



MEMOIRE DE RECHERCHE

Bachelor of Business 3ème Année

Présenté et soutenu par:

Luis GOMEZ

Année 2015

Comment se préserver de l'intelligence économique
de la concurrence ?

Sommaire:

Introduction.....	3
Première Partie: L'intelligence économique et veille stratégique.	
I. <u>Intelligence économique</u>	5
a. Définition.....	5
b. Les principes de l'IE.....	6
c. Les enjeux et apport de l'intelligence économique.....	8
d. Analyse du macro-environnement.....	9
II. <u>Veille stratégique</u>	11
a. Contexte.....	11
b. Définition.....	11
c. Veille technologique.....	12
d. Veille concurrentielle.....	13
e. Veille commerciale.....	14
III. <u>Les moyens d'action</u>	16
Deuxième Partie: Les menaces de la concurrence	
I. <u>Les menaces sur le patrimoine matériel</u>	18
a. Les atteintes aux personnes.....	18
b. Les atteintes aux biens.....	19
II. <u>Les menaces sur le patrimoine immatériel</u>	19
a. Atteintes à l'information stratégique.....	20
b. Atteintes au système d'information.....	23
c. Atteintes à l'image et à la réputation.....	25
d. Atteinte au capital.....	28
Troisième Partie : Les moyens de protections des menaces	
I. <u>Les moyens de protections du patrimoine matériel</u>	31
a. Les moyens de protections des personnes.....	31
b. Les moyens de protections des biens.....	32
II. <u>Les moyens de protections du patrimoine immatériel</u>	33
a. Les moyens de protections de l'information stratégique.....	33
b. Les moyens de protections du système d'information.....	36
c. Les moyens de protections de l'image et la réputation.....	38
d. Les moyens de protections du capital.....	40
Conclusion.....	42

INTRODUCTION:

L'intelligence économique est aujourd'hui un concept essentiel aux organisations, cela est dû au fait que l'intelligence économique permet de répondre à un grand nombre de questions que les entreprises se posent tous les jours. Pendant longtemps ce concept était utilisé uniquement par les Etats et les grands groupes puissants, mais les avancées techniques en informatique et en communications ont rendu l'utilisation de l'intelligence économique accessible à toutes les organisations et entreprises. C'est peut être même devenue un concept indispensable dont les entreprises ne peuvent se permettre de ne pas y prêter attention, effectivement avec la mondialisation la concurrence est devenue très nombreuse et redoutable pour les entreprises et cela de plus en plus tous les jours. Une entreprise qui ne cherche pas à connaître, comprendre et analyser son environnement s'engage à se retrouver en difficulté face au marché et de ne pas pouvoir assurer sa pérennité et son existence dans le temps en revanche l'entreprise qui s'informe se renseigne sur son environnement obtient un avantage certain et pourra assurer son existence sur le marché. L'intelligence est aujourd'hui un outil stratégique pouvant améliorer la performance de l'entreprise.

On constate que le parti prenant de l'entreprise qui va chercher le plus à déstabiliser est la concurrence, c'est pourquoi se mémoire va principalement étudier la concurrence grâce au concept de l'intelligence économique et se poser la problématique suivante, comment se préserver de l'intelligence économique de la concurrence ?

La pertinence de cette problématique s'est d'ailleurs confirmée au cours des travaux préparatoires de la présente étude, la problématique est intéressante car son étude peut apporter des vraies réponses à des questions que les entreprises se posent chaque jour et ainsi qu'à des problèmes qu'elles peuvent rencontrer au quotidien. L'intérêt de consacrer un mémoire sur ce sujet est que cette étude peut être utilisé par des organisations et de créer une vraie synthèse des réponses à la problématique.

C'est en se fondant sur l'abondante bibliographie consacrée à la matière, et tout particulièrement sur « l'intelligence économique et entreprise » de Louis Hausser mais également des divers revue littéraire d'Eric Delbecque comme « l'intelligence économique » et «intelligence économique » écrit avec Jean Renaud,le livre « l'intelligence économique »

de François Jakobiak ou encore « intelligence économique et gestion des risques » de Michel-Henry Bouchet et Alice Guillon le fraper du Hellen qu'il fût possible de déterminer qu'elles sont les moyens de protections qu'ont les entreprises pour se protéger de la concurrence. L'exploitation de ces sources devrait permettre de répondre à une série de questionnement inhérent au sujet : Est-il possible de se protéger totalement de sa concurrence ? Qu'elles sont les moyens de protection existant ? Comment l'entreprise peut-elle mettre en place ces moyens de protections ?

Ce mémoire tend ainsi à démontrer qu'il est aujourd'hui essentiel pour une entreprise d'anticiper les risques, les menaces que peuvent exercer leur concurrent et de savoir comment les gérer: Il n'y a pas de méthode infaillible pour se protéger de l'intelligence économique de la concurrence mais il existe un grand nombre de moyens d'atténuer les menaces ou de rattraper les dégâts fait par une atteinte commise précédemment par un concurrent.

Après une premier partie qui portera sur l'intelligence économique et sur la veille stratégique, où l'on présentera le concept de l'intelligence économique ainsi que celui de la veille stratégique (I), dans une seconde partie les menaces de la concurrence qui va mettre en évidence l'ensemble des menaces que peut craindre une entreprise de ses concurrents, en fonction de la nature du patrimoine visé par les concurrents, le patrimoine matériel et le patrimoine immatériel(II).

Enfin, on verra dans une dernière partie les moyens de protections des menaces et d'apporter dans cette partie l'ensemble des solutions pour répondre au menace soulever dans la deuxième partie(III).

PARTIE 1 : L'INTELLIGENCE ECONOMIQUE ET VEILLE STRATEGIQUE

Introduction:

L'intelligence économique concerne la plupart des organisations : les grandes entreprises privées, les entreprises et les organismes publics, les PME... Elle est indispensable aux entreprises qui veulent rester compétitives car elle permet de surveiller le secteur d'activité notamment en analysant les marchés, les coopérations, les nouvelles technologies...

Nous verrons dans un premier temps la définition et l'utilité de l'intelligence économique puis dans un second temps la définition de la veille et les avantages qu'elle présente.

I. Intelligence économique

a. Définition

Définition du commissariat général au Plan en 1994 (publication du rapport national) :

¹ “ L'Intelligence Economique 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.

Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût ”

L'intelligence économique est un processus de recueil (légal) et de traitement d'informations stratégiques pour l'entreprise, l'acquisition de ce savoir est essentiel et permet à l'organisation de se développer et de se protéger face aux menaces et aux risques liés à l'environnement tels que la concurrence déloyale, l'espionnage, le vandalisme et tout type d'atteintes pouvant porter préjudice à l'entreprise.

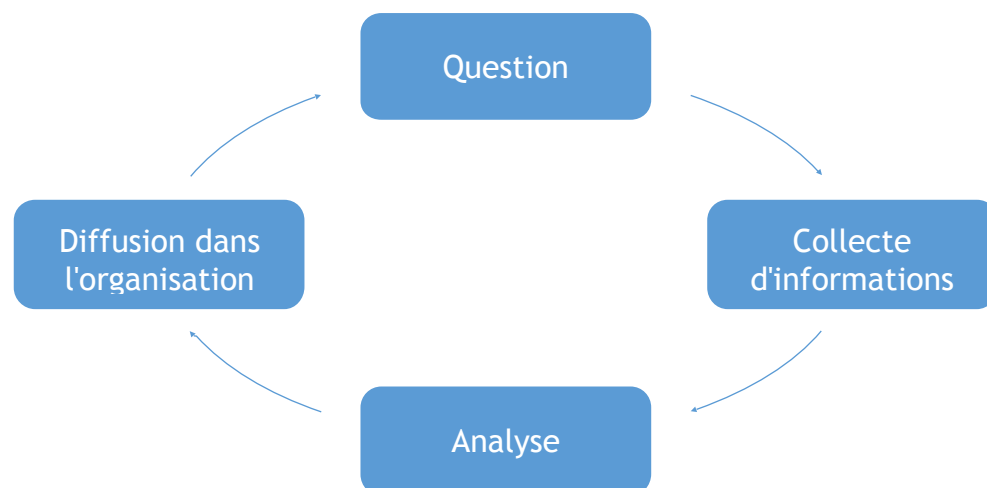
¹ Définition du commissariat général au Plan, 1994.

Il est essentiel de distinguer l'intelligence économique de l'espionnage économique, la distinction se fait au niveau de la légalité des moyens utilisés car l'intelligence économique contrairement à l'espionnage utilise uniquement des moyens légaux.

b. Les principes de l'IE

L'intelligence économique est une démarche qui a pour but l'association de la stratégie de l'entreprise et sa culture de l'information. Le processus mis en place est :

- Le recueil de l'information stratégique qui se fait grâce aux moyens mis à disposition au sein de l'organisation.
- Le suivi de l'information, les façons dont elle évolue et la perspective d'évolution pour permettre de qualifier la pertinence de cette information.
- Le traitement de l'information, c'est utiliser tous les moyens à disposition dans l'organisation pour agir sur l'information et obtenir des résultats.
- La diffusion, c'est transmettre et communiquer l'information aux différents acteurs de l'organisation.
- La protection, c'est mettre en place des moyens pour se protéger suite aux résultats obtenus par le traitement de l'information.



Le schéma ci-dessus permet de visualiser le déroulement logique de ce processus, qui est dans un premier temps un questionnement suivi d'une collecte d'informations qui seront analysées

pour obtenir des résultats, une fois les résultats obtenus ils devront circuler et être diffusés dans l'organisation, par la suite cela pourra rebondir sur de nouveau questionnement.

Ce processus est en permanence actif et l'entreprise ne peut se permettre d'être continuellement en train de traiter les informations de son environnement c'est là-dessus que repose le développement permanent de son activité sous peine de stagner face à la concurrence qui elle est en permanence à la recherche de développement.

L'intelligence économique est la culture de l'information qui comprend:

- La culture stratégique : ²« une culture de la stratégie se traduit donc comme un ensemble d'habitudes de penser, de se comporter et d'agir lorsque l'on doit atteindre un objectif. »
- La culture collective interne : la recherche d'information s'effectue à partir de données détenues par des acteurs internes à l'organisation. l'information est partagée dans l'entreprise et fait l'objet d'une émulation interne.
- La culture collective externe : les informations sont récupérées d'acteurs externes à l'entreprise faisant partis du réseau de l'organisation.
- La culture subversive: la recherche d'information présente également un caractère subversif. En effet l'information peut subir des biais perceptuels. on peut également lors de cette recherche être victime de désinformation ou de contre information qui est une information écrite ou télévisée qui s'oppose aux organes d'information classiques.

L'Intelligence Economique n'est pas de l'espionnage

L'espionnage est la prise d'information par une action illégale, l'espionnage est condamné pénalement par la loi contrairement à l'intelligence économique qui se restreint aux activités déontologique et légales.

L'objectif n'est pas de voler l'information mais de la collecter.

² <http://www.portail-ie.fr/lexiques/read/84>

³« La majorité de l'information s'obtient sans difficulté et en toute légalité, cependant, une information sur trois s'acquiert par le biais de protocoles plus sophistiquées, voire illégaux.

On estime, à ce titre, que :

- 70 % de l'information est blanche, c'est-à-dire, qu'elle circule librement par le biais de canaux

dits ouverts. Il s'agit, par exemple, d'un article de presse, d'informations émanant d'internet, de documentations promotionnelles, de salons, etc. Le recoupement des informations blanches est parfois surprenant tant il permet d'obtenir un aperçu précis des positions et des intentions stratégiques.

- 25 % de l'information est grise, c'est-à-dire, qu'elle circule par le biais de canaux dits semi- ouverts. Leur collecte est légale mais impose une maîtrise plus élaborée des méthodes de renseignement. L'information grise s'obtient généralement au travers de fausses identités, d'entretiens d'embauches factices, etc. »

c. Les enjeux et apport de l'intelligence économique

Les enjeux de l'intelligence économiques sont:

- Connaître l'environnement qui l'entoure : Une bonne compréhension de l'environnement est essentiel pour l'entreprise, c'est identifier les acteurs externes et internes à l'organisation pouvant influencer la situation de l'entreprise sur le marché et les distinguer selon leurs impacts positifs ou négatifs sur l'organisation.
- Anticiper les fluctuations de l'environnement : l'environnement est en évolution permanente. Les attentes et les besoins du marché évoluent constamment, il est important de connaître les attentes actuelles du marché pour y répondre mais il est d'autant plus important de les anticiper pour être les premiers à agir en connaissance de cause.

³ Romain Zerbib, 2012

- Etre plus compétitif : Répondre rapidement aux besoins permet d'obtenir un avantage concurrentiel. La concurrence est rude, il est important pour exister sur un marché d'afficher une distinction et de se démarquer des autres entreprises.

Les apports de l'intelligence économique sont multiples.

L'intelligence économique permet dans un premier temps de se poser les bonnes questions, comme se poser la question de savoir si l'on est sûr d'être bien informé ? Si l'on peut s'informer seul ou si on a besoin d'acteur extérieur ? Les décisions sont-elles prises en toute connaissance de cause ? Avons-nous conscience que la concurrence nous surveille également ?

Elle permet de mettre en place un véritable management de l'information qui va permettre à l'entreprise d'introduire des moyens de protection de son patrimoine, mobiliser son personnel à l'importance des informations au sein de l'entreprise, d'utiliser les bons outils de prise d'information. Cela va également permettre de mettre en œuvre le système d'information et de veille de l'entreprise et de déterminer la stratégie de communication et d'influence que l'entreprise doit adopter.

L'intelligence économique va donc permettre à l'entreprise de disposer des bonnes informations au bon moment et de savoir comment les traiter, pour prendre les décisions les plus judicieuses, de pouvoir développer de nouveaux produits grâce notamment à la connaissance acquise par l'écoute des attentes et des besoins du marché. Par conséquent cela va rendre l'entreprise plus performante et l'aider à mieux vendre et obtenir un avantage concurrentiel.

d. Analyse du macro-environnement

Le macro-environnement peut être étudié avec le modèle PESTEL qui prend en compte

Les facteurs politiques, économiques, sociaux, technologiques, écologiques et légaux.



L'environnement Politique : c'est l'ensemble des décisions prises par les gouvernements au niveau national mais également international comme le gouvernement français, l'union européenne ou les organismes de type OMC (Organisation mondial du commerce).

L'environnement économique : la prise en compte des indicateurs économiques, le taux de croissance actuel, le pouvoir d'achat des consommateurs ou bien encore l'inflation ou déflation. Ce sont tous les facteurs ayant une influence sur la consommation.

L'environnement social: ce sont toutes les caractéristiques des populations qui déterminent les comportements d'achats des consommateurs, dont la démographie, la pyramide des âges, les comportements socioculturels.

L'environnement technologique: c'est prendre en compte toute les recherches et avancées technologiques qui peuvent créer une rupture technologique et remettre en cause la place des leaders actuels sur le marché.

L'environnement écologique: les contraintes liées aux réglementations écologiques et normes mises en place par les gouvernements pour protéger l'environnement. Le développement durable est aujourd'hui une notion importante à respecter pour les entreprises.

L'environnement législatif prend en compte les normes législatives que l'entreprise doit respecter et suivre les évolutions notamment celles du droit du travail et le droit du commerce.

II. Veille stratégique

a. Contexte

On distingue différentes époques au début du 20ème siècle l'offre est nettement inférieure à la demande: la préoccupation essentielle des entreprises est de produire un produit de qualité standard. Puis au milieu du 20ème l'offre a évolué et rattrape la demande, les phénomènes de concurrence commence à apparaître, il ne suffit plus d'apporter au consommateur un produit de qualité standard. Le prix se doit d'être attractif, d'où une nécessité de diminuer les couts de revient. Afin de diminuer le cout unitaire les entreprises ont eu recours aux économies d'échelle.

De ce fait l'offre a fini par dépasser la demande: les marchés sont devenus surcapacitaires (développement du one to one).

Il est important d'exercer une veille car l'environnement économique est de plus en plus turbulent. Les besoins de la clientèle changent de jour en jour, les tendances et produits se renouvellent vite, la technologie évolue en permanence une rupture technologique peut arriver à tous moments, la concurrence est mondial et très nombreuse et on voit apparaître de nouvelles normes et contraintes législatives qui contraignent les entreprises à être flexibles en permanence.

Les entreprises se vouent une véritable guerre de l'information.

b. Définition de la veille

⁴« *La Veille Stratégique est un système d'aide à la décision qui observe et analyse l'environnement scientifique, technique, technologique et les impacts économiques présents et*

⁴ David Coudol et Stéphane Gros

futurs pour en déduire les menaces et les opportunités de développement. Elle s'appuie essentiellement sur les informations ayant un caractère stratégique ou décisions importantes lui associant le terme de veille stratégique » David Coudol & Stéphane Gros

c. Veille technologique

La veille technologique est l'ensemble des moyens de collecte d'informations technologiques qui a pour but de les analyser et les exploiter dans le but de développer l'entreprise au niveau technologique.

Cette recherche s'intéresse à toutes les nouveautés et avancés technologiques, scientifiques, à de nouveaux procédé de fabrication, d'utilisation de nouveaux matériaux qui pourraient présenter dans l'avenir un impact économiques pour l'entreprise.

La veille technologique va permettre à l'entreprise de détecter les nouvelles technologies qui apparaissent sur le marché ou risque de faire leur apparition, grâce à ce recueil d'information l'entreprise pourra anticiper toutes les évolutions de son marché et par conséquent réduire le risque d'être touchée par une rupture technologique.

Il est essentiel également pour l'entreprise d'avoir un œil sur les technologies utilisées par les acteurs qui l'entourent comme ses concurrents, ses fournisseurs, ces clients et ses partenaires.

L'ensemble de ces informations va permettre de faciliter l'orientation de l'entreprise dans le domaine de la recherche et développement et de rendre ce domaine plus efficace car une bonne connaissance de son environnement technologique permet de connaître les axes et les domaines de recherche essentiels au développement de l'entreprise.

La veille technologique peut trouver ses sources dans divers endroits et par divers moyens, d'abord l'entreprise doit utiliser tous les médias d'informations comme le web, les magazines spécialisés ou les reportages qui montrent et informent des tendances actuelles. L'entreprise doit surveiller également les bases de données telles que les bibliothèques de brevet pour ne pas utiliser ses ressources dans un projet déjà breveté. Les universités et les grandes écoles mènent des recherches actives il est important de suivre leur recherche de près car beaucoup

de nouveautés apparaissent au sein de ces établissements, les salons et les foires sont des moyens de recueil d'informations très importants c'est là que beaucoup d'entreprises présentent leurs recherches et leur avancés technologiques, l'entreprise peut en apprendre grandement sur sa concurrence.

d. Veille concurrentielle

⁵« La veille concurrentiel, c'est rechercher, analyser et exploiter les informations relatives à son entreprise, ses concurrents et son secteur d'activité, dans le but d'accroître sa productivité et sa compétitivité. »

L'importance de la veille concurrentielle est de connaître tous les risques que peut présenter la concurrence et de s'en prévenir, en répertoriant les points forts des concurrents, leurs faiblesses mais également la stratégie qu'ils mettent en place.

L'enjeu de cette veille est de connaître les nouveaux concurrents qui arrivent sur le marché, de connaître les produits que proposent les entreprises concurrentes, leurs prestations et de savoir le prix auquel elles facturent cela pour pouvoir s'aligner et garder une certaine cohérence avec le marché.

Les faits à surveiller sont principalement :

- Les pratiques commerciales des concurrents
- Les actions des concurrents (offres promotionnelles, actions marketing...)
- Les nouvelles opportunités : nouveaux clients,...
- Les changements sociopolitiques et économiques ; réglementation...

On peut également approfondir nos connaissances sur la concurrence en récoltant des données sur leur situation financière, les ressources et les technologies qu'ils emploient et les stratégies mises en place.

On peut récolter ses diverses informations en ligne notamment, en consultant des sites de la presse spécialisée dans le secteur d'activité de l'entreprise. Il existe également des moteurs de

⁵ <http://www.commentcamarche.net/faq/9736-la-veille-concurrentielle>

recherche spécialisés (Manageo, Infogreffe...) dans la recherche d'entreprises et qui peuvent fournir des informations sur leur situation financière et administrative. L'INPI propose également un service nommé Euridile qui fournit des données importantes : comptes annuels, immatriculations...

e. Veille commerciale

« La veille commerciale consiste en la collecte, le traitement et la diffusion d'informations afin de servir une entreprise dans un but de développement commercial. »

Une bonne définition des objectifs de l'entreprise est cruciale. Elle va permettre d'identifier correctement la nature de l'information puis la source visée.

Ces objectifs peuvent être : le lancement d'un nouveau produit ou service, les intentions d'achat...

Les sources sont diverses : journaux officiels, presse écrite, Internet ou encore des entretiens.

Les principaux bénéfices d'une veille commerciale efficace sont de 4 ordres :

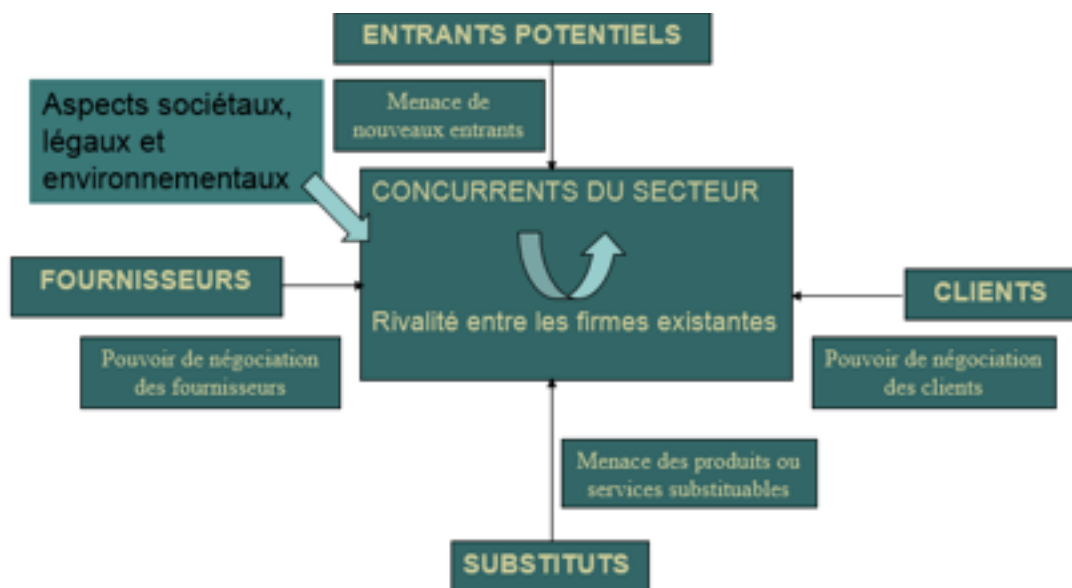
- Le temps : les commerciaux de l'entreprise vont gagner un temps précieux car ils disposeront d'informations pertinentes et précises dans leur fonction.
- La productivité : grâce aux informations dont il dispose, le commercial ne se disperse pas en démarches inutiles (approches téléphoniques, recherches d'informations complémentaires...).
- La performance commerciale
- Le chiffre d'affaire

f. Méthode Porter

⁶VECTEURPLUS, l'art de l'information qualifiée : quelle est l'utilité d'une veille commerciale pour la prospection, juin 2009

Les études de Michaël Porter dans Choix stratégiques et concurrence, Economica, Paris 1986 ⁷« montrent que l'intensité de la concurrence qui prévaut dans un secteur n'est ni une coïncidence, ni le fait du hasard. »

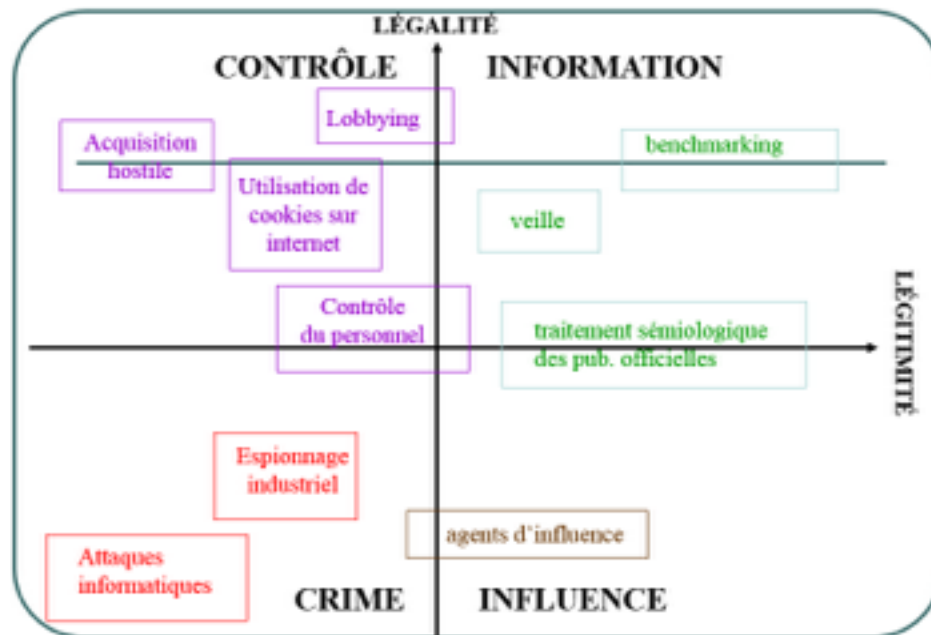
Cette concurrence trouve ses origines dans la structure économique du secteur et dépasse le seul comportement des concurrents existants.



On peut analyser l'environnement d'une entreprise grâce à la matrice de Porter qui permet d'identifier les acteurs pouvant influencer le secteur. On y retrouve : les entrants potentiels, les fournisseurs, les aspects sociaux et environnementaux, les clients et les produits de substitution. Cette matrice met en avant les rapports de force entre les différents acteurs du secteur.

⁷ Michaël Porter, 1986

III. Les moyens d'action



On peut classer les moyens d'actions selon leur légalité et leur légitimité. On distingue ainsi quatre grandes catégories: contrôle information crime et influence.

Tout d'abord pour la catégorie « contrôle », les moyens d'actions ont une légitimité faible tous en étant légaux, on y répertorie le lobbying, les acquisitions hostile, utilisation de cookies, contrôle du personnel.

Ensuite on identifie la catégorie information dans laquelle on retrouve des méthodes de recherche légales et légitimes : la veille, le benchmarking, traitement sémiologique des publicités officielles.

Puis on remarque une troisième catégorie « l'influence » qui regroupe des moyens de collecte d'informations légitimes mais illégaux: les agents d'influences.

Enfin il y a la catégorie « crime » qui utilise des moyens d'actions illégaux et illégitimes comme les cyberattaques et l'espionnage industriel.

L'économie est complexe, il en résulte donc une méconnaissance de l'environnement. En effet la concurrence s'est mondialisée grâce au progrès technologie notamment aux nouvelles technologies de l'information. Les produits et les besoins des clients changent à un rythme

effréné. De plus, les dirigeants sont confrontés actuellement à un problème de sur ou de sous information.

Conclusion:

Grâce à cette partie nous avons pu mettre en avant le lien qui unissait la veille stratégique et l'intelligence économique ainsi que les avantages qu'elles présentent. La veille concurrentielle permet de surveiller les entrants potentiels et les menaces qu'ils représentent, la veille commerciale permet de mettre en avant les attentes des clients et les exigences des fournisseurs et la veille technologique permet de faire ressortir les menaces que représentent les produits de substitution. Cependant cette démarche a une limite de taille : elle ne prend pas en compte les actions illégales des concurrents ou autres que nous allons aborder en seconde partie.

PARTIE II: LES MENACES DE LA CONCURRENCE

Introduction:

Pour qu'une entreprise puisse se protéger des menaces de sa concurrence, il faut dans un premier temps qu'elle définisse les menaces potentielles qu'elle peut subir et de les distinguer en fonction de leur nature de la menace et de ce qu'elle vise. Les menaces peuvent toucher deux types de patrimoine de l'entreprise, le patrimoine matériel et le patrimoine immatériel. Cette démarche de recherche et d'analyse des menaces est essentielle pour se prémunir des risques liés à cela car l'entreprise ne peut se protéger d'une menace qu'elle ne connaît pas.

⁸« Réduire sa vulnérabilité passe par une compréhension préalable de ce qu'est le patrimoine d'une entreprise ou d'un laboratoire :

⁸ Laurier,P , 2004 « Déstabilisation d'entreprise »

- ce qui fait entrer l'argent : ses produits et ses prestations ; - ce qui la représente : ses hommes et ses biens ;

- ce qui la fait bouger : son identité et sa vision ;

- ce qui la fait survivre : sa cohésion et sa capacité de remise en cause.

[Ces menaces] sont certes multiformes – manipuler, mettre sous surveillance, déstabiliser, voler, détruire – mais elles ont toutes pour point commun un passage obligé : nos faiblesses, nos routines ».

I. Les menaces sur le patrimoine matériel

A. Les atteintes aux personnes

L'attaque physique d'un membre de l'entreprise est un fait rare mais il n'est pas inexistant pour autant.

En effet il existe au sein des entreprises et des organisations des employés clé dont l'absence pourrait être un handicap pour celle-ci. C'est pourquoi la concurrence pourrait être tentée de porter atteinte à ces collaborateurs.

Dans un premier temps la concurrence pourrait tenter de récupérer cet élément au sein de son entreprise, c'est un moyen de déstabiliser son concurrent en lui ôtant un élément important à sa réussite mais également un moyen pour le concurrent de renforcer son effectif. C'est une manœuvre qui s'utilise fréquemment et l'on voit arriver des plus en plus au sein des entreprises, des chasseurs de têtes dont le métier est justement d'aller récupérer des éléments importants pour l'entreprise.

Cette méthode reste un moyen légale de porter atteinte au personnel d'une entreprise, mais certaines entreprises peuvent mettre en place des actions illégales et très dangereuses pour porter atteinte à leurs concurrents, toutefois cela reste des actions isolées et rares mais elles ne doivent pas être négligées pour autant.

Les actions malveillantes pouvant être réalisées sont tout simplement un attaque physique de la personne dans le but de le blesser et de l'empêcher d'exercer ses fonctions de travail. Cette

acte semble inimaginable pour certains mais dans certains domaines d'activité les enjeux et les sommes d'argent sont tels que les pires actes peuvent être commis.

B. Les atteintes aux biens

Le patrimoine matériel de l'entreprise peut aussi être atteint par des concurrents mal intentionnés, les outils et machines de l'entreprise peuvent être cassés, détériorés ou volés dans le but de stopper ou ralentir une production et causer des pertes financières à celui-ci.

Un concurrent peut également saboter des produits finis exposé en magasin ou lors de salon pour nuire à la qualité de vos produits face à la clientèle.

Affaire LG, Samsung:

9« Un sabotage de lave-linge, l'affaire n'est pas banale. Et pourtant, les enquêteurs prennent les faits très au sérieux puisque qu'elle implique les deux géants sud-coréens LG et Samsung, concurrents dans le domaine des smartphones et de l'électroménager.

Le siège du groupe LG à Séoul et une usine de Changwon ont été perquisitionnés ce vendredi selon l'agence Yonhap. Des documents et disques durs ont été saisis.

Samsung Electronics accuse de hauts responsables de LG, dont le président de son département électroménager, Jo Seong-Jin, d'avoir volontairement endommagé des lave-linge de sa fabrication dans deux grands magasins d'appareils électroniques de Berlin au mois de septembre, avant le salon professionnel de l'électronique IFA.

Sur les images enregistrées par les caméras de surveillance des boutiques, plusieurs hommes d'origine asiatique -et identifiés comme étant des cadres de LG- détruisent les portes de lave-linge avant de s'enfuir, affirme Samsung Electronics. »

II. Les menaces sur le patrimoine immatériel

⁹<http://www.francesoir.fr/societe-faits-divers/lg-accuse-davoir-sabote-des-lave-linge-samsung>

A. Atteinte à l'information stratégique

Aujourd'hui les entreprises se vouent une véritable guerre de l'information et chaque information détenue par la concurrence est une vraie menace pour l'entreprise.

Certaines informations peuvent être obtenues de façon légale et d'autres de façon illégale, les informations obtenues de manière légale sont généralement des informations publiques que l'entreprise ne peut cacher et dont la connaissance par la concurrence ne présente pas un risque important pour l'entreprise. En revanche les informations obtenues illégalement sont des informations privées que l'entreprise ne souhaite pas divulguer car elles sont des informations essentielles pour la pérennité de l'entreprise et dont la connaissance par la concurrence présente un risque important pour l'avenir de l'entreprise.

Quelles sont les informations stratégiques que la concurrence souhaite récupérer et dans quels domaines se trouvent-elles ?

La recherche et développement :

¹⁰« La fonction Recherche & Développement regroupe l'ensemble des processus qui, partant de la recherche fondamentale ou d'une invention, assurent sa faisabilité industrielle. Il s'agit donc de l'ensemble des étapes permettant de passer du laboratoire de recherche à la production industrielle en usine. »

Le domaine de l'entreprise le plus sensible dont les informations sont certainement les plus vitales pour l'entreprise à surveiller est au niveau de la recherche et développement.

La recherche et développement est le pôle de recherche et d'innovation de l'entreprise c'est là où se conçoit les projets futurs de l'entreprise pour assurer sa pérennité en se développant, l'entreprise doit être en développement constant pour obtenir un avantage concurrentiel. Car une entreprise qui reste sur ses acquis est une entreprise qui recule car le marché lui évolue en permanence.

¹⁰ <http://www.economie.gouv.fr/facileco/fonction-recherche-developpement>

Mais ce domaine possède une contrainte de couts, l'investissement dans la recherche et développement représente un cout énorme pour l'entreprise c'est pour cela que les concurrents peuvent tenter de porter atteinte à la confidentialité de ces informations.

Dans le but de connaitre les projets de ses concurrents leur niveau de recherche actuel et les moyens mis en œuvre pour se comparer face à la concurrence mais le but peut être aussi de voler ses informations et de s'en servir au sein de leur propre pôle de recherche et développement. Cela est un gain énorme financier car c'est l'obtention d'informations pouvant permettre le développement de l'entreprise sans l'investissement financier qu'il en impose.

Pour exemple prenons le cas du Concorde:

Le 29 novembre 1962, un accord est réalisé entre un constructeur d'aéronautique français Sud-Avion et un constructeur britannique Bristol Aéroplane Company dans le but de créer le premier avion civil supersonique. Mais ce projet va être devancé par la Russie grâce à leur avion nommée Tupolev 44.

On se rend vite compte que cet avion présente de troublantes ressemblances avec le Concorde et une enquête est menée et en 1965 Sergei Pavlov, directeur du bureau parisien d'Aeroflot, est arrêté en possession de plan du Concorde.

Les plans retrouvés sont les plans détaillés des freins, les plans du train d'atterrissage et la cellule du Concorde. Cela montre belle et bien que la création du Tupolev 44 a pu se faire grâce à des informations volées.

Alors que le Concorde devait être le premier avion civil supersonique il a vu apparaitre un concurrent inattendu et cela à cause d'un espionnage dans leur recherche. Le Concorde a donc perdu son avantage concurrentiel et le monopole du marché qu'il était censé obtenir.

L'information Marketing :

La concurrence a également grand intérêt à obtenir des informations sur la stratégie marketing de l'entreprise.

Au niveau marketing la concurrence peut obtenir des informations liées à un nouveau produit qu'il souhaite commercialisé, toutes les études qui entourent ce produit comme le prix de vente le plus juste, les cibles, la manière de le commercialiser.

Toutes ces informations sont déterminées grâce à une étude de marché, celle-ci peut revenir très chère à l'entreprise en fonction du produit mais est essentielle pour ne pas commettre d'erreur. Il peut arriver qu'un produit ayant pourtant une demande importante sur le marché ne se vende pas et cause des pertes à l'entreprise du fait d'un prix non cohérent avec la demande, d'un mauvais point de vente ou d'un mauvais choix de positionnement.

Avec ces informations l'entreprise concurrente peut éviter de réaliser elle-même une étude et réaliser des économies financières à l'insu d'une autre entreprise.

Management:

Le management d'une entreprise peut être décisif dans la réussite de celle-ci, c'est pour cela que dans des domaines d'activités où il est parfois difficile de trouver un mode de management efficace permettant d'accroître la motivation des salariés et d'améliorer la productivité.

C'est pourquoi une entreprise qui fonctionne bien en terme de management peut se voir espionner par des concurrents, mais elle a tout intérêt de conserver pour elle ces informations pour conserver l'avantage qu'il lui confère.

Financier:

¹¹« L'information financière est bien souvent la seule source disponible pour un analyste externe, d'où l'importance de disposer d'une information détaillée reflétant la réalité économique de l'entreprise. » Les Echos.

Des informations sur l'état financier d'une entreprise peuvent être très utiles pour porter atteinte à celle-ci, dans le cas où une entreprise présente certaine difficulté financière les concurrents en ayant l'information peuvent être tentés d'entreprendre une action visant à la déstabiliser davantage.

En effet si un concurrent voit une faiblesse financière comme des marges faibles chez son concurrent et que pour lui en revanche elles sont plus grandes il pourra créer une nouvelle politique de prix en les réduisant sachant bien que le concurrent ne pourra pas s'aligner et par conséquent faire couler l'entreprise concurrente.

¹¹ http://www.lesechos.fr/finance-marches/vernimmen/definition_information-financiere.html

Au contraire si les concurrents ne connaissent la situation des autres entreprises ils n'iront pas tenter de telles actions car on ne se s'attaque pas à un concurrent que l'on pense solide.

B. Atteinte au système d'information

¹²« La technologie évolue à une vitesse fulgurante, plus un seul métier n'est exclu du système d'information. Tous les dirigeants d'entreprises intègrent dans leur stratégie le fait que le XXI ème siècle sera celui de « l'information. ». La fonction informatique, ou plutôt la fonction système d'information, est au coeur du déploiement des stratégies d'aujourd'hui et de demain. Son caractère essentiellement transverse en fait l'une des fonctions les plus difficiles à gérer, donc à piloter. » Christophe LEGRENZI et Jacques NAU.

L'entreprise doit être vigilante à son système d'information car une atteinte de la concurrence envers son système d'information peut engendrer de lourdes conséquences.

Le système d'information c'est un ensemble organisé des ressources de l'entreprise permettant d'acquérir, de traiter, de stocker et de communiquer les informations au sein de l'organisation.

Quels est le but d'une atteinte du système d'information par la concurrence ?

- Déstabiliser l'entreprise: En bloquant l'accès a certain service ou supprimer des données se trouvant dans le système pour handicaper l'entreprise dans son bon fonctionnement.
- Prendre des informations stratégiques: Le piratage du système d'informations donne accès à des données confidentielles dont un concurrent pourra se servir à l'encontre de celle-ci.

Quels dispositifs l'entreprise doit-elle surveiller ?

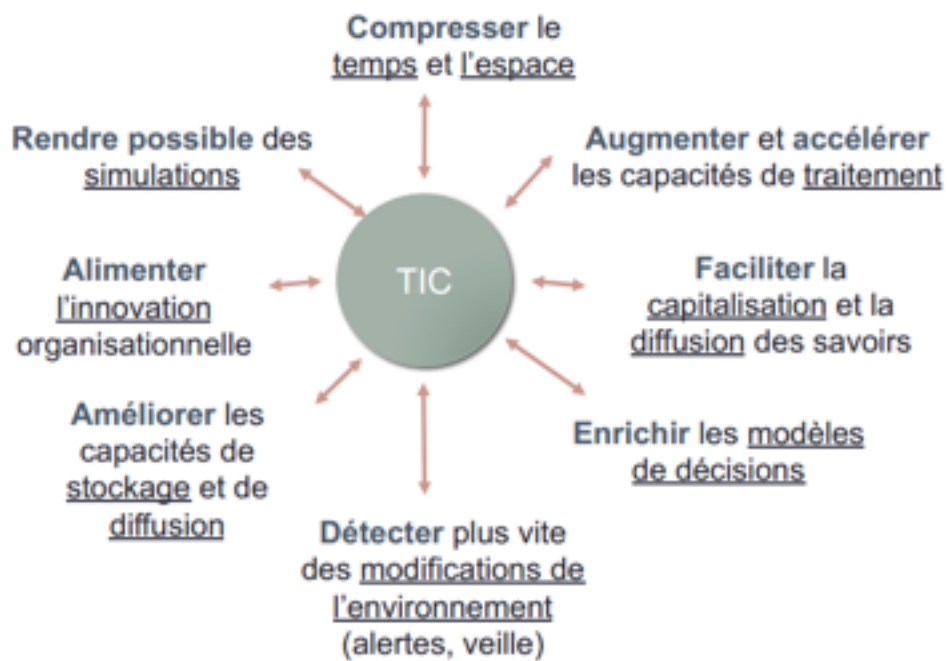
¹² Christophe LEGRENZI et Jacques NAU

- Les Routeurs: La connexion à internet et au réseau interne se fait grâce au routeur, c'est pourquoi la fiabilité du routeur doit être irréprochable. L'entreprise doit sécuriser et surveiller au maximum celle-ci. Une attaque sur cet équipement va engendrer une exposition de l'intégralité des données du routeur.
- Les Liens physiques: Ils permettent le transfert des informations, le danger est qu'ils peuvent être mis en écoute et détournés.
- Les Postes clients: C'est l'outil le plus utilisé au sein de l'entreprise, toutes les caches quotidiennes et le stockage d'informations passent par les postes. La plus grande partie des erreurs et malveillances des employés sont faites sur ces postes c'est pourquoi cet outil est important à surveiller, mais pourtant il est très complexe de les sécuriser.
- Les équipements mobiles: Ces équipements sont de plus en plus utilisés dans les entreprises il s'agit des ordinateurs portables et des téléphones portables, mais ces appareils sont très vulnérables aux attaques.

Quels sont les moyens d'attaque ?

- Un Ver : c'est un logiciel malveillant qui se transmet d'un ordinateur à un autre via internet ou un réseau pour perturber le fonctionnement du système. il se distingue du virus car il ne s'implante pas dans un autre programme.
- Un Virus: c'est un logiciel malveillant de petite taille, qui est transmis par des réseaux ou des supports d'informations amovibles, il s'implante dans des programmes en les parasitant. Les effets d'un virus causent de véritables dommages au système.
- Le Phishing: il a pour but de tromper l'internaute, c'est par exemple une fausse page d'un site bancaire. Grâce à cela il peut obtenir des informations confidentielles. Ces données pourront être utilisées pour détourner de l'argent.
- Les réseaux de robots: cela permet au pirate informatique une prise de contrôle des machines de l'entreprise et de s'en servir.

Les apports:



Comme le montre le schéma ci-dessus les TIC permettent d'améliorer le fonctionnement d'une entreprise de divers moyens:

Ils permettent un gain de temps et d'espace, la capacité de traitement des informations est augmentée et améliorée. La communication interne est améliorée ainsi que la diffusion des savoirs. Cela permet l'enrichissement des modèles de décisions, d'améliorer la détection des modifications de l'environnement, améliorer les capacités de stockage notamment grâce à la dématérialisation, alimenter l'innovation organisationnelles et la possibilité de faire des simulations.

C. Atteinte à l'image et à la réputation

Aujourd'hui l'image de l'entreprise est essentielle à sa compétitivité sur le marché ; à produits égaux l'image d'une marque vis à vis de l'autre peut être un facteur décisif chez le client. Ce phénomène est très présent notamment dans le secteur de la téléphonie entre Apple et Samsung. Leurs smartphones ont des caractéristiques techniques, des prix et des prestations

similaires donc le choix du client se fait selon l'image que reflète pour lui l'une ou l'autre marque.

On peut définir l'image de la façon suivante: ¹³« *L'image c'est la façon dont l'entreprise est perçue par les consommateurs.* ».

Mais cette image est pour l'entreprise de plus en plus compliquée à contrôler et cela est dû principalement à Internet.

80% des discours tenus sur les marques sont effectués par les internautes, cela montre l'importance des commentaires qui sont diffusés et l'impact qu'ils peuvent avoir sur l'entreprise.

Le danger d'internet vient du fait que tous les internautes peuvent s'exprimer librement, en soit cela est la liberté d'expression et ne pose aucun problème mais certains commentaires ou avis peuvent être les fruits d'un concurrent peu scrupuleux dans le but d'entacher l'image et les réputations des autres entreprises du marché.

C'est pour cela qu'il est important pour l'entreprise de prendre en compte un certain nombre de facteurs lorsqu'elle met en place son positionnement. En effet, il est compliqué aujourd'hui de faire coller parfaitement son positionnement avec l'image qu'a le consommateur de la marque. Il y a de cela plusieurs années où il suffisait à une entreprise de choisir son positionnement et d'en faire la promotion au travers d'une campagne publicitaire, pour que celle-ci soit acceptée et comprise par les clients potentiels.

Pour exemple, auparavant, une entreprise qui souhaite se donner une image écologique et soucieuse de l'environnement, n'avait qu'à faire passer cette image au sein de sa campagne publicitaire pour que les clients aient cette image en tête de l'entreprise.

Cela était possible car il y avait peu de moyens de recherche et de diffusion de l'information pour démonter le contraire.

Aujourd'hui cela est totalement différent, l'image de l'entreprise peut être vite entachée par un scandale fondé ou non, car les informations se propagent très rapidement, l'insatisfaction d'un client peut faire le tour du monde en peu de temps.

¹³ <http://www.definitions-marketing.com>

Le site journal nous donne les pratiques couramment utilisé pour détériorer la réputation de l'entreprise

¹⁴« -Les faux avis de consommateurs mis en ligne par une entreprise visant à manipuler sa réputation ou mis en ligne par une entreprise concurrente, et édités par ses salariés ou des entreprises spécialisées dans la rédactions de faux commentaires.

-Le dénigrement et la diffusion de fausses informations.

-La divulgation d'informations personnelles sur les clients ou dirigeants de l'entreprise pouvant porter atteinte à leur vie privée ou au droit à l'image ou la divulgation d'informations confidentielles.

-La diffamation et l'injure. »

Comment l'image de la marque peut-elle être détériorée ?

L'entreprise peut subir:

➤ Un dénigrement de sa marque.

La jurisprudence exige trois conditions pour que le dénigrement soit reconnu:

- ¹⁵« Les propos doivent avoir un caractère péjoratif. »
- « Les propos doivent être rendus publics »
- « Les propos doivent viser une entreprise identifiable, sa marque ou ses produits »

Le dénigrement est défini par un arrêt de la cour d'appel de Versailles du 9 septembre 1999.

¹⁶« *Le dénigrement se définit comme le fait de porter atteinte à l'image de marque d'une entreprise ou d'un produit désigné ou identifiable afin de détourner la clientèle en usant de propos et d'argument répréhensible ayant ou non une base exacte, diffusés ou émis de*

¹⁴ <http://www.journaldunet.com/ebusiness/expert/51170/les-atteintes-a-l-e-reputation-de-l-entreprise---comment-defendre-son-image-de-marque-sur-internet.shtml>

¹⁵<http://www.le-droit-des-affaires.com/denigrement-definition-et-sanctions-article233.html>

¹⁶ Arrêt de la cour d'appel de Versailles du 9 septembre 1999

manière à toucher les clients de l'entreprise visée, concurrent ou non de celle qui en est l'auteur. »

➤ Diffamation d'un dirigeant.

La diffamation est similaire au dénigrement en revanche il existe une distinction, la diffamation contrairement au dénigrement touche une personne physique.

La diffamation est définie par une loi sur la liberté de la presse de 1881.

¹⁷« *L'allégation ou l'imputation d'un fait qui porte atteintes à l'honneur ou à la considération de la personne à laquelle le fait est imputé. »*

Une atteinte sur un dirigeant pour mettre en cause la crédibilité de l'entreprise, les salariés peuvent remettre en question l'autorité de ses dirigeants et par conséquent créer un dysfonctionnement au sein de l'organisation.

➤ Utilisation de la marque sans autorisation

L'utilisation de la marque à des fins frauduleuses peut porter grandement atteinte à la marque, notamment les contrefaçons qui entraîne une perte de l'image de la marque et une perte de notoriété, cela est très dévalorisant pour les entreprises qui en sont victimes.

D. Atteinte au capital

Une entreprise peut être victime d'une OPA hostile c'est à dire une offre publique d'achat sans le consentement du conseil d'administration et qui va s'opposer à cette OPA.

Le but de l'OPA est d'acquérir une part significative du capital d'une société pour prendre le contrôle de celle-ci.

¹⁷ Loi du 29 juillet 1881 sur la liberté de la presse, Article 29

Les grandes sociétés à forte capitalisation sont susceptibles d'être victime d'une OPA hostile car une grande partie des actions appartiennent à des milliers de petits actionnaires qui eux risquent de vendre facilement lors d'une offre publique d'achat.

Le risque également lié à une OPA est la déstabilisation de la société, effectivement une OPA agressive peut entacher le moral des salariés et inquiéter les dirigeants à l'inverse d'une OPA amicale.

Une entreprise extérieure peut également utiliser une méthode nommée « ramassage de titres », qui consiste à acheter des actions de la société visées directement sur les marchés boursiers en passant des ordres de bourses. Ces achats se font au prix réel de l'action au moment donné. Cette méthode d'acquisition de titres peut être nuisible pour l'entreprise car elle ne s'aperçoit pas immédiatement de l'entrée en capital du concurrent car celle-ci se fait progressivement.

Prenons en exemple l'affaire en le groupe de luxe LVMH et Hermès, celle ci racontée dans un article de Le Huffington Post du 30 mai 2013:

¹⁸« En 2010 le groupe LVMH fait une entrée frauduleuse au sein du capital de son concurrent Hermès.

Il est essentiel d'étudier ce cas pour comprendre comment un concurrent peut porter atteinte au capital d'une autre entreprise.

Le ramassage d'action d'Hermès par LVMH a commencé en 2001, cette année-là le groupe LVMH achète précisément 4,9% des actions Hermès en passant par des filiales du groupe au Luxembourg et aux États-Unis. Volontairement le groupe n'a pas acquis plus de 4,9% du capital d'Hermès car lorsqu'une entreprise possède au moins 5% du capital d'une autre entreprise elle doit en informer celle-ci.

Puis c'est en 2006 que le groupe va poursuivre sa prise du capital de Hermès, c'est au travers d'*equity swaps* qui est un moyen de jouer des titres boursiers sans pour autant les posséder avec l'option de les obtenir à terme que le groupe LVMH va poursuivre son offensif. Et c'est par l'intermédiaire de trois banques que va procéder le rachat des titres, 4,7% par Natixis, 4,5% par la Société Générale et 3% par le Crédit Agricole.

¹⁸http://www.huffingtonpost.fr/2013/05/31/affaire-hermes-lvmh-bernard-arnault-puech-equity-swaps_n_3364469.html

Et au mois de juin 2010 le groupe LVMH demande à ces trois banques Natixis, la Société Générale et le Crédit Agricole d'être payé en actions et non pas en argent, c'est à ce moment-là que Bernard Arnault PDG du groupe fait l'annonce officielle de la possession de 14,1% de Hermès. LVMH ira jusqu'à posséder plus de 23% du capital Hermès. »

Cela a été une vraie atteinte pour Hermès car son concurrent détient désormais un pourcentage significatif de leur capital et fait partie des plus importants actionnaires du groupe, il a donc maintenant un contrôle au sein du groupe et peut prendre part aux décisions du conseil d'administration.

Conclusion: Lorsque l'on répertorie toute les menaces potentielles on s'aperçoit qu'elles peuvent toucher l'ensemble de l'activité et les services de l'entreprise aucun service n'est pas concerné par cela. On s'aperçoit également que se travail de protection ne peut pas se faire par le biais d'un seul service dédié à cela, mais que c'est chaque services qui doivent être concerné et mettre en place des mesures de protection pour protéger domaine d'activité. »

PARTIE III: LES MOYENS DE PROTECTIONS DES MENACES

Introduction:

Chaque menaces que l'entreprise peut subir sont différente et aucune ne peut se traiter de la même façons, d'où l'importance de les avoir distinguer précédemment.

C'est pourquoi il est également essentiel de trouver des solutions spécifique pour chaque menaces en fonction de leur nature et du domaine visé.

On apportera dans cette troisième partie les plus grand nombre de moyens de se protéger de menaces mais également des moyens de résoudre des problèmes suite à une menace subit, car comme on pourra le voir certaine atteinte ne peuvent être évite c'est pourquoi il faut réfléchir et anticiper des moyens de les résoudre ultérieurement.

I. Les moyens de protection sur le patrimoine matériel

A. Les moyens de protection contre les atteintes aux personnes

Pour se prémunir d'une perte d'un élément important à l'entreprise il est essentiel de mettre en place des moyens pour le conserver. Comme on l'a vu dans la partie précédente un concurrent peut vouloir récupérer un des collaborateurs d'une autre entreprise, en passant notamment par un chasseur de tête.

Pour éviter cela il faut tout d'abord savoir reconnaître les collaborateurs clé de l'entreprise. En mettant en place un système qui permet de cibler et mettre en avant les compétences des salariés l'entreprise. Une fois que l'entreprise a distingué ses éléments clé il doit tout mettre en place pour les conserver en son sein.

Et cela passe par:

- Une rémunération cohérente au travail: le salarié ne doit pas réaliser des tâches et avoir des responsabilités élevées et une rémunération inférieure à la valeur qu'il crée pour l'entreprise.
- Un environnement de travail agréable: Le salarié ne doit pas travailler dans de mauvaises conditions et l'entreprise doit veiller à lui mettre les moyens nécessaires à disposition pour la réalisation des tâches qui lui sont demandées.
- Considérer le salarié: Aujourd'hui la rémunération n'est pas le seul facteur de motivation pour un salarié, il a également besoin que son travail soit reconnu. Mettre en avant ses bons résultats et le féliciter est essentiel.

Cette manœuvre de la concurrence ne fait pas l'objet d'une condamnation devant un tribunal car c'est une action parfaitement légale devant la loi.

En ce qui concerne une atteinte à la personne physique du salarié il existe peu de moyens de prévenir cet acte mais il existe des moyens d'atténuer le préjudice causé.

L'entreprise peut prévoir une assurance pour un homme clé.

Que prend en charge l'assurance homme clé ?

- L'assurance prend en compte les pertes d'exploitations
- Elle rembourse les prêts bancaires
- Les frais liés à la réorganisation.

L'assurance est une charge pour l'entreprise mais elle présente un grand nombre d'avantages lors d'un problème de ce genre.

B. Les moyens de protection contre les atteintes aux biens

Les attaques sur les biens sont généralement réalisées par des infractions au sein de l'entreprise ou du site de production.

C'est pour cela que pour se prévenir de ces délits l'entreprise doit mettre en place des moyens de sécurité.

Les moyens de sécurité sont divers. Tout d'abord l'entreprise doit bien veiller à avoir la meilleure assurance possible pour gérer une telle situation. Il est très utile pour l'entreprise de mettre en place un dispositif de caméra de surveillance. Les caméras permettent d'une part de dissuader les potentiels malfrats et également d'obtenir une preuve réelle du délit commis et d'accélérer les procédures de remboursement des assurances.

Mais les caméras n'agissent que une fois le délit commis, il faut également des moyens de sécurité qui empêche l'acte en lui-même, faire appel à une compagnie de surveillance et de

mettre un maitre-chien sur les lieux pour sécuriser l'entreprise est un moyens efficace de se protéger.

Ce dispositif comme les assurances représente un coup pour l'entreprise mais il faut regarder les pertes qu'une atteinte à ce patrimoine pourrait couter à l'entreprise.

II. Les moyens de protection sur le patrimoine immatériel

A. Les moyens de protection contre les atteintes à l'information stratégique

Si l'entreprise a été victime d'un espionnage industriel et que le concurrent a obtenu des informations sur des avancées technologiques il pourra s'en servir pour son développement et devancer son concurrent grâce à ses propres recherches.

La solution la plus efficace pour empêcher le concurrent d'exploiter ces informations est de faire breveter toutes les nouvelles découvertes trouvées par l'entreprise.

La définition du brevet donné par l'INPI (institut national de la propriété industrielle) est :

¹⁹« *Le brevet protège une innovation technique, c'est-à-dire un produit ou un procédé qui apporte une nouvelle solution technique à un problème technique donnée.* »

C'est à dire que l'exploitation du brevet ne pourra se faire uniquement par le détenteur de celui-ci, donc aucune entreprise concurrente ne pourra pas l'utiliser son peine de poursuites juridiques pour atteinte à la propriété intellectuelle.

Cette exclusivité aura pour effet 20 ans.

Toute fois si il est possible pour l'entreprise de conserver les informations liés à son brevet il peut être parfois judicieux de ne pas breveter immédiatement une découverte. Le brevet rendent l'invention public la concurrence pourra pas conséquent avoir accès aux informations

¹⁹ <http://www.inpi.fr/fr/brevets/qu-est-ce-qu-un-brevet.html>

relative à celui là et de le copier de façons différente et par conséquent de ne pas être illégale vis à vis de la loi.

Les informations peuvent être transmises par les salariés eux même, c'est rarement dans le but de nuire à l'entreprise mais cela est souvent fait de façon intentionnelle. Un ingénieur fier du travail qu'il est en train de réaliser peut facilement en parler autour de lui, sans se rendre compte que ses paroles peuvent arriver aux oreilles des concurrents. Lors de salon ou congrès ou sont réunis plusieurs concurrents du même secteur d'activité il est de coutume qu'ils viennent se questionner entre eux pour obtenir des informations sur la concurrence.

Pour prévenir cela il est essentiel de sensibiliser les salariés à l'importance des informations qu'ils diffusent et de montrer les enjeux de ses informations pour l'entreprise.

Il faut également surveiller les stagiaires, présents dans l'entreprise pour une durée temporaire. Les entreprises sont généralement peu méfiantes d'eux mais durant leur période de stage ils ont un accès à un grand nombre d'informations. On n'imagine jamais la possibilité qu'il soit envoyé par un concurrent pour espionner mais cela existe vraiment, c'est pourquoi il faut avoir un œil attentif au stagiaire que l'entreprise prend et de ne pas leur donner une trop grande liberté d'accès aux fichiers. Et même si ce stagiaire n'est pas envoyé directement par un concurrent on ne sait pas si un jour il ira postuler pour une entreprise concurrente et divulgué ce qu'il a vu lors de son stage.

L'entreprise doit éviter de prendre des stagiaires hors convention scolaire et de bien comprendre ses motivations lors d'un entretien effectué préalablement avant d'accepter sa candidature.

Un ancien salarié peut être également tenté de nuire à l'entreprise en allant divulguer des informations à la concurrence, si son licenciement c'est passé dans de mauvaises conditions. Il faut faire signer une clause de confidentialité au salarié.

Une clause de confidentialité oblige le salarié à ne pas divulguer des informations sensibles au sujet de l'entreprise.

Cela prend en compte:

- Les données et les informations stratégiques de l'entreprise.
- L'état financier de l'entreprise, le portefeuille-clients, la stratégie commerciale etc...

La clause de confidentialité peut être faite signer à un salarié peu importe son échelon cadre ou non cadre et à tous types de contrat à durée indéterminé, déterminée et également au stagiaire.

Le salarié qui ne respecte pas cette clause risque un licenciement s'il est toujours salarié de l'entreprise et il prend la responsabilité civile et financière des dommages et préjudices subis par l'entreprise.

Si l'entreprise concurrente tente de concurrencer grâce à des prix faibles, il est essentiel pour pouvoir s'aligner de comprendre comment le concurrent fait-il pour baisser ses coûts. Pour cela il faut chercher à connaître ses modes de fabrications, de distribution ... surement plus efficace les vôtres. Mais également se renseigner sur ses fournisseurs les prix qu'ils pratiquent et si les prix de ceux ci sont plus attractif alors chez de fournisseurs.

Affaire Oberthur:

²⁰« Les collaborateurs d'Oberthur, troisième imprimeur mondial de billets de banque et spécialiste des moyens de paiement, se souviendront longtemps de l'année 2011 qui s'annonçait pourtant sous les meilleurs auspices, puisque leur entreprise confortait de manière insolente son leadership sur le marché comme en témoigne l'émission d'une proposition de rachat de l'un de ses concurrents. Paradoxalement ce fut aussi une année de sueurs froides. L'entreprise fut en effet victime d'une action de renseignement économique. Les espions tentent des approches humaines de certains collaborateurs, « contactés par téléphone ou via les réseaux sociaux

comme LinkedIn dans un français parfois approximatif. Ces interlocuteurs étaient tantôt journalistes, tantôt stagiaires, voire même... de prétendus représentants de banque centrale! » Des approches par mail sont également détectées. L'attaque prend une telle ampleur que le management d'Oberthur est obligé de réagir en sensibilisant le personnel par écrit en

²⁰ Romain Zerbib, 2012

l'invitant à la plus grande prudence. Les informations collectées probablement par un concurrent peuvent servir à savoir pour agir ou comme outil de déstabilisation. Didier Lucas et Alain Tiffreau soulignaient que »²¹« les cas de déstabilisation stratégique par l'information abondent (...) pour des entreprises confrontées quotidiennement aux agissements agressif de la concurrence»

B. Les moyens de protection contre une atteinte au système d'information.

Le système d'information d'une entreprise est capital pour une entreprise car il contient l'intégralité des informations de l'entreprise, c'est pourquoi il faut se protéger de toutes menaces venant de la concurrence.

Il est essentiel pour l'entreprise de créer un véritable service dédié à cette mission, pour les PME et TPE qui ne peuvent pas se permettre de créer un tel service, il ne faut pas pour autant déléguer cette mission et la confier alors à un sous-traitant spécialisé.

L'information numérique est vulnérable. En effet, elle peut être détruite, falsifiée ou modifiée. Pour ce type d'informations, il n'existe pas d'original, ni de copies mais des clones.

De plus l'information numérique est volatile qui peut être ajustée, personnalisée.

La sécurité des technologies de l'information peut s'évaluer suivant 3 principaux critères :

- Disponibilité : garantit l'accès aux informations du système
- Intégrité : prévention de modifications ou de suppressions non autorisée d'informations
- Confidentialité : absence de divulgation non autorisée d'informations

Afin de garantir la sécurité du système d'informations, l'entreprise est dans l'obligation de définir une Politique de Sécurité (PSI).

Les principales étapes d'une politique de sécurité d'un système d'informations sont :

²¹ Alain Tiffreau, 2001

1. Audit : des besoins qu'on a en termes d'information
2. Elaboration des règles et de procédures pour chaque situation
3. Surveillance de la vulnérabilité du SI
4. Actions à entreprendre en cas de menaces

Cette politique de sécurité passe par la mise en place de différents outils technologiques :

- Contrôle d'accès (blocage d'accès aux personnes non-autorisées en interne et en externe / authentification : mot de passe, carte à puce, biométrie)
- Pare-feu (placé entre les réseaux privés internes et les réseaux externes non sécurisés comme internet)
- Anti-virus (protection de l'ordinateur)
- Normes de sécurité des réseaux sans fil

L'entreprise a également la possibilité d'externaliser la sécurité du système d'information. Cette externalisation permet d'éviter les coûts importants de mise en place des précédentes étapes. On également faire appel à un fournisseur de gestion de services de sécurité qui va être en charge de la surveillance de l'activité du réseau, des tests de vulnérabilité, de l'infrastructure de secours. De plus cette externalisation va permettre à l'entreprise de disposer du savoir-faire pointu du sous-traitant car ce sont des métiers très techniques dans lesquels la moindre erreur peut être fatale.

Les informations sont vitales pour les entreprises. La sécurité informatique est incontournable et nécessite une recherche indépendante.

²²« Au moins 48 sociétés du secteur de la défense et de l'industrie chimique ont été victimes d'une série d'intrusions informatiques coordonnées, selon un nouveau rapport de sécurité du

²²Plusieurs groupes de défense et de chimie victimes de cyberespionnage, LeMonde.fr, 14/03/2012, http://www.lemonde.fr/technologies/article/2011/11/01/plusieurs-groupes-de-defense-et-de-chimie-victimes-de-cyberespionnage_1596689_651865.html?xtmc=espionnage_industriel&xtcr=15

groupe Symantec. Les ordinateurs de ces sociétés ont été infectés par un programme malveillant connu sous le nom de "PoisonIvy". Ce maliciel est utilisé pour dérober des informations. Les noms des sociétés concernées n'ont pas été révélés mais le groupe précise que la plupart des ordinateurs touchés se situent aux Etats-Unis, au Bangladesh et au Royaume-Uni. Parmi les

entreprises affectées, 29 sont des groupes chimiques. Certaines d'entre elles développent par ailleurs des matériaux utilisés pour les véhicules militaires. "Ces attaques semblent avoir pour objectif de l'espionnage industriel. Il s'agit de rassembler des informations protégées par la propriété intellectuelle pour avoir un avantage concurrentiel", explique Symantec [...] Au mois d'août, la société américaine de sécurité informatique McAfee a rapporté que plus de 70 organisations et gouvernements - dont l'ONU et des groupes américains de défense - ont été victimes d'une vaste opération de cyberespionnage ces dernières années».

C. Les moyens de protection contre une atteinte à l'image et à la réputation.

Une image dégradée de l'entreprise peut vite impacter ses résultats financiers c'est pourquoi il faut réagir vite et mettre en place des moyens pour empêcher une dégradation de l'image et la réputation.

Henry Ford mentionnait déjà cette notion de réputation à son époque en disant ²³« *Deux choses importantes n'apparaissent pas au bilan de l'entreprise, sa réputation et ses hommes.* »

Pour donner un exemple prenons l'affaire du saumon:

²³ Henry Ford

²⁴« Une étude publiée, en 2004, par la revue Science prétendait démontrer les risques pour la santé que pouvait présenter une consommation de saumon d'élevage. [...] Cette étude qui opposait la nocivité du saumon d'élevage (essentiellement européen et chilien) aux bienfaits de la consommation de saumon sauvage (en particulier celui provenant d'Alaska) ont fait énormément de mal à l'industrie européenne [...] On estime les pertes à 25 millions d'euros [...] L'étude a été financée par une fondation, la Pew Charitable Trusts, où siègent des producteurs de saumon d'Alaska [...]. Depuis longtemps, les Américains tentent d'exclure le saumon d'élevage de leur marché. Les producteurs chiliens de saumon d'élevage, qui produisent 70 % du saumon consommé aux Etats-Unis, ont déjà été victimes de ces tentatives d'exclusion».

La première chose que doit faire une entreprise pour ne pas perdre le contrôle de son image est avant tout de repérer qui sont les influenceurs (blogueur, journaliste, forum ...)

L'entreprise doit mettre en place une veille pour évaluer sa réputation et son image, pour agir l'entreprise doit savoir où elle se situe vis à vis de ses clients. Il existe pour cela des sites comme TrebbyBuzz qui réalise ce travail en s'appuyant sur les discours faits par les internautes et blogueur, le site Wasalive lui trace les mots clé sur tous les supports web.

Mis à part pour les petites sociétés, une grosse société ne peut se contenter d'outils gratuits pour réaliser cette veille, elle a besoin d'outils professionnels performants. Ces logiciels permettent de collecter l'ensemble des messages qui correspondent à l'entreprise et de les transmettre hiérarchisés.

Mais il existe également des sociétés spécialisés qui peuvent réaliser cette veille pour l'entreprise et proposer des stratégies adaptées au problème soulevé.

Le facteur principal au contrôle de la réputation et à l'image de l'entreprise est la réactivité de l'action, lorsque que l'entreprise est victime d'une information dégradante à son image sur

²⁴Affaire du Saumon, Interview de Philippe Barbe, PDG de Direct Ocean, Infoguerre.fr, 16/05/2004 : <http://www.infoguerre.fr/interviews/affaire-du-saumon-interview-de-philippe-barbe-pdg-de-direct-ocean/>

internet elle ne peut se permettre d'attendre et de prendre du recul sur l'information il faut impérativement réagir vite pour stopper la propagation de celle-ci.

L'entreprise doit se créer une communauté sur internet et pour passer d'un média qui échange directement avec le consommateur et non pas d'un média classique où le discours na vas uniquement dans un sens.

Il est également important que l'entreprise ne voit pas un mauvais buzz comme une attaque mais comme une réflexion de sa clientèles et de comprendre la source de celle-ci et d'y répondre pour satisfaire sa clientèles.

D. Les moyens de protection d'une atteinte au capital

Les sociétés qui ont un risque fort d'être atteintes au niveau de leur capital sont les sociétés anonymes mises en bourse.

L'affaire Goldsmith, BTA:

²⁵« L'OPA la plus ambitieuse de la décennie a surgit en juillet à la city de Londres. Sir James Goldsmith part en croisade pour conquérir BAT (British American Tobacco). Pour ce coup, James Goldsmith s'assure de puissants alliés, Jacob Rothschild et Kerry Packer. Les trois mauvais garçons des finances se fédèrent dans une holding: Hoylake. Les sommes en jeu représentent 135 milliards de francs. Pour se défendre, BAT engage Kroll Associates.

L'agence

possède un dossier sur James Goldsmith depuis 1979. Le pilier de la finance britannique, endurci par plusieurs années à la City - où toute notion de fair-play se volatilise devant le tableau des valeurs -, prévient tous les coups, évite les pièges. Probablement épaulée par d'anciens des services anglais, la holding Hoylake identifie les activités et méthodes nouvelles de Kroll et les dénonce publiquement. L'affaire fait grand bruit. Le Sunday Times explique

²⁵DASQUIE, G. (1999), Les services secrets infiltrent les entreprises, Flammarion.

comment les agents de Kroll fouillent les poubelles. À la Chambre des communes, le député Gerald Howarth, ami du financier, prononce un bref discours alarmiste : il soupçonne les agents de Kroll de pratiquer des écoutes téléphoniques sauvages».

Le danger fort est une OPA hostile (non amicale) pour une société dont un actionnaire est majoritaire, c'est à dire qu'il détient plus de 50% du capital de la société les risques d'OPA sont faibles. En revanche dans le cas contraire les risques sont forts.

Pour une société où il n'y a pas d'actionnaires majoritaires et dont le capital est majoritairement flottant, c'est à dire que la majorité des actions sont détenues par des petits actionnaires, l'entreprise peut être facilement la cible d'une OPA et un nouvel actionnaire pourra facilement prendre le contrôle de celle-ci.

Si la société est victime d'un ramassage d'action celle-ci est protégée par l'AMF (Autorité des marchés financiers) qui oblige la société qui rachète des actions à en informer celle-ci à partir d'un certain pourcentage : 5%,10%

Conclusion:

Même si il est impossible pour une entreprise de se protéger entièrement des menaces qu'elle peut subir par sa concurrence, on s'aperçoit que si celle ci fait un travail d'étude de ces menaces, elle peut en éviter un grand nombre et réagir plus vite lorsqu'elle en subit. Certain moyens de protection nécessite des outils et un investissement et d'autre ne sont simplement que des conduites à adopter au sein de l'organisation.

Les entreprises ne doivent pas reculer face au investissement financier que certain moyens de protection peuvent couter car les conséquences de certaines atteintes sont parfois beaucoup plus couteuse.

Conclusion

Ce mémoire a pour visé de répondre à la problématique suivante, Comment se préserver de l'intelligence économique de la concurrence ?

L'étude de cette problématique a été traité en trois parties, tout d'abord une première partie où l'on a définie l'intelligence économique et la veille stratégique, leur principe, leur enjeux.

L'intérêt de cette partie était de montrer les outils dont les organisations peuvent faire usage pour le développement et la protection de leur activité.

La deuxième partie de ce mémoire a elle pour but de répertorier l'ensemble des menaces qu'une organisation peut subir de la part de ses concurrents, en les catégorisant selon la nature de la menace.

La troisième partie elle met en lien les deux première parties et montre comment les outils et les concept exposé en premier partie peuvent répondre et être essentiel à la protections des menaces définis dans la seconde partie.

Cette étude montre qu'une organisation avec des moyens mis en oeuvre peut se protéger, anticiper et contrer les actions vulnérables de la concurrence. Bien évidemment il existe des menaces qu'une entreprise ne peut anticiper mais si elle est préparer à tous types de déstabilisations et qu'elle à mis en place les outils nécessaires elle pourra alors réagir rapidement et limiter l'impact de celle ci. L'entreprise doit être constamment sur ses gardes et ne jamais sous estimer une menace, on peut notamment citer pour illustrer cela Nokia, fabricant de téléphonie et leader mondial faire faillite car elle n'a pas su anticiper les menaces qui présenter l'arrivé des smartphones.

Certaines menaces peuvent présenter des signaux menaçant fort mais leur impact seront faible mais au contraire des signaux de menaces qui peuvent paraître faible mais auront un impact fort sur l'entreprise. Cela montre l'importance pour une entreprise d'être en veille constante.