INTELLIGENCE ECONOMIQUE ET STRATEGIQUE

Les systèmes d'information au cœur de la démarche

Mots clés

Management de l'information, Entreprise, Système d'information, Protection de l'information, Direction du Système d'Information, DSI, Patrimoine immatériel, Cycle du renseignement

03/2003

Auteur :

CIGREF

L'analyse, l'opinion et/ou la recherche reposent sur l'utilisation de sources éthiquement fiables mais l'exhaustivité et l'exactitude ne peuvent être garantie. Sauf mention contraire, les projections ou autres informations ne sont valables qu'à la date de la publication du document, et sont dès lors sujettes à évolution ou amendement dans le temps.

Le contenu de ces documents et/ou études n'a, en aucune manière, vocation à indiquer ou garantir des évolutions futures. Le contenu de cet article n'engage la responsabilité que de ses auteurs, il ne reflète pas nécessairement les opinions du(des) employeur(s), la politique ou l'opinion d'un organisme quelconque, y compris celui de gouvernements, d'administrations ou de ministères pouvant êtres concernés pas ces informations. Et, les erreurs éventuelles relèvent de l'entière responsabilité des seuls auteurs.

Les droits patrimoniaux de ce document et/ou étude appartiennent leur(s) auteur(s), voire un organisme auquel les sources auraient pu être empruntées.

Toute utilisation, diffusion, citation ou reproduction, en totalité ou en partie, de ce document et/ou étude ne peut se faire sans la permission expresse du(es) rédacteur(s) et du propriétaire des droits patrimoniaux.

INTELLIGENCE ÉCONOMIQUE ET STRATÉGIQUE

Les systèmes d'information au cœur de la démarche

Cigref
www.cigref.fr

MARS 2003

LE CIGREF

Le Cigref, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le Cigref réalise des études sur des sujets d'intérêt commun.

Rapports publiés par le Cigref en 2002-2003 :

Alignement stratégique du système d'information

Comment faire du système d'information un atout pour l'entreprise ?

Dynamique de la relation entre direction générale

et direction des systèmes d'information dans les grandes entreprises

(avec McKinsey & Company)

E-procurement et places de marché

Quels enseignements tirer à l'issue du projet IMP ?

Gouvernance du système d'information

Problématiques et démarches

Nomenclature 2002

Les emplois-métiers du système d'information dans les grandes entreprises

Sécurité des systèmes d'information

Quelle politique globale de gestion des risques ?

Ces publications peuvent être obtenues en se connectant sur le site web du Cigref :
www.cigref.fr

PARTICIPANTS

Ce rapport a été rédigé par Ludovic Etienne, chargé de mission du Cigref, dans le cadre de sa thèse professionnelle pour l'obtention du mastère spécialisé « management des systèmes d'information et des technologies » de HEC – École des Mines de Paris.

Cette étude constitue un rapport introductif à cette thématique. Elle a été réalisée grâce à la participation active des personnes suivantes :

François Galas, Alstom
Christian Pilaud, Club Méditerranée
Jean-Marie Faure, Crédit Lyonnais
Mohamed Marfouk, Danone
Patrick Lier, Giat Industries
Georges Epinette, Groupement des Mousquetaires
Philippe Copello, LVMH
Hubert Certes, Ondeo
Philippe Plin, Peugeot
Jean-Paul Sandré, Renault
Serge Druais, Thales
Christophe Binot, TotalFinaElf

Nous tenons également à remercier :

Christian Harbulot, École de guerre économique
Daniel Martin, OCDE
Marc Louichon, Consultant
Philippe Lorec, DREE
Bernard Besson, ministère de l'Intérieur
Pascal Lointier, Clusif

Nous remercions Christophe Binot, responsable du département gestion et valorisation de l'information au sein du groupe TotalFinaElf, qui a accepté de préfacer ce rapport.

PRÉFACE

« En tant que militant pour l'intelligence économique au sein de différentes directions des systèmes d'information (DSI) de grands groupes depuis 8 ans, je me réjouis que le Cigref consacre des travaux à ce sujet et sensibilise les DSI à cette opportunité. Car c'est bien cela dont il s'agit : une nouvelle opportunité pour la DSI d'apporter de la valeur dans son entreprise. Certes, la DSI continuera toujours à fournir des services liés aux infrastructures, aux grands applicatifs, au support utilisateur, mais de plus en plus elle aura un rôle majeur dans la gestion et la valorisation du patrimoine intellectuel de l'entreprise. Par sa vision transverse, elle facilitera l'échange et la circulation des informations et des connaissances au sein de l'entreprise mais aussi à l'extérieur, en particulier en outillant de manière performante toutes les formes de veille présentes et à venir. La récupération, le traitement et la présentation de gigantesques quantités d'informations textuelles est un challenge *technique brillant et motivant pour les équipes d'une DSI. C'est enfin là que se créeront les véritables avantages concurrentiels et c'est le plus important dans le contexte économique actuel. »*

Christophe Binot
Gestion et valorisation de l'information
DSIT TotalFinaElf

SOMMAIRE

1 PRÉAMBULE 11

2 LE CIGREF ET L'INTELLIGENCE ÉCONOMIQUE 13

2.1 Le contexte 13
2.1.1 L'intelligence économique, nouvelle orientation du Cigref 13
2.1.2 Actions concrètes 13
2.2 Légitimité de l'étude 15
2.3 Veille stratégique et Internet dans l'entreprise 19
2.3.1 La veille 19
2.3.2 De la veille à l'intelligence économique 20

3 L'INTELLIGENCE ÉCONOMIQUE OU LE MANAGEMENT GLOBAL DE L'INFORMATION STRATÉGIQUE 25

3.1 Définition de l'IES 25
3.1.1 Ce que l'intelligence économique n'est pas ! 25
3.1.2 Définition du rapport Martre 26
3.1.3 Définition de l'IHEDN 27
3.2 La prise de conscience des entreprises 27
3.2.1 Une prise de conscience variable 27
3.2.2 Les actions des pouvoirs publics 28
3.2.3 Résultats de deux enquêtes 29
3.3 L'information, matière première de l'intelligence économique 30
3.3.1 L'information, le carburant de l'entreprise 30
3.3.2 Typologie de l'information et des sources 31
3.3.3 Surabondance d'informations 32
3.3.4 Maîtriser l'information pour renseigner 33

4 LA DÉMARCHE D'INTELLIGENCE ÉCONOMIQUE ET STRATÉGIQUE 35

4.1 Gérer l'information : Le cycle du renseignement 36
4.1.1 L'expression des besoins 37
4.1.2 La collecte de l'information 41
4.1.3 Le traitement et l'analyse de l'information 49
4.1.4 La diffusion de l'information 53
4.2 Dans un contexte sécurisé : la protection de l'information 58
4.2.1 Quelques exemples… 58
4.2.2 L'information, source de convoitises 58
4.2.3 Les menaces envers le patrimoine informationnel 59
4.2.4 La sécurité ne peut qu'être globale 60
4.3 Face aux menaces omniprésentes : l'intelligence économique offensive 61
4.3.1 Quelques exemples 62
4.3.2 Contexte et définition 62
4.3.3 Les stratégies 64
4.3.4 La dominance par l'information 64
4.3.5 Info-déstabilisation, le rapport du faible au fort 66
4.3.6 Une prise de conscience nécessaire 69
4.3.7 Comment réagir ? 69

5 LES SYSTÈMES D'INFORMATION AU CŒUR DE LA DÉMARCHE 73

5.1 La technologie au service de l'IES 73
5.1.1 Le cyberespace 73
5.1.2 Nouvelles perspectives 73
5.2 L'impact d'internet 75
5.2.1 Abondance de l'information 75
5.2.2 Des outils de plus en plus performants 75
5.3 Vers des solutions globales d'intelligence 90
5.3.1 L'intégration des outils d'intelligence économique 90
5.3.2 Cas concret 92
5.4 Un système d'information adapté à l'intelligence économique 96
5.4.1 Définition 96
5.4.2 Dysfonctionnement des systèmes d'information dans le cycle du renseignement 96
5.4.3 Les structures transversales propices au développement de l'IES 99
5.4.4 L'exemple de France Télécom et de l'Aria 101
5.5 Les systèmes d'information, cible et vecteur offensif 102
5.5.1 Des menaces bien réelles 103
5.5.2 Les systèmes d'information cibles de l'infoguerre 105
5.5.3 Les attaques 106
5.5.4 Technologie et contre-intelligence 113

6 LE DSI, UN ÉLÉMENT MOTEUR DU CONCEPT D'INTELLIGENCE ÉCONOMIQUE ? 117

6.1 Le DSI, du technicien au stratège 117
6.2 Le DSI, expert et conseiller technique 118
6.3 Le DSI, manager fédérateur de projets 120
6.4 Le DSI, stratège et force de proposition 121

7 CONCLUSION 125

ANNEXE : BIBLIOGRAPHIE 127

Tableaux

Tableau 1 : Éléments déterminant le coordinateur de l'activité IES. 16
Tableau 2 : De la documentation à l'intelligence économique - graduation des pratiques. 21
Tableau 3 : Typologie de l'information. 31
Tableau 4 : Panorama des sources formelles et informelles. 45
Tableau 5 : Tableau des menaces externes. 59
Tableau 6 : Le rôle des agents intelligents dans le cycle du renseignement. 81
Tableau 7 : Internet et ses outils. 88
Tableau 8 : Évolution du rôle des responsables des systèmes d'information. 118
Tableau 9 : Responsabilités et compétences du DMSI. 122

Figures

Figure 1 : Fonction chargée de la coordination de l'IES (plus de 10 000 salariés). 17
Figure 2 : Liens entre les activités d'IES et la sécurité des SI. 18
Figure 3 : Concept d'intelligence économique. 22
Figure 4 : Des données au renseignement. 33
Figure 5 : Le cycle du renseignement. 34
Figure 6 : Démarche d'intelligence économique et stratégique. 35
Figure 7 : Fiche de synthèse du processus « Expression des besoins ». 40
Figure 8 : Fiche de captation. 44
Figure 9 : Fiche exemple d'une note d'étonnement. 47
Figure 10 : Fiche de synthèse du processus « Collecte ». 48
Figure 11 : Fiche de synthèse du processus « Traitement et analyse ». 52
Figure 12 : La valeur de l'information. 59
Figure 13 : Le processus et les trois finalités des guerres de l'information. 67
Figure 14 : Site StopEsso.com. 68
Figure 15 : Exemple de collège invisible. 78
Figure 16 : Structure d'un agent. 80
Figure 17 : Atlas des outils de cartographie de l'information. 82
Figure 18 : Carte d'information Umap. 83
Figure 19 : Peoplegarden, visualisation de conversations dans des forums internet. 84
Figure 20 : Navigation sur internet. 84
Figure 21 : Performance boursière de 500 entreprises. 85
Figure 22 : Carte de visualisation synthétique de dépêches d'agences de presse. 85
Figure 23 : Représentation multidimensionnelle de pages web. 86
Figure 24 : Outil de visualisation (*Mind-Mapping*). 87
Figure 25 : Panorama des outils sur le cycle du renseignement. 89
Figure 26 : Passage d'une structure fonctionnelle à une organisation par processus 99
Figure 27 : Axes de la planification stratégique des systèmes d'information compétitifs. 100
Figure 28 : Principales attaques subies en 2001-2002 par les membres du Cigref. 104
Figure 29 : Corrélation entre la nature des incidents et leur origine. 105
Figure 30 : Des procédures d'attaque qui nécessitent de moins en moins de compétences. 107
Figure 31 : Représentation du réseau anti-Esso. 110

« Le développement de la micro-informatique a permis l'individualisation et l'interactivité de l'information, cette nouvelle informatique étant désormais ouverte, partagée et accessible. Cette évolution concerne la totalité du système d'information de l'entreprise. La généralisation de l'informatique a créé une nouvelle architecture entrepreneuriale. Désormais, chaque entreprise ressemble, quelle que soit sa taille, à un système nerveux qui relie la hiérarchie, les cadres et leurs subordonnés à la vitesse de l'électron. Et ce système nerveux, qui autorise à chaque instant des échanges en temps réels, ne véhicule pas autre chose que de l'information. Ce concept d'information traitée déborde donc très largement le monde des médias pour toucher l'ensemble du substrat entrepreneurial des économies développées. L'information et sa maîtrise sont aujourd'hui devenues un enjeu majeur pour les sociétés développées[1]. »

[1] Allain-Dupré Patrice et Duhard Nathalie, *« Les armes secrètes de la décision »*, Gualino Éditeur, 1997.

1 PRÉAMBULE

L'information et le savoir, à la base du succès économique, sont devenus des biens stratégiques de première importance. En effet, dans un contexte de mondialisation, la turbulence des marchés génère une concurrence sans précédent entre les entreprises. La capacité à comprendre son environnement et à anticiper les changements constitue, plus qu'avant, le facteur clé de la productivité et de la croissance des organisations. Cette nouvelle approche de la compétition économique nécessite de gérer la connaissance de façon globale. L'intelligence économique s'inscrit comme ce nouveau mode de management basé sur la gestion optimale de l'information stratégique.

« Dans son approche globale, l'intelligence économique se fonde sur la maîtrise de l'information et la production de connaissances nouvelles. »
J.-L. Levet[2]

L'apparition des nouvelles technologies a radicalement transformé le fonctionnement des organisations. Dans cette période de transition, les systèmes d'information apparaissent comme une solution pouvant garantir un avantage concurrentiel pour les entreprises. L'ensemble des échanges économiques et culturels est peu à peu transféré au sein d'une infrastructure d'information globale, qui oriente la stratégie et transforme les processus de l'entreprise.

Le management de l'information stratégique préfigure la nouvelle dimension de l'intelligence économique. Trop longtemps assimilé à de l'espionnage, le concept doit aujourd'hui être appréhendé dans sa forme la plus globale. Casser les tabous et faire évoluer les mentalités en changeant nos rapports avec l'information. Les systèmes d'information, de par leurs performances techniques et leurs ramifications transversales peuvent radicalement accélérer le développement de l'intelligence économique et favoriser une culture collective de l'information.

[2] Président de l'Association française pour le développement de l'intelligence économique (AFDIE), *in* Levet Jean-Louis, *L'intelligence économique, mode de pensée, mode d'action*, Economica, 2001.

Conscient des possibilités offertes par les technologies de l'information et de la communication, dans un environnement où le savoir et la connaissances deviennent une source de conflit, le Cigref souhaite, à travers cette étude, répondre à deux questions centrales :

- Quelle est la place actuelle des systèmes d'information dans la démarche d'intelligence économique ?
- Le directeur des systèmes d'information (DSI) peut-il avoir un rôle à jouer dans cette démarche ?

Ce rapport n'a pas la prétention de réinventer le concept d'intelligence économique. Il se veut juste être une première ébauche de réflexion sur le positionnement des systèmes d'information. Le domaine étant relativement vaste, il ne sera pas possible de balayer l'ensemble du sujet ; certains points seront sûrement omis, les spécialistes nous pardonneront ces oublis.

2 LE CIGREF ET L'INTELLIGENCE ÉCONOMIQUE

2.1 Le contexte

2.1.1 L'intelligence économique, nouvelle orientation du Cigref

Système nerveux de l'entreprise, les systèmes d'information se positionnent de plus en plus comme l'élément central des stratégies des organisations. Améliorant la compétitivité de l'entreprise, ils redessinent l'organisation de l'entreprise en optimisant les processus. Comme le précise Philippe Baumard[3] : « Nous vivons une période de transition où l'ensemble des échanges économiques et culturels va peu à peu être transféré au sein d'une infrastructure d'information globale, où les organisations seront constituées de systèmes complexes et temporaires d'interactions entre différentes technologies de l'information. »

Le Cigref a parfaitement appréhendé cet état de fait et mesure pleinement le champ d'action que laisse augurer le développement des systèmes d'information. Cette perspective préfigure également une évolution évidente du rôle du DSI au sein de l'entreprise. En créant le projet Cigref 2005, il s'agit de redéfinir et d'élargir le domaine d'activités stratégiques de l'association en y introduisant notamment de nouveaux axes de réflexion. Trois pôles ont ainsi été définis : le pôle Entreprises, le pôle DSI et le pôle Société de l'information.

« Promouvoir les systèmes d'information comme facteur de création de valeur pour l'entreprise. »
Cigref

Dans ce cadre précis, l'intelligence économique et stratégique est apparue comme un sujet qu'il était nécessaire de traiter. Inclus dans le comité de pilotage sur la Société de l'information, il s'agit d'un thème émergent qui préfigure l'ouverture du Cigref et le développement des systèmes d'information dans notre société.

2.1.2 Actions concrètes

Aborder le thème de l'intelligence économique et stratégique (IES) reste encore une démarche délicate. En effet, le sujet souffre toujours d'une image négative, sur laquelle viennent se greffer des relents d'espionnage et de méthodes illicites. Malgré les nombreux ouvrages qui tentent de banaliser le concept, parler d'intelligence économique et stratégique reste tabou, et faire témoigner les entreprises qui la pratiquent s'avère toujours difficile. En conséquence de quoi, répondre à notre problématique est plus compliqué qu'il n'y paraît.

---

[3] Baumard Philippe et Benvenuti Jean-André, *Compétitivité et systèmes d'information,* InterEditions, 1998.

Pour susciter l'intérêt parmi ses membres, déterminer les orientations futures sur le thème de l'IES et donner les premiers éléments de réponse concernant la place des systèmes d'information et le rôle du DSI dans la démarche d'IES, le Cigref a mis en œuvre plusieurs actions concrètes. La première étape doit consister en une sensibilisation sur le sujet, en procédant à un tour d'horizon des différents concepts qu'il sous-tend. La deuxième étape doit permettre aux DSI de disposer d'un support constituant une première ébauche de réflexion sur ce thème.

Le Cycle IES, une sensibilisation au concept, aux modes d'action et aux outils

Composé de trois matinées réparties sur cinq mois, le Cycle d'intelligence économique et stratégique du Cigref a permis de traiter de thèmes aussi divers que la guerre de l'information, la cybercriminalité, la gestion de l'information et ses outils, la mise en place d'une politique d'intelligence économique ou d'une cellule *web* de crise. Les plus grands spécialistes sont intervenus pour informer les membres et débattre avec eux sur le sujet. Recueillir le témoignage de ces derniers était important, pour pouvoir, dès à présent, entrevoir des scénarios prospectifs pour l'année suivante.

Réalisation d'un rapport, premier élément de réflexion

Parallèlement à ce projet, la rédaction d'un rapport devait permettre d'apporter les premiers éléments de réponses aux questions posées et constituer un support de base pour poursuivre les réflexions. Cependant, il s'avéra plus difficile que prévu d'obtenir le témoignage des entreprises. Face à cette difficulté, deux constatations :

- soit le DSI est impliqué dans la politique IES de son groupe, mais le sujet demeure trop sensible ;
- soit le DSI est peu impliqué dans la politique IES de son groupe, il est alors prêt à témoigner mais ne peut guère apporter d'éléments de réponse.

Par conséquent, face à ce constat, ce rapport est bâti en partant des sources suivantes :

- les témoignages obtenus au cours du Cycle IES ;
- les entretiens réalisés avec des DSI ou leurs collaborateurs ;
- les différents ouvrages écrits sur ce thème (voir bibliographie en annexe).

2.2 Légitimité de l'étude

Évaluer la perception des entreprises françaises face au concept d'intelligence économique n'est pas une chose aisée. Quant à l'implication de celles-ci dans la mise en place d'une politique, autant dire que le souci de confidentialité a freiné de nombreuses initiatives. Pour parer à ce manque, la direction des études de l'IHEDN[4] (Institut des hautes études de la Défense nationale) a décidé de lancer une vaste enquête nationale auprès des entreprises de plus de 200 salariés, et d'effectuer avec toutes les garanties de confidentialité sur les données transmises, un panorama de l'IES en France. Jamais une action de ce type n'avait été menée à si grande échelle.

Outre le fait qu'elle se positionne comme une étude de référence pour les entreprises, cette enquête constitue un point de départ intéressant pour le Cigref et confirme le choix de faire de l'IES un nouveau thème d'étude. En effet, au travers des résultats obtenus, il est possible d'avoir un point de situation ou une vision prospective sur le positionnement des directions des systèmes d'information et de leur responsable, dans la politique d'IES.

Plusieurs éléments importants en ressortent.

Les systèmes d'information font partie intégrante de l'IES

Pour les entreprises de plus de 10 000 salariés, ou grands groupes, l'étude a montré que les activités d'IES englobaient les systèmes d'information : *l'IES est conçue comme un produit dérivé des systèmes d'information de l'entreprise et du traditionnel « système informatique ».*

Le DSI, un coordinateur de l'IES

Le tableau suivant fait le point sur les personnes chargées de coordonner les activités d'IES au sein de l'entreprise. On constate que plus l'organisation est importante et plus ce rôle est dévolu à un service autre que la direction générale. Parmi les cinq acteurs clés amenés à être le coordinateur, le DSI apparaît dans 9 % des cas, en priorité pour des groupes de grande taille tournés vers l'international et, par conséquent, soumis à une forte concurrence.

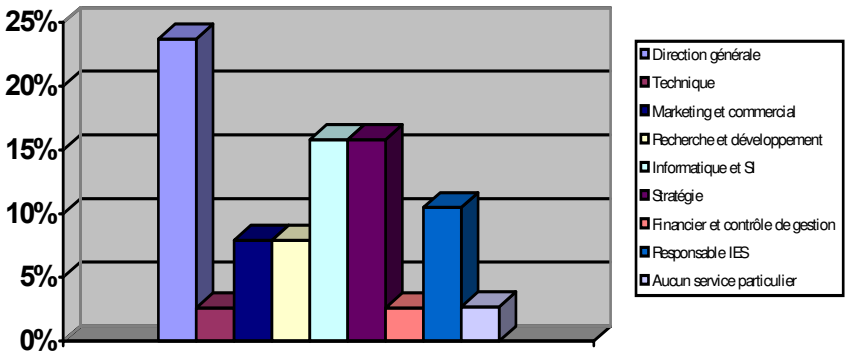
[4] Bournois Franck et Romani Pierre-Jacquelin, *L'intelligence économique et stratégique dans les entreprises françaises*, IHEDN, Economica 2000. www.ihedn.fr.

Caractéristiques du contexte	– → = → +			
1. Taille	DG	Marketing Commercial		Stratégie RIES DSI
2. Chiffres d'affaires	DG	Marketing Commercial	Pas de service particulier	Stratégie RIES
3. Pourcentage du CA à l'export	DG	Technique Finance	Marketing Commercial Stratégie	Stratégie RIES
4. Nombre de filiales	DG	Stratégie		RIES
5. Concurrence mondiale	DG	Stratégie		Stratégie R&D RIES DSI
6. Structure : de fonctionnelle (-) à divisionnelle (=) à matricielle (+)	DG	RIES R&D		Stratégie
7. Nombre et intensité des attaques	Aucun service	Stratégie	DG Technique R&D RIES	Marketing Commercial R&D

RIES = responsable de l'intelligence économique et stratégique. *Source : IHEDN*

Tableau 1 : Éléments déterminant le coordinateur de l'activité IES.

Ce constat est confirmé par la figure 1, qui place le DSI en troisième position parmi les coordinateurs de l'IES, pour les entreprises de plus de 10 000 salariés. L'étude évalue à 16 % le nombre de coordinateurs qui occuperaient également une fonction de DSI. Il ne semble donc pas illusoire de penser que les DSI peuvent effectivement se positionner comme « chef d'orchestre » des activités d'IES.



Source : IHEDN

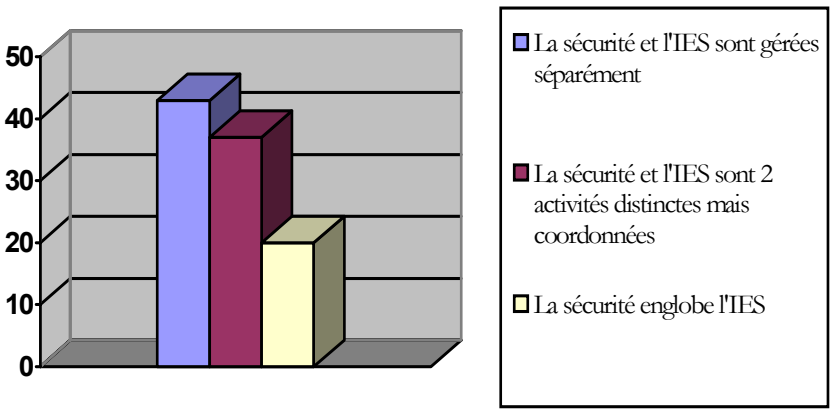
Figure 1 : Fonction chargée de la coordination de l'IES (plus de 10 000 salariés).

La sécurité des systèmes d'information et l'IES

L'étude a également pu mettre en évidence le rôle prépondérant accordé à la sécurité des systèmes d'information, mission qui incombe à la DSI. Dans l'ensemble, les connexions et les coordinations existent puisque dans 61 % des cas, le responsable de l'IES participe à la définition de la politique de sécurité des systèmes d'information de l'entreprise. La figure 3 résume le positionnement des entreprises sur ce sujet en mettant en évidence les liens entre la sécurité des systèmes d'information et les activités d'IES.

Deux particularités sont à noter :

- le responsable l'IES est d'autant plus impliqué dans la sécurité des systèmes d'information que l'entreprise appartient aux trois plus grands compétiteurs du marché (réduction des vulnérabilités et maintien de la position de leadership) ;
- il est d'autant moins impliqué que l'entreprise n'a pas identifié d'attaques particulières.



Source : IHEDN

Figure 2 : Liens entre les activités d'IES et la sécurité des SI.

Cette constatation met en évidence l'importance qui est accordée à la sécurité des systèmes d'information dans le concept d'IES.

Cette étude réalisée auprès de nombreuses entreprises apporte des éléments de confirmation quant à l'orientation que souhaite prendre le Cigref sur le thème de l'intelligence économique et stratégique. Elle valide plusieurs faits que nous tenterons d'expliciter dans la suite du rapport :

- parce qu'ils véhiculent et gèrent l'information dans sa quasi-globalité, les systèmes d'information peuvent constituer l'épine dorsale du concept d'IES ;
- les systèmes d'information s'intègrent parfaitement aux processus utilisés dans les activités d'IES. Parce qu'ils sont stratégiques, ils demeurent un point névralgique qu'il est facile de neutraliser, ou détruire. En assurer leur sécurité, telle doit être la préoccupation des entreprises qui désirent mettre en place une politique d'IES ;
- le DSI doit participer à la définition des activités d'IES dont il peut être le coordonnateur.

Partant de ce constat, nous pouvons affirmer que l'intelligence économique et stratégique n'est pas un thème irréaliste dans la sphère des systèmes d'information. Le Cigref a choisi plusieurs axes d'orientation, concrétisés par différents projets, afin d'imposer l'IES comme un sujet d'avenir auquel il était souhaitable que les DSI s'intéressent.

Dès 1997, des travaux de recherche étaient entrepris par le Cigref. En effet, les rapports sur la « Veille stratégique » publié en 1998 et « Internet dans l'entreprise » publié en 2001, amorçaient déjà une réflexion sur l'intelligence économique et

stratégique. Avant de développer plus amplement ce thème, revenons sur les points importants de ces deux études.

2.3 Veille stratégique et Internet dans l'entreprise

Beaucoup d'entreprises pensent faire de l'intelligence économique alors qu'elles ne font en fait que de la veille. L'amalgame et la confusion sont souvent faits entre ces deux pratiques ne permettant pas d'avoir une vision claire de ce qu'est l'intelligence économique. Le Cigref a souhaité, dès 1998, effectuer une étude sur le thème de la veille stratégique, appliquée à l'entreprise et plus particulièrement au secteur de l'informatique. Par la suite, en 2001, le rapport sur l'internet dans l'entreprise a introduit le concept d'intelligence économique au sein de l'association.

2.3.1 La veille

On définit la veille comme un sous-ensemble de l'intelligence économique. La norme expérimentale française XP X 50-053 de l'Afnor[5] « Prestation de veille et prestation de mise en place d'un système de veille » (avril 1998) définit la veille comme « l'activité continue et en grande partie itérative visant à une surveillance active de l'environnement technologique, commercial, etc., pour en anticiper les évolutions » et l'anticipation comme la « détection d'une situation avant qu'elle se soit réellement manifestée ».

Le rapport du Cigref détermine quatre types de veille :

- *la veille scientifique* : sciences, techniques, technologies, procédés et méthodes ;
- *la veille commerciale et concurrentielle* : aspects commerciaux (marchés, clients, méthodes) et concurrentielle (concurrents, nouveaux entrants, nouveaux produits, relations clients et fournisseurs…) ;
- *la veille sociétale* : facteurs culturels, politiques, sociaux, historiques, acteurs institutionnels, opinion publique, réglementation, environnement ;
- *la veille stratégique* : approche plus globale qui doit fédérer les différents types de veilles de l'entreprise et intégrer la dimension stratégique. Cette démarche reste plus orientée vers l'action.

L'origine du terme de veille est le résultat d'une négation du terme « intelligence économique ». Alors que les pays anglo-saxons font un usage courant des termes « *Economic Intelligence* », « *Business Intelligence* » ou encore « *Competitive Intelligence* », la France utilise encore rarement le terme d'intelligence économique. Comment exprimer alors

[5] Afnor : Agence française de normalisation.

une activité d'ingénierie offensive de l'information ? Il était hors de question d'utiliser le terme « renseignement », à trop fortes connotations militaires, ni le terme « intelligence » qui faisait référence à la notion d'espionnage. Dès lors les entreprises françaises ont choisit le terme « veille » pour décrire leur ingénierie stratégique de l'information[6]. Mais, malgré qu'elles demeurent nécessaires, les activités de veille ne représentent qu'une étape de l'intelligence économique.

2.3.2 De la veille à l'intelligence économique

L'approche gestionnaire de la veille répond à un besoin de savoir un maximum d'informations possible et de ne rien perdre de ce qui est accessible. Alors que l'approche stratégique de l'intelligence économique répond au besoin de prendre une décision. Elle répond à un besoin de savoir un minimum d'information nécessaire et d'agir pour progresser vers une situation plus favorable[7].

L'intelligence économique intervient à partir du moment où l'on a réussi à extraire des informations issues d'une veille active, les données les plus pertinentes qui vont pouvoir être utilisées par les décideurs. Le rapport sur « L'Internet dans l'entreprise », définit l'intelligence économique comme l'aboutissement d'un long processus dont l'origine est la veille documentaire.

[6] Commissariat général du plan, *Intelligence économique et stratégie des entreprises,* La Documentation française, 1994.

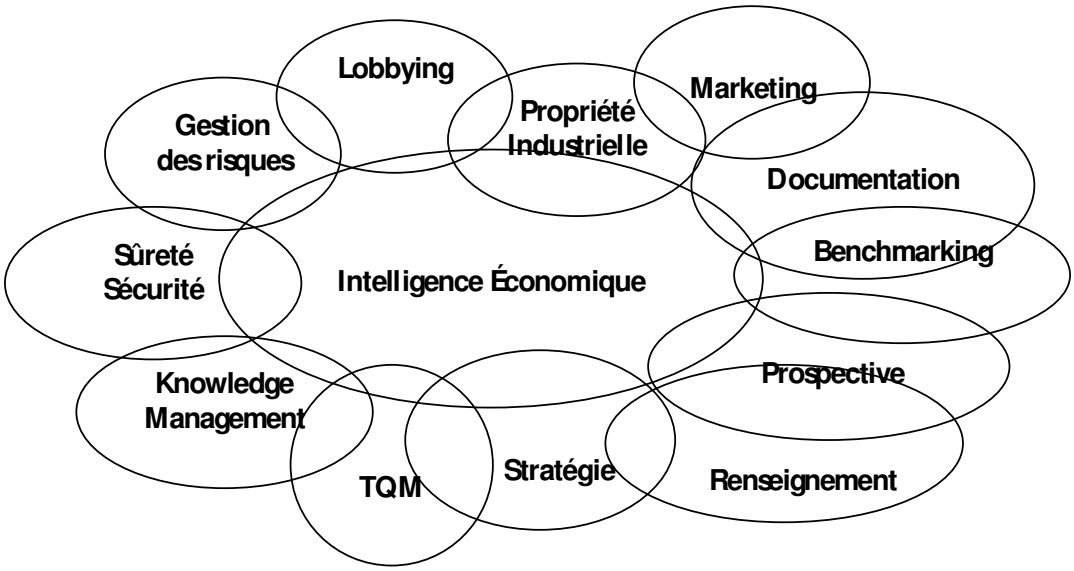
[7] Frion Pascal (ACRIE réseau national), « Entre veille et intelligence économique, il faut choisir »*, in* Technologies Internationales, n° 84, mai 2002.

Documentation ↓	- Exploitation de sources formelles et ouvertes d'information uniquement - Parfaite connaissance des sources	Diffusion et informations brutes
Veille documentaire ↓	- Surveillance de certains secteurs - Spécialisation des documentalistes - Profils de veille	
Veille spécialisée ou **sectorielle** (technologique, brevet, juridique, normative, commerciale, concurrentielle…) ↓	- Exploitation d'informations informelles et fermées - Mobilisation des réseaux	
Veille globale (stratégique ou tactique) ↓	- Approche plus globale : fédère les différentes veilles de l'entreprise et intègre la dimension stratégique	
Intelligence économique	- Intègre les actions d'influence et le lobbying - Suppose une culture collective de l'information - Intègre un ensemble large d'acteurs dans l'entreprise - Se doit d'être érigée en véritable mode de management	

Source : TotalFinaElf

Tableau 2 : De la documentation à l'intelligence économique - graduation des pratiques.

La veille est l'étape ultime avant de passer à une stratégie d'intelligence économique. Comme le spécifie le groupe TotalFinaElf dans le tableau ci-dessus, l'intelligence économique est un mode de management qui dépasse le processus de veille parce qu'il est global : le concept induit une culture collective de l'information accompagnée d'actions offensives, avec le souci constant de protéger le capital informationnel de l'organisation. Concept à part entière, il est un assemblage de diverses notions, comme le montre le schéma suivant.



Source : TotalFinaElf

Figure 3 : Concept d'intelligence économique[8].

Cette première étude sur l'intelligence économique a mis en évidence plusieurs idées forces pour que ce concept s'insère parfaitement dans l'entreprise :

- véritable projet, il nécessite de bâtir une démarche ;
- l'organisation d'une structure d'intelligence économique doit se faire autour d'une cellule de veille stratégique, ce qui suppose des orientations précises sur l'organisation et l'implantation de cette entité ;
- l'engagement et le soutien de la direction générale ;
- la sensibilisation de l'ensemble des salariés ;
- l'insertion des cellules de veille dans le processus de décision ;
- l'existence de capteurs suffisamment nombreux pour favoriser la remontée d'informations du terrain ;
- la prédominance de plus en plus forte des outils informatiques.

Enfin, le Cigref entrevoyait des tendances quant à l'orientation que prenait l'intelligence économique :

- l'évolution vers la gestion des connaissances ;
- l'importance croissante des « portails décisionnels » ;
- le développement par des prestataires externes d'offres de solutions de veille sur mesure et à la demande.

[8] *op. cit.*

La place des systèmes d'information dans le concept d'IES semble omniprésente. Les premières réflexions du Cigref et les chiffres de l'enquête réalisée par l'IHEDN paraissent confirmer la prédominance des technologies de l'information et de la communication dans la gestion de l'information stratégique de l'organisation et justifier l'intérêt de la question suivante :

Comment peuvent se positionner les systèmes d'information dans une démarche d'intelligence économique ?

Avant d'apporter les premiers éléments de réponses, il semble nécessaire de donner une définition de l'IES et de définir les principaux axes qui pourraient constituer cette démarche.

3 L'INTELLIGENCE ÉCONOMIQUE OU LE MANAGEMENT GLOBAL DE L'INFORMATION STRATÉGIQUE

3.1 Définition de l'IES

3.1.1 Ce que l'intelligence économique n'est pas !

Le nombre croissant d'ouvrages traitant de l'intelligence économique ainsi que la méconnaissance du domaine ont souvent donné à ce concept une image fausse et galvaudée. Par conséquent il semble primordial, avant de définir précisément ce qu'est l'intelligence économique, d'affirmer ce qu'elle n'est pas. Leonard M. Fuld, président du cabinet américain d'intelligence économique Fuld & Company[9], résume parfaitement les fausses idées auxquelles on associe l'intelligence économique.

L'intelligence économique n'est pas…

- *De l'espionnage* : l'intelligence économique ne peut pas être de l'espionnage car les sociétés ne peuvent prendre le risque de se retrouver au tribunal ou de contrarier leurs actionnaires.
- *Une boule de cristal* : l'intelligence économique ne peut dire ce qui va se passer exactement demain. Elle donne aux sociétés de bonnes images de la réalité à court et moyen terme.
- *Une activité de recherche sur les bases de données* : Les bases de données n'offrent rien d'autre que des données. Ces dernières sont très utiles et appréciables. Toutefois on ne peut réduire l'intelligence économique à l'accumulation de données. Elle va beaucoup plus loin en les analysant et en proposant des scénarios. L'activité nécessite de l'expérience, un travail de réflexion et de l'intuition.
- *De la recherche sur internet ou la chasse aux rumeurs* : internet est avant tout un moyen de communication et non un fournisseur d'intelligence. Les données sont brutes et ne peuvent être interprétées qu'après avoir été analysées. On peut trouver des indices, des pistes sur des concurrents, des évolutions sur l'environnement, mais il faut savoir discerner ce qui est vrai de ce qui ne l'est pas. Il faut également nuancer les rumeurs qui ne sont pas toujours fondées. Agir avec une grande finesse pour faire le tri et sélectionner judicieusement l'information.

[9] www.fuld.com. Leonard Fuld est le fondateur et le président de Fuld & Company, cabinet situé à Cambridge dans le Massachusetts. Fondée en 1979, cette société est pionnière dans le domaine de l'intelligence économique. Durant les vingt dernières années, le cabinet a mené des actions pour la moitié des entreprises américaines classées au Fortune 500.

- *Simplement du papier* : Le papier tue l'intelligence économique. Une conversation directe ou téléphonique est plus rapide. Rédiger prend du temps, or l'information collectée n'est utile que si elle est transmise rapidement. De plus les idées transcrites par écrit sont parfois déformées ou mal interprétées. Elles suppriment également la possibilité d'argumenter, de se défendre.
- *Le travail d'une personne* : Une personne seule ne peut accomplir toute l'activité d'intelligence économique. Au mieux, elle coordonne l'ensemble de l'activité. On introduit ainsi la notion de réseau dans lequel circule l'information. Le responsable de l'intelligence économique doit continuellement s'assurer que tous les membres de l'entreprise s'impliquent et font circuler l'information.
- *Une invention du vingtième siècle* : L'intelligence économique a toujours existé. Son apparition dans les entreprises date du début des années 80. Auparavant le concept existait surtout dans le domaine militaire.
- *Un travail fait par des logiciels* : Comme pour les bases de données, on ne peut réduire l'intelligence économique à la simple utilisation des logiciels. Ils sont les outils essentiels à l'activité mais ils ne peuvent remplacer l'analyse de l'expert.
- *Une histoire de journaux :* Les informations récoltées dans les médias (presse, radio télévision) ne constituent pas à elles seules un moyen efficace de faire de l'intelligence économique.

3.1.2 Définition du rapport Martre

À la fin des années 80, le concept d'IES est solidement implanté dans les pays tels que le Japon, l'Allemagne, la Suède ou les États-Unis, qui en ont fait le moteur stratégique de leur développement et de leurs succès commerciaux. La pratique de l'intelligence économique apparaît alors comme un levier essentiel de la performance globale des nations. Mais en France, face à l'efficacité des dispositifs étrangers, comment se positionnent les entreprises ?

Afin d'effectuer un état des lieux et de proposer les adaptations indispensables, le Commissariat général du Plan a réuni en 1994, sous la présidence de Henri Martre, président de l'Afnor et président d'honneur d'Aérospatiale, un ensemble de praticiens formant une première communauté française de l'intelligence économique : industriels, représentants de l'administration, des collectivités territoriales, des organismes consulaires, des syndicats et consultants[10].

[10] Commissariat Général du Plan, *Intelligence économique et stratégie des entreprises*, La Documentation française, 1994.

De cette initiative est née une définition de l'intelligence économique à laquelle il est judicieux de se référer, même si d'autres ont été citées par la suite au fur et à mesure de l'évolution du concept. La définition donnée par le Commissariat général du Plan en 1994 est la suivante:

« L'intelligence économique peut-être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques, obtenue légalement dans les meilleures conditions de qualité, de délais et de coût. »

3.1.3 Définition de l'IHEDN

Aujourd'hui, le concept a évolué vers le domaine plus large de la gestion de l'information. Le développement de l'internet ces dernières années ayant eu un impact considérable sur la discipline. En effet, le web, les messageries et les intranets ont transformé les méthodes d'acquisition et de circulation de l'information. De nouvelles disciplines comme la gestion des connaissances élargissent encore le concept, que l'IHEDN définit à présent comme l'intelligence économique et stratégique. En partant de cette définition, nous pouvons dire que l'intelligence économique et stratégique représente :

« Une démarche organisée, au service du management stratégique de l'entreprise, visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement (menaces et opportunités) ; ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes. »[11] À cette définition peut être ajoutée une dimension supplémentaire. « Cette démarche implique une politique adaptée de protection des connaissances et du savoir de l'entreprise et peut nécessiter l'emploi d'actions offensives. »

3.2 La prise de conscience des entreprises

3.2.1 Une prise de conscience variable

Depuis le rapport Martre, une prise de conscience collective s'est instaurée au sein du tissu économique français. Les entreprises moins « timides », mettent en place des stratégies d'intelligence. Néanmoins des contrastes très marqués entre petites et grandes entreprises demeurent. Parmi les cinq types de veilleurs identifiés par Daniel Rouach[12] en 1996 : (guerriers,

[11] Bournois Franck, Romani Pierre-Jacquelin, L'intelligence économique et stratégique dans les entreprises françaises, IHEDN, Economica, 2000.
[12] Rouach Daniel, *La veille technologique et l'intelligence économique*, PUF, Collection « Que sais-je ? », 1996.

offensifs, actifs, réactifs, dormeurs), la majorité des grands groupes n'étaient classés que dans la catégorie des actifs, alors que la plupart des PME-PMI étaient considérées comme réactives. Les « offensifs » disposent de moyens tels que les cellules de veille. Aux États-Unis et en Asie, la plupart des grands groupes entrent dans cette catégorie, voire dans celle des « guerriers ». Ces derniers intègrent la veille technologique et concurrentielle à la stratégie de l'entreprise et disposent de moyens importants.

3.2.2 Les actions des pouvoirs publics

Depuis, des initiatives se sont mises en place notamment par l'intermédiaire des pouvoirs publics, mais également des associations privées. Des organismes indépendants tels que la Scip France (Society of Competitive Intelligence) ou l'Afdie (Association française pour le développement de l'intelligence économique) développent le concept d'intelligence économique au travers de réseaux. L'État intervient de manière directe et indirecte. Ainsi, le ministère de l'économie, des finances et de l'industrie mène des actions par l'intermédiaire du HFD (Haut fonctionnaire de défense), mais aussi de la DREE (Direction des relations économiques extérieures). Les CCI (chambres de commerce et d'industrie) jouent un rôle prépondérant en accompagnant les PME. Enfin, mais nous ne pourrions citer toutes les actions entreprises, l'IHEDN (Institut des hautes études de la défense nationale) et l'IHESI (Institut des hautes études de la sécurité intérieure), respectivement rattachés au ministère de la défense et au ministère de l'intérieur, organisent pour les chefs d'entreprise et leurs cadres, des cycles de formation à l'intelligence économique et stratégique, ainsi que des études sur tous les thèmes s'y rapportant[13].

Une réelle impulsion est donnée pour sensibiliser les acteurs du monde économique. Ces initiatives ont-elles porté leurs fruits ? Qu'en est-il actuellement de l'acceptation du concept par les entreprises ? Quelles sont encore les réticences ?

[13] www.scipfrance.org ; www.afdie.fr ; www.dree.org ; www.ihesi.interieur.gouv.fr.

3.2.3 Résultats de deux enquêtes

En partant de deux enquêtes, l'une réalisée par le cabinet Deloitte & Touche[14](A), en 1998, à partir d'un questionnaire envoyé à 2 250 entreprises implantées en France, et celle de l'IHEDN[15](B), en 1999, à partir d'une base de données constituée de 1 200 entreprises françaises, nous pouvons faire les constatations suivantes :

Prise de conscience effectuée (B)

70 % des entreprises se déclarent mobilisées autour du concept, qu'elles pratiquent (51 %) ou en ont l'intention (18 %). Néanmoins, cette prise de conscience est liée d'une part à la taille de l'entreprise et d'autre part à la concurrence à laquelle elle doit faire face, nationale ou internationale.

Les grands groupes (B)

Les entreprises qui pratiquent l'IES sont majoritairement de grande taille, fortement exportatrices et en proie à une concurrence très concentrée. 82 % des entreprises ayant intégré cette pratique font plutôt des bénéfices.

Les victimes d'attaques (B)

Les entreprises reconnaissent que les attaques subies par l'entreprise sont une raison supplémentaire pour mettre en place une structure adaptée d'IES.

L'amélioration de la gestion de l'information (A)

La recherche d'une meilleure gestion de l'information (collecte, stockage et diffusion) est mise en tête des objectifs visés par les dirigeants pour améliorer leur dispositif d'IES.

Les pratiques offensives de l'intelligence économique (B)

Pour les dirigeants, l'IES est plus large et plus offensive que la veille, elle sous-entend notamment les actions de *lobbying* et d'influence.

L'intelligence économique demeure une pratique confidentielle (B)

7 % des dirigeants interrogés estiment que leurs salariés sont biens sensibilisés aux enjeux de l'intelligence économique.

---

[14] Deloitte&Touche Consulting Group et CEPS (Centre d'étude et de prospective stratégique), « Pratiques et attentes des entreprises en matière d'intelligence économique », enquête réalisée d'avril à juin 1998.

[15] Bournois Franck, Romani Pierre-Jacquelin, L'intelligence économique et stratégique dans les entreprises françaises, IHEDN, Economica, 2000.

Au vu des résultats de ces deux enquêtes, plusieurs constats ressortent et montrent que des efforts sont encore à réaliser :

- l'intelligence économique est une démarche collective, elle ne peut fonctionner sans l'implication de chacun au sein de l'entreprise ;
- l'optimisation du dispositif d'intelligence économique et stratégique passe obligatoirement par l'amélioration du processus de gestion de l'information ;
- les attaques existent, des actions préventives doivent être entreprises afin de se protéger ;
- l'IES intègre les actions offensives (influence, désinformation, *lobbying*…). Il est nécessaire de s'en prémunir mais également d'en comprendre les schémas pour éventuellement s'en servir.

Les pays anglo-saxons ou asiatiques ont depuis longtemps compris l'importance de l'intelligence économique et stratégique. Les entreprises françaises semblent réaliser quel peut être leur intérêt à maîtriser ce concept et à l'utiliser. Néanmoins, dans nombre d'organisations, cette activité reste limitée à quelques personnes et par conséquent vouée à l'échec en raison de son impact restrictif. Pour qu'elle soit efficace, elle doit mobiliser l'ensemble des salariés dans leur vie quotidienne. Elle n'est pas ponctuelle, elle est continue. Elle s'appuie sur une circulation accrue des informations, une ouverture de chacun à la communication et à la connaissance de son entreprise ainsi qu'une prise de conscience des menaces en présence. Mode de management à part entière, elle se base sur une gestion optimale de l'information.

3.3 L'information, matière première de l'intelligence économique

3.3.1 L'information, le carburant de l'entreprise

« Si tu ne connais pas les montagnes et les vallées, les cols et les ravins, les marais et les tourbières, tu ne pourras pas conduire de force armée. »
Sun Tsu (L'art de la guerre)

Le renseignement a toujours été, pour les stratèges militaires, le facteur clé de succès essentiel pour bâtir leur stratégie. Les entreprises ont acquis une dimension internationale dans un environnement particulièrement instable et soumis à une concurrence croissante. Dans ce contexte de compétition économique, l'information, plus qu'autrefois, est devenue une composante essentielle de la réussite des organisations. Car seules les entreprises qui sauront prévoir l'évolution des marchés, cerner les besoins potentiels, identifier les innovations technologiques, anticiper les modifications de comportement des acteurs économiques, politiques et sociaux maintiendront

un bon niveau de compétitivité. Améliorant la connaissance et réduisant l'incertitude, l'information de qualité permet :

- de garantir la pertinence du processus décisionnel de l'entreprise ;
- d'assurer la pérennité de l'entreprise en milieu fortement concurrentiel.

Primordiale pour l'entreprise, l'information peut être de diverses formes et de sources multiples.

3.3.2 Typologie de l'information et des sources

L'information est graduée et de divers types en fonction des sources, de son contenu et de la façon dont on la récupère.

Information blanche, grise et noire

	Information blanche	**Information grise**	**Information noire**
Code couleurs	Zone blanche Ce que chacun peut voir et recueillir	Zone grise - Ce qui résulte de « l'accouchement des esprits » - Par le traitement de l'information (confidences) - Par l'habilité de l'accoucheur - Ce qui peut être immoral sans être illégal	Zone noire Ce qui est protégé par la loi ou le contrat et réservé aux personnes autorisées
Qualification	Information ouverte (90% du total) Publique	Information sensible (% croissant) de l'ouvert au fermé	Information fermée (10% du total) secrète
Qualification juridique des infractions	Pas d'infractions au recueil : - Recueil licite - Propriété intellectuelle Possibilité d'infraction à l'emploi	Domaine de l'infraction jurisprudentielle : - Litige de concurrence ? - Débauchage de cadres ? - Atteintes au secret professionnel ?	Infraction aux lois civiles et commerciales : - Atteintes aux intérêts fondamentaux de la nation - Atteinte à l'administration - Atteinte à la personnalité - Atteinte aux intérêts de l'entreprise - Infraction aux lois et réglementation
Sources	- médias - réunions publiques - BD et centres de documentation - Organismes publics INPI, ARIST, CRCI, CCI… - Greffes des tribunaux de commerce	- Documentation réservée à l'entreprise - Personnel de l'entreprise - Toute information non publique obtenue de manière non illégale	- Sources consultées légalement sous autorisations officielles ou privées - Sources illégales (interceptions techniques) - Sources humaines se mettant dans l'illégalité

Source : Général Pichot-Duclot, ESLSCA

Tableau 3 : Typologie de l'information.

Information ouverte et fermée

La définition donnée par Philippe Baumard[16] est celle reprise par une majorité de spécialiste du domaine :

- information ouverte : la source délivre une information de son plein gré ;
- information fermée : la source ne délivre pas une information de son plein gré.

Les sources formelles et informelles

- Les sources formelles : représente les sources où il existe un support papier, filmographique, informatique : presse, livres, banques de données, films, rapport de sociétés d'études.
- Les sources informelles : toutes celles qui n'appartiennent pas à la première catégorie et qui nécessitent généralement des actions de terrain (fournisseurs, sous-traitants, voyages d'étude, expositions, congrès, stagiaires, comités, sources internes à l'entreprise…). On considère que les trois quarts des informations nécessaires proviennent de sources informelles, plus particulièrement des prestataires extérieurs et des réseaux personnels.

Variée, d'origine diverse, l'information est extrêmement abondante. En déterminer la pertinence relève d'une véritable méthodologie.

3.3.3 Surabondance d'informations

À cette croissance exponentielle du volume d'informations s'ajoute les choix parfois irrationnels des entreprises quant à leurs besoins. Les organisations collectent toujours plus d'informations qu'elles n'en utilisent et en redemandent sans cesse.

Deux raisons expliquent cette surconsommation d'informations :

- l'incitation à collecter plus d'informations qu'il n'en faut, avant la prise de décision, mais également après afin de se justifier dans les choix que l'on a faits ;
- la dispersion des actions de veille, qui privilégient l'observation tous azimuts, et par conséquent collectent plus d'informations que nécessaire.

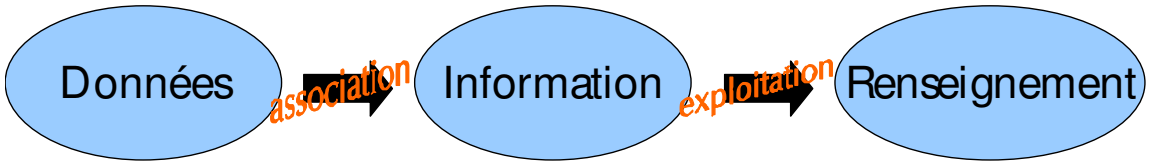
Par conséquent, pour que l'information soit une force et non pas une faiblesse (par perte de temps et de moyens), une politique de management de l'information doit être lancée. Son but : la maîtrise optimale de l'information stratégique.

[16] Baumard Philippe, Stratégie et surveillance des environnements concurrentiels, Masson, 1991.

3.3.4 Maîtriser l'information pour renseigner

3.3.4.1 De l'information au renseignement

Largement inspirée des méthodes de raisonnement militaire, l'intelligence économique et stratégique fonde sa démarche sur le renseignement. Cependant, entre le renseignement et l'information, la frontière n'est pas toujours très visible. On peut définir le renseignement comme la somme d'informations élaborées, vérifiées et synthétisées, destinées à un groupe restreint d'individus. Il répond souvent à des questions préétablies et sert une démarche opératoire[17]. Le schéma ci-dessous représente la transformation des données, brutes (papiers, images, notes) en information, puis en renseignement.



Source : Cigref

Figure 4 : Des données au renseignement.

Vu par les spécialistes, « le renseignement est une activité qui transforme des faits, représentés sous formes de données brutes, en données plus ou moins élaborées, au cours d'un processus complexe allant de leur observation à leur communication[18]. »

Pour permettre à une direction d'exprimer ses besoins en information dans un cadre sécurisé, et diffuser ainsi aux échelons subordonnés de l'information nécessaire à leur propre fonctionnement, une méthodologie s'impose. Car, entre l'acquisition des données, brutes et inexploitables, et l'utilisation des renseignements pour prendre des décisions, un certain nombre d'étapes est nécessaire. L'information de valeur qui est alors extraite est le fruit du processus moteur de la démarche d'intelligence économique et stratégique : Le cycle du renseignement.

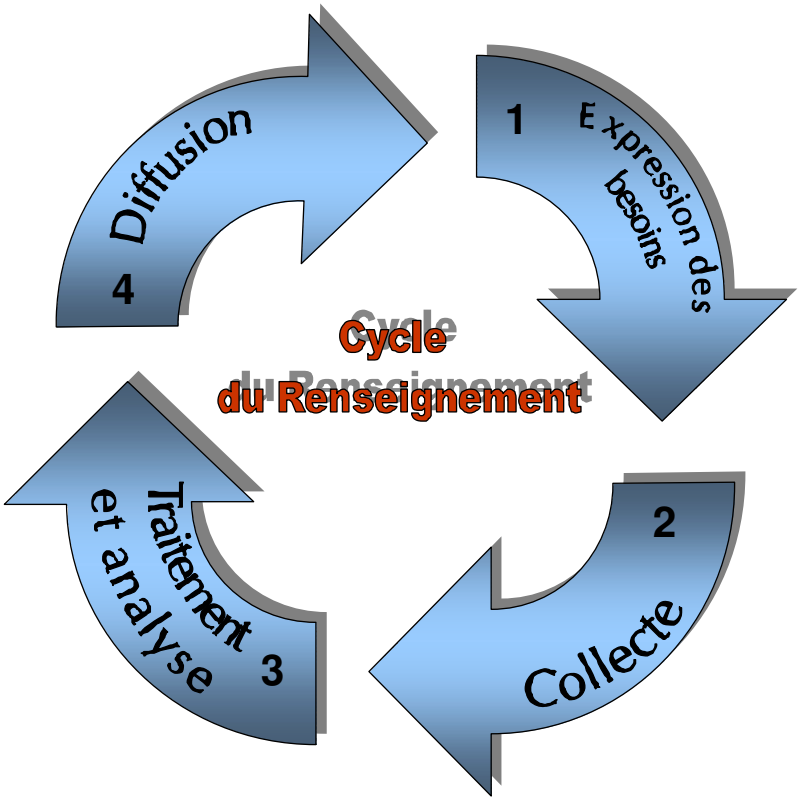
[17] Henri Brigitte, Le renseignement : un enjeu de pouvoir, Economica, 1998.
[18] Beau Francis, *Renseignement et société de l'information*, Fondation pour les études de défense, 1997.

3.3.4.2 Le cycle du renseignement

La connotation militaire du mot « renseignement » a induit une nouvelle appellation de ce cycle que beaucoup appellent aujourd'hui « cycle de l'information » ou parfois même « cycle de l'intelligence économique ».

Le cycle du renseignement est un processus itératif, qui se compose de quatre étapes :

- l'expression des besoins ;
- la collecte ;
- le traitement et l'analyse ;
- la diffusion.



Source : École de guerre économique.

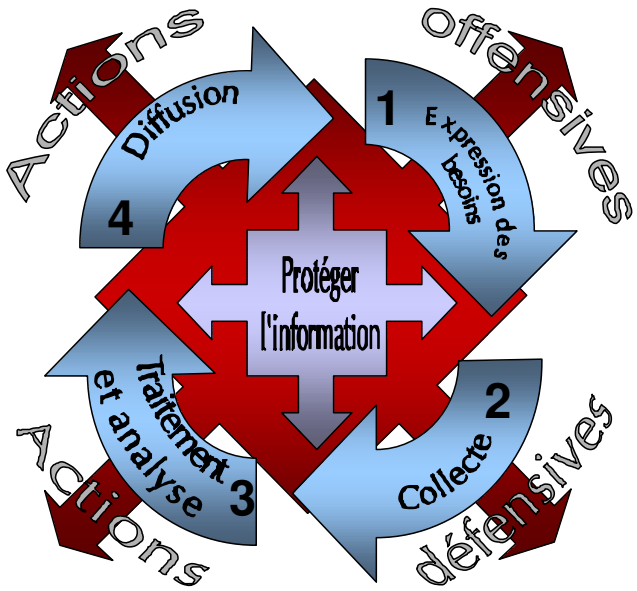
Figure 5 : Le cycle du renseignement.

4 LA DÉMARCHE D'INTELLIGENCE ÉCONOMIQUE ET STRATÉGIQUE

« Se faire battre est excusable, se faire surprendre est impardonnable. »
Napoléon

Définir une démarche d'intelligence économique et stratégique semble difficile tant le domaine paraît large et étendu. Le cycle du renseignement constitue le processus cœur de la démarche d'IES. Sa mise en place et son application vont permettre de définir les actions défensives et offensives à entreprendre. Mais la politique d'IES doit s'instaurer dans un climat de sécurité globale. Dans ce contexte, il nous a semblé utile de diviser la démarche d'IES en trois phases distinctes :

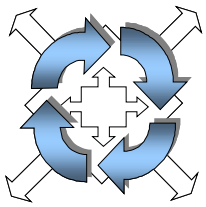
- le cycle du renseignement ;
- la protection de l'information ;
- la prise de décisions (les actions défensives et offensives).



Source : Cigref

Figure 6 : Démarche d'intelligence économique et stratégique.

4.1 Gérer l'information : Le cycle du renseignement



Afin d'appréhender la démarche du cycle du renseignement, il paraissait essentiel de demeurer le plus concret possible, en détaillant chaque étape pour comprendre comment les systèmes d'information allaient optimiser le processus. Sur ce thème, rares sont les études qui ont été menées de façon concrète et détaillée. Néanmoins, en 1996, le secrétariat d'État à l'industrie [19](Direction de l'action régionale et de la petite et moyenne industrie) a souhaité qu'une action pilote soit conduite en France, sur le thème de l'appropriation de l'intelligence économique par les PME. Une étude très précise fut réalisée par le cabinet Intelleco Consultants et l'Arist[20] de Bourgogne auprès de sept entreprises. Leurs travaux sont centrés sur l'exploitation du cycle du renseignement. C'est par conséquent en nous inspirant de leurs recherches que nous détaillerons les étapes successives du processus. Cette étude a été réalisée auprès de PME-PMI et ne peut correspondre totalement à un groupe de grande envergure. Mais au-delà des détails, il s'agit avant tout de matérialiser une méthodologie, libre à chacun ensuite de l'adapter à sa guise.

Nous agrémenterons nos explications d'exemples extraits en particulier du Cycle IES du Cigref.

En effet, à cette occasion, Marc Louichon, ex-directeur général d'une entreprise du secteur de l'aéronautique, nous expliquait comment il avait mis en place une cellule d'intelligence économique qui, au fil des années, s'était positionnée comme une composante majeure de la stratégie de l'entreprise.

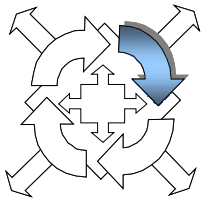
C'est au début des années 90 que nous avons pris conscience de l'importance des informations que l'on pouvait collecter, en interne, mais également en externe. Au fur et à mesure, les quelques mesures de départ ont donné naissance à un concept qui en s'affirmant est devenu une composante de poids dans la stratégie du groupe. Ne pas subir le quotidien pour les décideurs, était devenu primordial, afin d'anticiper et de prendre les orientations les plus judicieuses.

Cycle IES

[19] Intelleco Consultants et Darpmi, *Intelligence économique, outils et méthodes développés en PMI,* Les éditions de l'industrie, 2000 ; www.intelleco.fr.

[20] Les Arist, au sein des chambres régionales de commerce et d'industrie, constituent un réseau de 25 agences au service des entreprises.

4.1.1 L'expression des besoins



Objectif

L'expression des besoins consiste à déterminer quelles sont les informations utiles et prioritaires dont les décideurs auront besoin pour assurer le développement de l'entreprise.

Méthodologie

L'expression des besoins en information repose sur trois phases :

- une bonne connaissance de l'entreprise et de son environnement ;
- une analyse du positionnement stratégique et le choix des axes de développement prioritaires ;
- la décomposition des axes en questionnement opérationnel.

4.1.1.1 Bonne connaissance de l'entreprise

Dans une entreprise, il est assez simple de définir ce que l'on souhaite savoir. En revanche, il devient plus difficile de déterminer ce l'on doit savoir. Deux questions sont donc essentielles dans le processus d'analyse des besoins :

- que veut-on savoir ?
- que doit-on savoir ?

Quels sont ces domaines où l'on doit avoir un maximum de renseignements ? Pour répondre précisément à ces questions, la première étape nécessite de connaître parfaitement l'entreprise et son environnement :

- activités, résultats financiers, filiales, partenaires ;
- métiers de l'entreprise et sa stratégie ;
- produits ou services ;
- marchés (clients, analyse globale des marchés) ;
- concurrence (directe et indirecte) ;
- recherche et développement, innovation ;
- production (savoir-faire, sous-traitance, qualité…) ;
- fournisseurs clés ;
- hommes et organisation (fonctions, formations, qualifications et compétences…) ;
- implantation de l'entreprise.

4.1.1.2 Analyse du positionnement stratégique et choix des axes de développement prioritaires

Étape généralement complexe, l'analyse du positionnement stratégique est bien entendu spécifique à chaque entreprise concernant les méthodes utilisées. Qu'il s'agisse d'une matrice SWOT (forces, faiblesses, opportunités, menaces) ou d'une grille d'analyse stratégique plus complexe, l'utilité de ce type d'outils est avérée pour déterminer les axes de développement stratégiques de l'entreprise desquels découleront des axes prioritaires. Pour permettre un choix pertinent et judicieux, une évaluation doit être réalisée en attribuant des notes aux différents axes de développement en fonction de facteurs internes et externes :

- *facteurs internes* : capacité financière, culture d'entreprise, compétences et savoir-faire des salariés, outils et capacité de production, attentes des dirigeants et des actionnaires ;
- *facteurs externes* : réceptivité à court terme, réceptivité à long terme, positionnement concurrentiel, environnement réglementaire.

Cette analyse va permettre de déterminer :

- le degré d'urgence des axes ;
- leur degré de confidentialité (l'axe pourra-t-il faire l'objet d'une large information ?) ;
- en fonction de ce constat, précautions à prendre dans les phases de collecte et de traitement ;
- les compétences à mobiliser (internes et externes).

4.1.1.3 Décomposition des axes en questionnement opérationnel

La détermination des axes prioritaires va ainsi permettre d'orienter les premiers travaux de recherche en recensant toutes les questions opérationnelles auxquelles il s'agira d'apporter des réponses.

Au sein de l'entreprise, nous nous posions par exemple les questions suivantes :

Les produits et services

- *Propriété industrielle : certaines entreprises se lancent sur un nouveau produit sans se préoccuper de savoir si un concurrent n'est pas déjà sur ce marché. La situation est d'autant plus délicate si le concurrent est étranger.*
- *Réglementation, risque de substitution fonctionnelle.*

Les clients et les fournisseurs

- *Quelle est leur santé économique, sociale et financière ? Quel rôle joue-t-on pour eux ?*
- *Subissent-ils eux-mêmes des contraintes de leurs clients ou fournisseurs ? Peuvent-ils passer sous le contrôle de concurrents ?*
- *Qui est le décideur ? (Question essentielle car il est toujours difficile de déterminer qui prend les décisions.)*

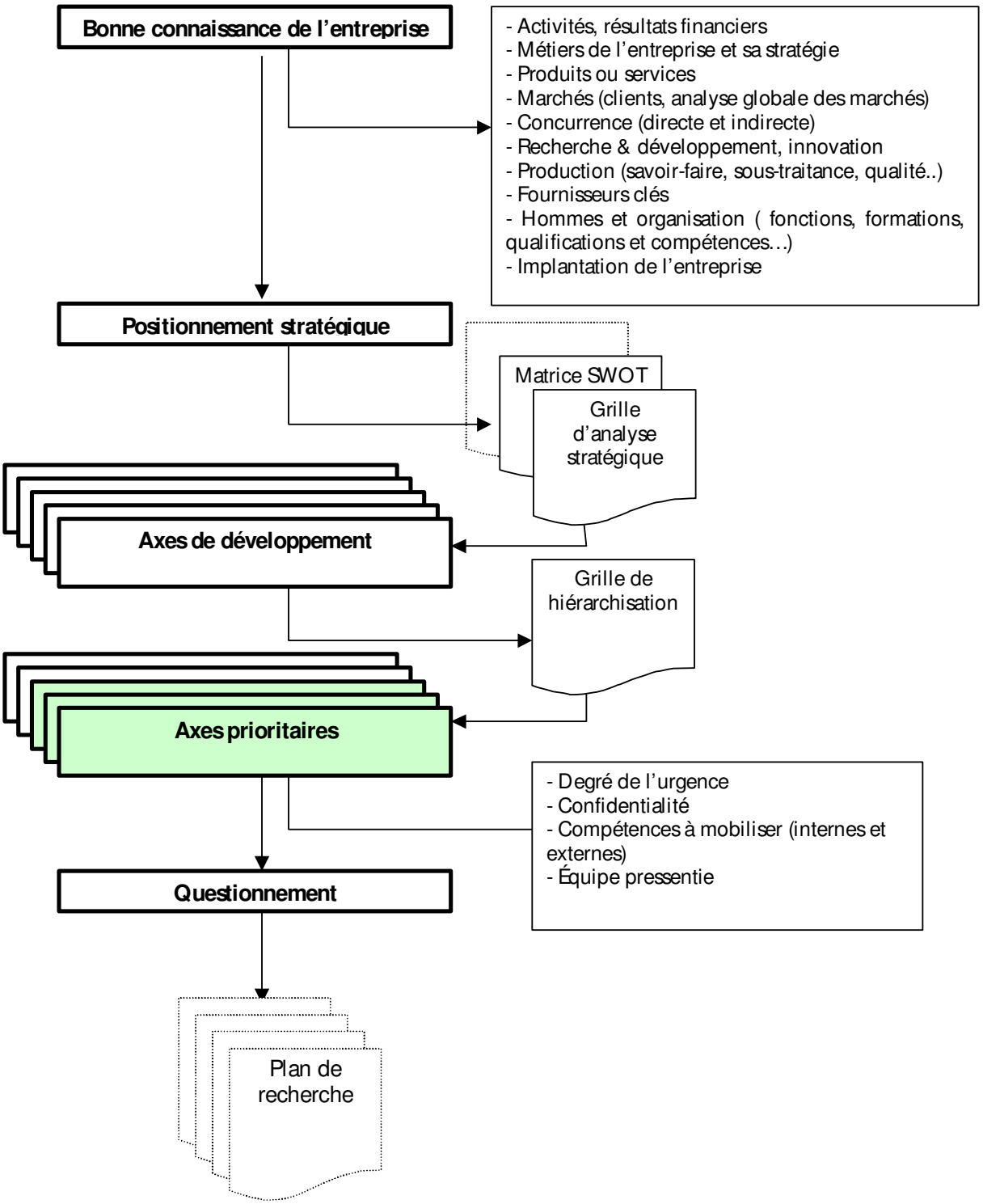
Les concurrents

- *Quels sont les concurrents directs, potentiels ?*
- *Les actions commerciales qu'ils lancent cachent-elles une réalité ?*
- *Quelles sont leurs situations économique, financière et sociale ?*
- *Quelles sont leurs intentions stratégiques supposées ?*
- *Quels sont leurs objectifs de résultats ?*

Les autres, filiales, partenaires…

Il ne faut en aucun cas négliger les entreprises du même groupe avec qui le partage d'informations ne se fait pas toujours dans les meilleures conditions. De même, les sociétés partenaires et amies, qui peuvent donner des réponses aux interrogations.

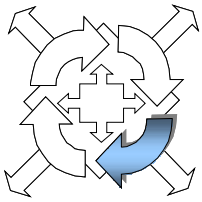
Cycle IES



Source : Intelleco

Figure 7 : Fiche de synthèse du processus « Expression des besoins ».

4.1.2 La collecte de l'information



Objectif

En fonction des axes d'orientation définis dans la phase précédente, il va s'agir de rechercher les informations les plus pertinentes, à l'intérieur et à l'extérieur de l'entreprise.

Méthodologie

Aujourd'hui, les sources d'informations dans l'entreprise sont devenues innombrables : journaux, revues, rapports, connaissances et compétences du personnel, savoir-faire internes, expériences passées… internet a bien entendu surmultiplié les possibilités d'accéder à l'information. Ce que l'on appelle la mémoire d'une organisation, c'est-à-dire l'ensemble de son savoir et de ses connaissances, représente une formidable source. On estime, effectivement, que la moitié des informations collectées à l'extérieur se trouvent déjà au sein de l'entreprise. Les deux premières phases du cycle du renseignement doivent permettre de canaliser l'information disponible en interne mais inaccessible faute d'organisation. Cette étape met en évidence la nécessité de définir précisément les axes de recherche pour éviter l'accumulation excessive des données récoltées.

Les évènements du 11 septembre ont montré que collecter des masses importantes de données ne suffisait pas. Il fallait extraire les informations pertinentes au bon moment et de façon méthodique. En effet, il n'aura fallu que 48 heures aux agents de la NSA pour obtenir de précieux renseignements sur le réseau Ben Laden dans l'amas d'informations du système Échelon[21].

Cycle IES

L'expression des besoins en informations va poser les bases du cycle. On mesure combien cette étape est primordiale pour la suite des opérations. La phase de collecte doit également procéder de façon méthodologique pour optimiser la rapidité des recherches, ainsi que la précision. Elle va permettre de minimiser l'accumulation de « bruits », c'est-à-dire les informations inutiles camouflant les informations pertinentes.

[21] www.echelon-online.fr.st.

La phase de collecte va nécessiter plusieurs étapes :

- réaliser un plan de recherche et définir des groupes d'experts ;
- identifier les sources pertinentes et des actions de terrain ;
- déterminer les capteurs.

4.1.2.1 Réaliser un plan de recherche et définir des groupes d'experts

Véritable cahier des charges et calendrier des actions à accomplir, le plan de recherche doit devenir le réceptacle du questionnement opérationnel de l'entreprise. Fixant le cadre de travail et les lignes d'action, il est mis à jour régulièrement et mesure l'état d'avancement du projet. Pour chaque axe de développement, il détermine :

- les besoins en informations et les sources ;
- les moyens de collecte et les capteurs ;
- le traitement ;
- l'urgence du besoin.

En règle générale, ces plans de recherche, que d'autres nomment aussi plans de renseignement, sont dévolus à un groupe d'experts chargés d'un sujet bien précis ou par exemple d'un projet. Chacun de ces groupes aura la responsabilité de son plan de recherche, ce qui peut faire plusieurs dizaines de plans pour un grand groupe. Ces cellules sont par conséquent responsables de la récolte des informations formelles et informelles aussi bien à l'intérieur qu'à l'extérieur de l'entreprise.

4.1.2.2 Identifier les sources pertinentes et les actions de terrain

Le plan de recherche va permettre d'évaluer quelles sont les sources les plus pertinentes pour l'entreprise. Comme nous l'avions expliqué dans le chapitre précédent, nous distinguerons deux types de sources :

- les sources formelles ;
- les sources informelles.

Une majeure partie des réponses aux questions recensées dans l'expression des besoins sera rassemblée grâce aux sources formelles. Car 90 % des informations recherchées se trouvent déjà au sein de l'entreprise. Néanmoins, chercher certaines informations peut nécessiter un coût important, du temps et une mobilisation excessive de personnels. Le recours aux prestataires de service devient un moyen de plus en plus efficace de minimiser le temps passé sur certaines actions de collecte, à un moindre coût.

Les sources de collecte sont nombreuses (voir le tableau 4). Seules les méthodes dites « classiques » y sont recensées, indépendamment des possibilités offertes par les technologies de l'information et de la communication. Car celles-ci ont radicalement transformé les perspectives et les modes de collecte. L'étendue des possibilités offertes par les systèmes d'information, plus particulièrement internet, fera l'objet du prochain chapitre.

Dans l'entreprise de M. Louichon, la phase de collecte était simple mais très efficace :

L'entreprise avait désigné une personne responsable de la veille interne, en relation directe avec le DG. Sa mission principale consistait en une quête régulière de toute l'information latente détenue par le personnel de la société. Concrètement, cette personne passait régulièrement dans les bureaux des cadres pour récolter une à deux informations par salarié. Le contact physique est essentiel, il permet de discuter, de faire émerger les idées et de rebondir sur d'autres sujets. Le croisement des différentes informations amenant de nouvelles questions et ainsi de suite.

Cycle IES

En parallèle, certaines réponses nécessitent la mise en place d'actions extérieures, dites « de terrain », afin de récolter des informations non disponibles dans l'entreprise. Les manifestations de type salons, colloques, conférences, etc. seront l'occasion d'accéder à des sources plus informelles mais aussi de cultiver les réseaux relationnels, qui demeurent une des bases de l'IES. Véritables électrons informationnels, certains personnels de l'entreprise constituent des observateurs privilégiés : cadres en mission ou visite, ingénieurs d'affaire, commerciaux…

Les visites d'entreprises apportent de précieuses informations, par exemple les panneaux syndicaux, les annonces des comités d'entreprises ou encore les notes de direction.

Cycle IES

Mais il ne faut pas se méprendre, de telles démarches sont de véritables missions à elles seules, qu'il convient de préparer soigneusement, d'analyser puis de « débriefer ». Dans cette optique, des fiches de « captation » sont utilisées pour transmettre les informations aux groupes d'experts. L'exemple de fiche ci-après est tiré d'un ouvrage de François Jakobiak[22].

[22] Jakobiak François, *L'intelligence économique en pratique*, Éditions d'Organisation, 2001.

SOURCES SPECIFIQUES D'INFORMATION – EXEMPLE DE FORMULAIRE POUR LES INFORMATEURS

Thème : **Information :**				
Estimation du degré de validité				
Expéditeur	1	2	3	4
Destinataire	1	2	3	4
Code expéditeur : Destinataire : Source : Date :				

Une ou deux phrases indiquent le renseignement capté

1. certain
2. probable
3. douteux
4. ?

Notes :

- Le nom de l'expéditeur n'est jamais porté sur le formulaire, son code s'il existe peut l'être.
- Le nom du destinataire est indiqué, soit en clair, soit en code.
- L'indication de la source est facultative, elle n'est généralement pas indiquée
- La date est un élément important
- Les formulaires sont transmis par courrier ou messagerie électronique

Source : F. Jakobiak

Figure 8 : Fiche de captation.

	Sources	Avantages	Inconvénients
FORMELLES	**Presse**	- Publique - Bon marché - Information exhaustive - Sources innombrables	- Difficultés de sélection pertinente - Info publiée obsolète - Information enjolivée
	Livres	- Synthèse d'un maximum d'informations	- Nombreux titres - Information obsolète
	Autres médias	Peu intéressant	
	Banques de données	- Exhaustivité et accès de facile - Faible coût	- Information rarement nouvelle - Méthodologie de recherche difficile - Peu de documents originaux
	Brevets	- 80% des informations techniques se trouvent dans les brevets	- Dépôt de brevets intervient tard (18 mois) - Compréhension difficile - Langues étrangères - Certains secteurs non couverts
	Sources d'informations légales	- Facile d'accès	- Informations de caractère limité
	Études prestataires	- Information de qualité traitée	- Coût important
	Sources	**Avantages**	**Inconvénients**
INFORMELLES	**Concurrents**	- Par leur communication commerciale et financière - Journée portes ouvertes - En devenant son fournisseur , client - Par leur presse interne	- Difficulté d'accès
	Fournisseurs et sous-traitants	- Sources d'information intéressante	- Fournisseurs des concurrents
	Missions et voyages d'étude	- Sources extrêmement riche	- Onéreuses
	Expositions, salons	- Source importante	- Demande une préparation
	Colloques, congrès	- Pour développer son réseau	
	Étudiants, stagiaires	- Source très intéressante	- Problèmes déontologiques
	Candidats à l'embauche	- Renseignement de premier choix	- Problèmes déontologiques
	Comités divers	- Syndicats, comités de normalisation	
	Sources internes	- 80% des informations s'y trouvent	- Trouver les bonnes informations

Source : Cigref

Tableau 4 : Panorama des sources formelles et informelles.

4.1.2.3 Déterminer les capteurs

La recherche d'information fait partie du rôle de chacun au sein de l'entreprise, elle induit une sensibilisation collective sur ce réflexe à avoir. Néanmoins, certaines personnes plus que d'autres doivent jouer le rôle de « capteurs ». Désignées dans le plan de recherche, ces capteurs d'informations ont deux particularités :

- ils collectent des informations sur l'environnement stratégique de l'entreprise au cours de leurs activités (internet, presse, réseau humain, rencontres informelles, salons, conférences…) ;
- ils participent à l'animation d'une communauté de veille stratégique (réseaux d'échanges d'informations).

En règle générale, ces capteurs sont des experts dans leur domaine de compétences : DG, systèmes d'information, marketing, communication, achats, chefs de projets, ressources humaines, etc. et également les professionnels internes de l'information : documentalistes, chargés de veille, analystes…

4.1.2.4 Les notes d'étonnement

La note d'étonnement est un formulaire préformaté utilisé pour rendre compte d'une information intéressante. La rédaction de ce type de document, généralement réservée à une minorité (responsable de la veille, visiteur de salons professionnels…), doit être encouragée auprès de tous les salariés ayant une réelle valeur ajoutée. Nombreuses sont les personnes qui possèdent, parce qu'elles les ont vues, lues ou entendues, des informations intéressantes, mais qui ne les diffusent jamais. La crainte du ridicule, la méconnaissance de l'intérêt que celles-ci peuvent représenter, ou alors un manque de culture de partage collectif (chez les commerciaux par exemple) peut priver l'entreprise d'informations pertinentes. Une sensibilisation est par conséquent nécessaire. Ces notes d'étonnement doivent permettre à chacun, rapidement, de manière synthétique, de livrer des informations qui seront peut-être essentielles à l'entreprise.

NOTE D'ETONNEMENT			
Emetteur : Notation : Date :		Destinataires et notations* :	
Information ayant retenu votre attention : Source :			
Commentaires de l'émetteur (questionnement, impact pour l'entreprise, analyse) :			
Impact possible sur un projet ou une action menée par l'entreprise :			
Commentaires du récepteur :		Date de retour vers l'émetteur :	
***Grille de notation**			
Intérêt pour l'entreprise	Fort	Moyen	Moindre
Info nouvelle pour le destinataire	B1	B2	B3
Info déjà connue du destinataire	A1	A2	A3

Source : Intelleco

Figure 9 : Fiche exemple d'une note d'étonnement[23].

Des groupes comme L'Oréal ou Aérospatiale demandent aux chercheurs en déplacement de remplir des rapports d'étonnement relatant tout ce qui les a surpris. Ainsi chez Aérospatiale, les projets technologiques concurrents sont l'objet d'un *reverse engineering*: les chercheurs reconstituent pièce par pièce les plans concurrents pour en estimer le risque[24].

[23] Intelleco Consultants et Darpmi, *Intelligence économique, outils et méthodes développés en PMI*, Les éditions de l'industrie, 2000.
[24] Pateyron Emmanuel, *La veille stratégique*, Economica, 1998.

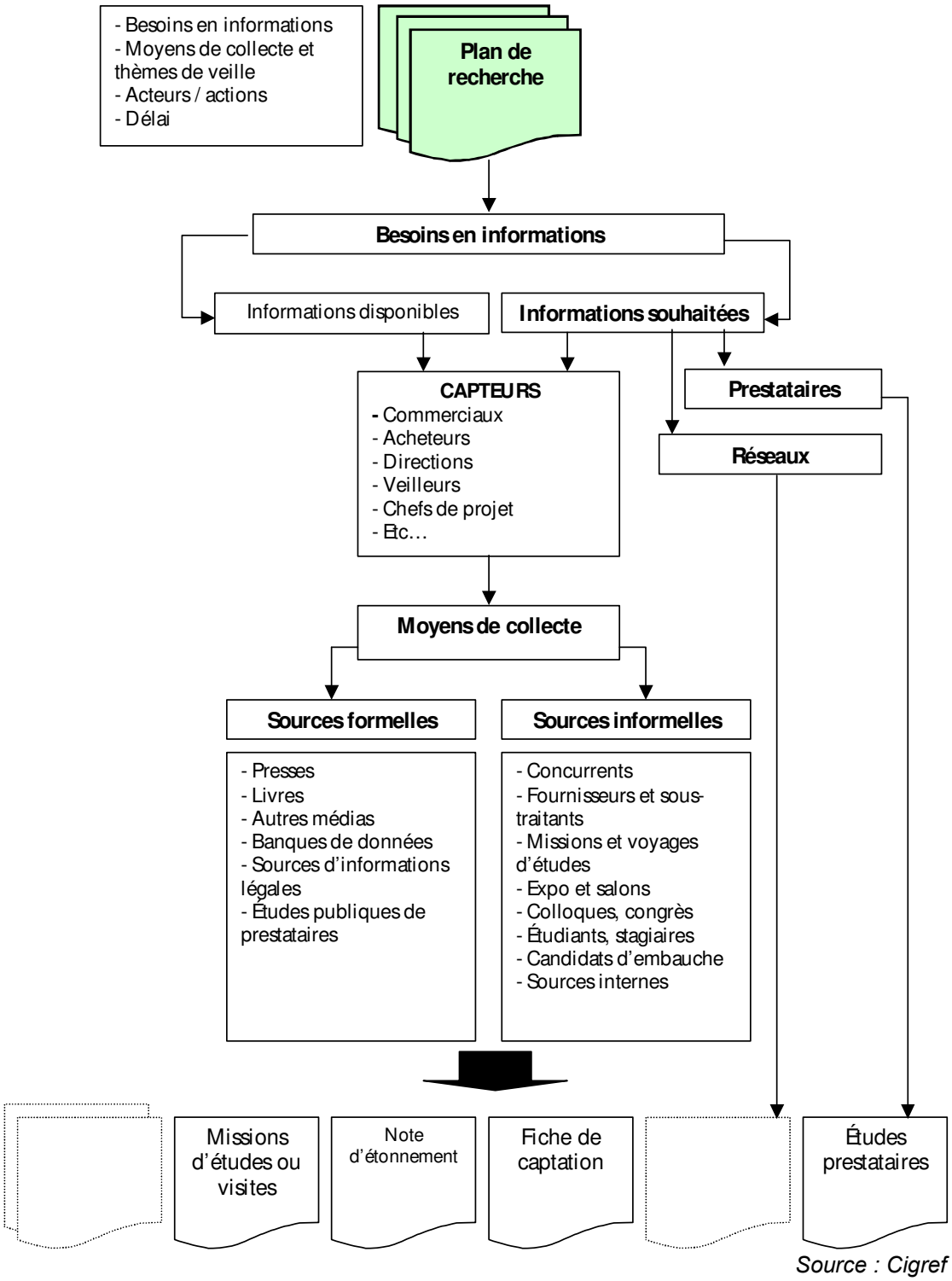


Figure 10 : Fiche de synthèse du processus « Collecte ».

Dans l'entreprise que dirigeait M. Louichon, la sensibilisation du personnel était permanente et clairement définie. Personne ne pouvait ignorer l'importance de cette quête collective de l'information pertinente.

La collecte de l'information s'appuyait sur une veille individuelle permanente de chacun. Tous les cadres y étaient sensibilisés et cette mission particulière était inscrite « noir sur blanc » sur chaque fiche de définition de fonction. On pouvait y lire le paragraphe suivant :

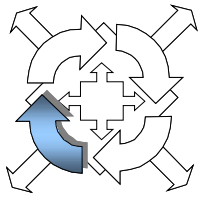
« Veille Technologique :

Recueillir en permanence toutes les informations d'ordre technique, scientifique ou économique et communiquer celles qui stratégiquement peuvent avoir un impact sur les activités de la société. »

Par conséquent, aucun cadre ne pouvait ignorer cet aspect particulier de son travail au sein de l'entreprise. L'implication du personnel dans cette mission faisant l'objet d'une évaluation au cours de l'entretien annuel.

Cycle IES

4.1.3 Le traitement et l'analyse de l'information



Objectif

Donner du sens aux informations collectées en les traitant et en jugeant de leur pertinence.

Méthodologie

L'information utile arrive rarement sous la forme souhaitée qui permettrait aux décideurs de s'en servir immédiatement. Parcellaire, elle n'a que peu de sens si elle n'est pas remise dans son contexte. En outre, l'information pertinente est noyée parmi une somme d'informations sans importance (le « bruit »). Le traitement, va donner à l'information sa valeur ajoutée. L'analyse qui s'ensuit va nécessiter une étude en profondeur des documents, pour en tirer l'essentiel et déterminer les décisions qu'il s'agira de prendre.

Ces phases de traitement et d'analyse, vont nécessiter plusieurs actions spécifiques :

- grilles de traitement ;
- mobilisation des compétences internes ;
- gestion des expertises externes.

4.1.3.1 Grilles de traitement

L'information, avant d'être analysée, doit être traitée, autrement dit triée et classée afin de pouvoir être utilisée. Cette première phase incombe généralement aux spécialistes de l'information documentaire ou de la cellule d'intelligence économique ou de veille stratégique. Ces spécialistes vont identifier les documents et les zones de texte susceptibles de correspondre aux besoins exprimés par les experts. Les axes de développement définis durant l'expression des besoins vont permettre au responsable de l'intelligence économique de faire ressortir les problématiques de choix.

La phase de traitement a souvent pour objectif de trouver des réponses aux questions posées par les opérationnels mais aussi de mettre en exergue le choix fait par d'autres entreprises ou organismes (concurrents, fournisseurs, organismes de recherche, etc.). La phase de traitement permet également de réaliser une notation des sources d'information, en mettant en exergue les sources qui ont été les plus fertiles. La mise en place de grilles de traitement a plusieurs avantages :

- faire apparaître les informations disponibles et les manquantes (meilleure lisibilité) ;
- croisement des informations détenues en interne avec celles collectées en externe ;
- mise en évidence des problématiques de choix sur lesquelles l'entreprise va devoir se positionner ;
- possibilité de formuler de nouvelles questions et lancer de nouvelles recherches d'information.

4.1.3.2 Mobilisation des compétences internes

Une fois les documents triés, les groupes d'experts vont se charger de l'analyse en se basant sur les compétences internes et les réseaux d'experts. L'intelligence économique et stratégique est une démarche collective, un temps précieux peut parfois être perdu à chercher la bonne personne ayant la compétence requise. La valorisation et la capitalisation des compétences internes de l'entreprise est par conséquent essentielle et constitue une dimension transversale de la démarche d'IES. C'est à ce titre qu'interviennent la constitution et l'enrichissement de la mémoire de l'entreprise et la gestion des connaissances (*Knowledge Management*), dont les projets fleurissent de plus en plus. Les axes de développement vont donner les orientations sur les connaissances à capitaliser. Au-delà des compétences classiques qu'il est bon de recenser, certaines actions nécessitent d'être réalisées :

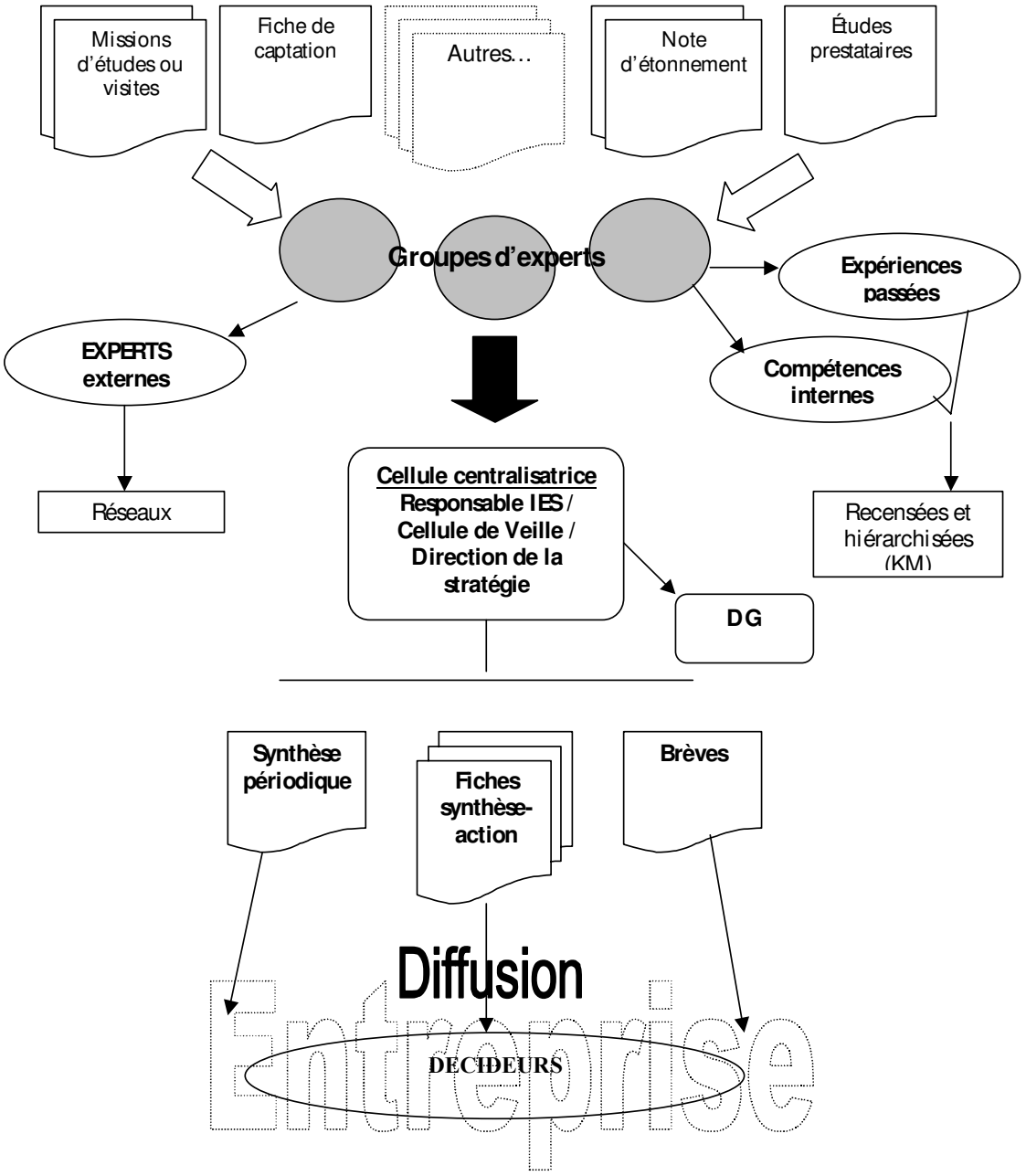
- « débriefer » les cadres partants en retraite ;
- constituer des dossiers d'analyse sur les projets, échecs ou succès de l'entreprise ;

- faire un état des compétences spécifiques de l'entreprise.

Toutes ces informations constituent le savoir de l'entreprise et participent à enrichir la mémoire de l'organisation.

4.1.3.3 Gestion des expertises externes

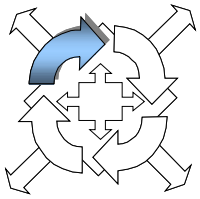
Certaines réponses ne peuvent être obtenues qu'en utilisant des réseaux relationnels. Une entreprise doit parfaitement structurer ce type de relations avec l'extérieur. Ces « partenaires », représentent un enjeu pour la collecte et le traitement de l'information, et peuvent détenir des informations ou des connaissances intéressantes. La notion de temps étant toujours réduite, il s'agit d'identifier et de choisir les interlocuteurs les plus pertinents. Pour ce faire, chaque partenaire doit être désigné par une fiche, qui pourra être réactualisée par une personne de l'entreprise ayant de nouvelles informations.



Source : Cigref

Figure 11 : Fiche de synthèse du processus « Traitement et analyse ».

4.1.4 La diffusion de l'information



4.1.4.1 Faire circuler l'information

« L'information ne devient utile et stratégique que lorsqu'elle parvient aux bons destinataires, au bon moment et sous une forme pertinente. »
Amiral Pierre Lacoste[25]

Pour qu'une information soit vraiment pertinente, il ne suffit pas qu'elle réponde à un besoin particulier, il faut aussi qu'elle puisse être diffusée au bon moment à la bonne personne. Il faut donc trouver des solutions pour que l'information puisse circuler efficacement au sein de l'organisation. Or cette phase très importante est souvent négligée. En effet, de nombreuses cellules de veille passent la plupart de leur temps et de leurs moyens sur les phases de collecte et de traitement, négligeant ainsi la diffusion. Mépriser cette étape cruciale revient à créer une rupture dans le cycle du renseignement. Cette dernière phase du cycle, va donc nécessiter la mise en place de moyens de communication complémentaires ainsi qu'une modification des cultures.

L'exemple japonais

Le système d'intelligence économique japonais est l'un des plus performants. Sa force réside principalement dans la capacité de chacun d'une part, à prendre conscience de la valeur de l'information et, d'autre part, à partager et faire circuler les renseignements en sa possession. La culture japonaise, induite par les menaces répétées de l'environnement physique, politique et économique, est à l'origine de cette forte implication des salariés. Ce comportement s'applique à toute la chaîne du cycle du renseignement. Comme l'explique Jean-François Sabouret directeur de recherche au CNRS dans l'ouvrage de B. Martinet et Y.-M. Marti[26] :

- l'information est échangée, chacun met en commun son savoir et ses ignorances ;

[25] Ancien patron des services secrets français (DGSE) de 1982 à 1985.
[26] Martinet Bruno et Marti Yves-Michel, L'intelligence économique, comment donner de la valeur concurrentielle à l'entreprise, Éditions d'Organisation, 2001.

- partager l'information crée une émulation entre les salariés, une information échangée entraînant d'autres interrogations ;
- les salariés s'expriment librement sans que leur emploi ne soit menacé ;
- l'information circule parfaitement, on la transmet aux autres afin d'éviter que l'absence de quelqu'un n'entraîne un arrêt du travail. Chacun est informé des métiers qui l'entourent ;
- curiosité de chacun vis-à-vis des informations extérieures (lecture de la presse, visites extérieures…).

4.1.4.2 L'information circule mal

Beaucoup d'entreprises ont saisi les répercutions que pouvait avoir ce partage collectif de l'information et une politique de communication adaptée. Car au-delà du pouvoir décisionnel que donne l'information, c'est aussi pour l'entreprise un facteur de cohésion indéniable qu'il faut cultiver et développer. Néanmoins, de nombreuses réticences demeurent encore, dues à diverses origines :

- l'information, encore synonyme de pouvoir ;
- la valeur de l'information est sous-évaluée, voire ignorée ;
- mauvaise organisation, structure inadaptée ;
- crainte de parler par peur du ridicule ou des réprimandes ;
- une culture scolaire inadaptée qui pousse encore à l'individualisme.

La transmission de l'information est totalement tributaire du comportement des salariés. Les meilleurs outils sont inefficaces face à la réticence que l'on peut avoir à livrer ce que l'on sait. Les américains l'ont bien compris et ont fait du slogan « *Think global, Act local* », un mode de management. Et toutes les mesures sont prises pour que les acteurs de l'entreprise aient une vision globale de l'organisation dans laquelle ils évoluent. Mobilité dans les postes occupés, responsabilités variées, politique de communication sur les métiers et les objectifs de l'entreprise, réunions interservices…On encourage les salariés de tous niveaux à avoir une vision plus stratégique pour comprendre la valeur de l'information dont ils disposent et inciter l'échange.

Nos commerciaux ont encore du mal à échanger les informations en leur possession et à voir l'intérêt que cela représente pour l'entreprise. La prise en compte de l'outil que nous mettons en place passe par un changement de mentalité.

Entretien avec un DSI

4.1.4.3 Comment améliorer la circulation ?

L'approche japonaise appréhende cette étape du cycle du renseignement de manière globale, et pas seulement comme le résultat d'outils adaptés. Améliorer la circulation de l'information est complexe car cela nécessite d'analyser non seulement l'organisation mais aussi la culture et les moyens techniques utilisés.

Sélectivité des destinataires

Une sélection doit se faire pour diffuser les informations aux personnes pour qui elles auront une réelle valeur ajoutée.

Chaque membre du comité de Direction choisissait les personnes qu'il souhaitait voir destinataires, en fonction de leurs compétences, responsabilités et intérêts.

Cycle IES

L'oral, vecteur de communication

Dans beaucoup d'entreprises, à présent, on mesure l'importance des lieux informels d'échange et de discussion. Le groupe L'Oréal, par exemple, a mis en place dans tous ses centres des « salle de confrontation », lieux où chacun peut donner son avis, faire part de son désaccord[27]. Les spécialistes de l'intelligence économique savent que les meilleurs endroits pour récupérer des informations intéressantes ou prendre le pouls d'une entreprise demeurent les lieux d'échanges informels, machine à café, cafétéria, salle de sport…

L'exemplarité

« Suivez-moi ! » plutôt que « En avant ! ». Cette comparaison entre ces deux ordres est souvent faite en école militaire pour montrer l'implication et l'exemplarité dont doivent faire preuve les officiers dans le commandement de leurs hommes. Susciter l'adhésion par l'exemplarité. Tel pourrait être le maître mot pour inciter chaque salarié à communiquer les informations qu'il a en sa possession. Valable dans les deux sens, ce comportement sera plus facilement adopté si les dirigeants montrent l'exemple en donnant plus d'informations à leurs subordonnés.

Susciter la culture des réseaux

Les réseaux demeurent le moyen le plus efficace pour obtenir des informations ou en diffuser. Une entreprise, si elle souhaite mettre en place une politique d'IES, doit impérativement s'attacher à déterminer ses réseaux existants mais également être en mesure d'en développer de nouveaux. Cette notion doit

---

[27] *op. cit.*

être inculquée à chacun en fonction de sa spécialité, de son parcours professionnel (anciennes entreprises), de ses origines (écoles, universités..) ou de son appartenance à un groupe particulier (syndicats, associations, etc.). Les réseaux se cultivent et se développent avec le temps. Néanmoins, en fonction des besoins, il est possible d'en créer pour un laps de temps déterminé (pour un projet par exemple).

Les récompenses

Le système de récompense s'avère extrêmement efficace. Les informations pertinentes diffusées par les salariés étaient portées à la connaissance du directeur général, de plus le rapport de synthèse diffusé tous les deux mois au sein de l'entreprise mentionnait le nom des informateurs, ce qui se révélait être valorisant et gratifiant pour l'employé.

Cycle IES

L'importance du feed-back

Le caractère itératif du cycle du renseignement rend le processus modulable et ajustable en fonction du retour suscité par la diffusion des informations. Cette phase, appelée « *feed-back* » revêt une importance capitale car elle permet d'améliorer la phase de diffusion en détectant les dysfonctionnements et confirmant le choix des destinataires.

D'une manière générale, ce retour d'informations permettait :

- *une sensibilisation du personnel, qui voit ainsi redescendre les informations qu'il a livrées. Ce facteur augmente de manière importante le sentiment d'appartenance à l'entreprise ;*
- *une action de fertilisation, les informations amenant de nouvelles questions ;*
- *l'augmentation du capital immatériel ;*
- *un infléchissement des orientations stratégiques.*

Cycle IES

Formats de diffusion adaptés

Les moyens de diffusion sont multiples et malgré les transformations insufflées par les TIC et les possibilités qu'offrent maintenant les systèmes d'information d'entreprise, des supports papier peuvent encore être utilisés. Néanmoins, la notion de temps et de distance incite à la numérisation. Chaque entreprise adapte ses supports de diffusion en fonction des destinataires et de ses besoins (revue de presse, journaux internes, lettre d'information, *newsletter*, comptes-rendus de visite, fiche synthèse-action,…). Mais une diffusion efficace de l'information sous-tend de respecter les nombreux principes qui régissent la communication écrite et orale et permettent ainsi à l'information de conserver sa valeur d'un destinataire à l'autre.

Pour l'exploitation des informations, un résumé mensuel et une synthèse bimestrielle. Sur ces fiches, les sources étaient personnalisées (origine, valorisation du salarié) et les messages condensés (résumés en style télégraphique).

Cycle IES

Les principaux avantages du cycle du renseignement

- La simplicité du concept permet une compréhension aisée par les équipes quelles que soient leurs fonctions.
- Le processus itératif permet de corriger les dysfonctionnements par un *feed-back* efficace.
- L'importance donnée aux étapes préliminaires (expression des besoins) et finales (traitement, diffusion) évite la tentation d'assimiler trop rapidement l'intelligence économique avec la simple collecte d'informations. La collecte ne représente finalement qu'une partie du travail à réaliser.
- La décomposition du processus en étape successive facilite la transposition aux systèmes d'information et par conséquent l'amélioration technologique du cycle.

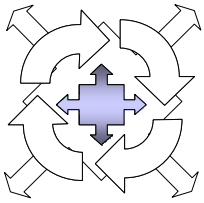
Le caractère récurrent du cycle facilite la compréhension d'un processus dynamique et permanent que les systèmes d'information peuvent considérablement optimiser : ciblage des recherches, gain de temps dans l'analyse et la diffusion, prise en compte du processus par l'ensemble de l'entreprise…

La mise en place de cette politique d'intelligence se révéla être extrêmement efficace. Les informations recueillies permettaient en effet de confirmer ou remettre en cause les objectifs à très court terme ou les orientations prises par le comité de direction. Nous n'utilisons pas à proprement parler des systèmes d'information spécialisés, la taille de l'entreprise ne le justifiant pas. Mais il est bien évident qu'un grand groupe, s'il souhaite lancer une démarche similaire, doit avoir un système d'information extrêmement performant technologiquement.

Cycle IES

Le cycle du renseignement ou cycle de l'information ou encore cycle de l'intelligence économique, constitue le rouage central de la démarche d'IES. L'information, qu'elle soit en mouvement ou stockée, en est la matière première. Face aux menaces, il est essentiel de développer ce processus moteur dans un environnement sécurisé garantissant ainsi la protection des données et la conservation du savoir de l'entreprise.

4.2 Dans un contexte sécurisé : la protection de l'information



4.2.1 Quelques exemples…

Mai 1998, l'agence de presse Reuters a accusé l'un de ses anciens employés d'être parti chez un concurrent emportant avec lui un document confidentiel regroupant la liste complète de tous les clients en Grande-Bretagne[28].

Une société canadienne fabricant des autobus envoie ses ingénieurs se présenter sous de faux noms et avec de faux curriculum vitæ, à des entretiens d'embauche chez des concurrents.

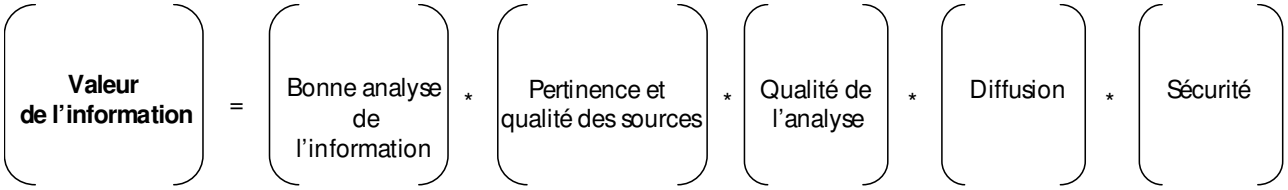
Une société de logiciels finance les recherches d'un professeur d'université. Ce dernier envoie chaque année des stagiaires chez les concurrents de son sponsor et les soumet à un débriefing complet en fin de stage. La synthèse du débriefing se retrouve sur le bureau de la société commanditaire quelques jours plus tard[29].

4.2.2 L'information, source de convoitises

Les exemples précédents traduisent la diversité des menaces qui pèsent aujourd'hui sur le capital informationnel de l'entreprise. Ils montrent également l'ingéniosité dont peuvent faire preuve certains salariés, concurrents ou cabinets spécialisés.

L'information et le savoir sont de plus en plus convoités. Biens immatériels et précieux, ils doivent être protégés, conservés, transmis et utilisés en se protégeant des menaces et des dangers. Si l'on tient compte de la définition donnée par B. Martinet et Y.-M. Marty[30] sur la valeur de l'information, la composante sécurité ne peut être négligée et s'inscrit comme une dimension transversale au cycle du renseignement.

[28] Guichardaz P., Lointier P. et Rosé P., L'Infoguerre, stratégie de contre intelligence pour les entreprises, Dunod, 1999.
[29] *op. cit.*
[30] *op. cit.*



Source : Y.-M. Marti et B. Martinet

Figure 12 : La valeur de l'information.

4.2.3 Les menaces envers le patrimoine informationnel

Il existe aujourd'hui un éventail de risques et de menaces externes beaucoup plus large qu'auparavant. Cette augmentation peut s'expliquer par la maîtrise de l'information ouverte et fermée. Ainsi, les produits, les sites, les personnes et l'environnement direct des entreprises sont devenus des cibles.

Il est possible de distinguer deux types de menaces[31] :

- *les menaces accidentelles* : catastrophes naturelles (incendies, explosions ou courts-circuits) et les erreurs dues à un manque d'inattention ou de compétence (effacement de données, erreurs de saisie…) ;
- *les menaces intentionnelles* : elles traduisent une démarche volontaire pour acquérir une information stratégique de manière illicite : espionnage, perturbation des systèmes d'information, vol de données ou fraudes physiques, chantage, usurpation et sabotage.

Le tableau suivant résume parfaitement le répertoire des risques externes tels que les appréhendent les entreprises.

En %	Global
- Lobbying, influence……	30,2
- Désinformation……	12,6
- Interception d'informations noires……	12,6
- Débauchage de cadres……	11,6
- Infiltration……	7,2
- Manipulation……	4,6
- Intrusion……	4,1

Source : IHEDN

Tableau 5 : Tableau des menaces externes[32].

[31] *op. cit.*
[32] *op. cit.*

Une grande partie de ces menaces concerne les systèmes d'information. Ce thème sera plus spécifiquement abordé au cours du prochain chapitre.

4.2.4 La sécurité ne peut qu'être globale

Lorsqu'on parle de sécurité globale[33], on entend non seulement les procédures techniques de protection, mais aussi et surtout la sensibilisation du personnel sur l'attitude à avoir quotidiennement. Cette prévention s'inscrit dans la politique globale d'IES d'une organisation. Car quiconque mesure l'impact stratégique de l'information comprend qu'il est nécessaire de la protéger.

Cette attitude « défensive » contribue à poser les premières bases d'une politique de contre-intelligence. Car, au-delà des pratiques offensives, la contre-intelligence consiste à minimiser les risques d'attaques. Et dans ce cadre précis, certaines règles doivent être inculquées aux managers détenteurs d'informations à forte valeur ajoutée :

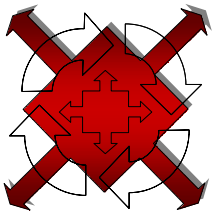
- *savoir si une information est stratégique ou non* : toutes les informations ne nécessitent pas d'être protégées. Il s'agit donc de déterminer quelles informations peuvent être divulguées et diffusées de façon globale, et celles dont la diffusion doit être restreinte ;
- *repérer les circuits d'informations* : d'une part afin de pouvoir s'en servir mais également pour éviter d'y livrer des informations trop sensibles ;
- *être méfiant vis-à-vis des personnes extérieures* : les relations avec les clients, mais surtout les fournisseurs, notamment dans le secteur informatique, où ceux-ci peuvent avoir des points d'entrée dans le système d'information ;
- *savoir qui écoute* : il est souvent facile, dans les lieux publics ou en présence de personnes extérieures à l'entreprise, de savoir qui écoute ou cherche à glaner des informations. Il suffit de faire preuve de vigilance et d'être conscient des pratiques utilisées ;
- *sensibiliser ses subordonnés* : informer et former sur la nécessité de protéger les informations, sur les règles, habitudes à avoir ;
- *éviter la paranoïa* : il est impossible de tout protéger et toute l'information ne le nécessite pas forcément.

Il ne s'agit pas ici de définir une façon de se protéger, mais bien de montrer que la protection de l'information fait partie intégrante de la démarche d'IES. Le capital informationnel de l'entreprise est une source de convoitise sujette à une menace grandissante. Prendre conscience de cet état de fait est

[33] Voir le rapport « La sécurité des systèmes d'information », Cigref, 2002.

nécessaire, mettre en place des mesures concrètes de protection est primordial. S'inscrivant dans les actions de contre-intelligence, elles permettent d'anticiper et de contrer les attaques informationnelles auxquelles les entreprises doivent faire face. Car, le développement des TIC a considérablement modifié la diversité des menaces, favorisant l'émergence d'un nouveau conflit pour le contrôle de l'information : l'infoguerre.

4.3 Face aux menaces omniprésentes : l'intelligence économique offensive



« En répandant des bruits, tant pour faire connaître ce que vous voulez qu'on croit de vous sur les prétendues démarches entreprises par les généraux ennemis, en faisant parvenir ces nouvelles tendancieuses jusque dans les conseils du Prince que vous combattez, en faisant planer le doute sur les intentions de ceux dont la fidélité est pourtant de notoriété publique, vous ne tarderez pas à constater que chez l'ennemi, des soupçons remplacent la confiance, qu'on y repense ce qui devrait être châtié et qu'on punit ce qui méritait la récompense. »
Sun Tsu (L'art de la Guerre)

Les pratiques d'intelligence économique offensives sont devenues une réalité pour de nombreuses entreprises. Face à des marchés inconnus ou émergents, la connaissance approfondie des jeux d'acteurs devient un élément critique de succès. Nous nous limiterons ici aux techniques de guerre de l'information et plus particulièrement à la désinformation, thème qui fut abordé durant le Cycle IES par Christian Harbulot[34]. L'objectif de ce chapitre est de montrer qu'il s'agit d'une réelle menace contre laquelle il faut se prémunir en étudiant les techniques employées. Qu'en maîtrisant ces modes d'action, on peut s'en préserver mais aussi s'en servir. Enfin, montrer que les systèmes d'information sont au cœur de cette menace.

[34] Coauteur du rapport Martre, Christian Harbulot est le directeur de l'École de guerre économique et l'auteur de nombreux ouvrages et articles sur la guerre de l'information

4.3.1 Quelques exemples

Philips Millenium et Belvédère se dispute le marché de l'embouteillage… Philips Millenium choisit l'offensive et demande à la société de communication Edelman de créer un site internet offensif contre Belvédère. Celui-ci est mis en ligne le 12 octobre à 20 heures, alors que Belvédère présente ses comptes semestriels le lendemain, 13 octobre. Les effets sont dévastateurs : le cours boursier de l'entreprise s'effondre, la presse économique et financière reprend en majorité les thèses de Millenium, la COB ouvre une enquête sur la communication financière de Belvédère[35].

Nous subissons régulièrement des attaques, comme tous les grands groupes de cosmétiques. Ligues antivivisection, désinformation sur nos produits (parfums, perspirants…) ou sur les molécules qui les composent. Il est vrai qu'internet peut constituer une formidable caisse de résonance pour véhiculer des rumeurs infondées, néanmoins la phase critique intervient avec une surmédiatisation de ce type de bruit. En effet, dès qu'un canal médiatique plus fort, télévision ou presse, s'empare de l'affaire, le danger est plus important. La mise en cause d'un produit au « 20 h », entraîne le retrait quasi obligatoire de celui-ci sur le marché. De toute façon, on constate que dans ce genre d'affaire, les consommateurs boycottent automatiquement le produit incriminé[36].

Ces deux exemples traduisent parfaitement les nouvelles menaces qui pèsent sur les entreprises. L'émergence de nouveaux canaux tels qu'internet et l'accès illimité aux sources dites « ouvertes » font, plus qu'autrefois, de l'information une arme offensive.

4.3.2 Contexte et définition

Contexte

Les technologies de l'information ont modifié de manière significative les techniques d'attaque. Aujourd'hui, connaître l'autre ne suffit plus, l'empêcher d'agir est devenu l'un des objectifs et les pratiques pour arriver à ses fins peuvent aller loin. Passés maîtres dans l'art de la polémique, ces agresseurs identifient les failles afin de mieux agir : parler à la place d'un concurrent, influencer ses alliés, fragiliser son image ou démoraliser son personnel. Ces méthodes sont de plus en plus courantes, et internet, caisse de résonance mondiale, est le vecteur de communication rêvé pour de telles actions.

[35] www.guerreco.com.
[36] Entretien avec M. Perrier, ex-directeur R&D de la branche Parfums et Cosmétiques (LVMH) et Philippe Copello, adjoint du directeur des systèmes d'information du Groupe LVMH.

L'utilisation de l'information à des fins d'influence, de contrainte ou de persuasion se développe dans tous les secteurs du marché économique. Les nombreuses affaires passées ou en cours sont là pour le prouver : le naufrage de l'Erika, le retrait du médicament anti-cholestérol de Bayer, les affaires Perrier... Déstabiliser ou détruire une entreprise par l'information, c'est ce que l'on appelle l'infoguerre, cette nouvelle technique d'attaque prend une ampleur généralement sous-estimée.

Cycle IES

Aujourd'hui, de petites organisations (PME-PMI, organisations non gouvernementales, groupe de *lobby*...), des particuliers ont la possibilité d'attaquer de grands groupes, sans crainte de représailles. Mal préparés, incapables de réagir dans les temps impartis (par manque d'informations pertinentes), ne possédant pas de cellules de crise opérationnelles et une communication inadaptée, il leur est souvent difficile de réagir dans les meilleures conditions.

Ces constatations ne font que conforter les chiffres de l'IHEDN concernant les attaques dont ont été victimes les entreprises françaises. Dans ce chapitre, nous nous attacherons à définir ce qu'est l'infoguerre et brosser de manière exhaustive les différents axes stratégiques de ce concept que l'on classe dans l'intelligence économique dite « offensive ».

Définition

Traduit de l'américain *Infowar* (*Information Warfare)*, ce concept à pris de l'essor durant la guerre du Golfe. D'origine militaire, l'infoguerre s'applique aujourd'hui à la sphère économique. Dans leur ouvrage sur le sujet, P. Lointier et P. Rosé[37] donnent une définition de l'infoguerre et en présentent les caractéristiques :

« L'infoguerre peut se définir comme l'ensemble des actions mises en œuvre pour affecter les informations et les fonctions informationnelles d'un concurrent dans le but de dégrader son système de décision. Elle concerne toutes les activités qui pourront apporter une domination informationnelle ».

Caractéristiques :

- n'importe qui peut attaquer (les moyens technologiques actuels le permettent) ;
- on ne sait pas qui est attaqué, par qui et qui en est le responsable ;

[37] *op. cit.*

- on ne sait pas ce qui est réel (notamment avec les cas de désinformation, les informations fausses étant généralement dissimulées dans le tissu des 90 % à 95 % d'informations exactes selon l'IHEDN) ;
- on ne sait pas qui est l'adversaire (intentions et moyens dont il dispose) ;
- une entreprise est vulnérable par sa relation avec des tiers (clients, fournisseurs, etc.), source d'attaques indirectes ;
- la notion de frontière tend à s'estomper.

4.3.3 Les stratégies

Nombreux sont les ouvrages qui ont été écrits sur « la guerre de l'information ». L'École de guerre économique s'est spécialisée sur ce thème. Elle en développe les concepts et effectue de nombreuses recherches autour de ce thème.

Les stratégies d'infoguerre sont de trois types :

- *la guerre POUR l'information*, qui s'appuie au maximum sur l'utilisation des sources ouvertes. Interception d'informations stratégiques et confidentielles (système Échelon, piratage informatique et contrôle global de réseaux) ;
- *la guerre CONTRE l'information*, qui consiste à priver un adversaire de son accès à l'information ;
- *la guerre PAR l'information*, touche plus particulièrement les actions de désinformation et de manipulation.

4.3.4 La dominance par l'information

Selon Christian Harbulot[38], « l'information dominance » constitue un axe majeur du concept de guerre de l'information.

Aux États-Unis, cette doctrine de « l'information dominance » issue du monde militaire est parfaitement mise en application dans le secteur économique. S'accaparer et maîtriser toutes les ressources, sources, flux et vecteurs d'information pour obtenir un avantage durable, en terme de puissance, face à ses concurrents. Ce qui s'applique aux puissances politiques sied parfaitement aux puissances économiques et industrielles.

Cycle IES

[38] Harbulot Christian et Lucas Didier, *La guerre cognitive, l'arme de la connaissance*, Lavauzelle, 2002.

Selon lui, cette dominance par l'information peut se décliner sous plusieurs formes :

- *Reputation :* phénomène qui apparaît aux États-Unis où les entreprises font de moins en moins preuve d'improvisation en cas de crise informationnelle. À cet effet, des structures se mettent en place, ainsi que des schémas afin d'agir ou de réagir dans les meilleures conditions.
- *Perception management* **:** action qui consiste à fournir ou à camoufler une information sélectionnée et des indices à des audiences étrangères de façon à influencer leurs émotions, leurs motivations et leurs raisonnements objectifs. Ce nouveau concept américain souligne l'importance du renseignement humain dans les nouvelles démarches offensives. Le but est d'occuper le terrain et de donner des clés à des consommateurs pour que ce soient leurs références.
- *Psy ops (opérations psychologiques) :* définie comme l'utilisation planifiée ou programmée de toute forme d'action humaine non coercitive désignée pour influencer les attitudes ou les actions de groupes ennemis, neutres ou alliés de manière à servir les intérêts nationaux (Mc Laurin 1982).

Les pays européens comprennent que la mise en place d'un tel concept passe obligatoirement par une indépendance technologique et des moyens adaptés. Le projet Galiléo pourrait en constituer une première étape.

Un groupe comme Thales, à travers sa branche Thales Communications, mesure l'ampleur de ce phénomène et conçoit des systèmes d'information adaptés pour maîtriser et diffuser les données stratégiques. La création d'une branche *Information Dominance Systems* traduit le rôle prépondérant des systèmes d'information dans ce concept.

« Facteur clé de succès des opérations dans lesquelles nos forces sont engagées, la maîtrise de l'information devient un domaine à part entière. Traiter un nombre croissant d'informations diffusées à haut débit sur les théâtres d'opérations, intégrer les données d'écoute et de surveillance, d'observation d'image et de renseignement dans les systèmes d'information et de commandement, proposer des solutions de systèmes d'information et de communications sécurisées et interopérables, tels sont nos challenges. Regroupant les compétences techniques des systèmes d'information opérationnels, écoute et brouillage des communications, exploitation du renseignement, imagerie et géographie numérique, sécurité et durcissement, Information Dominance Systems ***répond également à un marché civil en forte croissance*** *(sécurité des systèmes, surveillance du spectre, observation terrestre, guerre informatique). »*

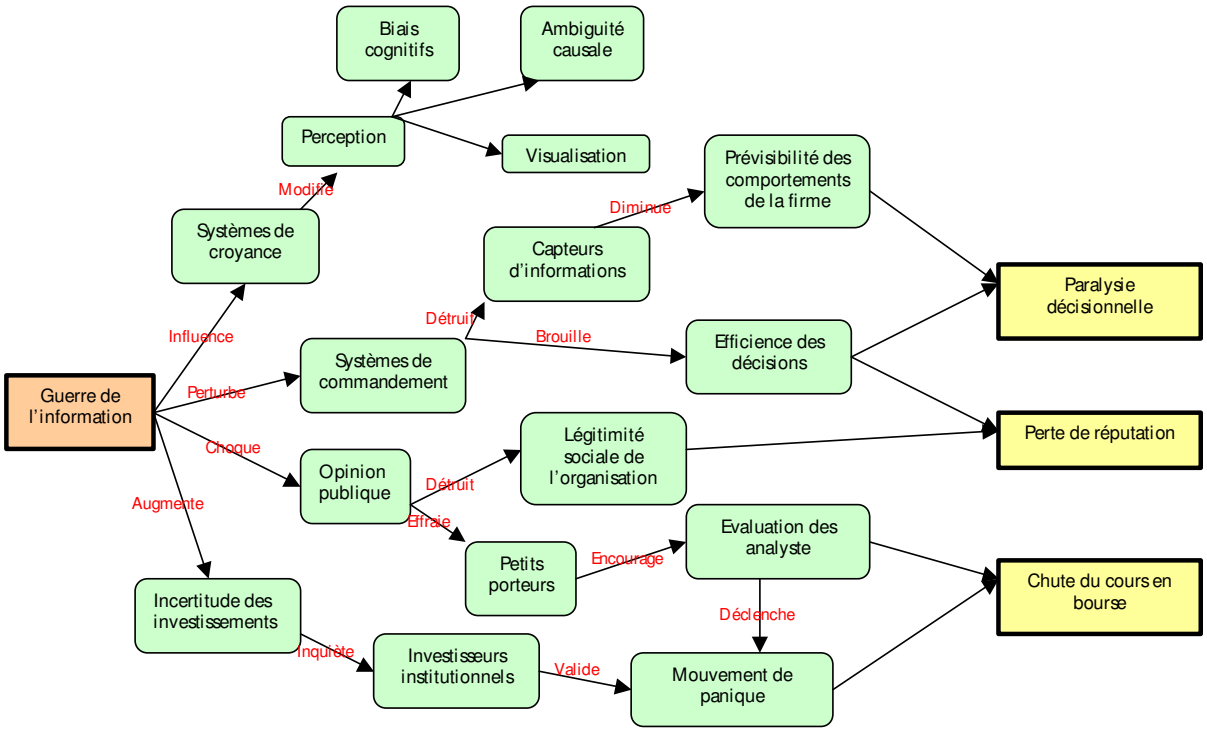
Site Thales Communications[39]

4.3.5 Info-déstabilisation, le rapport du faible au fort

Dans ce contexte de dominance de l'information, les modes d'action dits « du faible au fort » mettent en évidence certaines techniques d'attaque. La désinformation ou info-déstabilisation en fait partie. Cette méthode s'appuie sur l'utilisation des sources ouvertes (informations accessibles à tous) et l'art de manier la polémique.

Pour Philippe Baumard[40], les campagnes de déstabilisation ont trois objectifs : la perte des moyens psychologiques de l'adversaire, c'est-à-dire générer une paralysie décisionnelle dans le camp adverse ; la perte de réputation ou de légitimité de l'adversaire, aussi bien dans l'opinion qu'auprès des investisseurs institutionnels, des marchés financiers et surtout de ses partenaires, en particulier si elle est en situation d'interdépendance stratégique ; et la chute de ses soutiens financiers. Les trois cibles de telles campagnes sont les systèmes de croyance, le système de commandement et l'opinion publique.

[39] www.thales-communications.com.
[40] Baumard Philippe, « Les limites d'une économie de la guerre cognitive » in La guerre cognitive, l'arme de la connaissance, Lavauzelle, 2002.



Source : P. Baumard

Figure 13 : Le processus et les trois finalités des guerres de l'information[41].

[41] Philippe Baumard, Analyse Stratégique : mouvements, signaux concurrentiels et interdépendance, Dunod, 2001.

Selon lui, pour qu'une campagne de désinformation soit efficace, il faut qu'elle touche l'opinion publique. Les thèmes les plus sensibles sont liés aux risques alimentaire, d'hygiène et physique. Par conséquent, les industries agroalimentaire, pétrolière, pharmaceutique ou cosmétique, sont les plus sujettes à ce type de menaces. La dernière campagne de Greenpeace contre le groupe pétrolier Esso est là pour le prouver (StopEsso.com).

Source : internet

Figure 14 : Site StopEsso.com.

Dans ce domaine, l'exemple le plus frappant reste l'affaire Perrier[42], au début des années 90. Parce qu'elle ciblait les trois secteurs (alimentaire, hygiène et physique), cette campagne, fut l'une des plus efficaces.

Face à de telles menaces, les entreprises se doivent de réagir et d'appréhender les rapports avec l'information sous une nouvelle forme.

[42] Voir Jacques-Gustave Pascal, « Guerre et contre-guerre de l'information économique », Revue Échanges, 1994.

4.3.6 Une prise de conscience nécessaire

Certaines entreprises ont pris conscience de la menace. Selon l'IHEDN[43], les actes de désinformation constituent la deuxième préoccupation des entreprises en matière de pratiques offensives. Néanmoins, le tissu économique français demeure encore réticent et ce, pour diverses raisons :

- cet univers est peu identifié par les directions d'entreprises et globalement méconnu car diffus et impalpable ;
- les décideurs, mais pas seulement, n'ont pas encore intégré la dimension réelle de ce que la société de l'information peut changer ;
- les directions générales ne cherchent pas à évaluer la valeur ou la rentabilité des coups portés ;
- les attaquants ont l'avantage et ne sont quasiment jamais réprimés ;
- les entreprises faisant appel en justice ne s'y retrouvent pas financièrement par rapport à l'ampleur de l'attaque et de ses conséquences (chute de l'action, réputation de l'entreprise…).

4.3.7 Comment réagir[44] ?

Occuper le terrain par la connaissance : domination linguistique, éducative et morale

- Certains groupes investissent de l'argent pour charger de l'information sur des sites afin de se déculpabiliser, fiabiliser leur image, consolider le lien au client ou maintenir leur distance par rapport aux concurrents en influençant leurs orientations.

Dans les années 80, grâce aux informations transmises à la DST par Farewell, un indicateur soviétique, les Occidentaux bombardent les Soviétiques d'informations scientifiques erronées ou tronquées, avec le soutien de chercheurs et de revues réputées sérieuses. L'URSS perdra ainsi beaucoup d'argent dans des recherches inutiles[45].

- Autrefois utilisées par les militaires, cette pratique se généralise.

[43] Bournois Franck, Romani Pierre-Jacquelin, L'intelligence économique et stratégique dans les entreprises françaises, IHEDN, Economica, 2000.
[44] Extraits des propos de C. Harbulot durant le Cycle IES du Cigref.
[45] Guyaux Jean (Général), *L'espion des sciences*, Flammarion, 2002.

Parfois, nous mettons quelques informations tronquées sur notre site afin d'orienter nos concurrents sur de fausses pistes.

Cycle IES

- Utilisation de tous les canaux informationnels (internet, médias..), adaptation aux possibilités offertes par les nouvelles technologies de l'information.
- Coordination entre les organes de renseignements de l'État et les entreprises.
- Participation et soutien politiques pour l'approche des marchés étrangers.
- Prise de conscience des jeux d'influences au travers de certaines organisations (notamment les ONG) ou la mise en place de fausses informations.

Mettre en place des structures d'anticipation

- Création de plans de gestion de crise.
- Politique de communication adaptée et préparée, aussi bien en cas de crise que pour la mise sur le marché des produits.
- Mise en place de *War-Room*, étude de leur fonctionnement, retour d'expérience.
- Réactivité de l'encadrement à tous les échelons, attitude appropriée.

Évaluer les menaces, prévoir des contre-actions

Des schémas d'analyse et d'action face aux menaces informationnelles doivent être enseignés :

- évaluer les sources disponibles ;
- établir une cartographie des acteurs ;
- visualiser les différents échiquiers ;
- tenir compte des grilles de lecture préalables ;
- fixer les règles du *management* de l'information ;
- identifier les risques informationnels ;
- appliquer une démarche d'influence.

Adopter une approche informationnelle

Mémorisation : il est souvent constaté une absence de mémoire dans beaucoup de cas. Les expériences précédentes sont–elles référencées ? Les succès et échecs de l'entreprise sont-ils répertoriés ? A-t-on mémorisé les marchés ? Un « débriefing » des personnels partants en retraite est-il fait ? Ces constatations viennent appuyer les projets de gestion des connaissances[46].

Visualisation des menaces : chaque salarié doit être informé sur les menaces dont peut-être victime l'entreprise. Cette sensibilisation doit être la plus large possible et toucher toutes les catégories de personnels.

Alimentation permanente en informations : l'information doit être actualisée et complétée en permanence, dans tous les secteurs de l'entreprise, chacun contribuant à son niveau à alimenter l'ensemble des connaissances de l'entreprise.

Orchestration des circuits informationnels : la guerre de l'information s'appuie sur la liberté de circulation des flux informationnels. La présence d'un cadre « chef d'orchestre », ayant une vision globale de ces circuits d'information, est primordiale. Capable d'anticiper les débuts de crise ou d'attaque, il sait également véhiculer de l'information qui indirectement deviendra offensive.

Procédures contre le risque informationnel : comme les procédures de réaction en matière de sécurité incendie, des schémas, plans d'action et infrastructure en matière de crises informationnelles doivent être mis en place. Dans ce cadre et à titre préventif, l'anticipation doit être omniprésente : sensibilisation et formation régulières des personnes, veille active tous azimuts (interne et externe), notes d'étonnement et actions de communication.

[46] Pour plus d'information, voir le rapport « Gérer les connaissances » publié par le Cigref en 2000.

Une véritable culture du management de l'information doit être développée. C'est dans ce cadre précis que la démarche d'IES se positionne ; aucune des trois étapes qui la composent ne doit être négligée. Le cycle du renseignement, « moteur » du concept, va livrer aux décideurs les renseignements pertinents pour leur permettre de prendre des décisions et mener des actions concrètes. Mais véritable « carburant » de l'entreprise, l'information doit être protégée et préservée. Négligée ou sous-estimée, elle représente un vecteur d'agression particulièrement efficace et destructeur. C'est dans ce contexte qu'il s'agit de définir la place des systèmes d'information.

En effet, les systèmes d'information ne peuvent-ils pas constituer un formidable accélérateur de processus, qui permettrait de globaliser le concept d'IES à l'ensemble de l'entreprise ?

Garantissant la circulation et le stockage des données essentielles au fonctionnement de l'entreprise, les systèmes d'information ne sont-ils pas le meilleur outil pour protéger les informations stratégiques de l'entreprise ?

Dans cette nouvelle aire des conflits informationnels, les systèmes d'information sont devenus les cibles privilégiées des actions d'infoguerre ; *a contrario*, ne peuvent-ils pas devenir de formidables vecteurs offensifs ?

5 LES SYSTÈMES D'INFORMATION AU CŒUR DE LA DÉMARCHE

Dans ce chapitre, nous verrons que l'information évolue et circule dans une nouvelle dimension. Cet espace géographique laisse augurer de nombreuses perspectives en matière de communication et de rapport avec l'information. Le développement d'internet a accru la composante cognitive de l'organisation. Cet afflux massif de données rend obligatoire la mise en place de nouveaux outils et l'apprentissage de nouvelles techniques. Face à ce besoin de connaissance, les systèmes d'information prennent une nouvelle ampleur au sein de l'entreprise. Garant de la stratégie et de la compétitivité de l'entreprise, des infrastructures globales d'information se mettent en place laissant envisager de nouvelles possibilités d'organisation pour l'entreprise.

5.1 La technologie au service de l'IES

5.1.1 Le cyberespace

Aujourd'hui, la capacité cognitive d'une organisation peut être considérablement augmentée, voire transformée. En effet, dans le domaine de la connaissance individuelle et collective, les technologies de l'information (systèmes de mémorisation, d'aide à la décision, systèmes experts) fournissent un support de plus en plus important. Les progiciels, la mise en réseau des entreprises, la numérisation généralisée, le multimédia, la téléphonie mobile, l'UMTS, la visioconférence, les réseaux satellites… sont autant de supports qui vont permettre de transformer radicalement notre rapport avec l'information. Cette mutation technologique traduit la mise sur pied d'un nouvel espace « géographique » : *le cyberespace*.

5.1.2 Nouvelles perspectives

« C'est un lieu de l'immatériel mais dont les liens avec le réel sont bien présents. Le cyberespace fonctionne parce qu'il est composé d'ordinateurs, travaillant grâce à des logiciels puissants, et reliés entre eux par des fibres optiques. Le cyberespace sera aussi un espace dans lequel les utilisateurs pourront interagir rapidement par l'écriture, le son et l'image animée. Le réseau internet permet déjà de se faire une première idée, modeste, de ce que pourrait être le cyberespace ».
Inspiré de l'imagination de l'écrivain William Gibson[47].

Dans le cyberespace, les notions de temps et d'espace sont radicalement transformées. Les militaires ont très tôt compris qu'il leur fallait maîtriser cette nouvelle dimension. La guerre du Golfe a mis en évidence le rôle prépondérant de l'information et

[47] Wautelet Michel, *Les Cyberconflits*, Éditions Complexe, 1998.

l'usage que l'on pouvait en faire au travers tous les canaux de communication (satellite, télévision, réseaux informatiques…). La mise au grand jour du système Échelon[48] prouve que les systèmes d'information puissants sont la solution en matière de gestion de l'information. Les « passerelles » technologiques entre le monde militaire et le milieu économique sont de plus en plus étroites. Ainsi, les Anglo-saxons multiplient-ils les cellules de veille économique et stratégique sous le modèle de la *War-room.* À l'image d'une salle de commandement d'un état-major militaire, il s'agit d'améliorer la communication et la coordination entre ceux qui détiennent l'information stratégique et ceux qui l'utilisent.

Le centre d'arbitrage du Département du commerce américain utilise ce type de salle, il traite l'information tactique et stratégique « minute par minute ». Des spécialistes traquent, à chaque instant, les positions de milliers de projets géants autour du monde dans lesquels les entreprises américaines défendent leurs intérêts. Le centre suit également l'avancée des concurrents[49].

Sans en arriver encore à de telles structures, il est possible de concevoir des solutions de mieux en mieux adaptées à la maîtrise de l'information stratégique. Là encore, les recherches entreprises pour la défense, dans le domaine des systèmes d'information, laissent présager des infrastructures « jumelles » pour les grands groupes.

À l'image, encore une fois, du groupe Thales qui développe actuellement des solutions « complètes, modulaires et interopérables » destinées à accroître la supériorité informationnelle des forces armées. Centrés sur les concepts du commandement, du contrôle, des communications, de l'informatique, du renseignement militaire, de la surveillance et de la reconnaissance (C4ISR)[50], ces projets présupposent la mise en place de systèmes d'information assurant une maîtrise permanente de la situation tactique, l'interprétation optimale des ordres, facilitant ainsi la pertinence des prises de décision et la conduite des actions résultantes. Déjà, on évoque le concept de « *Network Centric Warfare* » qui permettra de raccorder les différents intranets du champ de bataille numérisé[51].

La comparaison peut paraître excessive, mais une unité militaire n'est ni plus ni moins qu'une entreprise en secteur concurrentiel permanent. Sur le champ de bataille, la maîtrise de l'information permet à l'unité de bâtir sa stratégie, d'en déduire des schémas tactiques et des scénarios opérationnels.

[48] www.echelon-online.fr.
[49] Baumard Philippe, *Compétitivité et systèmes d'information*, InterEditions, 1998.
[50] C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance).
[51] www.thales-communications.com.

Les ordres adaptés sont ensuite donnés aux échelons inférieurs, pour mener des actions concrètes et ciblées. L'information temps réel, montante et descendante, mais également transversale, est permanente ; elle permet d'ajuster ou modifier les schémas tactiques ou les orientations stratégiques.

Les entreprises évoluent aujourd'hui dans un contexte similaire. Internet a révolutionné les moyens d'accéder aux sources d'informations ouvertes. Cette facilité d'accès aux données génère des techniques de plus en plus pointues de navigation, de recherche, de collecte, de tri, d'analyse ou de diffusion. Intégrés aux systèmes d'information des organisations, ces logiciels développés sont devenus les pièces maîtresses de la démarche d'IES.

5.2 L'impact d'internet

5.2.1 Abondance de l'information

La naissance d'internet a eu un impact considérable sur la veille et l'intelligence économique. Aujourd'hui, toutes les sources convergent progressivement vers internet. Mais paradoxalement des difficultés apparaissent ; car plus l'information est abondante, moins on dispose de temps pour la traiter. L'interprétation qui en découle peut être faussée et l'information pertinente négligée. Face à un potentiel informationnel incontestable, des obstacles demeurent :

- l'information est difficilement accessible ;
- l'information est trop abondante ;
- l'information se renouvelle sans cesse ;
- l'information n'est pas toujours fiable.

5.2.2 Des outils de plus en plus performants

Afin de réduire l'incertitude liée à l'abondance et la fiabilité des données, des outils de plus en plus performants et intelligents apparaissent sur le marché. Les éditeurs mesurent leur intérêt et la nécessité de les intégrer aux systèmes d'information existants. Ainsi, des solutions globales « d'intelligence » se développent, permettant de couvrir dans sa quasi-totalité le cycle du renseignement. Modulables, elles s'intègrent et s'adaptent aux besoins de chaque entreprise et permettent d'obtenir des résultats significatifs dans la gestion de l'information à haute valeur ajoutée.

Après les attentats du 11 septembre, la Fédération de la maille, qui regroupe les acteurs de l'industrie textile, a su, bien avant les autorités de Bruxelles, que le Pakistan allait demander à l'Union européenne un élargissement des quotas d'exportation pour ses textiles en échange de l'autorisation d'accès à son territoire, donnée aux armées occidentales. Comment l'a-t-elle appris ? Grâce à Watch Edition, le logiciel de recherche et de traitement de l'information sur internet de la société Arisem. Ce dernier a récupéré l'information sur le site web de deux journaux pakistanais[52].

Ces outils de veille et d'intelligence économique sont de plusieurs types :

- *outils de collecte et traitement* : moteurs de recherche, agents intelligents, visualisation et cartographie ;
- *outils d'analyse documentaires* : bibliométrie, analyse linguistique, statistique ou sémantique ;
- *outils d'agrégation de contenus* : portails d'information, gestion des sources ;
- outils de partage d'information et organisation des processus de veille : intranet, *workflow*…

Afin d'évaluer leur impact sur le processus du cycle du renseignement, effectuons un rapide tour d'horizon de ces principaux outils.

5.2.2.1 Les outils classiques

Les annuaires

Adaptés à l'exploration des domaines les plus vastes, ce sont les plus simples des moteurs de recherche. Regroupée par grands thèmes, l'information y est recensée et classée par des documentalistes. Utiles en début de recherche pour affiner les axes d'orientation. Les annuaires peuvent s'appliquer sur la globalité du cyberespace.

Les moteurs et les métamoteurs

Appelés également « *crawlers* », ces logiciels parcourent le web et indexent les documents. Ils sont efficaces pour des recherches plus précises, à l'aide de mots clés. Néanmoins, ces robots ne couvrent pas la totalité du web (40 % max.) et chacun a des modes d'indexation propres et des profondeurs de zones balayées différentes. Pour pallier ce manque, une nouvelle génération de robots a vu le jour, ce sont les métamoteurs. Il s'agit en fait de cumuler les recherches de plusieurs moteurs traditionnels en lançant une recherche personnalisable.

[52] Le Monde Informatique n° 932 – www.weblmi.com.

Les outils classiques sont très utiles pour des recherches « simples ». Néanmoins, ces outils ne balaient qu'une partie du web. De nombreuses zones sont extrêmement riches en informations. Elles nécessitent l'utilisation d'outils plus perfectionnés ainsi qu'une certaine maîtrise technique.

5.2.2.2 Les zones riches en information

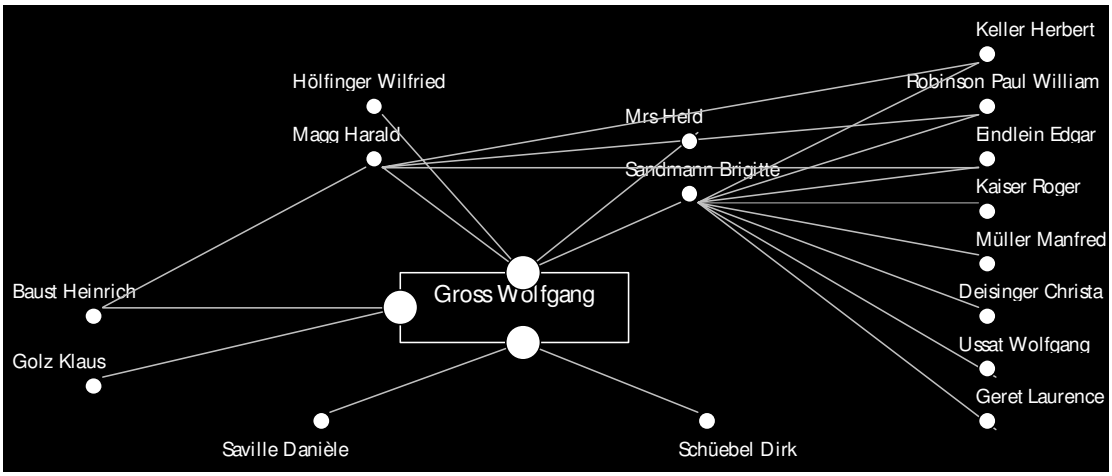
Le web invisible

Le web comprend une quantité importante de pages qui ne sont pas indexées par les moteurs classiques, elles appartiennent au web invisible. On y trouve :

- les pages récentes pas encore indexées ;
- les banques de données rattachées aux grands centres serveurs classiques (Dialog, Questel.Orbit, STN…) ;
- les pages web discrètes, contenues dans un site mais reliées à rien ;
- les sites web construits autour d'une base de données interrogeable uniquement par un moteur de recherche interne ;
- les pages générées de façon dynamique pour les sites de commerce électronique par exemple ;
- des sites qui refusent d'être indexés par les robots, par exemple les sites marchands de livres ou de musique ;
- les intranets.

Les forums de discussion et leurs archives

Les *newsgroups* sont légion sur le web, ils touchent tous les thèmes et permettent aux participants d'échanger des idées sur un sujet particulier. Des plus originaux au plus sérieux (discussions entre chercheurs par exemple), ces vecteurs de communication et d'échange sont également un moyen efficace pour faire de la désinformation et lancer de fausses rumeurs. Certains de ces forums peuvent parfois être à l'origine de crises informationnelles graves. Or, dans ce type de discussion rien ne se perd, ce qui s'y dit est archivé (Dejanews : www.deja.com/usenet) et peut être aisément retrouvé. De même, Il est possible d'identifier ce que l'on appelle des collèges invisibles, c'est-à-dire des groupes de professionnels qui travaillent sur le même projet.



Source : Y-M. Marti et B. Martinet

Figure 15 : Exemple de collège invisible[53].

5.2.2.3 Des outils de plus en plus performants

Aujourd'hui, des outils permettent de balayer les zones les plus inaccessibles du web et comprennent de nombreuses fonctionnalités.

Les moteurs dernière génération

Les moteurs dits « nouvelle génération » utilisent des technologies à base d'agents de recherche. Leur intérêt réside dans leur capacité à remplir et à automatiser des tâches à la place de l'utilisateur. Ils permettent notamment :

- de rechercher des informations de façon « intelligente » en utilisant des métamoteurs perfectionnés, des outils d'analyse linguistique des requêtes ou par exploration de liens hypertextes ;
- d'analyser les informations récupérées par indexation sémantique des résultats ;
- de filtrer et archiver les résultats ;
- de naviguer *off-line* parmi des pages et des sites téléchargés.

[53] Martinet Bruno et Marti Yves-Michel, *L'intelligence économique : comment donner de la valeur concurrentielle à l'information*, 2e édition, Éditions d'Organisation, 2001.

D'une grande diversité, les outils développés à présent sont de plus en plus complets, intégrant diverses fonctionnalités dans un même produit. D'après une étude réalisée récemment par Le Journal du Net[54] sur l'état actuel du marché, nous pouvons distinguer cinq catégories de moteurs :

- *les moteurs de recherche sémantiques généralistes et web* : intègrent le sens du langage au processus de recherche ;
- *les moteurs de recherche statistiques* : répondent à une requête en fonction de la fréquence d'apparition des concepts demandés et de leur répétition au sein d'un document ;
- *les moteurs de recherche multidimensionnels* : produits les plus avancés. Ils affinent la catégorisation des documents, ainsi que les procédés de requêtes croisées ;
- *les assistants de requêtes* : requêtes en langage naturel, reposant sur des fonctions d'analyse linguistique ;
- *les moteurs de recherche intégrés* : moteurs de recherche livrés au sein d'une solution de gestion de contenu web ou documentaire.

Offrant de multiples possibilités de traitement, ces outils fonctionnent à partir d'agents intelligents.

Agents intelligents

D'après l'Afnor :

« L'agent intelligent est un objet utilisant les techniques de l'intelligence artificielle. Il adapte son comportement à son environnement et en mémorisant ses expériences, se comporte comme un sous-système capable d'apprentissage. Il enrichit le système qui l'utilise en ajoutant, au cours du temps, des fonctions automatiques de traitement, de contrôle, de mémorisation ou de transfert d'information. »

[54] www.journaldunet.com.

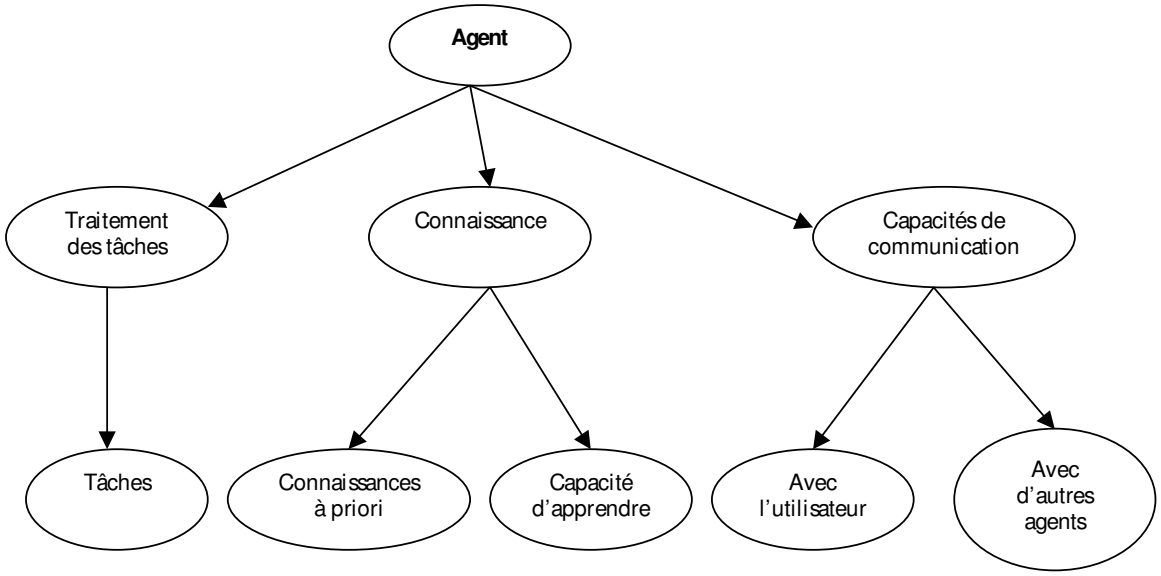


Figure 16 : Structure d'un agent[55]*.*

On distingue plusieurs types d'agents :

- *agents de recherche :* permettent de rechercher des informations par mots clés et en fonction de certains paramètres : secteur activité, analyse linguistique, filtrage et archivage… ;
- *agents de veille :* permettent de surveiller des sites web, archives de forums de discussion ou listes de diffusion. Deux grandes familles : *pull* et *push* :

  agents *pull* : agents d'alerte par courriel, agents d'alerte *off-line* ;

  agents *push* : agents *on-line* ou *off-line*.

La diversité des tâches dont sont capables ces agents permet aux outils développés la prise en compte de chaque étape du cycle, comme le montre le tableau ci-dessous.

[55] Revelli Carlo, *« Intelligence stratégique sur internet »,* 2° édition, Dunod, 2000. www.agentland.fr.

Rôle des agents intelligents dans le Cycle du Renseignement		
Etape du processus	**Description**	**Rôle des agents**
1. Rechercher	Définir les objectifs, les besoins en information, identifier les sources d'informations formelles et informelles (publications, articles, bases de données).	* * *
2. Collecter	Collecter toutes les informations (téléchargement de bases de données, rapports sectoriels, résumés, articles,…).	* * *
3. Traiter, analyser, stocker	- Mettre en forme et homogénéiser les informations - Vérifier, consolider et fiabiliser les informations - Stocker et archiver les informations (sources, résultats, décisions) - Mettre à jour les synthèses	* * * * * * *
4. Diffuser	- Diffuser les informations auprès des experts et décideurs	* * *

Tableau 6 : Le rôle des agents intelligents dans le cycle du renseignement.

Capables de « balayer » le *web* en profondeur, les cellules de veille reconnaissent l'intérêt de les utiliser.

De tels outils se révèlent très efficaces s'ils sont correctement paramétrés. Par exemple, pour évaluer le positionnement de nos véhicules, des agents balayent le web *et calculent le nombre de fois où le nom d'une de nos voitures est lié à un terme ou un domaine prédéfini. Nous pouvons ainsi estimer son positionnement sur le marché en fonction du nombre de fois où elle est associée à un modèle concurrent. Même chose pour l'insatisfaction des clients sur un aspect particulier de la voiture.*

Entretien dans une direction des systèmes d'information.

L'amélioration des modes de collecte affine les recherches mais n'exclue pas un volume d'information important à traiter. Apparus depuis quelques années sur le marché, les outils de cartographie tentent de donner une vision synthétique de l'information sur un domaine spécifique.

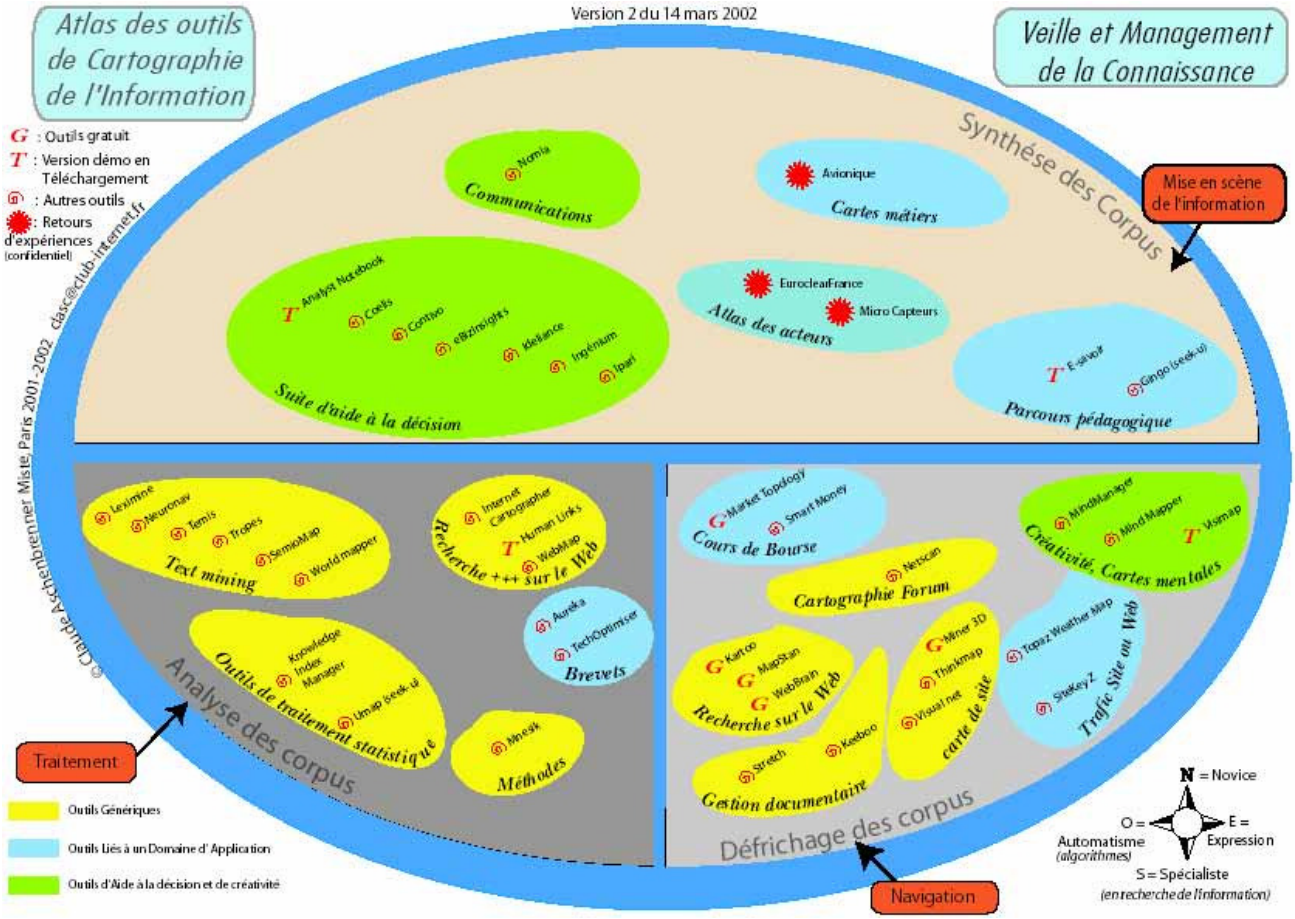
5.2.2.4 Les outils de cartographie

Le concept de cartographie s'applique-t-il pour identifier les liens entre les différentes informations ?

Question d'un DSI – Cycle IES

Représentant le cyberespace en deux dimensions, les cartes d'espaces informationnels peuvent être comparées par analogie aux cartes territoriales utilisées pour l'organisation d'une ville. Le but consiste à fournir un certain sens à l'étendue d'un domaine d'information pour l'aide à la navigation sur le réseau ou à la recherche d'information. Les outils de cartographie établissent des cartes visuelles des informations par thème. De plus en plus d'entreprises, notamment de cellules de veille, utilisent de tels outils. Le groupe EADS, par exemple, emploie le logiciel Neuronav qui permet d'indexer des

documents puis d'en visualiser la classification[56]. L'atlas ci-dessous réalisé par Claude Aschenbrenner[57], donne une vue d'ensemble des outils de cartographie du marché.



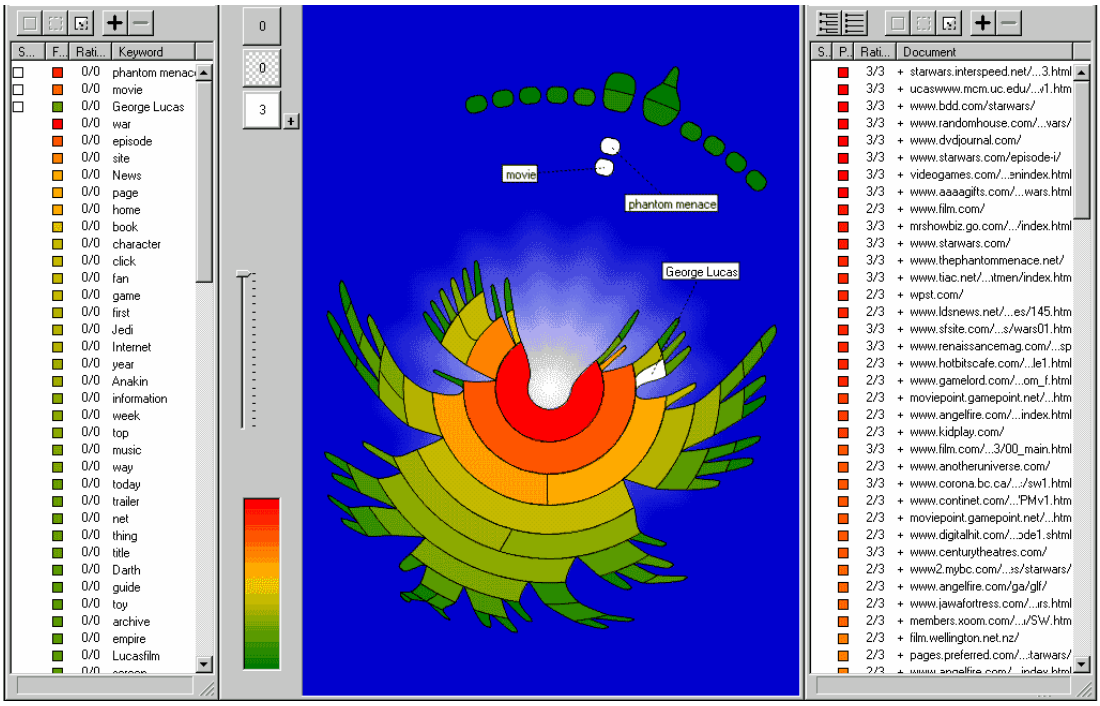
Source : C. Aschenbrenner

Figure 17 : Atlas des outils de cartographie de l'information.

[56] Magazine Veille, n° 55 du mois de juin 2002.
[57] www.esiee.fr/masteres/miste/.

Les exemples des pages suivantes illustrent ce qu'il est possible de faire avec les logiciels de cartographie.

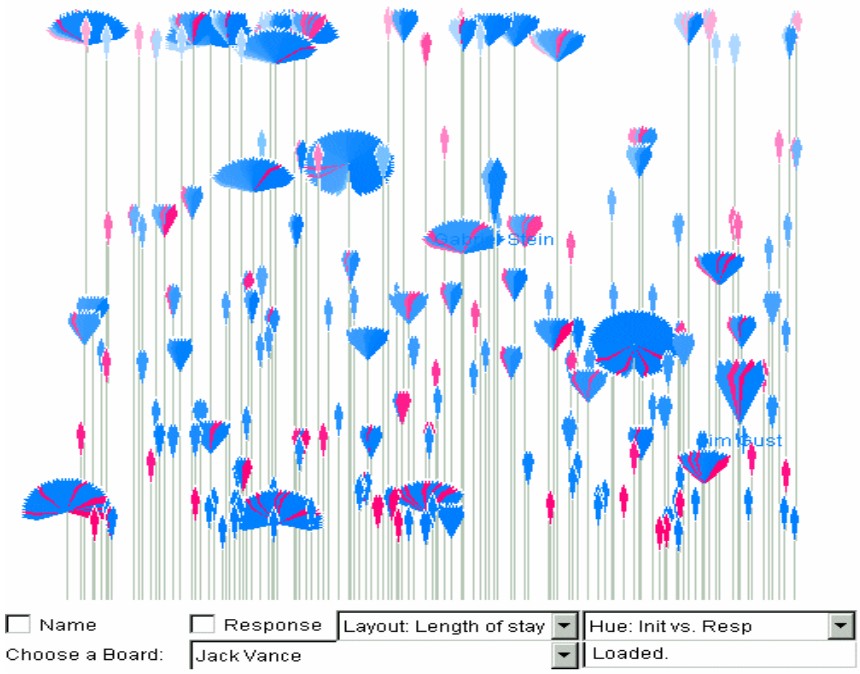
Le premier exemple représente une carte interactive d'un résultat de recherche sur le web.



Source : Trivium

Figure 18 : Carte d'information Umap.

L'exemple suivant est une visualisation innovante de conversation dans les forums de discussion, développé par le Media Lab du MIT. L'exemple s'appelle ***Peoplegarden***.



Source : MIT

Figure 19 : Peoplegarden, visualisation de conversations dans des forums internet.

Cartes des cheminements de dix semaines de navigation sur Internet. On peut chercher les chemins pour des pages web pertinentes, qui sont symbolisées par des points noirs.

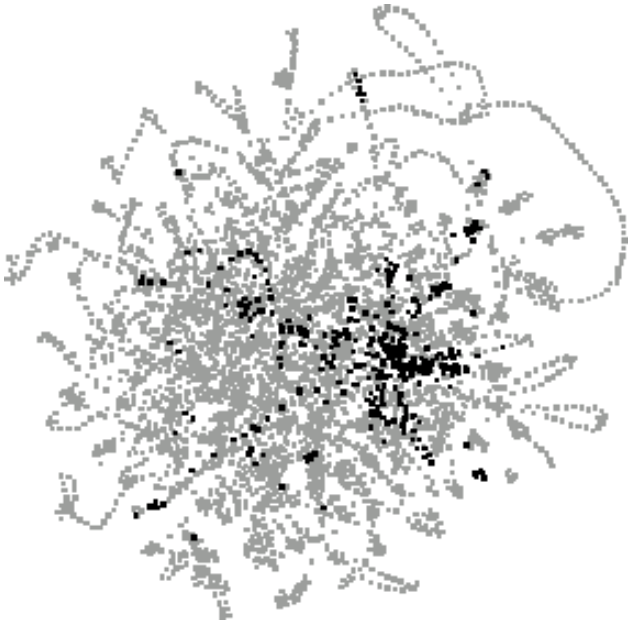
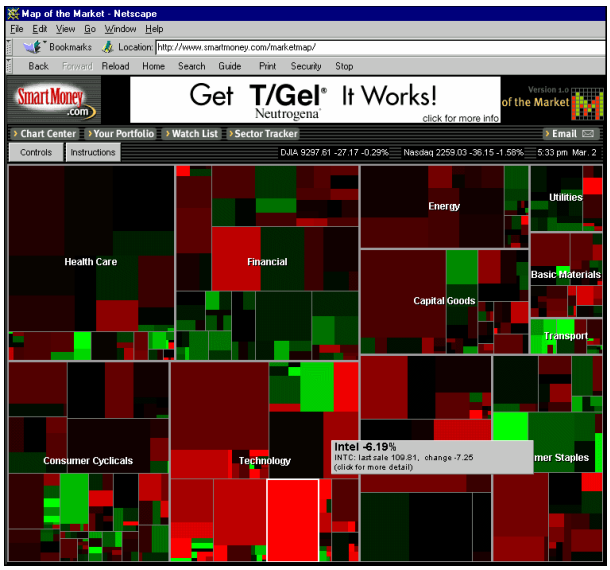


Figure 20 : Navigation sur internet.

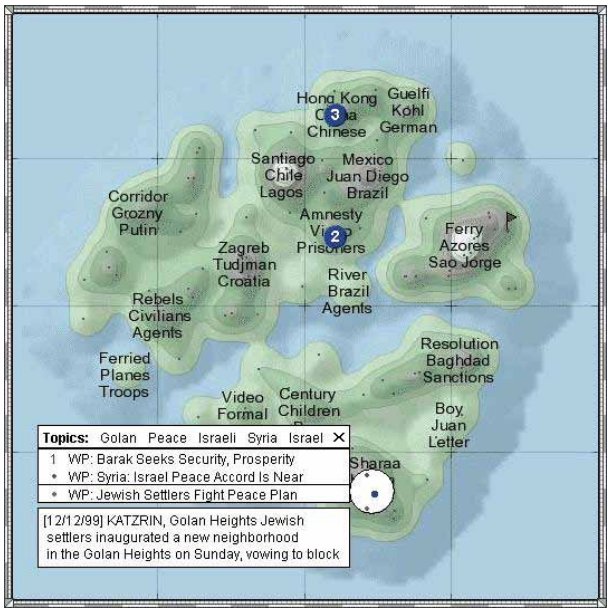
Carte de marché, **SmartMoney.com** cartographie la performance boursière de 500 entreprises américaines. Chaque compagnie est représentée par différents rectangles dont la taille correspond à la capitalisation sur le marché. La couleur du point indique les variations récentes du prix de l'action.



Source : Smartmoney

Figure 21 : Performance boursière de 500 entreprises.

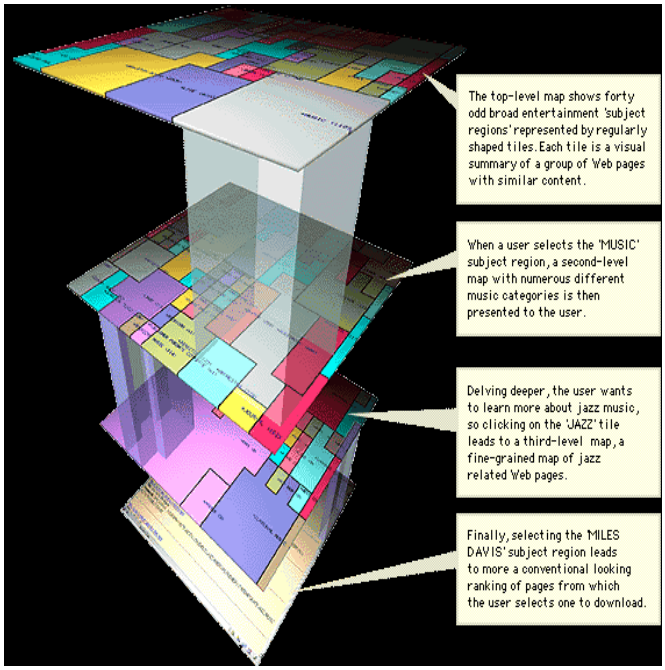
Une carte d'informations de dépêches mondiales de NewsMap (Cartia). La carte résume 121 rapports de dépêches en ligne depuis le 13 Décembre 1999.



Source : Cartia

Figure 22 : Carte de visualisation synthétique de dépêches d'agences de presse.

ET-Map - une carte de catégories multi-niveaux de l'espace informationnel constitué de plus de 100 000 pages relatives aux loisirs référencées par Yahoo!. ET-Map est une des nombreuses techniques de visualisation de l'information.

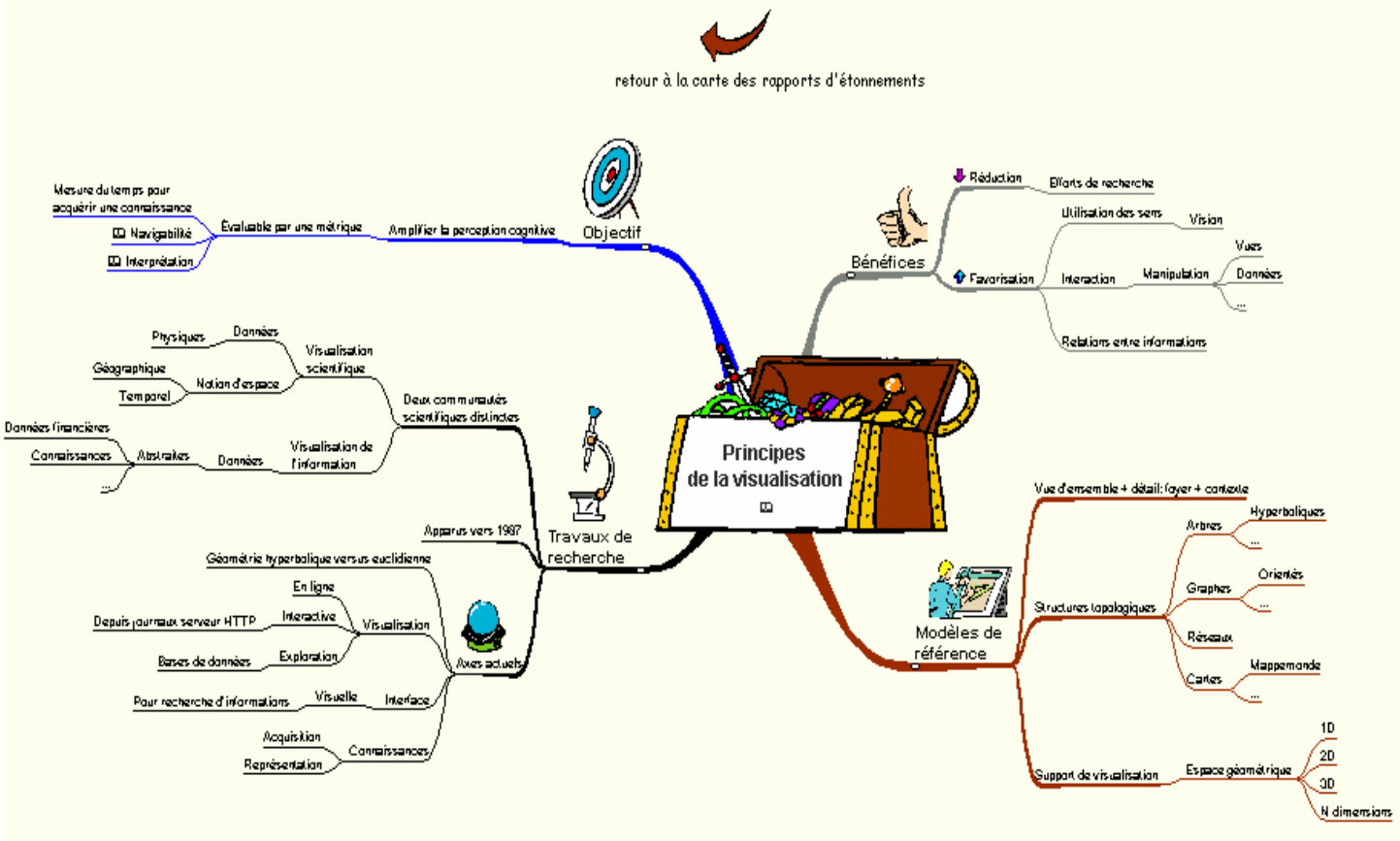


Source : ET-Map

Figure 23 : Représentation multidimensionnelle de pages web.

À propos du Mind-Mapping…

Le *Mind-Mapping*, en français réalisation de schémas heuristiques ou cartes mentales, a été créé dans les années soixante-dix par le chercheur anglais Tony Buzan, spécialiste du cerveau. L'informatique a renouvelé la création de *mind-mapping*, surtout la naissance d'internet. Car l'hyperlien permet d'associer des fichiers, des images, bref de recomposer ou restructurer un *corpus* de données. Plusieurs cellules de veille emploient ce type d'outil dans la construction d'équations de recherche ou pour synthétiser une situation.



Source : Miste

Figure 24 : Outil de visualisation (Mind-Mapping)[58].

Ce panorama des outils d'intelligence reste succinct, un site tel que agentland.fr (Société Cybion[59]) tient à jour les recherches en cours dans ce domaine et les nouveaux produits disponibles sur le marché. Le tableau ci-dessous regroupe les principaux outils de traitement de l'information sur internet.

[58] www.esiee.fr/masteres/miste/. www.petillant.com.
[59] www.cybion.fr.

Les annuaires	
Web	- Yahoo : www.yahoo.com - Excite : www.excite.com - Looksmart : www.looksmart.com - Go Infoseek : www.go.com - Open Directory: www.dmoz.org - Snap: www.snap.com - Magellan: www.mckinley.com - About: www.about.com - Voilà : www.voilà.fr - Nomade : www.nomade.fr
Forums de discussion	- Liszt: www.liszt.com/news/ - Tile.net : tile.net/news/listed.html - Deja: www.deja.com/home_bg.shtml
Liste de diffusion	- Liszt : www.liszt.com/ - Tile.net : tile.net/lists/alphabeticady.html - Listes françaises: www.cru.fr/listes
Les moteurs	
Web	- Altavista :altavista.digital.com - Excite : www.excite.com - Infoseek : www.infoseek.com - Lycos: www.lycos.com - WebCrawler: www.webcrawler.com - Google: www.google.com - Lokace: www.lokace.com (français) - Voilà : www.voilà.com (français)
Newsgroups **Mailing lists** **Web forums**	- Tile.Net : tile.net/ - Liszt: www.liszt.com (mailing lists); www.liszt.com/news/ (newsgroups)
Adresses e-mail	- Who Where: www.whowhere.com - People: www.people.yahoo.com - Internet Adress Finder: www.iaf.net
Les métamoteurs	
Web	- MetaCrawler: www.metacrawler.com - Profusion: www.profusion.com - MetaFind : www.metafind.com - SavvySearch: www.savysearch.com - Use-it: www.kamus.it/useadvfr.htm - Dogpile: www.dogplie.com - Supersearch:www.robtex.com/search/query.htm
Les moteurs dernière génération	
Moteurs sémantiques généralistes	Hummingbird (EIP), Verity (Portal One ou K2 Enterprise), Arisem (OpenPortal4U), Sinequa (Intuition), Convera (RetrievalWare), Inktomi (Inktomi Search)
Moteurs sémantiques généralistes / Web	Atomz (Atomz)
Moteurs de recherche statistiques	TripleHop (Matchpoint), Autonomy (KnowledgeServer)
Moteurs de recherche multidimensionnels	Instranet (Instranet2000)
Les assistants de requêtes	Lexiquest (Lexiquest), Albert (Albert Meaning Interpreter (AMI)), Alogic (Alcalimm), Auracom (Auraweb)
Moteurs de recherche intégrés	Mediapps (Net.Portal), Opentext (Livelink), Microsoft (Sharepoint Portal Server)
Les agents intelligents	
Agents de recherche	
Personnalisable par secteur d'activité	Webseeker
Veille, filtrage et archivage	Bullseye, Netattachepro
Analyse linguistique	Digout4U
Analyse des résultats	SemioMap, Umap
Agents pour la veille	
Pull	Teleport Pro, Web Whacker, Nearsite
Push	My NewsPage, Pointcast

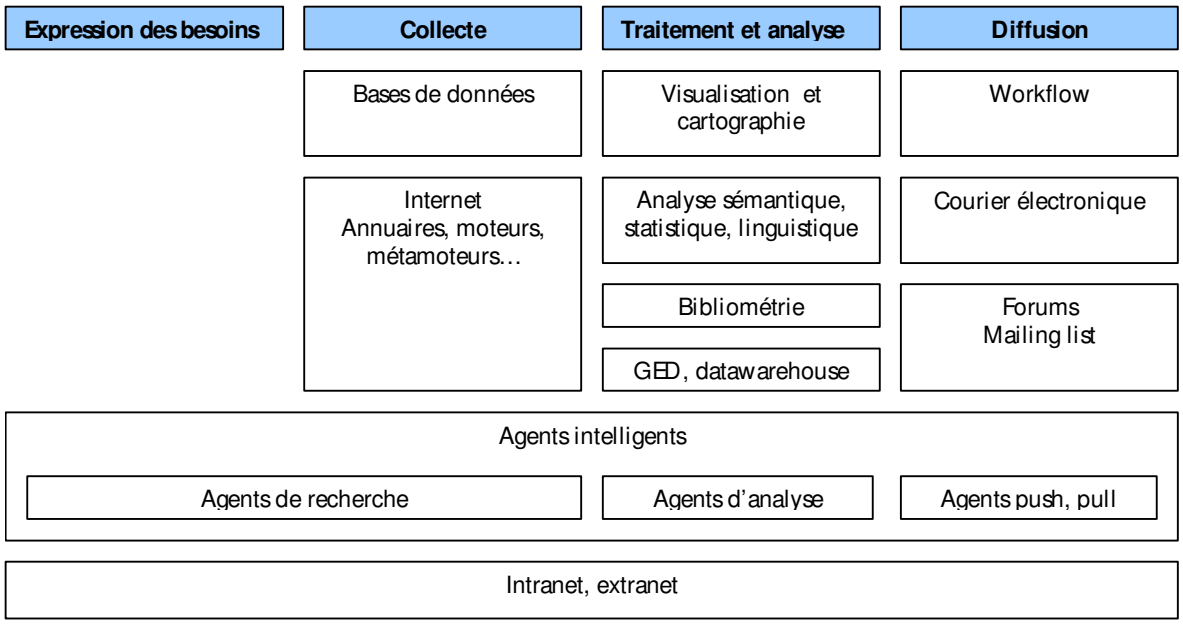
Source : Cigref

Tableau 7 : Internet et ses outils.

L'orientation vers des outils de plus en plus autonomes et intelligents a considérablement amélioré la gestion de l'information :

- précision des recherches par une meilleure identification des sources ;
- balayage étendu d'internet ou des bases de données ;
- concision et rapidité dans la collecte d'informations ;
- finesse de traitement et lisibilité accrue des résultats ;
- amélioration de la diffusion par un ciblage plus précis des destinataires.

Une fois les outils d'IES couplés aux techniques existantes de travail collaboratif ou de *business intelligence* (*workflow*, *groupware*, *datawarehouse*, *datamining, gestion électronique de documents*…), il est possible d'optimiser chaque étape du cycle du renseignement. Comme le montre le tableau suivant :



Source : Cigref

Figure 25 : Panorama des outils sur le cycle du renseignement.

Veille tous azimuts, détection des contrefaçons, anticipation des campagnes de désinformation, surveillance de personnes, de réseaux… ces logiciels accroissent considérablement la capacité cognitive de l'entreprise. Véritables accélérateurs de processus, ils permettent de cibler précisément les informations que l'on souhaite rechercher, de les collecter, d'améliorer leur traitement et d'accélérer leur diffusion aux décideurs, experts et

salariés concernés. Couplés avec des systèmes d'information collaboratifs tels que les portails intranet, ils préfigurent une nouvelle manière de partager l'information et de l'utiliser.

5.3 Vers des solutions globales d'intelligence

5.3.1 L'intégration des outils d'intelligence économique

Bâtir une solution globale qui puisse non seulement couvrir toute l'entreprise ou des secteurs ou branches spécifiques mais également s'adapter aux besoins de chacun est la solution idéale vers laquelle cherchent à se diriger les entreprises. Le portail de gestion de l'information est actuellement l'outil le mieux adapté pour implanter le concept et la culture IES à travers l'ensemble d'un groupe.

Comme le laissait présager les premières conclusions du rapport « Internet dans l'entreprise » du Cigref, des projets de ce type se développent dans certains grands groupes. Bâtis autour d'une solution logicielle dite « d'intelligence économique », l'avantage de ces systèmes d'information réside dans les aspects suivants :

Un affichage du dispositif de veille

- Une prise de conscience collective, chacun comprenant les enjeux de sa contribution au dispositif.
- Porte à la connaissance de tous les thèmes non confidentiels de veille et leur actualisation.
- Donne une identification des acteurs et de leur rôle en matière de projets et de gestion de l'information.

Un partage de l'information

- Améliorer la qualité de l'information et en créer de la valeur ajoutée (échange de points de vue et consolidations).
- Améliorer la circulation en offrant la possibilité d'assurer un *feed-back*.
- Créer des flux plutôt que des stocks d'informations vers des destinataires susceptibles d'en tirer profit.
- Favoriser la participation du plus grand nombre, avec possibilité de communication descendante, montante et transversale.
- Retenir des formats de diffusion ou de mémorisation adaptés à chaque type d'information et de destinataire.
- Avoir une traçabilité des demandes d'informations et des réponses.

Le processus du cycle du renseignement est un repère méthodologique commode pour créer ou enrichir son intranet. En effet, il permet de reprendre les instruments qui auront pu

être mis en œuvre dans l'entreprise, souvent sous format papier.

Les solutions globales évoquées précédemment permettent d'ajouter de nouvelles fonctionnalités au portail d'entreprise existant.

Interface personnalisée

- Personnalisation de l'interface (info du jour, par thème, moteur de recherche..) accès rapide à l'information.

Collecte plus précise et ciblée

- Moteur de recherche texte brut dans les informations collectées, sur internet, indexation, web invisible…
- Remontée rapide des sources informelles (clients, fournisseurs, commerciaux, réseaux personnels…) *via* certains outils (assistants numériques, courrier électronique, téléphone mobile, internet…).
- Création d'annuaires de liens internet pour l'ensemble des membres d'un réseau.

Traitement, analyse, stockage

- Représentation graphique des informations, croisement confirme ou infirme les rumeurs, suscite les questions, affine la perception des décideurs.
- Archivage spécifique des informations utiles aux décideurs en fonction de leur durée de vie (validité).

Diffusion

- Possibilité de générer des rapports à la demande pour les décideurs.
- Groupe de discussion avec droits d'accès échange et partage de l'information ; chacun profite des informations récoltées par les autres.
- Possibilité de *push* SMS pour les membres du réseau.

***Pilotage plus pointu,* feed-back**

- Ciblage par rapport aux axes de développement de l'entreprise suivi des acteurs, thèmes les plus actifs et sources surveillées.
- Pilotage temps réel de l'activité de veille, grâce à des tableaux de bords contrôle et réorientation en fonction des objectifs.
- *Profiling* des utilisateurs en fonction des thèmes consultés adéquation entre informations collectées et informations consultées ; correspondre aux besoins des utilisateurs.

Le Salon i-expo sur l'information numérique traduit l'effervescence qui règne autour de ce domaine. Les principaux acteurs du marché sont : *Digimind (V-Strat), Autonomy (Agent Ware), Search (Verity), Arisem (OpenPortal4U), ARIST (Viginov Logic).*

5.3.2 Cas concret

5.3.2.1 TotalFinaElf

Un groupe comme TotalFinaElf figure parmi les précurseurs français dans ce type de projet. Comme le précise Christophe Binot, architecte des systèmes d'information et responsable du département Gestion et valorisation de l'information, durant son intervention au Cycle IES, la mise en place d'une démarche d'IES doit s'accompagner d'une cohérence dans l'architecture des systèmes d'information. Ainsi, pour compléter la création de groupes projets, les actions de sensibilisation, la désignation d'experts et le recrutement de spécialistes IES, un certain nombre d'outils furent mis en place pour transformer les systèmes d'information existants :

- veille terrain : VSTRAT de Digimind ;
- portail d'information métiers : Sagewave ;
- veille internet / intranet : Watch4U d'Arisem.

Cette architecture fédère l'ensemble des informations du groupe : concurrentielles, environnementales, connaissances et savoir-faire, compétences internes, commerciales et marketing.

D'autres entreprises suivent cet exemple en démarrant des projets similaires.

5.3.2.2 Giat Industries

Ainsi chez Giat Industries, où le projet Ginet (Giat Intelligence Network) vu le jour. Comme le spécifie Patrick Lier, DSI du groupe :

L'objectif est d'améliorer la compétitivité du groupe en harmonisant les processus de gestion des connaissances et en augmentant l'efficacité commerciale. Nous procédons par étapes. Le but dans un futur proche est d'étendre cet outil à l'ensemble du groupe.

Entretien DSI

Patrick Cansell responsable de l'information stratégique et initiateur du projet, explique que dans un premier temps, cette initiative est limitée à un périmètre restreint. La nécessité d'évaluer le retour sur investissement d'une telle démarche est une condition essentielle pour étendre le projet à l'ensemble du groupe et développer d'autres fonctionnalités[60].

---

[60] www.journaldunet.com, *Comment Giat Industries aménage une gestion des connaissances très « stratégique »*, 7 mai 2002.

Comme nous l'avons vu précédemment dans les phases successives du cycle du renseignement, nous retrouvons dans la méthodologie employée par Giat Industries une vision commune des processus et outils employés pour lancer une démarche d'IES.

En effet, comme le spécifie Patrick Cansell, « la problématique du groupe se concentre sur la connaissance et l'analyse du marché ». Par conséquent, une attention particulière est mise sur la sensibilisation des « capteurs » et le rôle primordial qu'ils jouent dans la démarche. « Nos collaborateurs, qu'ils soient commerciaux, logisticiens, qu'ils travaillent en production ou à la R&D, ont des connexions avec les marchés qui leur sont propres. Un technicien qui a passé six mois dans un pays aura des connaissances dont il ne soupçonne parfois même pas l'intérêt que nous pouvons en tirer ». Le système mis en place par Giat Industries est à la fois un portail thématique d'accès à l'information, mais également un référentiel de ce que l'entreprise sait du marché et que chacun peut contribuer à enrichir.

Grâce à un tel outil, certains points positifs sont déjà constatés :

- circulation de l'information améliorée ;
- diffusion plus précise aux opérationnels ;
- meilleure identification des experts, de leurs connaissances et de leurs compétences ;
- partage des expertises et des connaissances ;
- instrument de cohésion, qui accroît l'implication de chacun dans les projets commerciaux du groupe ;
- vecteur pour une démarche d'intelligence économique dont le but est la maîtrise de son environnement extérieur.

Certaines entreprises, au sein de leur direction des systèmes d'information, ont mis en œuvre d'autres initiatives intéressantes. À titre d'exemple, le portail des collaborateurs de PSA Peugeot Citroën fédère l'ensemble des sites intranets des branches métiers du Groupe. Par ailleurs, un observatoire de l'internet a été créé, avec comme objectifs :

- le pilotage et l'animation du programme *e-business* du groupe ;
- la constitution d'un référentiel des initiatives du groupe sur internet ;
- l'identification et le suivi des initiatives internet hostiles : l'ensemble de ces initiatives est recensée et accessible à partir du portail des collaborateurs, ce qui peut aider à bâtir des scénarios adaptés en réponse aux attaques. Les dérives identifiées peuvent être de plusieurs sortes : consommateurs mécontents, désinformation ou trafic de noms de domaine, piratage de site…

Le portail des collaborateurs permet également à l'ensemble des employés d'accéder aux informations générales sur le groupe et aux grandes orientations stratégiques, un accès restreint étant réservé pour les informations les plus sensibles.

L'État est également conscient des possibilités offertes par les technologies de l'information et de la communication, comme le montre l'initiative de la Direction des relations économiques extérieures (DREE) durant son intervention au Cigref.

5.3.2.3 La DREE

Le contexte

L'implantation des entreprises françaises sur les marchés étrangers ne se fait pas sans difficultés, certaines affaires parfois étranges laissent supposer des actions de la concurrence. Les pays du globe dits sensibles ou à risques posent également des problèmes d'insécurité. Les faits sont réels et plus fréquents qu'on ne le pense : vols de micro-ordinateurs ou de serveurs, évènements survenant brusquement pour empêcher la signature de contrats, agressions, vols d'informations, virus dans les systèmes informatiques…

L'obligation de mettre en place une structure de gestion des informations pour minimiser les problèmes et ainsi faciliter l'internationalisation des entreprises s'est avérée nécessaire. Le ministère de l'économie et des finances a confié cette mission à la DREE qui a aussitôt créé un bureau de veille économique stratégique. Sa mission consiste à fournir aux entreprises et aux administrations les informations régaliennes et stratégiques, à partir des réseaux de correspondants permanents régionaux en liaison avec le réseau global.

La DREE est présente dans 135 pays, dans le cadre de 160 missions économiques, soit environ 2 000 personnes disséminées partout dans le monde. Pour fédérer le formidable réseau d'informations d'une telle structure, l'utilisation d'un portail intranet a été adoptée. La mise en place de cet outil a permis de fédérer l'ensemble des informations réparties sur les sites.

Le processus

Dans chaque région, les meilleurs experts dans les domaines clés de l'exportation sont désignés. Chacune de ces personnes (capteurs de rang 1) est elle-même en relation avec une dizaine de correspondants dans d'autres pays (capteurs de rang 2). L'équipe du siège (5 personnes) s'appuie donc sur ce réseau de capteurs de rang 1 pour filtrer les informations de rang 2 et ainsi ne faire remonter que les informations les plus pertinentes. La parfaite connaissance des environnements dans lesquels

évoluent les experts (les missions sont implantées dans les pays depuis 40 ans) donne aux informations recueillies une fiabilité avérée. La structure en réseaux sectoriels permet de :

- partager et capitaliser les connaissances au sein du réseau ;
- répondre aux besoins d'information des entreprises et des administrations ;
- participer à la réflexion stratégique des entreprises et des administrations ;
- accroître l'expertise sectorielle de la DREE.

La mise en place de l'intranet

La mise en place de cet outil s'est avérée nécessaire pour accroître la rapidité de circulation de l'information (collecte, traitement, stockage et diffusion). Outre les performances, la communication interne entre les différents experts s'est trouvée accrue de façon assez significative. Les décalages horaires ne permettant pas toujours de joindre les personnes par téléphone…

- utilisation systématique de documents numérisés (GED) ;
- mise en place d'un processus de gestion de la connaissance ;
- organisation de la gestion documentaire (référencement, formatage …) ;
- travail en commun ou en réseau.

Le forum : une zone privative permet aux experts d'échanger leurs idées sur des sujets particuliers. Cet outil de travail en réseau a également permis à des gens qui ne se connaissaient pas de travailler ensemble.

Aujourd'hui, de nombreuses entreprises du CAC40 font appel aux services de la DREE en matière d'informations. Ces missions représentent 70 demandes par an pour les entreprises, pour des domaines bien spécifiques et une centaine pour les administrations. Le système mis en place par la DREE peut parfaitement s'adapter aux entreprises dont les filiales sont implantées partout dans le monde.

Les systèmes d'information des grands groupes sont parfois extrêmement complexes. Certains possèdent plusieurs centaines d'intranets, des technologies vieillissantes, des bases de données éparpillées, mal structurées…. Par conséquent, la mise en place d'une démarche d'IES constitue un véritable projet d'une ampleur parfois sous-estimée. Car choisir de démarrer un tel projet, c'est analyser l'ensemble des flux informationnels, déterminer les blocages, comprendre les processus et parfois remettre en cause les systèmes

d'information existants ou dénoncer une organisation inadaptée au management de l'information.

5.4 Un système d'information adapté à l'intelligence économique

La mise en place d'une démarche d'intelligence économique efficace passe obligatoirement par une réflexion sur l'organisation interne et sur les systèmes d'information. En effet, il a été prouvé que l'organigramme traditionnel (par grandes fonctions de l'entreprise) est celui qui permet le moins à l'intelligence économique de s'implanter.

Enquête de l'IHEDN[61]

Cette observation faite par l'IHEDN confirme les analyses effectuées par P. Baumard et J.-A. Benvenuti sur l'impact des systèmes d'information sur la compétitivité de l'entreprise. Ce chapitre s'inspire de leurs écrits et reprend une grande partie de leurs conclusions.

5.4.1 Définition

Pour Patrick Romagni et Valérie Wild, la définition d'un système d'information adapté à la démarche d'intelligence économique est la suivante :

« Ensemble organisé de procédures permettant, à tout moment, de donner aux décideurs une représentation de la place de l'entreprise dans son environnement et sur son marché. Il produit de l'information pour assister les individus dans les fonctions d'exécution, de gestion et de prise de décision[62]. »

Il doit :

- faciliter les décisions : permet d'automatiser un certain nombre de décisions ou mettre à disposition des décideurs des éléments nécessaires à la prise de décision ;
- coordonner les actions par le traitement de l'information ;
- stocker de manière durable et stable les informations ;
- pouvoir traiter : fonction la plus importante du système d'information car il entraîne la création d'informations directement utilisables par les décideurs.

5.4.2 Dysfonctionnement des systèmes d'information dans le cycle du renseignement

De nombreux systèmes d'information d'entreprises ne sont pas adaptés pour faire face aux marchés actuels, turbulents et peu contrôlables et par conséquent peu enclins à supporter une démarche d'IES. Conçus pour des environnements stables et

[61] *op. cit.*
[62] Romagni Patrick et Wild Valérie, *L'intelligence économique au service de l'entreprise*, Les Presses du Management, 1998.

maîtrisés, ils sont bâtis sur des schémas organisationnels verticaux de plus en plus complexes qui ne permettent pas de réagir rapidement aux fluctuations. Parce qu'elles paraissent inadaptées au développement d'une politique de management de l'information, composante essentielle du pouvoir compétitif de l'entreprise, ces entreprises ne sont pas efficaces dans une démarche d'IES, et ce pour plusieurs raisons :

- cloisonnement de l'information ;
- mauvaise circulation de l'information et rupture dans le cycle du renseignement ;
- ralentissement des prises de décision ;
- liberté et autonomie décisionnelle des opérationnels limitées ;
- centralisation de la « production de connaissance ».

Conçus pour améliorer la fluidité des entreprises, les systèmes d'information en accentuent plus souvent l'inertie, entraînant des dysfonctionnements dans le cycle du renseignement[63].

Collecte

Constat

- Trop d'attention portée au recueil et au stockage des données.
- La quantité est privilégiée plutôt que la qualité.
- Rigidité des modèles imposés par le système.

Conséquences

Cet excès de modélisation confère un sentiment de contrôle induit par une récolte importante de faits, ce qui constitue une résistance aux données nouvelles et réduit les capacités d'interprétation. La sensibilité face aux informations pertinentes s'en trouve diminuée, les structures en place sont peu sujettes aux remises en cause et ne suscitent pas l'émergence de nouveaux projets de systèmes d'information.

Traitement

Constat

- La sûreté opérationnelle du système de traitement est privilégiée au détriment de sa diversité ou de sa versatilité.
- Le système est souvent imité d'une application d'un concurrent.
- Les schémas d'analyse sont standardisés et les traitements spécialisés par fonction.

[63] Inspiré de Baumard Philippe et Benvenuti Jean-André, *Systèmes d'information et compétitivité*, InterEditions, 1998.

L'environnement généralement perçu comme stable et protégé entraîne un sentiment de quiétude et une résistance à l'incertitude. Le système d'intelligence, inspiré d'un concurrent, minimise la culture d'entreprise, et génère des angles morts.

Conséquences

- Impossibilité de changer les processus décisionnels.
- Désir de conformité et refus d'expériences trop originales.
- Études approfondies perçues comme une perte de temps.
- Une vision en tunnel.

Circulation

Constat

- Le système d'information accentue le découpage vertical de l'organisation.
- Le système d'information accentue la spécification fonctionnelle.
- Le système d'information accentue la centralisation et l'accumulation exagérées de données.

Conséquences

- La remontée de l'information est bloquée, l'expertise reste subordonnée et isolée.
- La production de connaissances augmente, mais l'interopérabilité, interne et externe, diminue.
- Les décideurs sont débordés par l'excès de données, la centralisation cognitive est déconnectée des réalités locales.
- Difficulté pour mettre en place une communication transversale.
- Le manque d'interopérabilité des systèmes d'information ne favorise pas les échanges constructifs entre les différents métiers.

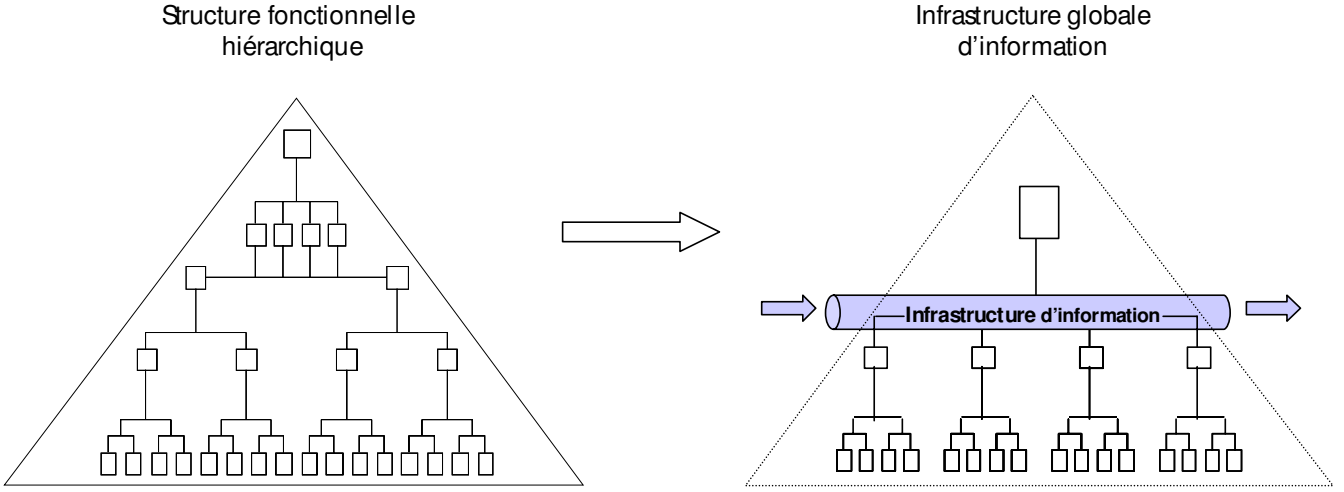
De nombreux systèmes d'information trop rigides et peu malléables ne facilitent pas l'implantation d'une culture cognitive sur laquelle reposerait la démarche d'IES. Loin de fluidifier et d'harmoniser les flux informationnels par le développement de réseaux transverses, ils augmentent le cloisonnement des architectures verticales, sclérosant ainsi les étapes du cycle du renseignement et réduisant par conséquent la capacité décisionnelle de l'entreprise.

5.4.3 Les structures transversales propices au développement de l'IES

Les systèmes d'information peuvent permettre à l'organisation d'optimiser ses investissements en fournissant au décideur les outils de coordination entre les actions des diverses unités de l'organisation. Cette « coordination horizontale » doit s'expliquer pour plusieurs raisons :

- chaque objectif ne peut être totalement isolé des autres ;
- chaque information prise en compte pour un projet peut intéresser une ou plusieurs autres entités ;
- chaque équipe a besoin des connaissances acquises par l'ensemble de l'entreprise.

Parce que la compétitivité de l'organisation dépend de sa capacité à gérer de manière efficace des processus transversaux entre ses différents domaines stratégiques, l'organisation de l'entreprise est fonctionnellement transversale. Pour permettre une gestion optimale de la connaissance, *elle doit s'appuyer sur une infrastructure informationnelle* dont les systèmes d'information constituent la clé de voûte. À cet effet, il est nécessaire d'évoluer d'une architecture verticale vers une architecture transversale qui facilitera le management global de l'information et par essence même l'implantation du concept d'IES.



Source : P. Baumard et J.-A. Benvenuti

Figure 26 : Passage d'une structure fonctionnelle à une organisation par processus[64] *.*

[64] Inspiré de *Systèmes d'information et compétitivité*, Baumard Philippe et Benvenuti Jean-André, InterEditions, 1998.

À partir d'une architecture modulaire et évolutive structurée autour des projets de l'entreprise, l'infrastructure informationnelle permet :

- de réduire les nombreuses coordinations verticales en diminuant les échelons hiérarchiques ;
- une meilleure surveillance de l'environnement des unités décentralisées ;
- un décloisonnement par une communication transversale ;
- des relations axées sur la complémentarité des métiers ;
- une stratégie informationnelle insufflée par la base (oriente la stratégie de la firme) ;
- une meilleure adaptation aux mouvances du marché.

Cette analyse confirme l'émergence de plates-formes d'information et l'enracinement de la stratégie dans les systèmes d'information. La démarche d'IES s'inscrit alors dans le schéma global du système d'information stratégique de l'entreprise.

Dans une étude réalisée auprès de cent cinq DSI, A.-L. Lederer et V. Sethi[65] définissent les systèmes d'information stratégiques (SIS) comme l'ensemble des applications informatiques qui assistent l'organisation dans la poursuite de ses plans et de ses objectifs stratégiques. Autrefois plus proche de ce qu'on appelle aujourd'hui un système d'intelligence économique, les grandes firmes tendent aujourd'hui à considérer le système d'information organisationnel dans son ensemble comme le SIS de l'organisation. Le tableau ci-dessous offre une synthèse des résultats de cette étude.

	Domaines d'intervention des SIS de l'organisation		
	Gestion de l'organisé (structures) et de l'organisant (processus)	**Gestion de la connaissance**	**Soutien de la stratégie**
Propriétés	Développement d'une infrastructure d'information	Système de représentation et d'identification des capitaux intellectuels.	Enracinement de la stratégie dans le système d'information.
Moyens	Intranets / Extranets. Gestion par processus.	Data Warehouse, SIG, Groupware, etc…	Système d'information stratégique.
Buts	Interopérabilité.	Capitalisation.	Synchronicité.

Source : P. Baumard et J.-A. Benvenuti

Figure 27 : Axes de la planification stratégique des systèmes d'information compétitifs.

[65] Lederer A.-L. et Sethi V., *Key Predictors of the Implementation of Strategic Information Systems Plans*.

5.4.4 L'exemple de France Télécom et de l'Aria[66]

Lorsque l'on parle de plate-forme de gestion de l'information ou de systèmes d'information d'intelligence économique, l'initiative la plus marquante est celle de France Télécom avec l'Aria. Faisant figure de modèle en matière d'intelligence économique, ce projet prouve que les systèmes d'information constituent la « charpente » de ce concept et représentent l'avenir en matière d'outils d'aide à la décision. La plate-forme conçue par l'Aria repose sur l'exploitation optimale du cycle du renseignement, grâce aux technologies de l'information qui permettent :

- de gérer de façon centralisée une somme considérable d'informations venant de l'ensemble du groupe ;
- de diffuser rapidement les informations stratégiques dans l'entreprise, par réseaux ;
- d'assurer une sélectivité et une personnalisation des informations transmises.

France Telecom : le développement de l'intelligence économique

«…En 1995, le Directeur général du Groupe s'émeut du problème de la maîtrise de l'information stratégique, à la fois en termes de coûts, de protection de l'information et de partage de la vision stratégique des acteurs du développement de France Telecom. Il me confie alors une étude pour repérer les producteurs et les consommateurs de l'information stratégique au sein du Groupe. Cette enquête a suscité la création d'Aria, un réseau pour l'information active. Aujourd'hui, l'Aria fédère les productions d'environ 70 observatoires au sein de France Telecom, et traite 1000000 d'informations par jour, sur une plate-forme de très haute technologie, capitalisant les productions internes, captant les ressources externes et distribuant l'information auprès de 5000 personnes, habilitées à avoir accès aux documents classifiés.

Le bénéfice d'un système d'intelligence économique pour l'Entreprise

Le fondement de l'intelligence économique consiste à :

- Connaître ses clients, ses marchés, les acteurs, produits et services de son domaine et des autres domaines économiques ;
- Permettre une performance collective de l'entreprise en termes de décision, grâce aux outils de personnalisation de l'information ;
- Permettre une vision stratégique commune avec une organisation centralisée ;
- Réunir l'ensemble des productions sur un site, exploité au plan local par l'Entreprise.

….

[66] Propos de Daniel Cade, France Télécom, extraits des actes du colloque du 25 janvier 2001, « Intelligence et défense économiques au service du développement économique », organisé par le ministère de l'économie, des finances et de l'industrie, à l'IHEDN. Extrait recueilli dans Levet Jean-Louis, *L'intelligence économique, mode de pensée et mode d'action*, Economica, 2001.

…

Le bénéfice collectif en termes économiques

La décision de création de l'Aria a été validée par le Président de France Telecom mais il était important de connaître le coût et les bénéfices d'une telle mesure. Le premier retour sur investissement est lié à la performance du système d'accès à l'information. Nous avons pu mesurer qu'un gain d'un quart d'heure par jour pour les 5000 utilisateurs du réseau dans la collecte de l'information correspond à un gain financier de 75 millions de francs. Par ailleurs, nous réalisons des économies d'échelle considérables dans l'achat des sources d'informations. Enfin, les acteurs locaux sont beaucoup plus performants dans la prise de décision.

Le bénéfice individuel

L'intelligence économique nécessite un ensemble d'outils importants pour offrir un accès personnalisé à l'information à l'ensemble des acteurs de l'Entreprise. Le bénéfice individuel est lié au sentiment d'appartenance et d'identification à des communautés de pratiques, grâce à l'utilisation de ces outils. Enfin, l'intelligence économique permet d'acquérir des outils performants de recherche d'informations.

Les facteurs de réussite

Les clés de succès de la réussite d'un projet d'intelligence économique au sein de notre entreprise sont les suivantes :

- La réussite suppose la présence d'un sponsor de niveau élevé dans l'Entreprise (un Directeur de plan de la stratégie, un Directeur financier…) ;
- Elle nécessite une étude approfondie des pratiques des réseaux déjà en place dans l'Entreprise ;
- Elle requière l'établissement des objectifs de performance économique pour l'Entreprise (l'Aria permet à France Telecom de gagner 150 millions de francs contre un budget annuel de 50 millions de francs) ;

Elle appelle la mise en place d'une plate-forme haut de gamme d'applications et de services ».

5.5 Les systèmes d'information, cible et vecteur offensif

« Il ne faut pas espérer que l'ennemi n'attaquera pas, mais compter sur le fait que l'on est dans une position inattaquable. »
Sun Tsu (L'Art de la guerre)

La mise en place d'une démarche d'IES passe obligatoirement par une analyse rigoureuse sur la sécurité des systèmes d'information. Les rapports sur ce sujet, rédigés par le Cigref, donnent un panorama exhaustif des différents types d'attaques pouvant menacer l'infrastructure informationnelle des entreprises. Il est souhaitable de s'y replonger pour avoir de plus amples détails sur la sécurité informatique.

À travers ce chapitre, il s'agit de montrer que la sécurité des systèmes d'information constitue une composante transversale de la démarche d'intelligence économique et stratégique et qu'à ce titre il s'agit de ne pas la négliger. Parce qu'ils contiennent les données et les font circuler, les systèmes d'information

représentent à la fois une cible de choix et une arme redoutable. Bâtir une politique de sécurité rigoureuse, c'est non seulement connaître les menaces pour s'en prémunir, mais aussi analyser les techniques d'attaques informationnelles pour être à même de les dépister, voire de s'en servir.

5.5.1 Des menaces bien réelles

1990, Apple suspecte un de ces anciens employés d'avoir volé une partie des codes informatiques utilisés pour concevoir le design *des Macintosh. Des copies de ces programmes ont été envoyées, par un réseau, à des développeurs de logiciels ainsi qu'à plusieurs journaux professionnels.*

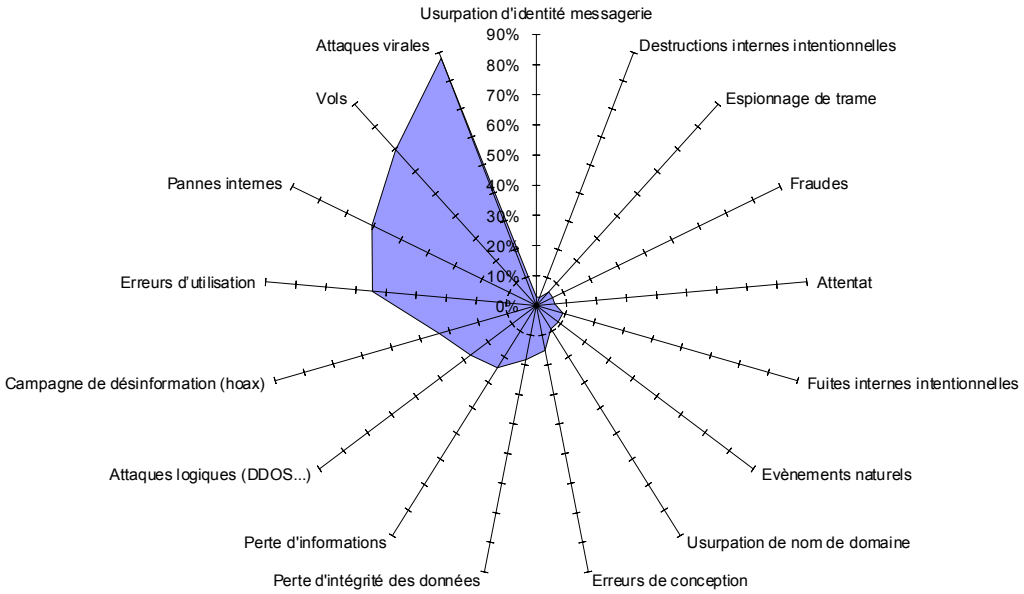
Un pirate informatique est parvenu à s'introduire dans le réseau administratif de l'opérateur Worldcom, cinq fois en deux mois. Celui-ci a repéré une faille de sécurité sur l'un des serveurs web de l'entreprise qui lui a permis d'accéder à son réseau administratif.

Après la marée noire de l'Erika, Total est à nouveau visé par une action d'internautes mécontents du prix de l'essence. Un appel au boycott de toutes les stations Total a circulé intensément sur le réseau en septembre 2000[67]*.*

Comme le montre ces exemples, ainsi que ceux qui suivront, dont la plupart sont tirés de l'ouvrage *L'infoguerre, stratégie de contre-intelligence économique pour les entreprises*[68], le danger peut venir de partout et avoir différentes formes. La dernière enquête réalisée par le Cigref, auprès de ses membres, confirme ce constat.

[67] www.hoaxbuster.com.

[68] Guichardaz P., Lointier P. et Rosé P., *L'Infoguerre, stratégie de contre intelligence pour les entreprises*, Dunod, 1999.



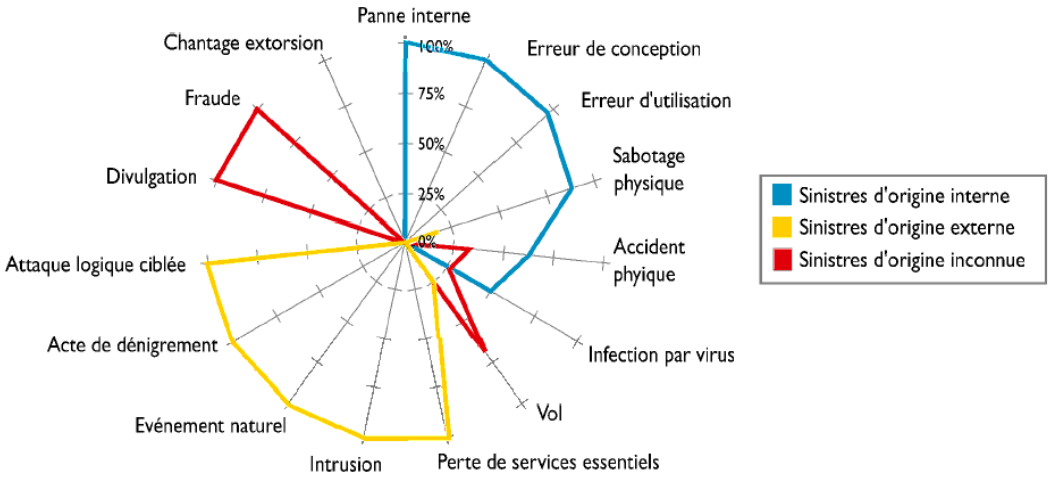
Source : Cigref

Figure 28 : Principales attaques subies en 2001-2002 par les membres du Cigref[69].

Malgré les erreurs d'utilisation internes et les négligences, qui demeurent majoritaires, les attaques volontaires et délibérées ne sont pas négligeables. Les résultats obtenus par le Cigref montrent qu'elles existent bel et bien, et sont plus fréquentes qu'on ne le pense : virus, vols de données, désinformation, attaques logiques… Le Clusif[70], dans son étude sur la sinistralité (2001), estime que les agressions ayant le plus fort impact sont les attaques logiques.

Mais leur étude a également mis en évidence l'origine omnidirectionnelle des incidents qui ont lieu sur les systèmes d'information. Les menaces externes sont la source des attaques les plus insidieuses car, même si elles demeurent minoritaires, il suffit d'une agression parfaitement ciblée, pour causer des troubles importants dans le système d'information concerné.

[69] Cigref, « Sécurité des systèmes d'information – Quelle politique globale de gestion des risques ? », Rapport, 2002.
[70] Clusif, « Études et statistiques sur la sinistralité informatique en France », Rapport, 2001.



Source : Clusif

Figure 29 : Corrélation entre la nature des incidents et leur origine.

Ces études mettent également en évidence les attaques de plus en plus importantes de désinformation, autrement dit d'utilisation offensive de l'information : contrefaçon, atteinte à l'image de marque, rumeur… Ces constatations confirment le positionnement des systèmes d'information comme cible prioritaire de l'infoguerre.

5.5.2 Les systèmes d'information cibles de l'infoguerre

Les systèmes d'information traitent l'information, la stockent et la font circuler. Pillés ou paralysés, ces centres névralgiques constituent des points faibles qu'il s'agit de protéger. Car, si la guerre de l'information n'est pas que de nature informatique, une majorité des actions qui sont menées touchent les systèmes d'information ou les utilisent comme vecteurs d'attaque.

Comme le précise Daniel Martin, conseillé spécial du directeur exécutif de l'OCDE, le système d'information, pièce maîtresse de l'entreprise, peut être l'un des principaux objectifs de ces attaques, qui pour la moitié sont issues d'internet. L'effet dévastateur peut-être catastrophique pour l'entreprise, puisque 60 % des PME-PMI qui subissent un sinistre disparaissent dans les cinq ans.

Cycle IES

Globales, ces menaces laissent présager des scénarios inquiétants. N'importe quel organisme ou individu peut en être la cible :

- *l'État* (services gouvernementaux, systèmes d'information fiscaux, financiers, de santé, réseaux télécommunication, contrôle aérien, etc.) ;
- *les entreprises* (personnels, produits, fournisseurs, clients…) ;
- *les individus* (vol d'identité, de données personnelles, de numéro confidentiel, numéro de carte de crédit…).
-

Le témoignage de la DREE confirme l'augmentation des problèmes de sécurité notamment dans un contexte international. Du vol d'ordinateurs portables dans les hôtels aux agressions, virus, vols de données ou encore disparition ou destruction de serveurs. Les comptes rendus des chefs de missions économiques sont accablants et montrent la détermination des « agresseurs ».

Cycle IES

5.5.3 Les attaques

Comme nous l'avons vu dans le chapitre 3, les stratégies de guerre de l'information sont de trois types : la guerre pour, par et contre l'information. Dans chacune de ces catégories, les systèmes d'information peuvent être une cible privilégiée. Même si l'on estime que plus de 50 % des fraudes informatiques sont d'origine interne, on assiste à un rééquilibrage au profit de menaces externes. Aujourd'hui, la délinquance informatique s'attaque beaucoup plus au contenu qu'au contenant.

5.5.3.1 Pour l'information

L'apparition d'internet et de ses dérivés (intranet et extranet), des réseaux, la tendance à la décentralisation des systèmes d'information a considérablement accru le nombre de fraudes informatiques. La valeur stratégique de l'information a également modifié les objectifs. Le matériel n'a plus guère d'intérêt, on vole un micro-ordinateur bien plus pour l'information qu'il contient ou celles auxquelles il donne accès, que pour la valeur de l'objet.

L'information circule plus vite et plus largement. Les menaces sont dorénavant plus diffuses et difficilement identifiables. Aujourd'hui, les actions individuelles ont laissé place aux actions collectives beaucoup plus délicates à contrer.

Ce changement de comportement a été mis en évidence en 1998 par les responsables de la sécurité des systèmes d'information de la marine américaine, dont les ordinateurs sont des cibles privilégiées d'attaques[71].

L'augmentation des attaques

L'étude réalisée cette année par le *Computer Security Institute*[72] auprès des entreprises américaines classe dans l'ordre des sources d'attaques les plus fréquentes : les *hackers*, employés insatisfaits, entreprises nationales concurrentes, entreprises étrangères, les gouvernements étrangers.

Les techniques, de plus en plus sophistiquées, nécessitent de moins en moins de compétences. Cet état de fait explique la cause d'augmentation des *hackers* potentiels (estimé de 35 000 à 50 000 dans le monde, susceptibles de pénétrer des systèmes d'information avec l'aide d'outils). En 1997, l'enquête réalisée par le cabinet de conseil Ernst & Young estimait à 38 % des entreprises interrogées celles ayant été victimes d'espionnage économique et industriel.

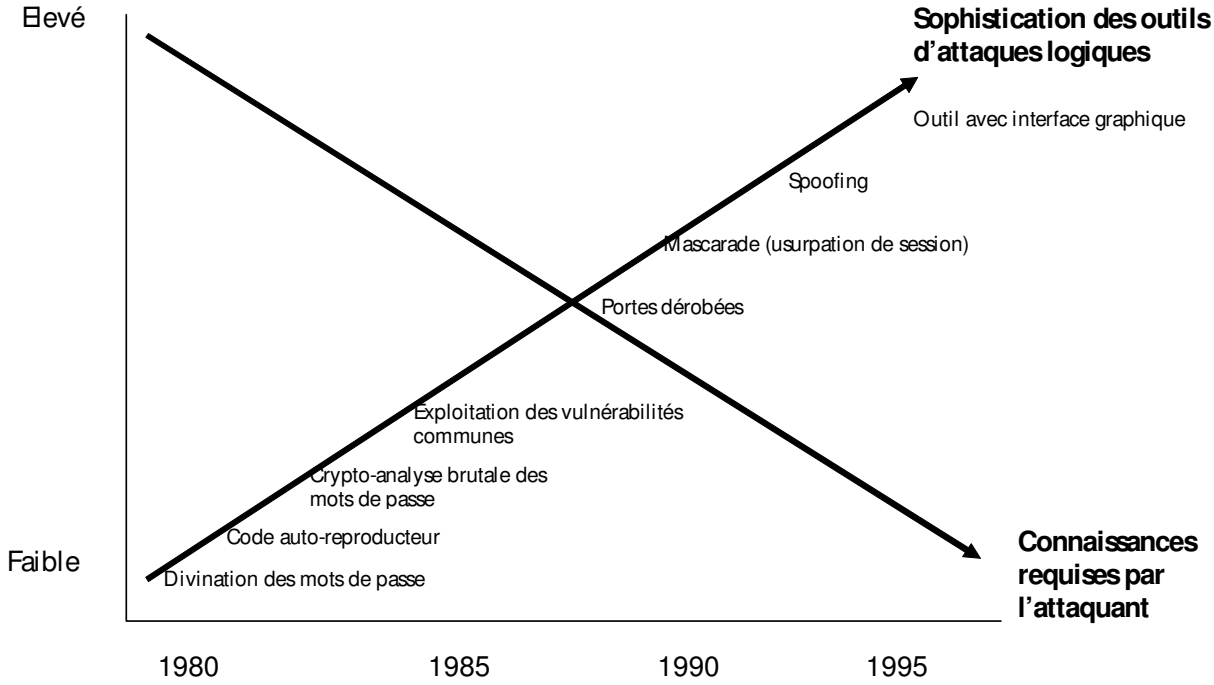


Figure 30 : Des procédures d'attaque qui nécessitent de moins en moins de compétences[73].

[71] *op. cit.*
[72] 2002 CSI / FBI Computer Crime and Security Survey (vol.III, n°1).
[73] Inspiré du Department of Defense (US), *L'Infoguerre, stratégie de contre-intelligence pour les entreprises*, Dunod, 1999.

Internet, la porte d'entrée…

Internet a augmenté les possibilités et le nombre d'attaques logiques. Cette réalité est confirmée par l'enquête 2002 du Computer Security Institute, qui cite internet comme le vecteur d'agression le plus utilisé.

- Les sites d'entreprises

Toutes les entreprises ont un site web sur lequel elles mettent des informations. Parfois développé par des sociétés de service, est-on sûr que l'information qui y est divulguée ne puisse pas compromettre la compétitivité de l'entreprise ?

Le Département de la défense américain a dû revoir le contenu de son millier de sites web pour identifier des informations qui pourraient être sensibles, non pas en tant que telles, mais en complément d'autres informations, obtenues par d'autres sources. Il a notamment été trouvé des données sur les équipements militaires, des numéros de sécurité sociale ou des adresses personnelles[74]*.*

- Les sites factices

Il est devenu relativement simple de créer des sites web…

Certaines personnes n'hésitent pas à créer de faux sites web où il est demandé aux visiteurs de rentrer leur nom et un mot de passe (action classique sur de nombreux sites). Partant de l'hypothèse qu'une personne qui se connecte au site fournit son vrai nom et souvent le même mot de passe, il est très facile de réutiliser ces données pour se connecter sur d'autres sites.

Cycle IES

- Le bavardage électronique

Forums de discussion, listes de discussion ou *chats*, les moyens d'échanges d'idées ne manquent pas sur le net. Ouvertes à tous, ces réunions virtuelles sont souvent utilisées pour débattre de thèmes particuliers. Spécialistes, amateurs éclairés ou alors désinformateurs potentiels et experts en intelligence économique. Car, si de nombreuses rumeurs informationnelles naissent par ce biais, les spécialistes de la contre-intelligence se servent de ces lieux de discussion pour détecter des attaques, des agresseurs ou préparer des actions de contre-offensive. Effectivement, les logiciels permettent de balayer les archives et d'établir un historique des contacts. Il est alors possible d'identifier une grande partie des listes et forums auxquels participe la cible (cf. Panorama des outils, Chapitre 4).

[74] *op. cit.*

Des attaques souvent indétectables

L'augmentation du nombre de *hackers*, le perfectionnement des logiciels et l'immensité du cyberespace rendent quasiment indétectables les attaques lancées contre un système d'information. Les chiffres sont éloquents : Winn Schwartau, qui dirige le cabinet de conseil en sécurité Interpact[75], avoue que sur les 2 300 tests de pénétration que ses équipes ont réalisés chez ses clients, seuls deux ont échoué[76].

Lors de la conférence Infowar de 1996, Robert Ayers, l'un des responsables de la sécurité des systèmes d'information du Département américain de la défense avait indiqué que sur 18 000 tests d'intrusion que ses services avaient réalisé en trois ans, 88 % avaient été réussis, 96 % n'avaient pas été détectés.

5.5.3.2 Par l'information

Dans les campagnes de désinformation, internet constitue le canal informationnel rêvé. Les exemples affluent et certaines entreprises se trouvent confrontées à de réels problèmes de crises informationnelles. Car aujourd'hui, n'importe qui peut raconter se qu'il veut (site, forum…), la technologie actuelle permettant de falsifier de nombreuses sources (photos, adresses électroniques…). Dans ce contexte, le rapport du faible au fort, prend sa pleine mesure. Comme le précise Alain Pajot, directeur associé de la société de veille Startem[77], dans Le Monde Interactif : *« Un individu a pour la première fois dans l'histoire de l'humanité, le pouvoir de déstabiliser une multinationale ».*

Au vu des possibilités offertes par internet, certaines organisations se sont spécialisées dans les actions de désinformation et de rumeur. Ainsi, RTMark, une organisation qui a déclaré la guerre à la mondialisation, s'est rendue célèbre pour son implication dans l'affaire eToys.

A l'actif de RTMark, constitué depuis 1993 d'une demi-douzaine de membres, une action d'éclat contre le fabricant de jouets eToys, qui a obligé ce dernier à lâcher prise contre une autre société, dont il essayait de récupérer le nom de domaine. RTMark invitait en ligne les internautes à jouer à « tuer eToys » pour que le cours en bourse s'écroule[78].

Les grands groupes français ne dérogent bien évidemment pas à la règle et certaines entreprises en font régulièrement les frais.

[75] www.interpactinc.com.
[76] *op. cit.*
[77] devenue depuis le groupe Datops (www.datops.com).
[78] Le Monde Interactif, « Du simple canular à la désinformation orchestrée », 23 mai 2001.

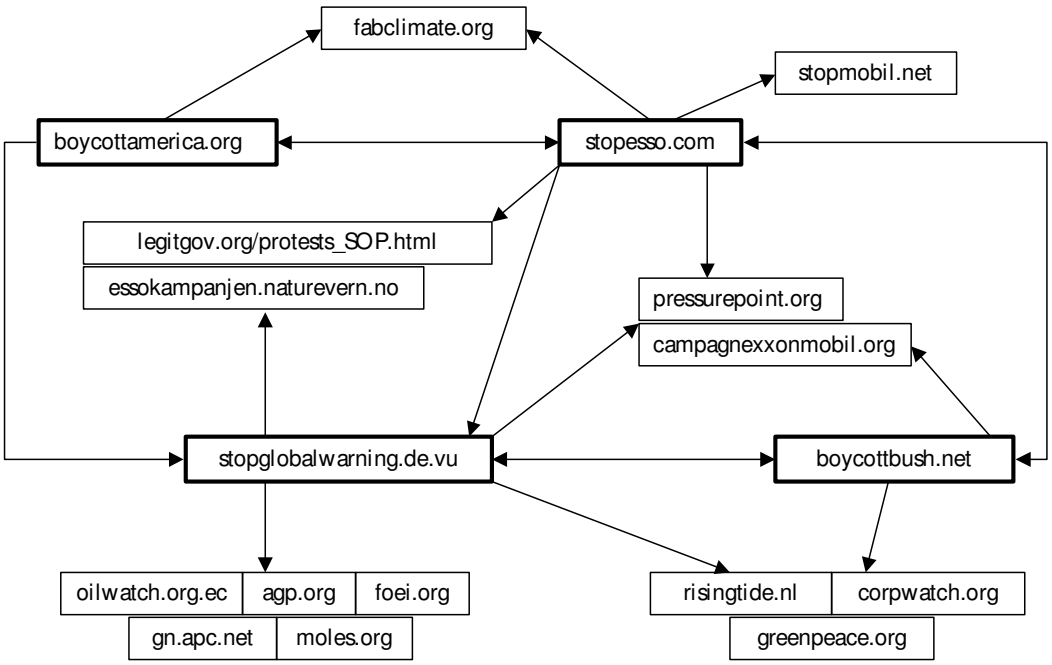
TotalFinaElf embarrassé par une campagne de désinformation en ligne, sur un prétendu échange de courrier électronique entre ses cadres dirigeants[79].

Ou encore, le groupe Danone qui a eu à subir ce genre d'attaque à travers un site diffamatoire.

11 avril 2001, le site « jeboycottedanone.com » voit le jour sur internet. Les médias en parlent, un premier constat d'huissier est fait à la demande du groupe. Le 4 juillet, les auteurs de ce site sont condamnés à verser 60 000 F (9 150 €) de dommages et intérêts à Danone. Un logo détourné et des images de « P'tits Lu » baignant dans une marre de sang constituant une contrefaçon pour la marque.

Ces attaques, lorsqu'elles sont menées par des organisations structurées et motivées, peuvent être d'une grande efficacité. Bâti selon une véritable stratégie, le schéma ci-dessous, est un exemple du réseau international qu'il est possible de mettre en place. Il représente l'ensemble des sites anti-Esso qui se sont développés depuis quelques années[80] :

Réseau anti-Esso



Source : École de guerre économique

Figure 31 : Représentation du réseau anti-Esso.

[79] www.haoxbuster.com

[80] École de guerre économique (promotion 2002), « La guerre de l'information du faible au fort : le cas « Vermillion, prospection pétrolière dans la vallée de Chevreuse » *in* Harbulot Christian et Lucas Didier, *La Guerre cognitive*, Lavauzelle, 2002.

Beaucoup d'actions de désinformation s'éteignent aussi vite qu'elles ont vu le jour. D'autres, en revanche, sont rapidement diffusées, capables de causer des effets néfastes aux personnes, groupes, organisations contre lesquelles elles sont ciblées. Les deux exemples suivants concernent deux canulars (*hoaxes*) que la plupart d'entre nous avons reçus.

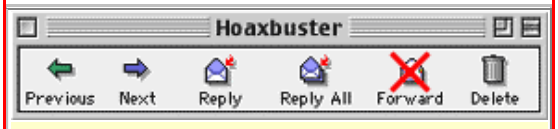
Exemples de désinformation par le net

Exemple 1

Piratage des portables, la rumeur revient à la charge

Victimes de leur succès, les téléphones portables font à leur tour l'objet de rumeurs de piratage à grande échelle. Un hoax très proche avait déjà fait le tour des messageries il y a quelques mois au sujet des téléphones fixes. Notre enquête auprès des différentes institutions citées dans le message (Office Central de Répression du Banditisme, France Télécom, Bouygues) nous confirme qu'il s'agit bien d'un hoax. Mais cette fois-ci, la désinformation se double d'une volonté délibérée de nuire. La société de télécommunications dont le numéro de téléphone est mentionné dans le texte est submergée d'appels et vient de porter plainte contre X. Ses responsables pensent à une vengeance.

LE HOAX DANS SON INTÉGRALITÉ



ATTENTION DANGER
Pour info aux détenteurs de portables !!!
Autre forme de piratage de la ligne portable.
Le correspondant laisse un message afin qu'on le rappelle au 01.41.45.54.14. Surtout ne pas répondre. Vos factures augmenteront sans commune mesure.
Cette information, communiquée par l'Office Central de Répression du Banditisme, est à diffuser le plus largement possible. Depuis quelques temps, des escrocs ont trouvé un système pour utiliser frauduleusement vos portables. Ils vous appellent sur votre GSM et se présentent comme le "provider" (Itinéris, SFR, Bouygues) auquel vous êtes abonnés. Ils vous demandent ensuite de composer un code qui est le 09# ou le 90# en vous expliquant qu'il sagit de vérifier le bon fonctionnement de votre portable.
NE COMPOSEZ SURTOUT PAS CE CODE ET RACCROCHEZ IMMEDIATEMENT.
Ils disposent d'un outillage permettant, grâce à ce code, de lire votre numéro de carte SIM. Il ne leur reste plus qu'à créer une nouvelle carte. Cette fraude se pratique à grande échelle.
Il est donc nécessaire de faire suivre cette information très
rapidement et de la diffuser au plus grand nombre (votre entourage, les particuliers, les entreprises, vos clients,...)

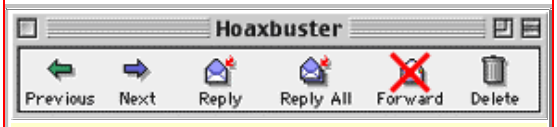
MERCI DE DIFFUSER AUTOUR DE VOUS
Information provenant du Ministère de l'Intérieur

Exemple 2

La CNIL utilise-t-elle les fichiers clients des fournisseurs d'accès ?

Depuis quelques temps, la rumeur circule à nouveau sur les newsgroups et via le courrier électronique. La Commission Nationale de l'Informatique et des Libertés (CNIL) aurait passé un accord avec l'Agence de Protection des Logiciels (APL) afin d'autoriser les éditeurs de logiciels à consulter les fichiers d'abonnés des fournisseurs d'accès à Internet. A ce jour et suite aux multiples démentis des parties, nous pouvons vous assurer qu'il s'agit bien d'un hoax.

LE HOAX DANS SON INTÉGRALITÉ



"La CNIL autorise l'Agence de Protection Logiciel (association d'éditeurs, d'auteurs, de distributeurs, etc...) à utiliser les fichiers des abonnés Internet afin de procéder à des contrôles de validité des applications utilisées sur les machines des abonnés. Actuellement seuls AOL, Wanadoo et Compuserve ont communiqué les fichiers abonnés. Aléatoirement il va y avoir des contrôles chez des particuliers.

Plus fort... Par ailleurs, l'APL attend l'autorisation de la CNIL afin de procéder directement à la consultation à distance via les providers Internet afin de vérifier la validité des applications installées. Tout serveur peut capter les identificateurs des machines qui le consulte et accéder aux versions des logiciels installés au travers de plug-in automatiquement chargés. Le recoupement avec le fichier utilisateurs est alors immédiat.

Pour finir l'APL a déposé une demande auprès de la CNIL visant à obliger les providers à lui communiquer la liste des abonnés qui téléchargeraient des logiciels contrefaits sur des sites pirates connus, le téléchargement n'étant pas répréhensible, il s'agit d'affiner la liste des personnes susceptibles d'être contrôlées ".

Source : www.hoaxbuster.com

5.5.3.3 Contre l'information

Les actions menées contre l'information vont s'attacher soit à la détruire, soit à empêcher son utilisation en neutralisant le réseau. Parmi les attaques les plus connues, nous retrouvons les bombes logiques, les dénis de service ou attaques logiques. Le rapport 2002 du Cigref sur la sécurité des systèmes d'information reprend dans le détail ces attaques.

5.5.4 Technologie et contre-intelligence

Toutes ces actions ne sont pas que d'origine individuelle ou interne. Le maintien des positions concurrentielles amène des entreprises à utiliser des méthodes de plus en plus « musclées ». La mise en place de faux sites web, de campagnes de désinformation sur le web, de manipulation d'informations, d'intrusion ou vol de données… toutes ces techniques peuvent être employées. Aujourd'hui, l'influence s'exerce également grâce au web.

Le net rassemble de nombreux facteurs susceptibles de favoriser la communication d'influence: une croissance de l'audience quantitative, la multiplication très forte des émetteurs d'informations, l'absence de contrôles et de règles. Internet est donc bien un terreau sur lequel peut facilement se développer et se propager une communication d'influence, c'est-à-dire manipulée et ciblée[81]*.*

Traiter, protéger, mais aussi contre-attaquer, l'utilisation des TIC s'inscrit également dans cette dernière action. La capacité des outils conçus aujourd'hui peut permettre de véhiculer de l'information dite « offensive » en influençant l'opinion de son entreprise auprès de l'opinion publique. De telles pratiques nécessitent, bien évidemment, de demeurer dans les limites de la légalité. Ainsi, en 2000, Thomson-CSF finalisait un ensemble d'outils particulièrement efficaces dont les principales caractéristiques furent présentées au salon IDT de la même année.

« Systèmes informatisés d'aide à la persuasion pour l'intelligence économique offensive », cette solution doit permettre d'aider les entreprises à gagner la bataille médiatique en facilitant la construction d'argumentaires persuasifs et la réfutation des attaques médiatiques des concurrents.

Thomson-CSF travaillait également sur d'autres projets : aide à l'argumentation pour la communication opérationnelle et « spéciale », aide à la détection de la désinformation, aide à la réfutation des arguments adverses. Ces travaux se poursuivent puisque le groupe Thales mène actuellement des projets soutenus par la DGA ou en cours de négociation.

[81] Rosé Philippe, « Quand l'intelligence économique devient offensive », Le Monde Informatique, 16 juin 2000.

Ainsi, plusieurs systèmes d'information d'aide à la prise de décision et d'assistance à la maîtrise des crises sont en cours de réalisation[82] :

- les projets de fouille de données Kalima : outils de datamining et de textmining qui permettront l'analyse décisionnelle de base de données hétérogènes et multiformes ;
- les projets de bases de données Idéliance : utilisation de l'intelligence artificielle et représentation des formations sous la forme de réseaux sémantiques ;
- ainsi que des projets comme Schopenhauer (système informatisé d'aide à la réfutation d'arguments), Gorgias (aide à la création de la mystification), etc.

Dans les domaines relatifs à la maîtrise des crises par la maîtrise de l'information, Thales Communications entreprend des travaux de recherche :

- le projet Mimesis : simulateur de crise ;
- le projet Ares : prévention, traitement et détection des crises ;
- le projet Sun Tzu : aide à la conception et à la validation des modes d'action indirects (stratagèmes et ruses de guerre) ;
- le projet Protagoras : détection des manipulations par analyse transactionnelle et psychologie sociale.

De là à s'inspirer de certains outils « défense » pour le secteur économique… il n'y a qu'un pas !

Les axes de recherche sur lesquels des groupes comme Thales s'orientent sont significatifs de l'implication grandissante des systèmes d'information dans l'intelligence économique offensive.

Garants du fonctionnement de l'entreprise, de la conservation de son savoir et de la circulation de ses connaissances, les systèmes d'information sont des cibles prioritaires qui doivent faire l'objet d'une attention particulière. Dans une démarche globale d'intelligence économique et stratégique, la sécurité des systèmes d'information est une nécessité. Les menaces peuvent être d'origines diverses : salariés, concurrents, consultants et prestataires, groupes terroristes ou mafieux, gouvernements étrangers... Pour et contre l'information, le développement d'internet et des logiciels associés a multiplié les attaques par l'information. Pour parer à ces actions, des techniques de recherche pointues sont nécessaires. Comme le confirme Philippe Caduc de l'Adit (Agence pour la diffusion de l'information technologique) :

[82] *in* Michel Claude, ingénieur Thales Communications, « Idées pour la défense et la sécurité », Agir, n° 13, hiver 2003.

« Les grandes entreprises françaises ont intégré internet comme un outil de déstabilisation. (…) Elles y surveillent leur présence, leur rayonnement. Pour un industriel, c'est difficile d'en parler. Mais ce serait vous mentir que de vous dire le contraire : oui, nous travaillons avec certains très grands groupes ». L'Adit a créé, en 1998, une cellule de veille de cinq personnes qui se consacre aux attaques à l'image sur internet et tente de passer tout le web au peigne fin. « Nous avons développé pour cela des logiciels qui permettent d'entrer dans des bases d'archives en ligne, de déceler l'apparition de termes, d'apprécier leur récurrence. » Mais ces recherches sont très coûteuses[83].

La démarche d'intelligence économique et stratégique s'inscrit dans un schéma global de management de l'information. Véritables supports et moteurs d'un tel projet, les systèmes d'information permettent de créer une infrastructure informationnelle intégrée au système d'information stratégique de l'entreprise. Conçue autour de solutions adaptées, de plus en plus pointues techniquement, cette infrastructure exploite au mieux chaque étape du cycle du renseignement et repose sur une architecture flexible et modulable. Facteur de compétitivité pour l'entreprise, un tel projet doit s'appuyer sur une infrastructure favorisant la culture de l'information. Surpassant le simple aspect technique, cette prise de conscience doit générer des interrogations sur l'organisation et le fonctionnement de l'entreprise.

Face aux menaces régulières, la démarche d'IES se conçoit dans un environnement protégé dépendant en grande partie des systèmes d'information. Les attaques informationnelles augmentent et touchent le contenu. Insidieuses, elles nécessitent la mise en place de techniques d'anticipation basée sur la détection des signaux faibles. Au cœur des trois phases de la démarche d'IES, les systèmes d'information ont un rôle prépondérant dans l'implantation et le déploiement du concept. Cette omniprésence des systèmes d'information doit permettre un début d'interrogation sur l'implication du DSI dans la démarche d'IES.

[83] « Du simple canular à la désinformation orchestrée », Le Monde Interactif, 23 mai 2001.

6 LE DSI, UN ÉLÉMENT MOTEUR DU CONCEPT D'INTELLIGENCE ÉCONOMIQUE ?

L'intelligence économique est l'affaire de tous au sein de l'entreprise, c'est une prise de conscience collective. Le DSI doit jouer un rôle dans la mise en place de ce concept. Car comme son nom l'indique, direction des systèmes d'information contient « information ». Par conséquent, le DSI intervient de manière prépondérante dans la gestion de cette information.

Entretien avec un DSI

6.1 Le DSI, du technicien au stratège

La dimension stratégique prise par les systèmes d'information a radicalement transformé le rôle et les responsabilités du « directeur informatique ». En vingt ans, le technicien est devenu un manager de projet pour se positionner aujourd'hui comme un véritable acteur de la stratégie de l'entreprise. Cette mutation est le résultat d'une évolution technologique et contextuelle rapide. En effet, l'ère de l'automatisation a laissé la place à l'ère du management informatique pour aborder aujourd'hui l'ère de l'informatique stratégique.

Selon *Le Monde Informatique*[84], aujourd'hui, les deux tiers des responsables informatiques dépendent directement de la Direction Générale. Cette prise de conscience des dirigeants positionne le système d'information comme la clé de voûte qui va consolider la stratégie de l'entreprise et permettre d'asseoir la démarche d'IES au sein de l'organisation. Face à cette mutation, le DSI doit apporter des solutions concrètes pour permettre à l'entreprise d'accroître sa compétitivité. Selon Philippe Baumard, les responsabilités actuelles qui incombent au DSI peuvent susciter une nouvelle appellation : d*irecteur du management des systèmes d'information (DMSI)*[85].

Le tableau traduit cette évolution du rôle et de l'horizon décisionnel des responsables des systèmes d'information.

[84] Le Monde Informatique, n° 744 du 28 novembre 1997.
[85] *op. cit.*

Niveau	RSI	Rôle	Horizon	Préoccupation	Epoque
Opérationnel	DI	Met en œuvre le système d'information	1 à 2 ans	Productivité	Ere de l'automatisation
Tactique	DSI	Conçoit le système d'information	2 à 3 ans	Rentabilité	Ere du management informatique
Stratégique	DMSI CIO	Participe à la définition des objectifs	Stratégie de la firme	Compétitivité	Ere de l'informatique stratégique

Source : P. Baumard

Tableau 8 : Évolution du rôle des responsables des systèmes d'information[86].

L'IES se positionne comme une composante majeure de la stratégie d'entreprise. Les nouvelles technologies ont donné une nouvelle dimension au concept, en permettant une gestion plus efficace de l'information et en développant la prise de conscience collective par une meilleure communication. Néanmoins, cette évolution technologique a fait émerger de nouvelles menaces contre lesquelles il est nécessaire de se protéger.

Aujourd'hui, comprendre la démarche d'IES et la mettre en place nécessite d'être à la fois :

- un technicien au fait des dernières innovations technologiques et des menaces en matière de sécurité ;
- un manager capable d'appréhender les processus métiers de son entreprise, de lancer des projets transversaux et de piloter l'ensemble des flux informationnels ;
- un stratège qui participe pleinement à la définition des objectifs du groupe et réalise l'adéquation entre les systèmes d'information et la stratégie.

6.2 Le DSI, expert et conseiller technique

La multiplication d'infrastructures globales d'information, tels que les portails d'information, nécessite de connaître parfaitement les possibilités et performances offertes par les solutions logicielles du marché de l'IES. En outre ces projets fédèrent généralement un ensemble d'outils qui touchent le groupe dans sa globalité. Les notions d'interopérabilité des différentes solutions induisent des complications techniques

[86] *op. cit.*

évidentes, car les solutions vendues aujourd'hui doivent s'imbriquer parfaitement dans le système d'information existant. Pour l'entreprise, il importe de posséder le bon interlocuteur, technicien et véritable architecte, qui puisse choisir les solutions adaptées mais également les mettre en œuvre. Cette personne doit :

- maîtriser parfaitement le système d'information existant, aussi bien concernant la technicité que les processus ;
- comprendre techniquement le produit qu'on lui propose, et faire les choix les plus judicieux en termes de coût, qualité et adéquation avec le système existant ;
- connaître les exigences et les besoins techniques des différents secteurs, branches de l'entreprise qui sont demandeurs ;
- harmoniser l'ensemble des initiatives techniques existantes : intranets, extranets, gestion des connaissances, gestion électronique de documents, *business intelligence*, gestion de la relation client ;
- effectuer une veille des technologies émergentes susceptibles d'améliorer et faire vivre le système.

Or personne, au sein de l'entreprise, n'est mieux armé que le DSI pour faire ces choix. À la fois conseiller et expert technique, il a un rôle prépondérant dans la mise en œuvre des outils et la sensibilisation des utilisateurs.

Technicien et architecte, ses connaissances lui confèrent également une légitimité en matière de protection de l'information. Parce qu'il est garant de la sécurité des systèmes d'information, il assure la pérennité du savoir et des connaissances de l'entreprise. Pour ces raisons, il ne peut faire abstraction des nouvelles menaces induites par le concept d'infoguerre. Conscient des risques, il doit s'informer et maîtriser ces notions. Par conséquent, là encore il peut jouer un rôle majeur :

- il identifie les menaces et détecte les attaques. Il met en place des produits de sécurité en adéquation avec les besoins ;
- il met en place les dispositifs techniques adaptés et sensibilise les utilisateurs ;
- il maîtrise les nouveaux risques liés à l'infoguerre. Il participe à la détection des signaux faibles et informe sur ces aspects ;
- il est un interlocuteur privilégié de la direction de la communication en matière d'actions de désinformation et d'attaques sur le contenu.

6.3 Le DSI, manager fédérateur de projets

Le positionnement transversal des systèmes d'information fait du DSI un chef d'orchestre de premier choix pour mettre en place des projets d'intelligence économique. Ses connaissances techniques et sa vision globale des processus de l'entreprise lui confèrent une solide approche des métiers et de leurs besoins. Dans ce cadre, il peut :

- piloter les flux d'information stratégiques et les optimiser ;
- fédérer l'ensemble des microprojets et initiatives éparses au sein du groupe ;
- coordonner les maîtrises d'ouvrage et maîtrises d'œuvre des différents domaines ;
- mener une réflexion sur ce qu'il est nécessaire de protéger et identifier les risques acceptables ;
- impliquer chacun dans la sécurité des systèmes d'information, quel que soit son rôle dans l'entreprise ;
- prendre en compte les menaces sur les systèmes d'information dans les contrats établis avec les prestataires extérieurs de confiance ;
- mettre en place une organisation adaptée (règles à suivre, modalités d'application, rôle de chacun) et réactive face aux scénarios de crise.

Il participe à l'organisation de la lutte contre les menaces liées à l'infoguerre, la désinformation, la contrefaçon[87] :

- désigne les responsables de la surveillance des médias numériques (actions de veille et d'attaques par l'information) ;
- met à disposition les ressources pour préparer une cellule web de crise ;
- permet la synchronisation des relais de communication ;
- optimise le traitement des remontées d'informations dans l'analyse d'images et d'opinions.

Les problèmes de déstabilisation ou de rumeur nuisent à l'image de marque de l'entreprise. Véhiculées ou amplifiées par internet, ces attaques peuvent être contrées par la direction de la communication qui peut préparer des discours adaptés. Néanmoins, anticiper ces attaques, c'est être en mesure de les détecter. Le DSI peut s'impliquer dans cette tâche en choisissant les outils adaptés (cf. chapitre 4), les collaborateurs « spécialistes » qui les mettront en œuvre, qui sauront détecter les signaux faibles. Cette connaissance des menaces et des parades, doit alors permettre de définir des possibilités de contre-offensive.

[87] Intervention de Pascal Lointier, président du Clusif, durant le Cycle IES du Cigref.

L'utilisation de la rumeur de manière contre-offensive requiert des compétences rares de spécialistes de la technologie. Ils doivent être capables de revenir à la source de la rumeur, mais aussi d'identifier par qui elle était manipulée, pour ensuite mieux passer à la contre-attaque, précise Sorbas von Coester, associé chez Salamandre, société de conseil en stratégie. Des experts en renseignement savent alors activer un réseau humain, auquel ils enverront la contre-information pour être sûrs qu'elle trouve un écho dans plusieurs médias crédibles qui la relaieront sans révéler leur source[88].

Dans les scénarios d'infoguerre, on dissocie de moins en moins le contenu du contenant. Le DSI parce qu'il lui faut appréhender toute la mesure des menaces peut, en collaboration avec les directions de la communication ou de la stratégie, apporter ses connaissances pour appréhender et détecter les menaces de guerre de l'information, mais aussi bâtir des solutions techniques adaptées aux scénarios de crise.

6.4 Le DSI, stratège et force de proposition

L'étendue des responsabilités du DSI a considérablement augmenté ces dernières années. Son champ d'activité ne se limite plus seulement aux seuls aspects techniques. En effet, le positionnement des systèmes d'information comme création de valeur pour l'entreprise rend les technologies de l'information et des communications indissociables de la stratégie.

Cette nouvelle donne permet de mettre l'accent sur de nouveaux thèmes de réflexion qui induisent l'analyse des aspects organisationnels ainsi que le fonctionnement de l'entreprise: alignement stratégique, pilotage et gouvernance du SI, urbanisation, refonte de processus…

À l'image des CIO anglo-saxons, nos DSI veulent étoffer leurs compétences stratégiques pour se positionner comme des membres à part entière des directions générales et avoir réellement la place qu'ils méritent au sein de leur entreprise. Cette nouvelle dimension sous-tend l'acquisition de connaissances nouvelles :

[88] « Du simple canular à la désinformation orchestrée », Le Monde Interactif, 23 mai 2001.

Nouvelles responsabilités	Compétences requises
- Identification des opportunités d'activités valorisant les technologies de l'information. - Supervision et animation de l'infrastructure de l'information de l'organisation. - Supervision de l'évolution des composants des systèmes et de leur amélioration. - Gestion opérationnelle et maintenance. - Service clientèle et support des consommateurs - Planification stratégique du rôle des systèmes d'information dans la politique concurrentielle et d'alliance de l'organisation.	- Stratégie d'entreprise, finance, marketing ; management des systèmes d'information. - Gestion des ressources humaines : motivation, gestion de crises, changement. - Management de la technologie ; veille. - Gestion de projets et compétences techniques. - Marketing direct et comportement du consommateur ; ergonomie. - Analyse concurrentielle ; analyse des mouvements compétitifs ; gestion des interfaces de commercialisation.

Source : P. Baumard

Tableau 9 : Responsabilités et compétences du DMSI[89].

Parce qu'il maîtrise l'ensemble des flux informationnels de l'entreprise, qu'il est capable de les modifier et de les améliorer par ses connaissances techniques et organisationnelles, parce qu'il est le mieux placé pour sécuriser l'information et visionner une grande partie des menaces, le DSI peut être ce fameux « chef d'orchestre » qui va sensibiliser et proposer des solutions à la DG pour asseoir la démarche d'IES au sein de l'entreprise.

Un veilleur

- Met en évidence les coûts induits par une mauvaise gestion de l'information. Sensibilise sur l'impact des systèmes d'information dans le management de l'information.
- Renseigne sur les initiatives et projets intéressants des autres groupes.
- Met en garde sur les dysfonctionnements organisationnels et leurs impacts sur la circulation de l'information. Sensibilisation sur la non-adéquation entre circulation de l'information et organisation.
- Alerte sur les risques de guerre d'information par les systèmes d'information, sur les risques inhérents à la sécurité.

[89] *op. cit.*

Un fédérateur d'idées

- Remonte les initiatives éparses ou les propositions intéressantes.
- Interface entre les directions métiers, la direction de la stratégie et la direction générale.
- Développe la promotion de l'IES comme facteur de création de valeur au travers des TIC.

Une force de proposition

- Fait des propositions pour développer l'IES au travers des systèmes d'information.
- Explique les répercussions en terme d'avantage concurrentiel, de cohésion, de culture d'entreprise et d'organisation.
- Démarre des projets pilote pour sensibiliser la direction générale et les directions métiers.
- Propose des contre-mesures, participe à la mise en place des cellules de crise, développe le concept de *war-room*.
- Met en évidence l'émergence de nouveaux outils ou concepts (*management cockpit*).

L'étude de l'IHEDN a mis en évidence le manque de réaction des entreprises françaises face aux crises informationnelles. L'absence fréquente de *war-room* (présentes dans les grands groupes aux États-Unis) en est un signe. Les Anglo-saxons mettent en place des salles de type « *Management Cockpit* » qui permettent non seulement de réagir rapidement aux crises mais également de faciliter le pilotage de l'entreprise, la décision en temps réel grâce aux nouvelles technologies. Le DSI est l'interlocuteur le plus à même de faciliter l'émergence de tels concepts. Ainsi les multinationales américaines mettent-elles en place ces cellules centralisées de veille économique et stratégique sous forme de salle de commandement. Objectif, améliorer la communication et la coordination entre ceux qui détiennent l'information stratégique et ceux qui l'utilisent. Ce type de salles de commandement traite l'information tactique et stratégique « minute par minute ».

De telles responsabilités demandent de la part des DSI une prise de conscience de ce que peut être l'IES grâce aux systèmes d'information. Cette implication passe également par l'ouverture sur les initiatives éparses ou les idées de certains collaborateurs passionnés sur le sujet. Parce qu'ils manquent d'appui, ces gens n'ont pas toujours l'écoute qu'ils mériteraient, le DSI peut constituer le relais qui leur fait défaut.

Jean-Pierre Corniou, dans son ouvrage « La société de la connaissance[90] », définit le DSI comme étant à la fois un pédagogue, un manager et un leader, capable d'être un moteur de changement au sein de son entreprise. C'est en se positionnant en tant que tel que le DSI peut jouer un rôle actif dans le concept d'IES. Certes, expert et conseillé technique, il peut également se positionner comme une force de proposition en matière de nouveaux projets. Car même si le démarrage d'une politique d'IES est du ressort du DG, le DSI doit avoir un rôle « proactif » pour susciter le démarrage de ces projets et alerter sa direction sur les enjeux qui peuvent en résulter.

Le DSI ne peut autodéfinir sa mission. Inséré dans le tissu complexe du management de l'entreprise, son rôle effectif dépendra autant de ses propres capacités que de l'espace de manœuvre que la direction générale décidera de lui laisser.

Jean-Pierre Corniou (DSI du Groupe Renault et Président du Cigref)

[90] Corniou Jean-Pierre, *La société de la connaissance*, Hermès-Lavoisier, 2002.

7 CONCLUSION

Les systèmes d'information font partie intégrante de la démarche d'intelligence économique et stratégique. Les technologies de l'information et de communication, surtout internet, ont largement favorisé le développement du concept dans les entreprises, mais également le positionnement de nombreux éditeurs sur ce marché. Les technologies actuelles utilisées par les solutions logicielles laissent encore augurer de nombreux progrès pour correspondre au mieux aux attentes des entreprises.

Quelques grands groupes développent d'ores et déjà des systèmes d'intelligence économique reposant sur des systèmes d'information spécifiques, ce rapport en a mis quelques-uns en évidence. À l'image des services de renseignement, mais également des forces armées qui mettent en place des systèmes d'information et de commandement numériques, les entreprises doivent réaliser que les systèmes d'information peuvent constituer une formidable « machine » pour gérer l'information stratégique sur l'ensemble du groupe et s'affirmer ainsi comme le réceptacle du dispositif d'intelligence économique et stratégique.

Responsable des systèmes d'information, le DSI peut jouer un rôle essentiel pour lancer de tels projets. Technicien et architecte, il est un facilitateur des démarches menées au sein du groupe. Il les instrumente, aide à leur mise en place, les coordonne et participe ainsi à mettre en relation entre eux les différents acteurs[91]. Véritable architecte des flux informationnels, sa connaissance des projets transverses lui confère une légitimité pour développer une structure globale d'information.

Confronté aux problèmes de sécurité, il est le plus à même de protéger le patrimoine informationnel. Conscient des attaques dont les entreprises sont aujourd'hui les cibles, il se positionne comme l'interlocuteur privilégié auquel il sera nécessaire de s'adresser pour anticiper, contrer et riposter. Cette nouvelle position oblige le DSI à s'intéresser de plus en plus au contenu et à la valeur de l'information véhiculée ou stockée.

[91] Intervention de Christophe Binot, responsable du département gestion et valorisation de l'information de TotalFinaElf, durant le Cycle IES du Cigref.

Le DSI doit avoir un rôle moteur dans la démarche d'IES. Conscient de ces possibilités, il peut alors se positionner comme une véritable force de proposition. Cette perspective constitue une réelle occasion pour asseoir sa place au sein de la direction générale. Mais débattre de l'implication du DSI dans le concept d'IES ne revient-il pas finalement à se poser l'éternelle question : le DSI, technicien ou stratège *?*

Annexe : Bibliographie

Ouvrages

- Allain-Dupré Patrice et Duhard Nathalie, *Les armes secrètes de la décisions,* Gualino Editeur, 1997.
- Baumard Philippe, *Stratégie et surveillance des environnements concurrentiels*, Masson, 1991.
- Baumard Philippe et Benvenuti Jean-André, *Compétitivité et systèmes d'information,* InterEditions, 1998.
- Baumard Philippe, *Analyse Stratégique : mouvements, signaux concurrentiels et interdépendance*, Dunod, 2001.
- Beau Francis, *Renseignement et société de l'information,* Fondation pour les Etudes de Défense, 1997.
- Besson Bernard et Possin Jean-Claude, *L'audit d'intelligence économique,* Dunod, 1998.
- Bournois Franck, Romani Pierre-Jacquelin, *L'intelligence économique et stratégique dans les entreprises françaises*, IHEDN, Economica, 2000.
- Cigref, *La veille stratégique*, Rapport, 1998.
- Cigref, *Internet dans les entreprises*, Rapport, 2001.
- Cigref, *Sécurité des systèmes d'information – Quelle politique de gestion globale des risques ?*, Rapport, 2002.
- Clusif, *Études et statistiques sur la sinistralité informatique en France*, Rapport, 2001.
- Commissariat général du Plan, *Intelligence économique et stratégie des entreprises*, La documentation française, 1994.
- Corniou Jean-Pierre, *La société de la connaissance*, Hermès-Lavoisier, 2002.
- Deloitte&Touche Consulting Group et CEPS (Centre d'étude et de prospective Stratégique), *Pratiques et attentes des entreprises en matière d'intelligence économique*, enquête réalisée d'avril à juin 1998.
- École de guerre économique (Promotion 2002), « *La guerre de l'information du faible au fort : le cas « Vermillion, prospection pétrolière dans la vallée de Chevreuse* »», in « La Guerre Cognitive », Lavauzelle, 2002.
- Guichardaz P., Lointier P. et Rosé P. *L'Infoguerre, stratégie de contre intelligence pour les entreprises*, Dunod, 1999.
- Harbulot Christian et Lucas Didier, *La guerre cognitive, l'arme de la connaissance*, Lavauzelle, 2002.
- Henri Brigitte, *Le renseignement : un enjeu de pouvoir*, Economica, 1998.
- François Ludovic, « *ONG, Entreprises : la guerre de l'information au nom de l'éthique* » *in* « Renseignement et opérations spéciales », n°8, l'Harmattan, 2001.

- Intelleco Consultants et Darpmi, *Intelligence économique, outils et méthodes développés en PMI*, Les éditions de l'industrie, 2000.
- Jakobiak François, *L'intelligence économique en pratique*, 2e édition, Éditions d'Organisation, 2001.
- Levet Jean-Louis, *L'intelligence économique, mode de pensée, mode d'action*, Economica, 2001.
- Levet Jean-Louis, *Les Pratiques de l'intelligence économique – Huit cas d'entreprises*, Economica, 2002.
- Martinet Bruno et Marty Yves-Michel, *L'intelligence économique, comment donner de la valeur concurrentielle à l'entreprise*, Éditions d'Organisation, 2001.
- Michel Claude, « Idées pour la défense et la sécurité », Agir, n° 13, Hiver 2003.
- Moinet Nicolas, « *Le réseau, cœur stratégique des guerres de l'information et de la connaissance* », in « La Guerre Cognitive », Lavauzelle, 2002.
- Pateyron Emmanuel, *La veille stratégique*, Economica, 1998.
- Revelli Carlo, *Intelligence Stratégique sur Internet*, Dunod, 2000.
- Rouach Daniel, *La veille technologique et l'intelligence économique*, PUF, Collection « Que sais-je ? », 1996.
- Romagni Patrick et Wild Valérie, *L'intelligence économique au service de l'entreprise,* Les Presses du Management, 1998.
- Wautelet Michel, *Cyberconflit*, Éditions Complexe, 1998.

Articles

- Rosé Philippe, « Quand l'intelligence économique devient offensive », Le Monde Informatique, 16 juin 2000.
- Le Monde Interactif, « Du simple canular à la désinformation orchestrée », 23 mai 2001.
- Le Journal du Net, « Comment Giat Industries aménage une gestion des connaissances très « stratégique », 7 mai 2002.
- Cabinet Eurodécision – AIS, *«* Attaque et contre-attaque par l'information *»*, *in* Magazine Veille n° 55 du mois de juin 2002.
- 2002 CSI / FBI Computer Crime and Security Survey (vol.III, n°1).

Sites

- www.arisem.com
- www.cigref.fr
- www.datops.com

- www.digimind.com
- www.echelon-online.fr.st
- www.esiee.fr/masteres/miste/
- www.fuld.com
- www.guerreco.com
- www.haoxbuster.com
- www.ihedn.fr
- www.infoguerre.com
- www.information4action.com
- www.interpactinc.com
- www.journaldunet.com
- www.stopesso.com
- www.strategic-road.com
- www.thales-communications.com
- www.weblmi.com
- www.zdnet.fr