Keep a Secret ?* », *Canadian Manager*, été 1986.
- CHURCHMAN C.W.**, « *The Design of Inquiring Systems: Basic Concepts of Systems and Organization.* », Basic Books, New York, 1971.
- DE GAUDEMAR J.P.**, *L'Ordre et la production, naissance et formes de la discipline d'usine*, Dunod, 1982, et plus particulièrement les passages consacrés au panoptisme : pages 20 à 23, pages 34 et suivantes: « L'usine forteresse ».
- DUMONT M.E., LAROCHE B.**, *Œuvres de Jérémie Bentham, jurisconsulte anglais*, traduction et édition critique, Louis Hausman et Cie, Bruxelles, 1829 - 1834, 4 volumes.
- DUMONT M.E.**, *Théorie des peines et des récompenses*, ouvrage réalisé à partir des travaux de Bentham de 1791, Vogel et Schulze, Genève, 1811.
- FAYOL H.**, *Administration générale et industrielle*, Dunod, 1916.
- FOUCAULT M.**, *Surveiller et punir*, Gallimard, 1975, et plus particulièrement, pages 197 à 229, *Le panoptisme*.
- PERROT M.**, *L'Œil du Pouvoir*, Entretien avec Michel Foucault, dans « Le panoptique », pages 9 à 31, et « L'inspecteur Bentham », pages 169 à 219, Belfond 1977.
- TAYLOR W.**, *La Direction des ateliers*, Dunod, 1919.

4. Surveillance de l'environnement de la firme

- AAKER D.A.**, « *Organizing a strategic information scanning system* », *California Management Review*, Volume 25, p. 76 et suiv., 1983.

- ADINE J.P.**, « *Les limiers du renseignement* », une interview de M. R. GUILLAUMOT, Président d'INFORAMA S.A. in LE POINT No 755, Paris, le 9 mars 1987.
- AGUILAR F. J.**, *Scanning the Business Environment*, Macmillan, New York, 1967.
- ANSOFF, I.**, *Managing strategic surprise through response to weak signals*, California Management Review, Vol. 23, 1975.
- BEQUAI AUGUST**, « *Management Can Prevent Industrial Espionage* », SAM Advanced Management Journal, New York, Hiver 1985.
- BRANDENBERG MARY**, « *Are Your Premises Free and Clear of Bugs ?* », Journal of Accountancy, New York, Juillet 1986.
- CALORI R., ATAMER T., LAURENT P.**, *Dynamique des marchés et veille stratégique*, Revue d'Economie Industrielle, n° 46, Quatrième trimestre 1988.
- DOU H., HASSANALY P.**, *Mapping the scientific network of patent and non-patent documents from Chemical Abstracts for a fast scientific analysis*, World Patent Information, Vol. 10, pages 133 à 149, 1988.
- DUMAINE B.**, « *Corporate spies snoop to conquer* », Magazine Fortune, Edition U.S., 7 novembre 1988.
- EELLS RICHARD , NEHEMIKIS PETER** , « *Corporate Intelligence and Espionage* », Macmillan, New York, 1986.
- FULD LEONARD**, « *Monitoring the Competition* », John Wiley, New York, 1988.
- FULD LEONARD**, « *Competitor Intelligence* », John Wiley, New York, 1985.
- GHOSHAL SUMANTRA**, « *Environmental Scanning : An Individual and Organizational Level Analysis* », Ph.D. dissertation, M.I.T. 1985.
- GIBSON RAY**, « *Competitive Espionage* », Small Business Reporter, pp. 32-33, Mai 1986.
- GILAD B., GILAD T.**, « *The Business Intelligence System* », Amacom Eds, New York, 1988.
- GILAD B., ROLLER L.**, « *Strategic Business Intelligence : An Experimental Approach.* », Working Papers Series # 16, Rutgers University, Dept. of Business Administration, 1986.
- GREENE RICHARD M.**, « *Business Intelligence and Espionage* », Dow-Jones Irwin Eds, Homewood, Illinois, 1966.
- GUILLOT JEAN-PAUL**, « *Prospective appliquée à la stratégie d'entreprise* », doctorat d'état en sciences de gestion sous la direction d'Edgar Andréani, Université de Paris-Nanterre, 1977.
- JAKOBIAK F.**, *Maîtriser l'information critique*, Les Editions d'Organisation, 1988.
- KAST F.**, *Scanning the future environment: social indicators*, California Management Review, Volume 23, p. 22 et suiv., 1980.
- LAMERE J.M., LEROUX Y., TOURLY J.**, *La sécurité des réseaux, méthodes et techniques*, Dunod, 1989.
- LESCA H.**, *Système d'information pour le management stratégique de l'entreprise*, McGraw Hill, 1986.
- MARTINET B., RIBAUT J.M.**, *La veille technologique, concurrentielle et commerciale*, Les Editions d'Organisation, 1989.
- MONTGOMERY DAVID B., WEINBERG CHARLES B.**, « *Toward Strategic Intelligence Systems* », Journal of marketing (Fall), Vol. 43, pp 41-52. 1979.
- PARKER DAVID**, « *Legal Implications of Competitor Intelligence* », in Business Competitor Intelligence, Edited by W.L. Sammon, M.A. Kurland, and R. Spitalnic, John Wiley & Sons, New York, 1984.
- PERSCHKE G.A., KARABIN S.J., et BROCK T.L.**, « *Four Steps to Security* », Journal of Accountancy, New York, Avril 1986.
- PRESCOTT J.E.**, Ed., « *Advances in Competitive Intelligence* », S.C.I.P. Ed., Vienna, Virginia, 1989.
- ROTHSCHILD WILLIAM E.**, « *How to Gain and Maintain the Competitive Advantage in Business* », McGraw-Hill, New York, 1984.

SACK STEVEN MITCHEL, «*You Can Keep a Secret*», Sales and marketing Management Journal, New York, Février 1985.

VILLAIN J., *L'entreprise aux aguets : information, surveillance de l'environnement, propriété et protection industrielles, espionnage et contre-espionnage au service de la compétitivité*, Masson, 1989.

WALL JERRY L., «*What the Competitor is Doing : Your Need to Know*», Harvard Business Review, Vol. 52 #6, pp. 1-12., November-December 1974.

5. L'économie de l'information au sein de la firme

ALCHIAN A.A., DEMETZ H., *Production, information costs and economic organization*, American Economic Review, December 1972.

COHENDET P., LLERENA P., *Flexibilité, information et décision*, ouvrage collectif, Economica, 1989.

COMMISSION OF THE EUROPEAN COMMUNITIES, *The review of the European Strategic Programme for Research and development in Information Technologies (ESPRIT)*, CEE, Mai 1989.

D'ASPREMONT C., GERARD-VARET L.A., *Concurrence et contraintes d'incitation*, pages 11 à 26, *Mécanismes et normes de comportement en information incomplète*, GREQE, document de travail n° 8802, Ecole des Hautes Etudes en Sciences Sociales, 1988.

GREMAQ A.A., *Dynamique, information incomplète et stratégies industrielles*, Economica, 1988, et notamment, dans la deuxième partie exposant les modèles en information incomplète, *Dissuasion et Réputation*, par Bernard Belloc, pages 201 à 216.

HURWICZ L.J., *On informationally decentralized systems*, pages 297 à 336 dans *Decision and organization. A volume in honor of Jacob Marschak*, McGuire Editors, Amsterdam, 1972.

KREPS D.M., WILSON R., *Reputation and Imperfect Information*, Journal of Economic Theory, 1982, n° 27, pp. 253-279.

MILGROM P., ROBERTS J., *Predation, Reputation and Entry Deterrence*, Journal of Economic Theory, 1982, n° 27, pp. 280-312.

MINISTERE DE LA RECHERCHE ET DE LA TECHNOLOGIE, *L'information scientifique et technique dans l'entreprise de production*, Colloque Savoir/Produire, La Documentation Française, 1984.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUE, *L'économie de l'information: tendances*, P.I.I.C n° 11, OCDE, 1986, et également, *Technologies de l'information et perspectives économiques*, P.I.I.C. n° 12, OCDE, 1987.

ORGANISATION DES NATIONS UNIES POUR L'EDUCATION ET LA CULTURE, *La circulation internationale de l'information: analyse et bilan*, UNESCO, 1985.

PONSSARD J.P., *Logique de la négociation et théorie des jeux*, Les Editions d'Organisation, 1977, et plus particulièrement, pages 95 à 106, *L'usage de l'information en situations compétitives*.

TURNER W.A., MICHELET B. , COURTIAL J.P., «*Scientific and Technological Information Bank for the network management of research*», Research Policy, Vol. 19, No 5, Octobre, 1990.

WALLER R.J., «*Knowledge for Producing Useful Knowledge and the Importance of Synthesis*», in *Producing Useful Knowledge for Organizations* (edited by Ralph H. Kilmann, Kenneth W. Thomas, Dennis P. Slevin, Raghu Nath and S. Lee Jerrell), Praeger Publishers, New York, 1983.

6. Utilisations détournées de l'information

ALLPORT G.W., POSTMAN L., *The psychology of rumor*, p. 156 et suiv., Holt & Co Publishers, New York, 1947.

- CREEL HERRLEE GLESSNERN**, « *Chinese Thought* », University of Chicago Press, Chicago, 1957.
- DOVRING K.**, *Road of Propaganda: the semantics of biased communication*, Philosophical Library, New York, 1959.
- HELLER M.**, « *Mon espion bien-aimé* », in *Géopolitique*, Revue de l'Institut International de Géopolitique, No 29, Printemps 1990, pp. 27-28.
- HOVLAND C.I.**, *Communication and Persuasion: Psychological Studies of Opinion Changes*, Yale University Press, New Haven, 1953.
- HUYN HANS GRAF**, « *La stratégie de la désinformation* », in *Géopolitique*, Revue de l'Institut International de Géopolitique, No 29, Printemps 1990, pp. 20-24.
- SMITH B.L.**, *Propaganda Analysis and The Science of Democracy*, Public Opinion Quaterly, Vol. 5, n°2, Juin 1941.
- SUN TZU**, *L'art de la guerre, Art.13: De l'utilisation des espions*, pages 41 à 94, traduction et édition critique de Niquet-Cabestan, Economica, 1988.

7. Relations de pouvoir dans l'organisation

- BACHARACH S.B., LAWLER E.J.**, *Power and politics in organizations*, Jossey-Bass, 1980.
- CROZIER M.**, *Le phénomène bureaucratique*, Collection Points, Edition du Seuil, 1963, et plus particulièrement, pages 176 à 214, *Relations de pouvoir et situations d'incertitude*.
- DE GAUDEMAR J.P.**, *Usines et ouvriers. Figures d'un nouvel ordre productif*, ouvrage collectif, Edition Maspéro, Collection Luttes Sociales, 1980. Passage intitulé: *De la fabrique au site, naissance de l'usine mobile*, pages 13 à 38.
- LARÇON J.P., REITTER R.**, *Structures de pouvoir et identité de l'entreprise*, Nathan, 1979.
- LASSWELL H.D., KAPLAN A.**, *Power and Society*, Chapitres 7 à 10, Yale University Press, 1950.
- LAW J.**, « *Power, Action and Belief* », Londres, Routledge and Kegan Paul Eds, Londres, 1986.
- LEMPEN B.**, *Information et pouvoir: essai sur le sens de l'information et son enjeu politique*, L'Age de l'Homme, Lausanne, 1979.
- MILGRAM S.**, *Soumission à l'autorité: un point de vue expérimental*, 2^e édition française, Calman-Lévy, 1982., pages 155 à 168, sur l'analyse des causes de l'obéissance.
- MILLER D., KETZ DE VRIES M.**, *Unstable at the top: inside the neurotic organization*, New American Library, 1988.
- MINTZBERG H.**, *Power in and around organizations*, Prentice Hall, 1983.
- WIENER N.**, *The Human Use of Human Beings, Cybernetics and Society*, Doubleday & Co, 1956.

8. Innovation technologique et compétitivité

- CLARK K.B., ABERNATHY W.J.**, *Innovation: mapping the winds of creative destruction*, in KANTROW W.J., *Industrial Renaissance: producing a competitive future for America*, Basic Books, 1983.
- DUSSAUGE P, RAMANTSOA B.**, *Technologie et stratégie d'entreprise*, McGraw Hill, 1987.
- GEST-EUROCONSULT**, *Grappes technologiques et stratégies industrielles*, Bulletin du Centre de Prospective et d'Evaluation, n° 57, mai 1985.
- KAMIEN M.I., SCWARTZ N.L.**, *Market structure and innovation*, Cambridge University Press, Cambridge, 1982.
- SALOMON J.J., SCHNEIDER G.**, *Les enjeux du changement technique*, ouvrage Collectif, Economica, Paris, 1986.
- TEECE D.J.**, *Innovations, Trade and Economic Welfare: contracts between petrochemicals and semiconductors*, University of California, Berkeley, 1985.

TEECE D.J., *Technology transfer by Multinational Firms: The Ressource Cost of International Technology Transfer*, Economic Journal, Juin 1977, p. 242-261.

9. Stratégie de l'entreprise

AGRAFIOTIS DEMOSTHENE, « *La stratégie de l'entreprise et les dimensions socio-culturelles de son interaction avec l'environnement* », doctorat de 3^e cycle sous la direction de Pierre Janiou, Université de Paris-Dauphine, 1976.

ANSOFF I., DECLERCK R.P., HAYES R.L., *From strategic planning to strategic management*, John Wiley, 1979.

ANSOFF I., *Stratégie du développement de l'entreprise*, traduction française de *Corporate Strategy*, Les Editions d'Organisation, 1989.

BERETTA V., *Politique et stratégie de l'entreprise*, Hommes et Techniques, Paris, 1975.

BIENAYME A., *Stratégies de l'entreprise compétitive*, Masson, Paris, 1980.

BOSTON CONSULTING GROUP, *Les mécanismes fondamentaux de la compétitivité*, Hommes et Techniques, 1980.

COOKE TERENCE E., « *Mergers and Acquisitions* », Basil Blackwell, Oxford, 1986.

CROZIER M., *L'entreprise à l'écoute, apprendre le management post-industriel*, InterEditions, 1989.

DECLERCK R.P., EYMERY P., CRENER M.A., *Le management stratégique des projets*, Hommes et Techniques, 1980.

EBELING H.W., DOORLEY T.L., « *A Strategic Approach to Acquisitions* », Journal of Business Strategy, hiver 1983.

FRY JOSEPH N., KILLING PETER J., « *Strategic Analysis and Action* », Englewood Cliffs, N.J., Prentice Hall, 1986.

GALBRAITH J.K., *Le nouvel état industriel*, Gallimard, 1968, et *Designing complex organizations*, Addison Wesley, 1973.

GELLINIER O., *Morale de la compétitivité : leçons du Japon pour la France*, Hommes et Techniques, Paris, 1978.

HAYES ROBERT H., ABERNATHY WILLIAM J., « *Managing Our Way to Economic Decline* », Harvard Business Review, July-August 1980.

HEC-ISA, *Stratégie, structure, décision, identité*, ouvrage collectif par l'équipe des professeurs du département Stratégie et Politique d'Entreprise, InterEditions, 1988.

HOGARTH R.M., « *Judgement and Choice* », John Wiley & Sons, New York, 1983.

KIRZNER I., *Competition and entrepreneurship*, University of Chicago Press, Chicago, 1973.

MAC-MILLAN I., *Strategy formulation : political concepts*, West Publishing Co, 1978.

MARTINET A.C., *Stratégie*, Vuibert, 1983, et *Management stratégique, organisation et politique*, McGraw Hill, 1984.

MILLER DANNY, FRIESEN PETER H., « *Strategy Making in Context : Ten Empirical Archetypes* », The Journal of Management Studies, October 1977.

MITROFF I.I., *Business Not as Usual : Rethinking Our Individual, Corporate, and Industrial Strategies for Global Competition*, Jossey-Bass, San Francisco, 1987.

NAYLOR THOMAS, *Strategic Planning Management*, Planning Executive Institute, Oxford, Ohio, 1980.

PORTER M.E., *Choix stratégique et concurrence*, Economica, 1982, traduction française de *Competitive Strategy*.

PORTER MICHAËL, *Competitive Advantage*, The Free Press, New York, 1985.

SALLENAVE JEAN-PAUL, *Dynamique concurrentielle et stratégie*, doctorat de 3^e cycle sous la direction de Maurice Sayas, Université d'Aix-En-Provence, 1974.

TREGOE B., ZIMMERMANN J., *La force motrice, une nouvelle stratégie pour l'entreprise*, InterEditions, Paris, 1982.

ZIMMERMANN J.B., DELAPIERRE M., *Towards a new europeanism strategic partnership by french firms*, GREQE, Document de Travail n° 89 B 02, Ecole des Hautes Etudes en Sciences Sociales, 1989.

Glossaire de la surveillance d'entreprise

A

ABSTRACTS : courts résumés de 4 à 8 lignes qui présentent un fait nouveau recueilli par une équipe de veille technologique et concurrentielle. Les abstracts sont réunis dans une lettre confidentielle hebdomadaire ou mensuelle qui est communiquée au coordinateur de la cellule de veille. Chaque abstract est précédé d'un code qui indique l'intérêt de l'information pour l'entreprise et la fiabilité de la source émettrice. Le coordinateur détient ainsi sur quelques pages un résumé factuel de la période. Il choisit ensuite les informations qu'il souhaite voir approfondir, abandonner ou mettre de côté en attente. Ces trois options correspondent à des codes que le coordinateur reporte sur un message contenant les numéros des abstracts. Le message est communiqué à la cellule qui reçoit ainsi le résumé décisionnel donnant suite à son travail.

AFFRONTLEMENT : comportement de deux firmes désirant une nouvelle distribution des ressources disponibles sur le marché chacune à son propre avantage. Il n'est pas recherché de bénéfice mutuel, mais le bénéfice de l'une au détriment de l'autre.

AGENT DOUBLE : personne chargée de recueillir de l'information pour un commanditaire et travaillant, dans le même temps, pour un autre commanditaire. Certains agents doubles sont clairement connus par les commanditaires et utilisés soit comme canal d'échanges d'informations, soit comme canal de désinformation.

AGENT DE LIAISON : personne en mission permanente dans un pays, dans une institution ou auprès d'une entreprise, qui est utilisée comme relais permanent pour organiser des missions ponctuelles (connaissance du pays, du secteur et logistique).

AGENT D'INFLUENCE : personne dont la mission est d'influencer une communauté scientifique, économique, juridique ou encore institutionnelle afin que celle-ci réalise des actions les plus conformes aux projets des commanditaires. Un agent d'influence peut également travailler auprès d'une seule personne. La mission de ce type d'agents n'est pas toujours connue d'eux-mêmes. C'est souvent le cas des missions de désinformation dans lesquelles l'agent désinformateur pense en fait réaliser un rôle d'information auprès du récepteur ciblé.

AGENT SACRIFIÉ : dans la typologie présentée par le stratège chinois Sun Tzu, il y a plusieurs dizaines de siècles, l'agent sacrifié est une personne introduite au sein d'une organisation adverse sans espoir de la voir revenir et avec une mission d'influence ou d'espionnage qui causera sa perte. La notion « d'agent sacrifié » ne donne pas lieu à des applications viables pour l'entreprise.

ALLIANCE : coopération formalisée entre plusieurs acteurs. L'alliance peut être secrète, privée ou publique.

ANALYSE CONTINGENTE : méthode d'analyse créée en réaction contre le déterminisme taylorien. L'analyse contingente est née du constat d'échec des approches trop normatives qui tentent de construire des systèmes de résolution « standards » applicables à tout problème. Cette forme d'analyse reconnaît au contraire à chacun la spécificité de sa situation (sa contingence).

ANALYSE CONCURRENTIELLE : méthode d'analyse focalisée sur la concurrence pour en identifier les forces, les faiblesses, les menaces d'entrée sur un secteur... Aux Etats-Unis, l'intelligence d'entreprise est souvent confondue avec l'analyse concurrentielle au travers de pratiques comme le benchmarking, le scanning ou le monitoring.

ASYMETRIE D'INFORMATION : situation dans laquelle deux acteurs ne sont pas informés au même niveau sur l'environnement qu'ils partagent. L'objectif de l'intelligence d'entreprise est de repérer les asymétries auxquelles il faut remédier quand elles sont au désavantage de l'organisation. Lorsque l'entreprise se considère en situation d'incertitude vis à vis de cette asymétrie, c'est à dire lorsqu'elle ne sait pas à qui elle profite, l'intelligence d'entreprise a pour objectif de révéler et de transformer cette asymétrie à l'avantage de l'organisation.

AUDIT D'INTELLIGENCE : diagnostic réalisé dans une organisation pour définir l'intelligence dont cette dernière a besoin. Il s'agit, au cours de cet audit d'analyser les circuits d'information existant dans l'entreprise en vue d'une meilleure exploitation, d'identifier les freins à la diffusion d'informations déjà détenues par le personnel (problèmes humains, freins psychologiques, freins hiérarchiques, culture d'entreprise), de définir des réseaux de collecte, d'analyse, d'expertise et de distribution sélective de l'information.

AVANTAGES CONCURRENTIELS : avantages détenus par l'entreprise de façon stable sur ses concurrents. La surveillance de l'environnement a pour mission de protéger les avantages concurrentiels de l'entreprise en repérant des signaux de menaces adressées à celle-ci.

B

BARRIERES A L'ENTREE : obstacles délibérés ou structurels qui empêchent l'entrée des concurrents sur un marché ou dans un secteur. Ce peut être l'avantage pionnier détenu par les firmes du secteur, mais aussi des normes sectorielles, des budgets de publicité élevés, des degrés d'intégration plus ou moins forts... La surveillance de l'environnement a une fonction de détection des vulnérabilités des barrières à l'entrée d'un secteur.

BARRIERES A LA SORTIE : obstacles empêchant l'abandon d'une activité par l'entreprise appartenant au secteur. Ces obstacles peuvent être un taux d'investissement déjà très élevé dans le secteur, un syndicalisme important propre au secteur, la spécificité des actifs qui ne permet pas de les céder facilement, l'impact d'un licenciement économique pour l'Etat dans les industries manufacturières dont les employés peuvent difficilement se reconvertir...

BASE D'EXPERIENCE : expérience cumulée au cours du temps par l'entreprise dans la réalisation d'une tâche élémentaire. Cette expérience constitue pour l'entreprise une base (un noyau d'activité) à partir de laquelle elle peut envisager des redéploiements et des changements d'orientations vers des métiers qui lui sont devenus accessibles.

BENCHMARKING : surveillance assidue et rapprochée d'un seul acteur au sein de l'environnement qui peut être un fournisseur, un entrant potentiel, une société à absorber, un client ou même une institution. La gestion des opérations de benchmarking est une gestion par projets. On désigne un chef de projet attiré au benchmarking d'un seul acteur et on évalue sa performance sur cette seule mission. Il peut être entouré d'une équipe. Organisation très coûteuse mais responsabilisante, et donc performante.

BIAIS IDEOLOGIQUE : dans l'interprétation des faits ou des signaux décelés dans l'environnement, de nombreux biais peuvent apparaître. Ce sont des biais d'incompréhension des

problèmes globaux, de réductionnisme, de subjectivisme et même parfois d'holisme... Mais le biais le plus dangereux reste le biais idéologique dans l'interprétation des faits par des chargés de mission.

BIBLIOMETRIE : la « mesure » des livres et des documents. La bibliométrie est une discipline qui consiste en la mesure des publications en termes de volumes, de fréquences et de contenu. L'analyse du contenu s'attache à repérer des termes, à établir des corrélations entre la présence simultanée de plusieurs termes importants pour l'entreprise, à dessiner et même cartographier des liens existant entre plusieurs publications (références à d'autres articles scientifiques, travail réalisé sur un même thème).

BUSINESS INTELLIGENCE : terme anglais pour « intelligence d'entreprise ». Aux Etats-Unis, on entend le plus souvent par business intelligence une veille assidue et permanente des concurrents. La conception européenne tend à être beaucoup plus générale et conçoit l'intelligence comme une veille relationnelle s'intéressant à tous les environnements de l'entreprise (économiques, financiers, culturels, sociaux, politiques, scientifiques, technologiques...).

C

CELLULE DE VEILLE : groupe restreint de 5 à 15 personnes chargées de veiller sur l'environnement pour une organisation. On différencie des cellules opérationnelles détachées à la surveillance d'un environnement spécifique (uniquement la recherche, ou la concurrence, ou la culture, ou les institutions) et des cellules stratégiques chargées de réaliser une veille globale et d'établir des liens d'analyse et de coordination entre les différents environnements surveillés.

CELLULE D'INTELLIGENCE : groupe restreint de 5 à 30 personnes chargées d'intervenir sur l'environnement pour le compte de l'entreprise. Plus active qu'une cellule de veille, la cellule d'intelligence non seulement recueille l'information mais la manipule, la diffuse, engage des actions de coercition et d'influence, et fait du lobbying. Sa relation avec l'environnement est une relation d'interaction et d'interstructuration. Elle constitue la « task force » de l'entreprise. La veille et l'intelligence correspondent à deux conceptions différentes de l'information.

CENTRALISATION DE L'INFORMATION : action qui consiste à ramener l'ensemble des informations recueillies en un seul point. La centralisation est coûteuse et difficile à imposer. Elle est pourtant nécessaire pour identifier dans l'environnement des menaces dites « transversales ».

CHAINE DE VALEUR : ensemble des valeurs distinctives de l'entreprise dans la chaîne de son métier (de la recherche à la commercialisation) telles qu'elles peuvent être perçues par les autres acteurs du secteur (fournisseurs, clients, Etat, concurrents).

CHAMP CONCURRENTIEL : domaines où la firme entre en concurrence. Ce peut être aussi bien un marché de biens de consommation, que le marché de l'emploi, la défense des intérêts de l'entreprise auprès des institutions ou encore la recherche. Cette globalisation de la concurrence, qui se traduit par la multiplication des champs de concurrence, est une donnée essentielle de l'évolution de la compétition.

COERCITION : action de l'entreprise consistant à contraindre un acteur (homme, entreprise, institution), à modifier son comportement en satisfaisant aux objectifs de l'entreprise. La coercition relève de l'influence positive et non de la menace.

COORDINATION DE L'INTELLIGENCE : mission donnée au responsable de la cellule d'intelligence de l'entreprise qui consiste au rapprochement des besoins et des ressources informationnelles des acteurs de celle-ci. C'est avant tout une mission d'arbitrage et de réallocation des ressources internes et externes d'information sur l'environnement.

CONFIDENTIALITE DE PROGRAMME : très utilisée dans l'aéronautique et le spatial, la mention « confidentiel programme » signifie que les informations contenues dans le document ne peuvent être communiquées à des personnes extérieures au programme ou au projet en cours de réalisation. Pour une gestion plus efficace, les confidentialités de programme doivent être gérées par l'écriture systématique de la diffusion des documents (notification) et remis contre décharge.

CONFIDENTIALITE NOMINATIVE : utilisées pour des projets secrets de l'entreprise, les mentions nominatives de confidentialité sont très coûteuses à gérer mais les plus efficaces. Chaque personne habilitée à connaître la nature des projets en cours reçoit un agrément et signe un engagement de confidentialité. Le non-respect de cet engagement est considéré comme faute grave ou faute lourde.

CONFIDENTIALITE SECTORIELLE : confidentialité qui s'étend à l'échelle d'un secteur. Ce type de confidentialité est de moins en moins utilisée dans la mesure où les secteurs sont devenus des lieux de forte compétition. Il peut subsister des documents portant la mention « confidentiel industrie » qui sont écrits par une organisation professionnelle à l'usage de ses membres ou adhérents.

CONFLITS (MODELE DES) : modèle politique d'interprétation des organisations qui ne voit le progrès d'un groupe qu'au travers de nombreux conflits d'intérêts. Chaque conflit correspond à une itération de l'évolution de l'entreprise. Ainsi, toute entreprise devient, sous cet angle, une « organisation négociée ». Ce modèle est très adapté à l'interprétation des bureaucraties contre lesquelles il avait, au départ, l'objectif de s'élever. Mais la bureaucratie a repris à son compte le modèle en encourageant son étude en son sein, si bien que le modèle existe désormais à travers la bureaucratie, et en quelque sorte, la justifie. C'est un modèle très intéressant pour repérer des vulnérabilités humaines dans des organisations concurrentes.

CONTRE-ESPIONNAGE : lutte contre l'espionnage. La conception classique du contre-espionnage est défensive. Sur un territoire délimité, une surveillance rapprochée d'un nombre défini d'acteurs suspects est mise en place. Avec des armes essentiellement juridiques (Articles 70 et suivants du Code pénal), les organisations de contre-espionnage tentent d'enrayer les processus d'infiltration. Dans le contexte actuel d'une mondialisation des échanges sociaux, culturels et économiques, cette conception risque de produire de moins en moins de résultats faute d'être interactive, dynamique et transnationale.

CONTROLE DE GESTION DE L'INTELLIGENCE : les activités d'intelligence sont très coûteuses. Elles nécessitent des achats d'informations, des déplacements, des prises de risques parfois sanctionnées par des coûts importants. Elles doivent être gérées et contrôlées. Le contrôle de gestion de l'intelligence fonctionne d'après des critères de performance (quantité et qualité des informations rapportées, taux d'utilisation de ces informations par leurs destinataires rapportés à leur coût).

COÛTS D'AGENCE : somme des coûts engagés par un agent et son mandant dans la réalisation d'un contrat. C'est à Berle et Means que l'on doit cette perception de l'entreprise comme un ensemble d'agences (réunion d'acteurs) ayant des contrats à remplir. La firme ne tarde pas à être un « nœud » de contrats dont l'augmentation en charge de chacun permet la réduction de leur nombre (intégration).

D

DEFICIT INFORMATIONNEL : manque important d'informations qui provoque, selon Weyergaus, une angoisse persistante qui ne disparaît que le jour où cette information est obtenue.

DEMONTAGE DE PRODUITS : activité qui consiste à démonter les produits des concurrents pour étudier leur conception.

DENI (DE LA COMPETITION) : refus psychologique d'entrer en compétition en pratiquant systématiquement l'évitement et le positionnement sur des activités où il n'y a pas de concurrents très actifs.

DESENGAGEMENT : action de retrait d'une activité par l'entreprise. Le désengagement peut faire suite à l'échec mais aussi au déplacement et à la concentration des forces dans des domaines d'activités stratégiques pour l'entreprise. Chaque désengagement offre une place libre à un concurrent. La surveillance de l'environnement doit être apte à repérer les désengagements potentiels de firmes pour évaluer la possibilité de se substituer à elles sur un marché ou au sein du secteur.

DESINFORMATION : action qui consiste à diffuser une information fautive pour modifier la connaissance d'un acteur et ainsi lui retirer l'information qu'il possédait, donc le « désinformer ».

DISCERNEMENT : première qualité des chargés de mission de veille concurrentielle et technologique. L'information concurrentielle est une information subtile et subjective dans la plupart des cas. Une base de données sur la concurrence n'a pas de sens si chacune de ces données n'est pas accompagnée d'une note qui montre l'effort de discernement de celui qui l'a recueillie. De façon générale, il faut éviter de dépouiller les informations de leur contexte.

DISTRIBUTION SELECTIVE : forme de distribution de l'information fondée sur une sélection préalable des récepteurs. Cette sélection est établie sur des profils d'intérêt des personnes ou des départements concernés. Pour chaque « profil », une liste de distribution contenant les coordonnées des personnes intéressées est utilisée. Cette liste peut être constituée d'adresses-réseaux ou adresses virtuelles (networking), ou d'adresses physiques pour un acheminement de l'information par courrier interne ou par courrier postal. Des réseaux de diffusion sélective d'urgence peuvent être constitués d'adresses-télécopie, d'adresses-télex ou encore d'adresses-télérel.

DOMAINE PUBLIC : domaine où ne peuvent être exercés des droits de propriété intellectuelle. La connaissance de la législation du domaine public est la première mission d'un responsable de veille. Tout objet ou document exposé à un salon ou diffusé par la presse appartient au domaine public et ne peut plus être protégé par un droit de propriété intellectuelle. De même, toute information acquise dans le domaine public est une information ouverte. Son acquisition ne constitue donc pas un vol. Il en est de même pour une information obtenue lors d'une interview réalisée dans le cadre d'un colloque ou d'un salon ouvert au public.

E

ECONOMIE DE DIVERSITE : économie réalisée grâce à la diversité des activités de l'entreprise. Celle-ci bénéficie en effet de la synergie et de la complémentarité de ses activités si elle améliore la circulation de l'information entre ses différentes divisions.

ECONOMIES SOUTERRAINES : ennemies de la libre entreprise et de la compétition réalisées conformément à certaines valeurs éthiques, les économies souterraines sont en très fort développement dans les pays appartenant à la périphérie des groupes de pays de grande tradition industrielle. Elles consistent à dissimuler une partie plus ou moins importante de l'activité économique pour éviter une fiscalité contraignante et obtenir ainsi une bonne position concurrentielle. Cette activité dissimulée peut consister en prestations intellectuelles non facturées, l'emploi de personnels non déclarés ou encore l'utilisation de procédés protégés sans s'acquitter des droits de licences.

ECOUTE (QUALITE) : l'écoute est une qualité humaine à développer au cœur des équipes de veille. Lors du recrutement (interne ou externe) des personnels devant constituer une telle cellule, la qualité d'écoute, avec le goût pour le domaine d'activité surveillé, seront parmi les critères les plus discriminants.

EFFET DE DEMONSTRATION : tactique qui consiste à réaliser une démonstration de force pour contraindre un acteur à agir dans le sens souhaité par l'entreprise ou pour lui interdire une action. Une effet de démonstration peut être accompagné d'une manœuvre de désinformation visant à exagérer l'impression obtenue sur les cibles de cette démonstration. Les effets de démonstration sont également utilisés dans des tactiques d'exaspération de la concurrence afin de démobiliser les hommes travaillant sur des projet ciblés et prendre ainsi de l'avance sur ceux-ci.

EFFET D'EXPERIENCE : diminution du coût unitaire de production suite à une augmentation des volumes.

EFFET DE SURPRISE STRATEGIQUE : tactique qui consiste à ne dévoiler ses intentions qu'au jour de leur exécution. A l'opposé de la guerre d'annonces, la tactique de surprise stratégique mise sur un effet de découragement direct et important. Ce n'est pas une guerre d'usure comme celle des annonces mais plutôt une « blitzkrieg » de l'économie et du commerce.

ENTENTE : accord réalisé à la discrétion d'autrui entre plusieurs acteurs afin de réduire la concurrence à leur profit. Il existe plusieurs formes d'entente comme les ententes de prix (carburants sur les autoroutes), les ententes de répartition géographique (industrie aéronautique), et les ententes de non-agression (partage d'un marché entre plusieurs grandes entreprises). La plupart des ententes sont interdites par les lois anti-trust, mais l'application de ces lois est difficile. Le Directorate Generale IV de la CEE a pour mission de surveiller ces ententes possibles afin de préserver la libre concurrence du marché européen.

ENVIRONNEMENT : ensemble des *espaces* — pris au sens large comme espaces historiques, juridiques, économiques, sociaux, culturels, technologiques — dans lesquels la firme entre en compétition avec d'autres acteurs agissant sur ces espaces. La relation de la firme avec son environnement est par là même étudiée en termes de *négociation*. Chaque avancée, chaque progrès de la compétitivité de la firme dans un de ces espaces est le résultat d'une négociation entre les acteurs constituant cet espace et la firme elle-même.

ENVIRONNEMENT EXPLICITE : environnement qui donne réellement à se faire connaître. C'est l'environnement qui ne nécessite aucun effort d'interprétation pour être perçu et assimilé. Une bonne politique de communication de la firme voudrait que son environnement explicite perçu soit égal à l'image qu'elle aimerait communiquer d'elle même.

ENVIRONNEMENT IMPLICITE : environnement qui est virtuellement contenu dans un environnement explicite. Il peut être découvert par induction, ou déduction, de la part des acteurs. L'environnement implicite est souvent riche d'enseignements pour l'entreprise et constitue une des cibles prioritaires d'une cellule de veille.

ESPIONNAGE : vol d'information. L'espionnage consiste à prendre de l'information à des acteurs sans leur consentement et même à leur insu. Une cellule de veille, ou même une cellule d'intelligence, ne font pas d'espionnage et exercent leur activité dans le cadre d'informations ouvertes.

ETAT AGENTIQUE : état dans lequel est plongé un individu qui obéit aux ordres d'un autre sans pour autant se sentir responsable de la conséquence de ses actes.

EVITEMENT : manœuvre consistant à réduire autant que se peut les champs de concurrence entre plusieurs firmes au profit de celles-ci. Le protectionnisme, le monopole, l'excès de normalisation sont autant de manœuvres ayant pour objectif l'évitement.

EXECUTIVE SEARCH : recherche de cadres supérieurs et dirigeants. Une des missions d'une cellule de veille est également de repérer les départs potentiels de cadres des organisations concurrentes, d'évaluer les motifs de ces départs éventuels et de produire des rapports sur l'intérêt de ces cadres pour l'entreprise.

EXTERNALISATION : démarche consistant à faire réaliser une partie de l'activité de l'entreprise par des tiers à celle-ci. L'externalisation transforme souvent l'entreprise en un réseau de partenaires réunis autour d'un même objectif par des liens contractuels.

F

FACTEURS CLES DE SUCCES : facteurs conditionnant le succès de l'entreprise d'une façon prépondérante. Il ne peut y avoir un nombre élevé de facteurs clés de succès. Tout au plus, on pourra rechercher une dizaine de facteurs essentiels au succès de l'entreprise. En tout état de cause, l'approche des F.C.S. (facteurs clés de succès) a l'avantage de focaliser l'entreprise sur ses objectifs prioritaires et l'inconvénient d'être très réductrice. Il est imprudent de bâtir un système d'information sur l'environnement à partir d'une telle approche.

FAUX RECRUTEMENT : action tout à fait illégale qui consiste à promettre un recrutement à une personne pour s'entretenir avec elle de son expérience au cours d'un entretien d'embauche fictif.

FEODALITE (VULNERABILITE DE LA) : les entreprises dites « féodales » sont celles dont le partage de l'autorité s'inspire tacitement des modèles féodaux de seigneurs, vassaux et serfs. Le peu de motivation de leurs éléments et la rigidité de leur système hiérarchique en font des entreprises parmi les plus vulnérables à une action d'intelligence car la caractéristique de ces « serfs » (employés, cadres moyens, agents de maîtrise) est le ressentiment vis-à-vis des « seigneurs » (direction et cadres supérieurs). Ce ressentiment constitue un des points d'entrées pour des manœuvres d'influence ou de mise en confiance destinées à détourner de l'information en exploitant des aversions internes à l'entreprise visée.

FILIERE DE TRANSFORMATION : ensemble des phases de transformation d'une matière première, d'abord en semi-produits, puis en produit fini. L'étude d'une filière permet d'identifier des possibilités de substitution dans le cadre d'une matrice dite « matériaux-marchés » qui retrace le cheminement réalisé par la firme, en partant du matériau, pour aboutir au consommateur du produit fini.

FORMULATION DE LA STRATEGIE : la formulation de la stratégie n'est pas sa simple mise sur papier. Elle consiste en un acte intellectuel visant à traduire en concepts et en manœuvres des informations obtenues dans l'environnement afin de satisfaire les objectifs de l'entreprise. La formulation de la stratégie conceptualise le métier, la mission et la « vision » de l'entreprise. Il est important de formuler sa stratégie, non pas que cela puisse améliorer sa mise en œuvre, mais simplement parce que cela permet de fédérer les hommes autour des projets de l'entreprise qui en découlent naturellement.

G

GAINS A L'ECHANGE (RECHERCHE DE) : pratique qui consiste à n'envisager l'échange que dans une perspective de gain. Les Japonais ne donnent jamais une information s'il n'y a pas de perspectives de gains à l'échange. Ce gain peut être, et il l'est le plus souvent, une autre information.

GRAPPES TECHNOLOGIQUES : forme de développement de la technologie en « grappes » ou « branches » à partir d'un tronc commun constitué des technologies génériques de l'entreprise, c'est-à-dire des technologies élémentaires qui par leur fertilisation croisée permettent la création de nouvelles technologies (l'optique et l'électronique croisées, puis fertilisées, ont donné naissance à l'optoélectronique).

GUERRE D'ANNONCES : affrontement virtuel entre deux concurrents qui se réalise au travers d'annonces plus ou moins démonstratives et menaçantes par voie de presse et de communiqués.

La désinformation, les démonstrations et l'émission parallèle de signaux perturbateurs accompagnent le plus souvent ces guerres d'annonces dont les objectifs sont multiples. Il s'agit de décourager l'entrée d'un concurrent sur un marché, l'entraîner sur de fausses pistes de recherches, le pousser à surdimensionner ses capacités de production ou détruire son image de marque.

GUERRE DES PRIX : affrontement réel d'entreprises qui baissent leur prix pour contrarier la rentabilité des concurrents qui vont suivre. Les guerres de prix sont souvent néfastes à tous les belligérants mais les ententes, à l'opposé, sont interdites par la loi et considérées comme concurrence déloyale vis-à-vis de tiers.

H

HACKING : terme anglais pour « piratage » informatique. Il s'agit d'un vol d'informations réalisés par des moyens informatiques. La pénétration des réseaux informatiques des concurrents est tombée en désuétude au fur et à mesure que la législation sur le piratage se renforçait. Les peines encourues par les pirates, surtout aux États-Unis, pays leader dans ce domaine, dissuadent avec de plus en plus de succès les candidats au piratage. Certains experts de la veille concurrentielle voient dans ce phénomène le regain d'intérêt de la fin des années 1980 pour une surveillance de terrain.

HARCELEMENT : tactique qui consiste à harceler une source d'information jusqu'à délivrance de l'information qui intéresse l'entreprise. Le harcèlement est aussi utilisé par une firme désirant en chasser une autre de son secteur. L'harcèlement peut prendre plusieurs formes. Dans le cadre de relations interpersonnelles, il peut y avoir un harcèlement affectif basé sur une relation de séduction entre les deux personnes, ou un harcèlement subjectif et virtuel. L'intimidation s'exprime le plus souvent sous la forme d'un harcèlement.

HOLISME : approche philosophique selon laquelle les propriétés d'un tout sont irréductibles à celles de ses parties, lesquelles n'ont de sens qu'en rapport au tout qu'elles composent. De ce point de vue, un énoncé quel qu'il soit est toujours tributaire du paradigme dont il est issu. En surveillance, une attitude holiste consiste à toujours rattacher les faits aux conditions sociales et politico-économiques qui les ont produits.

HOMME DE LIAISON : personne chargée de mettre en contact différentes personnes impliquées dans un projet complexe faisant appel à des compétences dispersées dans l'entreprise. L'homme de liaison n'est pas nécessairement chargé de la coordination du groupe au sein duquel il opère. Il est avant tout un facilitateur pour le groupe qui l'utilise.

I

INCERTITUDE : situation de déficit informationnel qui peut provenir de l'imperfection de l'information disponible ou du manque complet d'information. L'imperfection de l'information peut être due à son caractère ambigu, à sa contradiction intrinsèque (désinformation) ou encore à son aspect parcellaire. L'objectif d'une surveillance continue de l'environnement est de contribuer à réduire l'incertitude. L'objectif d'une cellule d'intelligence, sous un aspect offensif, peut être d'augmenter l'intensité de l'incertitude dans laquelle se trouvent les concurrents.

INCREMENTALISME : modèle politique de décision adopté par un groupe et qui s'exprime par un cheminement par ajustements successifs, par petits pas, de façon quasiment tactile. Au sein d'une bureaucratie, la superstructure se comporte typiquement de façon incrémentale, en n'agissant qu'en référence aux décisions prises par des groupes d'influence adverses. Ainsi, la décision collective ne naît qu'à la suite d'un jeu informel d'échanges de signaux signifiant aux groupes adverses soit un désaccord ou une menace de censure, soit un accord tacite.

INFLUENCE : action consistant à obliger un acteur à modifier son comportement dans un sens qui est favorable à celui qui exerce son pouvoir d'influence. Il existe plusieurs types d'influence qui peuvent naître de l'autorité, de l'affectivité, de la soumission (influence visant à encourager ou laisser faire une erreur en s'y soumettant), de l'expertise, du chantage affectif, subjectif, réel ou virtuel.

INFORMATION FERMEE : information dont l'accès est interdit par son détenteur. Cette interdiction fait référence à la législation qui prévoit des peines assez importantes pour les actions d'espionnage contre l'Etat ou la Défense, mais gère encore mal actuellement l'espionnage entre particuliers et entreprises.

INFORMATION OUVERTE : information appartenant au domaine public, ou mise dans le domaine public par son détenteur.

INTEGRATION : opération consistant à inclure dans les activités de l'entreprise des métiers qui se trouvent soit en amont, soit en aval, soit les deux, soit proches (intégration horizontale) du métier de l'entreprise. Si l'entreprise est un producteur, elle peut intégrer à son activité la recherche (en amont) et la commercialisation (en aval). Dans ce cas, on parle de degré d'intégration ou de verticalité de l'intégration.

INTELLIGENCE D'ENTREPRISE : activité qui consiste à « systémiser » le recueil, le traitement et l'exploitation de l'information environnementale au profit d'une organisation. A l'opposé de la veille, l'intelligence se conçoit comme une interaction de l'environnement et de l'entreprise. Elle n'a pas seulement un rôle passif d'observation, elle a aussi un rôle actif d'intervention.

INTERSTRUCTURATION : négociation entre la firme et son environnement qui a des effets de modification de structures sur l'une et sur l'autre.

INTIMIDATION : pratique qui consiste à impressionner un acteur par l'effroi. La menace n'est pas directement adressée à l'acteur visé mais des démonstrations de force et d'agression sont faites sous ses yeux. L'intimidation opère sur le registre de la subjectivité et de la suggestion. Elle provoque l'effroi en suggérant à l'acteur une projection de lui-même dans la situation à laquelle il assiste. L'intimidation sur des personnes physiques est interdite par la loi mais il est très difficile, d'un point de vue juridique, d'identifier l'intimidation destinée à une personne morale. Intimidation et désinformation sont souvent complémentaires.

J

JEU D'ACTEURS : ensemble de règles régulant les interactions entre plusieurs acteurs. Etre dans le jeu consiste à respecter les règles d'interrelation. Etre « hors jeu » consiste à perturber le jeu en ne respectant pas les règles. Il peut exister des stratégies dites de « hors jeu » lorsque l'entreprise pense que les acteurs ne réagiront pas et qu'elle pourra, grâce à sa position déviante, gagner des parts de marché. Elle perd cependant une partie de son pouvoir de négociation au sein de son secteur du fait de la condamnation tacite de son attitude par l'ensemble des autres acteurs du secteur.

K

KEEP : une cellule de veille délocalisée dans un pays étranger produit de façon régulière des « abstracts », courts résumés des opérations de 4 à 8 lignes, que le coordinateur demande de « laisser-tomber » (« abandon » en anglais) ou de « garder sous le coude » pour approfondir plus tard (« keep ») ou encore d'approfondir directement (plus d'information : « more »). Chaque abstract a un numéro. Le coordinateur peut donc envoyer un message du type : « K-3405, M-3608, A-3777, K-2341... ».

L

LEGITIMITE : revendication par l'entreprise d'un rôle strictement défini dans la société. L'entreprise considère comme « légitime » de connaître ce que l'Etat prépare comme modification des règles du jeu industriel si ces modifications peuvent porter atteinte à la pérennité de la firme. La légitimité réelle diffère souvent de la légitimité perçue par les acteurs d'un secteur (clients, fournisseurs, Etat, concurrents).

LEURRES : fausses annonces et désinformations réalisées dans l'objectif de tromper la concurrence pour l'attirer dans une interprétation erronée de son environnement concurrentiel.

LOBBYING : terme anglais qui provient de « lobby » (groupe de pression) et qui signifie la pratique régulière d'une pression auprès d'une organisation jouant un rôle important dans la modification de l'environnement de l'entreprise. Ces pressions peuvent être des chantages au licenciement économique, des manœuvres d'influence de personnes importantes appartenant aux organisations ciblées ou le prêt de « consultants » de l'entreprise à des organisations devant réaliser des normes pour un secteur ou pour l'aménagement supranational d'une industrie.

M

MANŒUVRE : littéralement, il s'agit d'une « œuvre réalisée par la main » qu'on peut traduire par un mouvement guidé par la main des hommes. Une manœuvre est donc la mobilisation des ressources de l'entreprise pour réaliser un déplacement. Ce déplacement peut être une diversification, une concentration, une intégration... La manœuvre est l'élément de base de toute stratégie.

MARKETING DE COMBAT : pratique du marketing qui s'inspire des théories militaires d'affrontement, de motivation des troupes, d'évitement et d'infiltration du territoire de l'adversaire en montrant l'analogie qui peut être faite entre un environnement concurrentiel et un champ de bataille. Le marketing de combat constitue une approche de l'environnement très utile au niveau local (segments de marché, produit) mais très réductrice quand il s'agit d'étudier la globalité de l'environnement car elle induit trop souvent l'idée de conflit et de destruction entre les acteurs.

MENACES : actions d'un acteur vis-à-vis d'un autre pour lui signifier qu'il a les capacités de remettre sa légitimité, sa présence ou son existence en jeu. Son objet est l'intimidation. Entre firmes, la menace peut avoir pour objectif de signifier une entrée dans un secteur ou la remise en cause d'une position concurrentielle adverse. Elle correspond à l'emploi de forces virtuelles pour contraindre un acteur à modifier son comportement sur un marché.

MENACES TRANSVERSALES : menaces dont les impacts portent sur différents secteurs et activités de l'entreprise. Le repérage des menaces transversales nécessite la constitution d'une équipe de veille globale qui centralise les informations recueillies dans les différents corps de métiers de l'entreprise.

METIERS (MECONNAISSANCE DES) : le métier constitue un cadre d'analyse pertinent pour la surveillance stratégique de l'environnement de la firme. Dans le cadre actuel de la mondialisation des marchés, la frontière géographique n'est plus un critère discriminant pour le tracé des frontières de la concurrence. La véritable concurrence s'exerce dans le cadre d'industries mondialisées, des métiers dont les frontières sont symbolisées par la spécificité des actifs, par une longue expérience et une accessibilité restreinte du métier à la concurrence. C'est la méconnaissance de ses propres métiers, notamment en termes d'accessibilité et d'imitation, qui conduit l'entreprise à sous-estimer les menaces et à perdre des marchés.

MISE EN CONFIANCE (TECHNIQUES DE) : la mise en confiance d'un acteur est préalable à toute opération de sollicitation de celui-ci. Très pratiquées par les services de contre-espionnage

de toutes les nations, les techniques de mise en confiance permettent à des agents de gagner la confiance d'un individu dans le seul objectif d'obtenir de lui de l'information ou une trahison. Elles consistent à dévoiler un point commun entre deux individus, à s'intéresser à lui, à l'appeler par son prénom, à s'échanger des adresses, à se confier ou encore à s'inviter au restaurant... L'ensemble de ces techniques, jouant de façon générale sur les faiblesses affectives de l'homme, sont mises en œuvre dans le cadre d'une approche de l'individu ciblé qui peut durer des semaines, des mois ou des années.

MOLE (TAUPE) : terme anglais désignant un agent infiltré dans une organisation sans être jamais sollicité. Cet agent qui « sommeille » n'est réveillée qu'en cas d'extrême nécessité afin de réaliser un effet de surprise et ramener à l'organisation qui l'a commanditée de nombreuses informations rares. De très rares cas de « taupes » ont été identifiés dans les entreprises.

MOTIVATION (TECHNIQUES DE) : techniques mises en œuvre lors de la formation et de l'entraînement des équipes de veille technologique et concurrentielle afin de motiver leur mission. Dans la pratique professionnelle de la veille, des sources de motivation différentes des motivations pécuniaires sont toujours recherchées en complément afin de protéger la stabilité des équipes.

MONITORING : issu du terme anglais « monitor », le monitoring consiste à s'aménager une fenêtre, ou un « écran », sur l'environnement et de veiller par ce moyen uniquement. Cette fenêtre peut être la connexion à une base de données ou l'affectation d'un veilleur auprès d'une organisation ou d'un secteur d'activité. Contrairement au benchmarking, le monitoring ne s'intéresse pas seulement à la concurrence mais à l'ensemble des informations de l'environnement.

N

NEOPANOPTISME : le principe du panoptisme est conservé : « celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir » (M. Foucault, *Op. Cit.*, p. 201), mais l'architecture physique d'une prison, ou d'un atelier, est remplacée avantageusement par *l'architecture virtuelle d'un système d'information*. sur l'environnement et la concurrence. La technologie, impersonnelle et précise, remplace le regard du surveillant, et réduit ainsi la tension que provoque une surveillance rapprochée comme celle du panoptisme.

NEGATION DE LA SURVEILLANCE : la surveillance est très souvent rejetée par les organisations comme une pratique trop peu éthique. Ce phénomène de négation de la surveillance accroît la vulnérabilité de ces organisations. Tandis que celles-ci considèrent la surveillance comme une spécialité confiée à des « agents », les entreprises concurrentes qui ont réellement saisi les enjeux de la surveillance de l'environnement déploient des effectifs, non pas d'agents spécialisés, mais de généralistes. Face à ces derniers, les entreprises qui ont adopté une attitude de déni sont incapables d'identifier la menace et accroissent ainsi leur vulnérabilité.

NEGLIGENCE (SIGNAUX DE) : dans une perspective offensive de l'intelligence, une pratique consiste à repérer des signaux de négligence en matière de sécurité des organisations adverses. Ces négligences repérées sont autant de points d'entrée d'une manœuvre d'infiltration.

NETWORKING : modèle d'organisation fondée sur le déploiement et l'utilisation de réseaux de compétences (« networks en langue anglaise anglaise). Ces réseaux virtuels peuvent être matérialisés par un réseau informatique mondial comme celui d'EDS, de Digital Equipment ou de la sogo-shosha Mitsui. Par extension, le networking est toute activité qui consiste à appréhender la résolution d'un problème par le développement d'un réseau de compétences et de contacts utiles.

NIVEAUX DE CONFIDENTIALITE : la confidentialité est toujours nivelée par le degré d'importance de l'information devant rester confidentielle au niveau d'un Etat, de la Défense de cet

Etat, ou au niveau d'une industrie du pays, d'une entreprise, d'un projet ou seulement au niveau d'un groupe restreint de personnalités nominativement désignées.

O

OBJECTIVITE : l'objectivité est toujours demandée à des veilleurs mais jamais acquise. Elle est seulement approchée. C'est avec cette idée qu'il faut aborder la mise en place d'un système de veille pour une organisation. Le degré de fidélité d'une information doit toujours être corrigée par la subjectivité qu'on accorde à celui qui l'a émise.

OBSOLESCENCE : état d'une technologie ou d'une technique qui est périmée du fait des progrès d'autres techniques lui étant concurrentes ou substituables. Contrairement à une croyance tacite et répandue, l'obsolescence n'est pas un phénomène nécessairement régulé et programmé. Une innovation majeure peut rendre obsolète une technologie dans un laps de temps très réduit. Détecter des menaces d'obsolescence est une des missions prioritaires d'une cellule de veille d'une entreprise.

OBSTRUCTIONNISME : tactique politique visant à systématiser l'obstruction aux projets d'une organisation dans l'objectif de défendre des acquis (salariaux, sociaux, subjectifs) ou de contribuer à l'avancement d'un autre projet. L'obstructionnisme est l'ennemi du développement intelligent de l'entreprise.

P

PANOPTIQUE : modèle architectural de maison d'inspection créé par Jeremy Bentham en 1787 : « à la périphérie, un bâtiment en anneau; au centre, une tour; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau; le bâtiment périphérique est divisé en cellules dont chacune traverse toute l'épaisseur du bâtiment; elles ont deux fenêtres, l'une vers l'intérieur, correspondant aux fenêtres de la tour; l'autre, donnant sur l'extérieur, permet à la lumière de traverser la cellule de part en part. Il suffit alors de placer un surveillant dans la tour centrale, et dans chaque cellule d'enfermer un fou, un malade, un condamné, un ouvrier ou un écolier. Par l'effet de contre-jour, on peut saisir de la tour, se découpant exactement sur la lumière, les petites silhouettes captives dans les cellules de la périphérie » (Michel Foucault, *Surveiller et Punir*, Gallimard, 1975, p. 201).

PANOPTISME : application du principe du panoptique — voir sans être vu grâce à la mise en œuvre d'une technologie — aux relations de pouvoir dans une organisation. Au sens large, le panoptisme est le regard de la surveillance par la médiation d'une architecture, ou d'une technologie.

PARADIGME : ensemble de schémas stabilisés de résolution de problèmes qui fournissent, pour un temps, des solutions types à un groupe déterminé d'individus. Au sens large, le paradigme suggère une attitude commune dans la conception et la gestion, qui s'étend à tous les concepts d'efficacité pour la production, aux modèles mis en œuvre, et aux relations interpersonnelles. L'appartenance à un paradigme peut tout autant être un facteur de progrès, en bénéficiant d'une réflexion collective, ou un frein à l'évolution, un « emprisonnement conceptuel ». En stratégie, les deux ouvrages de Michaël Porter (*Competitive Strategy* et *Competitive Advantage*) ont engendré un paradigme de résolution des problèmes stratégiques. En sociologie, le modèle d'interprétation des organisations sous formes de jeux d'acteurs et de conflits proposé par Crozier et Friedberg (*L'acteur et le système*) a engendré un paradigme de la sociologie des organisations. En espionnage, le paradigme dominant est celui de *L'art de la guerre* du stratège chinois Sun Tzu.

PARADIGME DE LA CENTRALISATION : premier paradigme des nouvelles technologies de l'information. Il fournissait aux chercheurs, et aux praticiens, des modèles de résolution des problèmes d'information les conduisant à un réflexe centralisateur.

PARADIGME DE L'INTERACTIVITE PARTIELLE : second paradigme des nouvelles technologies de l'information. Les modèles de gestion de l'information, de conception de systèmes d'information, amènent chercheurs et praticiens à concevoir les problèmes d'information en termes de *centre* et de *périphérie*. L'interactivité fait toujours partie des énoncés et des solutions, mais elle reste très partielle.

PARADIGME DE L'INDIVIDUALISATION : troisième paradigme des nouvelles technologies de l'information. Dans la conception des systèmes d'information, et dans la résolution des problèmes liés à leur gestion, l'individu est systématiquement mis au devant de l'analyse. On conçoit les systèmes à sa taille. On lui donne la capacité de traiter, lui-même, des quantités d'information de plus en plus importantes.

PARADIGME DE L'INFORMATION : coexistence des trois paradigmes des nouvelles technologies de l'information, puis *fusion en tout lieu où cela est possible*. Ces nouveaux modèles de résolution de problèmes traitent l'information dans sa globalité en jouant sur les combinaisons de systèmes centralisateurs, interactifs et individualisants. Chaque élément joue son rôle dans le cadre du paradigme auquel il appartient, mais il est connecté avec tous les autres éléments de tous les autres paradigmes. Il s'opère ainsi une régulation des trois paradigmes entre eux. Cette régulation est le lieu d'une négociation dont l'enjeu est un paradigme unique de l'information.

PARTENARIAT DE SYMBIOSE : partenariat entre deux entreprises fusionnant en une seule activité des activités substituables ou complémentaires. L'entité ainsi créée est voulue autonome et devrait se comporter comme une entreprise à part entière. A l'instar des joint-ventures, les partenariats de symbiose sont difficiles à réussir.

PARTENARIAT DE FAÇADE : partenariat temporaire entre deux entreprises voulant réaliser ensemble un objectif de court ou moyen terme. Une fois l'objectif atteint, l'organisation sera démantelée et le partenariat effacé. Ce type de partenariat, très tactique, exige une préparation minutieuse de la « sortie » de ce rapprochement. En effet, l'un des deux partenaires peut effectuer une sortie brutale du partenariat dès qu'il considère avoir acquis suffisamment d'informations pour réaliser seul ce qui était prévu à plusieurs. Faute de solides liens contractuels, ces stratégies de sorties inopinées seront toujours gagnantes.

PLANIFICATION STRATEGIQUE : le plan stratégique vise à formaliser et mettre en œuvre la pensée stratégique que l'entreprise a développée dans un réseau d'incertitude. Le plan explore les hypothèses et les confronte à différentes contraintes de temps, de moyens et de priorités que l'entreprise s'est fixée dans une période précédente pour répondre à d'autres enjeux stratégiques. Le planificateur a donc un rôle d'arbitrage qui nécessite une information précise sur l'environnement. C'est pourquoi les fonctions de veille sont souvent placées sous la bienveillance de la direction stratégique dans les entreprises.

POLITIQUE GENERALE : ensemble des grands principes de fonctionnement adoptés par l'entreprise afin de voir aboutir ses projets dans le cadre qui lui convient. Il peut s'agir d'un guide commercial pour l'entreprise (« maximiser les profits » ou « favoriser une meilleure rentabilité ») — on parle alors plus souvent de politique commerciale — accompagné d'un guide de conduite éthique et professionnel visant à fédérer le personnel dans le respect des règles de l'entreprise. Une vision stratégique claire est indissociable de l'excellence et de l'applicabilité de la politique générale de l'entreprise.

Q

QUANTITATIF / QUALITATIF : il existe deux modes majeurs de perception des signaux de l'environnement. Il s'agit, d'une part, du mode quantitatif ou « tous azimuts » qui consiste à recueillir la quantité la plus grande d'informations pour augmenter la probabilité de découvrir une information stratégique pour l'entreprise (monitoring), et d'autre part, du mode qualitatif qui consiste à focaliser les efforts de veille sur des zones restreintes d'observation (benchmarking).

QUASI-INTEGRATION VERTICALE (QIV) : organisation industrielle intégrée verticalement par des liens d'information et de relations continues (flux contractuels) entre une grande firme chef de file et des firmes de petites tailles satellisées.

QUESTIONS / REPONSES : mode de fonctionnement d'une antenne de renseignement délocalisée qui reçoit des séries de questions comme cahier des charges et doit fournir comme résultat les réponses correspondantes. Ce système simple de fonctionnement d'une cellule est l'un des plus efficaces et des plus pratiqués.

R

RATIONALITE LIMITEE : l'ensemble des décisions prises par un groupe d'individus le sont dans le cadre d'une démarche dont la rationalité est limitée par des réflexes intuitifs, le manque de temps ou encore des conflits affectifs internes au groupe.

RECOUPEMENT : activité qui consiste à confronter des faits obtenus de sources différentes pour les valider mutuellement ou les infirmer partiellement. Ces comparaisons deux à deux des informations obtenues de sources différentes sont répétées tant que l'information n'a pas atteint le seuil de fiabilité attendu (6, 7 ou 8 recoupements successifs n'ayant pu l'infirmer, par exemple).

REDUCTIONNISME : approche philosophique qui consiste à réduire les propriétés d'un tout à celles de ses éléments constitutifs et, par conséquent, à ramener un phénomène complexe à sa plus simple expression. En surveillance, la propension au réductionnisme s'exprime par la traduction précipitée de signaux de l'environnement en termes d'échecs ou de succès pour l'organisation sans prendre en compte la globalité de l'environnement dans laquelle doivent être situés ces signaux.

RENSEIGNEMENT : mobilisation de tous les moyens de recueil d'une organisation pour augmenter sa connaissance de l'environnement.

RESEAU : ensemble d'éléments ou d'acteurs interreliés. La nature des liens entre les éléments d'un réseau peut être contractuelle (entreprise), morale (clan), affective (famille), virtuelle (échange de menaces) ou encore coercitive (réseau d'informateurs). Les réseaux peuvent être permanents (réseaux diplomatiques) ou temporaires (management de projet).

RESEAU AGENTIQUE DE SURVEILLANCE : réseau d'informateurs dont tous les membres sont en état agentique lors de l'exécution de leur mission. Ce type de réseau caractérise l'approche technologique de la surveillance pour laquelle l'homme ne doit pas s'impliquer dans le traitement de l'information autrement que dans son recueil et son transport en l'état. Il est un *relais neutre* de l'information.

RESEAU MANAGERIAL DE SURVEILLANCE : réseau d'informateurs constitués de managers qui s'impliquent dans le traitement de l'information qu'ils recueillent et qui participent à la gestion de l'information de la firme. Ce type de réseau caractérise l'approche managériale de la surveillance pour laquelle l'homme est un *relais actif et participatif* de l'information.

RESEAU DE FIRMES : ensemble de firmes interreliées par des liens contractuels, professionnels (corps de métier) ou moraux (ententes de non-concurrence).

RESEAUX RELATIONNELS : ensemble d'acteurs interreliés par un choix mutuel des uns envers les autres qui peut être fondé sur l'intérêt (lobbying), sur l'affectif (amicale des anciens), sur le démonstratif (corporatisme et élitisme) ou encore sur un partage de compétences distinctives

(réseaux d'ingénieurs, de chercheurs, de radio-amateurs...). Les réseaux relationnels forment le plus souvent le canevas des réseaux de veille les plus performants.

RISQUE : le critère discriminant retenu pour décider de l'intérêt d'une opération de renseignement consiste à comparer le coût du risque encouru au coût de réduction de l'incertitude, c'est-à-dire le coût du renseignement.

S

SATURATION D'INFORMATION : fait significatif de la fin du XX^e siècle, les entreprises souffrent plus de l'excès d'informations que de leur manque. Dans un premier temps, elles accumulent excessivement l'information dans l'espoir de réduire l'incertitude grandissante qui les préoccupe. Dans un second temps, elles tentent de mettre en œuvre des méthodes visant à transformer la quantité en qualité (sélection, analyse, élimination). Les échecs sont nombreux.

SCANNING : proche synonyme de « monitoring », le terme est beaucoup moins employé dans la littérature récente de la surveillance que dans les années 1970. Peut-être semblait-il alors moins dénué « d'intelligence ».

SECRET : fait non porté à la connaissance d'autrui, le secret joue un rôle de premier plan dans la compétition en nivellant les positions concurrentielles. Il crée des asymétries d'information entre les acteurs qui se traduisent par des réactivités plus fortes, plus rapides, des mieux informés vis-à-vis de leur concurrent.

SECTEUR D'ACTIVITE : ensemble d'entreprises dont les offres sont soit substituables, soit complémentaires, interreliées et de natures analogues. L'offre du fournisseur est complémentaire à l'offre du donneur d'ordre puisqu'elle l'augmente. L'offre du concurrent lui est substituable. Les clients preneurs de ces offres entrent puis appartiennent au secteur.

SEGMENT : partie d'une activité qui peut être désignée parmi celle-ci par l'énonciation de critères peu nombreux et discriminants. Chaque discrimination supplémentaire correspond à la création d'un nouveau segment au sein du segment initial, ou « sous-segment ». Les télécommunications mobiles constituent un segment du marché ou de l'activité des télécommunications.

SIGNAUX : ce sont des émissions de l'environnement, des « signes » annonciateurs de nouvelles réalités environnementales. Les signaux peuvent être forts (dominant l'environnement, très faciles à détecter) ou faibles (dispersés, de faibles intensités et difficiles à détecter). La veille évolue actuellement du quantitatif, c'est-à-dire amasser le plus de signaux possibles, au qualitatif, c'est-à-dire détecter des signaux faibles très significatifs.

SOCIETE-ECRAN : société tout à fait réelle — puisque son nom est enregistrée et son capital créé — qui sert de couverture à des opérations secrètes d'une autre entreprise n'apparaissant dans les statuts de la société-écran qu'au travers de prête-noms et après de multiples participations en cascades dont l'objectif est de protéger l'identité réelle de l'entreprise.

SOGO-SHOSHAS : maisons de commerce japonaises organisées en véritables combinats bancaires, financiers et industriels et dirigeant de grands groupes japonais placés sous leurs tutelles. L'organisation de la veille japonaise est confiée au sogo-shoshas pour une meilleure « coordination / concertation » et des quantités d'informations recueillies plus importantes.

SOURCES : émetteurs d'une information.

SPHERE INFORMATIVE : ensemble indépendant d'informations nées de la duplication et de la déformation d'un groupe d'informations originales. Cet ensemble peut lui-même devenir le cadre de référence d'un groupe, et servir de base au développement de nouvelles sphères, plus limitées, plus éphémères, jusqu'à leur disparition.

SYNERGIE : réunion de moyens dont l'effet commun est supérieur à la somme des effets unitaires de chacun des moyens pris à part ($2 + 2 = \ll 5 \gg$).

T

TACTIQUE : tandis que la stratégie coordonne et prévoit les manœuvres devant aider l'entreprise à atteindre les buts qu'elle s'est fixée, la tactique contribue au succès de chacune de ces manœuvres sur le terrain. La tactique est la mise en œuvre répétée sur des horizons temporels finis, connus et limités des directives émises par la stratégie sur des horizons temporels plus longs et plus incertains.

TAUPE : agent infiltré (voir le terme anglais « mole »).

TECHNIQUE : activité qui consiste à créer des *objets techniques*, c'est-à-dire des *projections* du savoir scientifique sur la pratique, sans que cette pratique soit forcément effective. L'objet technique n'est pas obligatoirement disponible pour une application économique, industrielle et/ou sociale.

TECHNOLOGIE : combinaison de techniques qui nécessitent l'utilisation d'*information complémentaire* pour se réaliser. Les technologies ont pour finalité la production à laquelle elles participent. En d'autres termes, ce qui sépare l'objet technique du bien industriel, c'est la technologie.

TECHNOLOGIE GÉNÉRIQUE : technologie qui, par sa combinaison avec d'autres, permet la création de nombreuses technologies dans des domaines proches. C'est une technologie de base qui concentre suffisamment de savoir pour générer de nombreuses technologies d'application.

TECHNOLOGIE PANOPTIQUE : technologie de l'information mise en œuvre dans un réseau néopanoptique de surveillance. Elle recueille l'information pour l'autorité.

TECHNOSTRUCTURE : terme que l'on doit à J. K. Galbraith qui désigne la présence dans l'entreprise d'un groupe de fonctionnels qui conseillent et dirigent les divisions et filiales du groupe pour la formulation de chacune de leurs politiques. Une technostucture trop importante conduit l'entreprise à un management technocratique qui ignore le plus souvent une grande partie des réalités de l'environnement.

U

UNDERMEASUREMENT : terme anglais utilisé par les professionnels de la veille technologique et concurrentielle pour traduire la notion de sous-estimation des potentialités de son environnement par une entreprise. Elle correspond à une situation de sous-information.

V

VALIDATION : la validation d'une information consiste en l'attribution d'une note de fiabilité à une information suite à de nombreux recoupements.

VEILLE : synonyme de surveillance passive. Le verbe « veiller » est préféré par les praticiens au verbe « surveiller » qui se rapporte à l'univers carcéral, juridique et policier. La veille consiste à observer de façon systématique, mais passive, l'environnement sous tous ses aspects (économiques, juridiques, culturels, sociaux, historiques, écologiques...). La veille se différencie de l'intelligence en s'interdisant de modifier l'environnement sur lequel elle exerce une observation continue. La veille a un rôle de détection tandis que l'intelligence a une mission de positionnement de l'entreprise dans l'environnement qu'elle remplit par une stratégie d'influence et

de coercition des acteurs de cet environnement (lobbying, propagande, campagne de presse, networking).

VEILLE RELATIONNELLE : la veille relationnelle est née de l'échec des veilles quantitatives qui favorisaient l'étude des fréquences et des volumes des événements au détriment de leurs liens étroits, discrets, peu nombreux mais très significatifs avec d'autres événements. Cette forme de veille focalise toute sa puissance d'observation sur la détection de « liens cachés » entre plusieurs signaux faibles de l'environnement.

VIRTUALITE DES STRATEGIES : les stratégies actuelles sont marquées par des degrés de virtualité de plus en plus élevés. Une stratégie virtuelle consiste à signifier sa puissance et à communiquer son potentiel avant d'envisager son déploiement. Elle correspond à une volonté d'économiser les forces réelles, coûteuses à déployer, tout en obtenant des effets équivalents par le double jeu de la menace et de la coercition.

VIRUS : logiciel de quelques dizaines d'instructions détournant les capacités des systèmes informatiques à leur détriment. Il peut s'agir de « bombes logiques » qui inondent d'une même information l'ensemble d'un système informatique, ou encore d'un logiciel programmant la destruction des fichiers de données.

W X Y Z

WATCHING : terme anglais pour traduire la notion de veille permanente et assidue. Le terme traduit l'idée d'une sentinelle postée dans l'environnement pour veiller à la bonne connaissance de l'entreprise.

XENOPHILIE : l'ouverture d'esprit que réclame la fonction d'écoute au sein de l'entreprise réclame le recrutement de cadres et d'opérationnels aux « profils xénophiles », c'est-à-dire éprouvant de la sympathie pour les étrangers et une forte capacité d'adaptation à des environnements et des cultures différentes.

ZONES D'OBSERVATION : la veille ou « l'intelligence » de l'environnement nécessite un découpage de zones d'observation selon des critères qui peuvent être géographiques, techniques (par familles de technologies à surveiller), sectorielles ou encore stratégiques (surveillance des domaines d'activité stratégique). Dans tous les cas, il n'y a pas contradiction mais compatibilité et coopération entre l'organisation de l'entreprise (divisionnelle, fonctionnelle, géographique ou matricielle) et l'organisation de la surveillance (perçue comme un service interne, comme intégrée localement, ou encore comme proche de la direction générale).

INDEX

- accentuation*, 61
 acquisitions, 32
 acteurs, 26
 affrontement, 40, 111
 agents de l'intérieur, 68
 agents d'influence, 68
 agents sacrifiés, 68
 Allemagne, 40
 analyse historique, 128
 annonces, 109
 anticipation, 29
 apprentissage, 74
approche allemande, 44
approche cybernétique, 61
approche française, 44
approche japonaise, 46
approche managériale, 61
approche nord-américaine, 41
approche soviétique, 40
 approche spatiale de l'économie, 104
approche suédoise, 48
 architecture, 19
architecture virtuelle, 105
 aspirations éthiques, 138
assimilation, 61
 assujettissement, 98
asymétrie, 35, 122
 audit d'intelligence, 140
 autorité, 25
 barrières à l'entrée, 115
 bases de données, 41
 benchmarking, 43
 bombe logique, 84
 bureaucratie, 49
 canaux, 21
 capacité d'intelligence, 111
 capital, 15
capital gris, 32
 cellule, 39
 cellule de veille, 147
 cellule d'intelligence, 137
 cellules de coordination, 145
 cellules opérationnelles, 145
centralisation, 17, 93
 certitude, 21
 changement, 40
 circulation de l'information, 42
 clivage politique, 45
 cloisonnement, 45
 code déontologique, 138
 codification, 118
 coercition, 122
 cognitif, 38
 cohésion sociale, 113
 combinatoire de différenciation, 72
 combinatoire de structuration, 72
 combinatoires, 71
 commandement, 67
 communication, 28
 compétitivité, 12
 conception occidentale, 29
 concertation, 44
 concurrence, 10, 111, 128
 confidentialité, 117
 connaissance, 6
 contrôle de gestion, 148
 coopération, 40
 coordination, 13
 corporatisme, 45
 coût de transaction, 34
 coût économique, 112
 coût politique, 102
 coûts psychologiques, 115
 créativité, 97
 crédibilité, 62
 crise sacrificielle, 102
 culture, 29
 décision, 108
 défensif, 12
 délateur, 67
 démocratie, 28
 démonstration, 46
 déni de la compétition, 116
 désinformation, 46
 diffusion, 60, 75
 dilemme du néopanoptisme, 107
 dirigeants, 15
 discipline, 57
 discours, 103
 dissuasion, 21
 dissymétrie, 106
 domination, 73
 économie industrielle, 9
 effectivité, 111
 élitisme, 45
 émetteurs, 21
 enchère anglaise, 114
enchère hollandaise, 114
 environnement, 7
 environnement capitoné, 87
 environnements turbulents, 77
 espace, 10
 espionnage, 28
 État, 57
état agentique, 63
 États-Unis, 40

- éthique, 53, 126
- étonnement, 131
- existence de l'ennemi, 40
- extorsion, 139
- faux signaux, 114
- fichiers, 41
- filiale commune, 32
- filiales communes, 96
- firme-réseau, 35
- flexibilité adaptative, 29
- flexibilité décisionnelle*, 108
- flexibilité d'initiative, 74
- flexibilité organisationnelle*, 109
- flux d'information, 60
- flux physique, 60
- force réelle, 111
- force virtuelle, 111
- formel*, 59
- géopolitique, 48
- grappes technologiques, 108
- guerre, 86
- hiérarchie, 25
- histoire, 26
- hot-line, 42
- identité, 28
- illusion, 111
- image, 28
- impression, 19
- incertitude, 21
- inconscient collectif, 76
- individualisation**, 17, 95
- individualisme, 79
- influence, 140
- informateur, 61
- information ouverte, 135
- information privée, 107
- information publique, 107
- information secrète, 107
- information stratégique, 14
- informatique, 50
- informel*, 59
- inhibition, 64
- innovation, 8, 75
- intelligence d'entreprise, 121
- interaction, 130
- interactivité**, 17
- interstructuration, 86
- intimidation, 139
- intuition, 77
- Japon, 40
- jeu d'acteurs, 122
- joint-venture, 115
- KGB, 40
- libéralisme, 47
- liens, 127
- lobbying*, 65
- manipulation, 68, 97
- manipulation de l'information, 12
- manœuvres stratégiques, 37
- matrice, 150
- mécanisme d'expulsion de la violence, 89
- médiation, 85
- mémoire individuelle, 60
- mémoire sociale, 60
- menaces, 128
- messages, 21
- méthodologies, 6
- métier, 124
- mimétique, 76
- modernité, 28
- mondialisation, 39
- monitoring, 41
- motivation, 16
- mythe, 29
- néopanoptisme, 21
- networking, 50
- newsclipping, 41
- niveaux d'information*, 96
- normalité, 100
- obéissance, 64
- objet technique, 30
- offensif, 12
- offensive, 37
- ordre, 25
- organisation matricielle, 151
- panoptique, 19
- paradigme, 16
- partage des connaissances, 117
- partenariats, 96
- persuasion, 80
- pôles contractuels, 117
- politique, 7
- position transactionnelle, 92
- positionnement, 128
- potentialité, 108
- potentialité de l'inspection, 46
- pouvoir, 19
- prédiction, 62
- prédisposition agentique, 66
- pressions, 137
- prévention, 112
- principes de refuge, 77
- produits, 28
- profils d'intérêt, 141
- propagande, 80
- psychologie, 16
- qualité, 103
- quasi-intégralité verticale, 75
- rapport d'étonnement*, 62
- rationalistes, 80
- rationalité, 35
- réduction*, 60
- règles, 26
- régulation*, 61, 131
- relation instrumentale*, 25
- rente technologique, 73
- répression, 100
- réputation, 109
- réseau, 13
- réseau agentique, 65
- réseau managérial, 65
- réseau relationnel, 144
- réseaux, 3
- rétenion d'information, 45
- rituel, 87
- rumeur, 60, 61
- savoir, 26
- savoir collectif, 125
- savoir spécifique, 125
- secret, 49
- sécurité, 148
- sécurité informatique, 86
- signaux, 40, 128
- simulacre, 71
- sociologie, 9
- sogo-shosha, 47
- sources, 41
- souveraineté nationale*, 59
- sphère informative*, 60
- standard, 95
- stratégie, 9
- structure, 9

- structure mentale, 63
- sujétion*, 98
- surveillance économique, 12
- surveillance japonaise, 39
- symbiotique*, 46
- symbolique, 29, 61
- système de pertinence*, 131
- système de veille, 114
- système expert, 56
- systèmes de connaissance, 76
- tactique, 37
- technique, 30
- technologie, 10
- technologies de l'information, 7
- technologies génériques, 74, 115
- technostructure, 147
- tension essentielle, 78
- théorie de l'agence*, 22
- typologie de l'information, 41
- URSS, 40
- utilité, 121
- veille commerciale, 7
- veille concurrentielle, 7
- veille technologique, 7
- victime émissaire, 89
- violence, 49, 88
- virtualité, 111
- visibilité*, 21
- volumes, 127