L'utilisation des tic en intelligence économique : le revers de la médaille

Philippe Pinczon Du Sel, Philippe Dumas, Eric Boutin

L'UTILISATION DES TIC EN INTELLIGENCE ECONOMIQUE :
LE REVERS DE LA MÉDAILLE

Philippe Pinczon du Sel,
Doctorant en Sciences de l'information - communication
pinczon@univ-tln.fr, + 33 4 94 14 28 56

Philippe Dumas,
Professeur des universités en Sciences de l'information - communication
dumas@univ-tln.fr, + 33 4 94 14 22 36

Eric Boutin,
Maître de conférences en Sciences de l'information - communication
boutin@univ-tln.fr, + 33 4 94 14 23 56

Résumé : Les Tic sont présentes à tous les niveaux du cycle de l'intelligence économique au sein des entreprises, permettant en cela d'améliorer considérablement l'efficacité d'un tel système. Mais la méconnaissance des principes de fonctionnement des Tic, notamment ceux ayant un rapport direct avec l'utilisation d'internet, peut entraîner de graves préjudices en termes de sécurisation du processus. Cet article propose une modélisation du processus de l'intelligence économique conduit au travers des Tic et présente les conséquences d'une mauvaise prise en considération de la dimension sécuritaire.

Summary: New technologies are nowadays essential for business watch processes so much as they enhance business efficiency. But these new technologies, among which the internet, cause serious hacking problems and well-known techniques such as spywares offer anyone the possibility to retrieve information from any computer on-line. Introducing a global matrix, this article explains how these new technologies can corrupt the business watch process of a company.

Mots clés : Tic, cycle du renseignement, intelligence économique, veille technologique, internet, piratage informatique, cookies, logiciels espions, social-engineering.

L'utilisation des Tic en Intelligence Economique :

Le revers de la médaille

Les processus d'intelligence économique déployés dans les entreprises sont actuellement largement dépendants des Technologies de l'Information et de la Communication (Tic). Ces technologies offrent en particulier une grande vulnérabilité face aux attaques et aux tentatives d'intrusions. Le piratage en est la forme la plus médiatique mais il existe aussi des technologies moins connues permettant à tout un chacun de se procurer facilement de l'information privée sur toute personne ou entreprise régulièrement connectée sur un réseau.

Au travers de cet article, nous verrons dans un premier temps quelle est la place des Tic dans le processus d'intelligence économique en entreprise. Dans un second temps, nous analyserons le fonctionnement de ces Tic pour en déduire leurs menaces potentielles. Enfin, nous terminerons sur une présentation des conséquences de tels risques pour le processus d'intelligence économique si les capacités des Tic sont sous-estimées.

1. INTELLIGENCE ÉCONOMIQUE ET TIC

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 (Jacobiak, 1998). Le rapport Martre (1994) précise que ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaire à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût. Selon Carayon (2003), l'intelligence économique est une politique publique de compétitivité, de sécurité économique et d'influence qui concerne plus particulièrement les marchés « stratégiques » dans lesquels ce ne sont pas la qualité ou le prix des produits et services qui font la différence mais bien l'accompagnement politique des états qui permet de les conquérir. Enfin, Alain Juillet (2005) ajoute que l'Intelligence économique consiste en la maîtrise et la protection de l'information stratégique pour tout acteur économique et a pour triple finalité la compétitivité du tissu industriel, la sécurité de l'économie et des entreprises et le renforcement de l'influence de notre pays.

En pratique, l'intelligence économique est un processus découlant du cycle du renseignement : chacun des acteurs de l'IE se l'est approprié tout en l'habillant d'un vocabulaire distinct (Bulinge, 2001).

Le cycle du renseignement (figure 1) est divisé en quatre étapes (de Guerny, 1993) : *l'orientation* (ou *planification et conduite* selon Baud, 2002), *la collecte*, *l'exploitation* et *la diffusion* (ici associé à la notion *d'utilisation*). Il s'agit bien d'un cycle, puisque le renseignement obtenu d'une part permet d'orienter les besoins nouveaux en renseignements et que, d'autre part, le renseignement lui-même est réévalué en permanence, en fonction de l'évolution de la situation (Baud, 2002).

Au moment de son transfert vers le modèle d'intelligence économique, les termes employés pour décrire chacune des étapes du cycle du renseignement ont été modifiés et adaptés aux situations : ainsi, pour décrire l'étape d'*orientation*, on lit *ciblage* (Lesca, 1994), *expression des besoins* (Oberson, 1997), *identifier* (Allain-Dupré & Duhard, 1997) ou *orientation* (de Vasconcelos, 1999) ; pour la *collecte* on trouve les mots *traque* (Lesca, 1994), *trouver* (Fuld, 1995), *acquérir* (Allain-Dupré & Duhard, 1997), *recueil* (Oberson, 1997) *recherche* (Jacobiak, 2001) ou *appréhension* (Massé & Thibault, 2001) ; l'*exploitation* devient *traitement* (Martinet & Marti, 1995) puis *analyse* (Rouach, 1996) ; seule l'étape de *diffusion* semble faire l'unanimité bien qu'elle soit parfois ajoutée au milieu du processus. Lesca (1994) parle alors d'une première *circulation* entre les étapes de *traque* et d'*exploitation* et Jacobiak (2001) déplace le terme entre la *collecte* et le *traitement*.

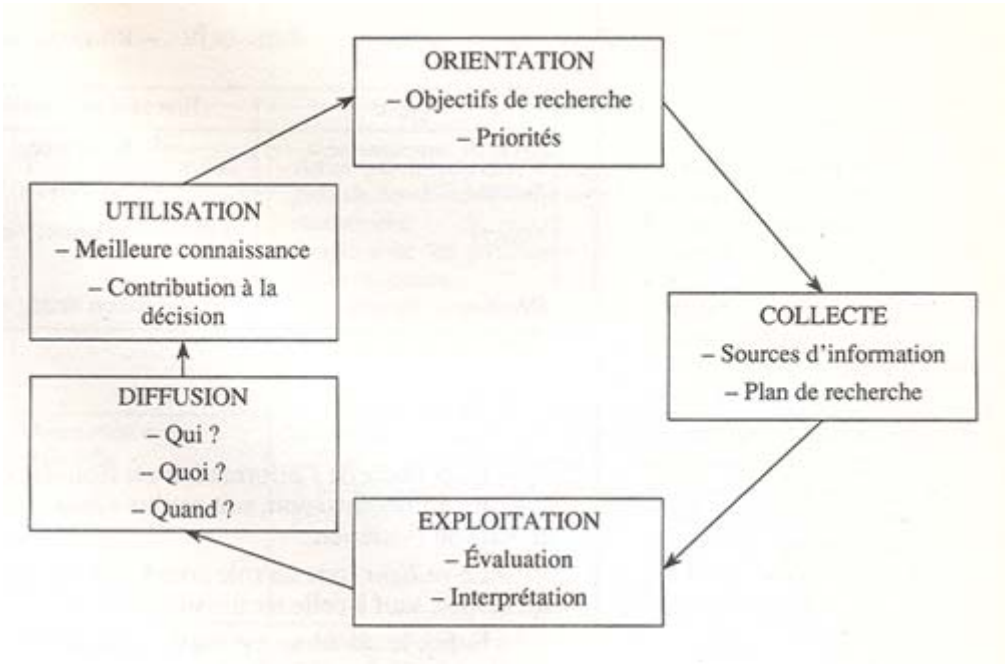

Figure 1 : Etapes du cycle du renseignement (Source : de Guerny, 1993)

1.1. Vers une analyse plus fine

Dans le même temps, le processus est revu pour être divisé, selon les auteurs, en trois à huit étapes. Ainsi Rouach (1996) propose un schéma simplifié ne mettant en valeur que trois étapes principales, la *collecte*, *l'analyse* et la *diffusion*. A l'inverse, des étapes considérées jusqu'alors comme secondaires sont mises en valeur, et d'autres apparaissent avec le développement des techniques : Lesca (1994) parle de *sélection* et de *stockage*, Allain-Dupré & Duhard (1997) ajoutent la *gestion* et la *protection*, Jacobiak (2001) pense aux étapes de *validation* et de *synthèse*, Massé & Thibault (2001) aux étapes de *sécurisation* et de *destruction*. Enfin, la notion d'*utilisation* à été séparée de l'étape de *diffusion* puis ajoutée à sa suite, notamment par de Guerny (1993), (Fuld, 1995), Jacobiak (2001) et Massé & Thibault (2001).

En regroupant dans un même schéma tous les termes répertoriés, nous obtenons en figure 2 ce que pourrait être la matrice complète du processus d'intelligence économique, mettant en évidence toutes les étapes intermédiaires proposées par les différents auteurs.

1.2. L'introduction des Tic dans le processus d'intelligence économique

Jacobiak (1993) prévoyait déjà l'introduction des Tic dans le processus de *veille technologique*, qu'il renommera plus tard *intelligence économique* (Jacobiak, 1998). Selon l'auteur, ces nouvelles technologies permettent non seulement de mieux accéder à l'information et de mieux la diffuser, mais les « plus » résident dans leurs possibilités d'archivage, de mémorisation et de création de bases de données internes personnelles.

Simon (1980), caractérisait de la même façon les technologies de l'information : toute information accessible à l'homme (livres, magazines) existera sous forme lisible par ordinateur et sera stockée dans les mémoires électroniques ; de nombreuses données seront transmises directement à des systèmes automatiques de traitement de l'information sans aucune intervention humaine ; les mémoires seront de taille comparable à celles des plus vastes mémoires actuelles ; le langage humain sera utilisé pour interroger la mémoire d'un système de traitement de l'information ; tout programme ou toute information pourront être recopiés en un autre point de ce même système ou dans un autre système ; la puissance de traitement des systèmes en feront des outils d'aide à la décision et enfin, ces systèmes de traitement de l'information seront de plus en plus capables d'apprendre et aptes à gonfler leurs propres fichiers.

Jacobiak (1993) parle alors de *réseau télématique*, de *bases de données*, de *réseau Transpac*, de *logiciels d'interrogation*, de *micro-ordinateur*, de *serveurs*, de *réseaux locaux de micro-ordinateurs* et de *réseau ethernet*. Pour l'étape de diffusion, l'auteur

avait identifié comme moyens de transmission *le téléphone*, *le telex*, la *messagerie électronique*, la *télécopie* et le *télétel*. Le micro-ordinateur est alors le centre du système car il possède toutes les fonctions utiles à la veille technologique : traitement de textes et de graphiques, bases de données internes, mémorisation et gestion d'archives et capacité à interroger des bases de données distantes par le biais des réseaux internationaux.

Pateyron (1998) ajoute à la liste des nouvelles technologies essentielles à la veille le *Cd-rom*, les *systèmes de recherche assistée par ordinateur (Rao)*, le *système interactif d'aide à la décision (Siad)*, l'*e-mail*, le *minitel* et *internet*.

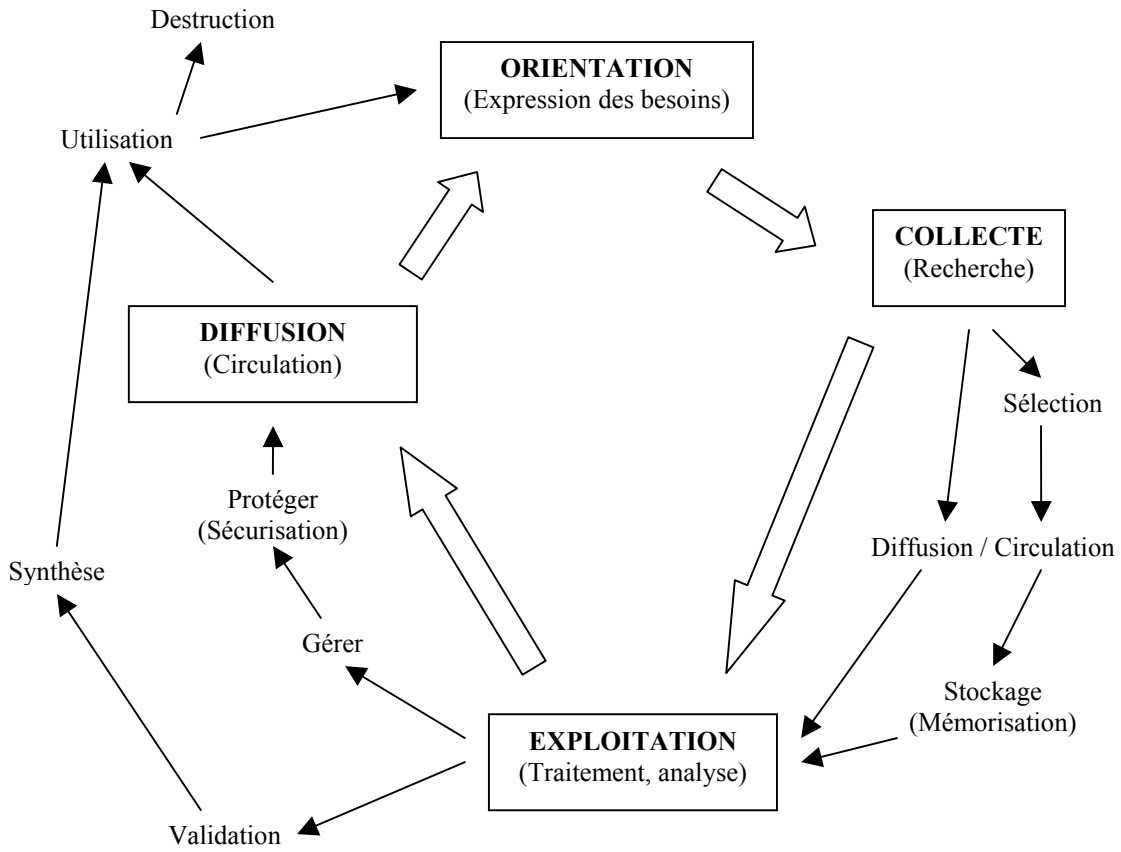

Figure 2 : Matrice des processus de l'intelligence économique

A la lecture de ces auteurs, nous remarquons que non seulement les fonctionnalités décrites comme indispensables à un bon processus de veille correspondent parfaitement aux capacités actuelles des technologies de l'information et de la communication, mais également que certaines technologies alors naissantes et considérées comme incontournables se sont en effet révélées comme telles.

Prenons le cas des fonctionnalités énoncées : meilleur accès à l'information, meilleure diffusion de l'information, capacités d'archivage et de mémorisation des systèmes, traitement automatique de l'information, traitement de textes et puissance de traitement sont, entre autres, les caractéristiques actuelles des Tic. Pour chacune d'elles nous pouvons respectivement associer au moins une Tic : internet, e-mail, serveurs, agents intelligents, logiciels de bureautique et ordinateurs.

De la même façon, les « nouvelles » technologies d'alors se sont imposées dans le processus de l'intelligence économique : les bases de données interrogeables à distance sont devenues les bases de données en ligne, le réseau Transpac est maintenant remplacé par le réseau Renater, les réseaux locaux de micro-ordinateurs sont désormais appelés intranet ou groupe de travail et les logiciels d'interrogation, micro-ordinateurs (PCs) ainsi que certains moyens de transmission de

l'information comme la messagerie électronique (maintenant communément appelée e-mail) sont désormais incontournables.

Le tableau 1 démontre que nous pouvons associer des Tic à chaque étape principale (orientation, collecte, exploitation et diffusion) du processus de l'intelligence économique.

Etapes principales du processus de l'IE	**Tic**
Orientation	Ordinateurs individuels, agents intelligents
Collecte	Ordinateurs individuels, internet, agents intelligents, documents électroniques
Exploitation	Serveurs, logiciels de traitement de l'information, documents électroniques
Diffusion	Ordinateurs individuels, intranets, e-mail, réseaux internes, documents électroniques

Tableau 1 : Application des Tic au processus d'intelligence économique

Le terme *internet* regroupe tous les outils proposés en ligne : sites Web, forums, chats, listes de discussion, revues en ligne, etc. Nous remarquons que certains outils comme les ordinateurs individuels (ou PC) sont utilisés tout au long du processus, de la même façon que les supports informatiques (documents électroniques) qui ont ici un rôle de vecteur de l'information.

Pour notre recherche, le processus de l'intelligence économique ne se réduit pas aux quatre principales étapes. Nous reprenons donc le schéma original du cycle de l'information auquel nous rajoutons les étapes intermédiaires proposées et réalisables avec des outils informatiques (stockage, protection, utilisation et destruction), nous obtenons une interprétation de processus de l'intelligence économique au travers des Tic, schématisée par la figure 3.

Les fonctions de *stockage* et de *protection* sont associées à l'étape d'*exploitation* car celles-ci se déroulent en en même lieu (un serveur d'entreprise) et se déroulent en même temps au regard des autres étapes. Nous avons également choisi d'associer la fonction d'*utilisation* à l'étape de *diffusion* puisque celles-ci sont relativement peu dissociables : en effet, il semble plus judicieux de proposer aux utilisateurs finals de l'information traitée et analysée plutôt que de leur soumettre de l'information brute. Enfin, nous avons ajouté dans ce schéma les différents outils utilisés à chaque étape et issus du tableau 1.

Un simple coup d'œil à la figure 3 permet de constater que les Tic se sont non seulement imposées dans l'ensemble du processus de l'intelligence économique, mais que le simple fait d'en retirer un compromettrait le bon fonctionnement de l'ensemble, ou arrêterait le cycle.

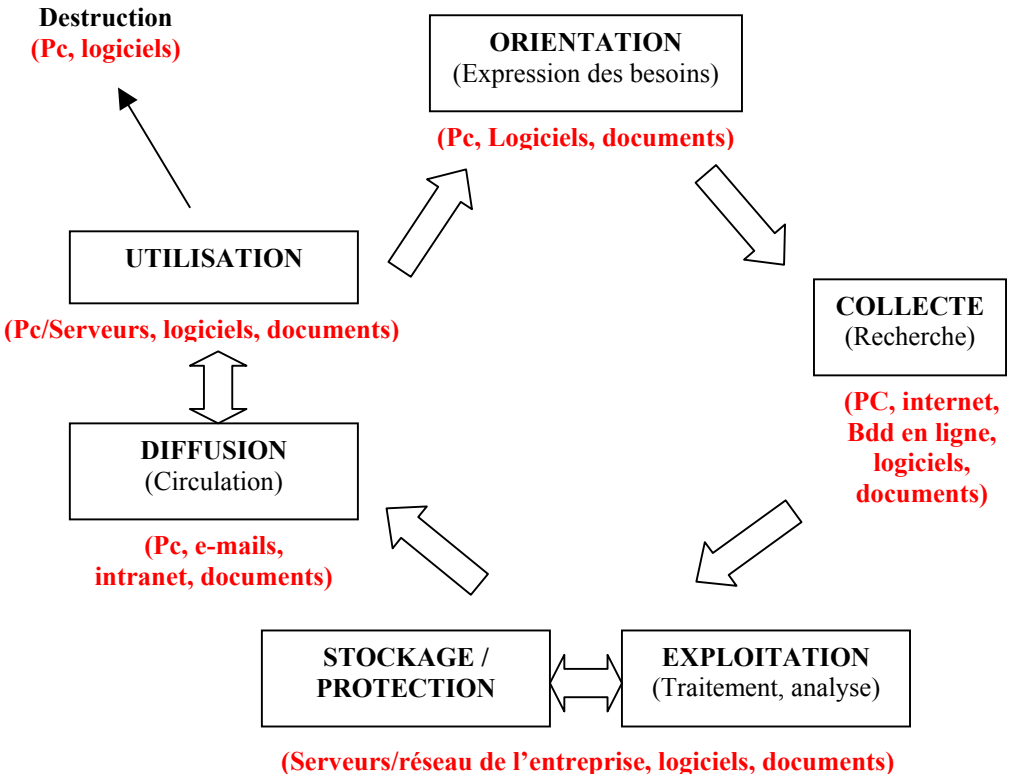

Figure 3 : Rôle des Tic dans le processus de l'intelligence économique

2. LES RISQUES LIÉS AUX TIC

Toute information manipulable par un outil Tic acquiert deux caractéristiques : numérisée, elle devient accessible et duplicable. Il suffit en effet de connecter un ordinateur individuel à un réseau (interne ou internet) pour lire une information stockée sur un serveur distant. Cette information peut être ensuite dupliquée aisément puis être stockée en un laps de temps très court sur des dizaines, voire des milliers d'ordinateurs.

L'information n'est plus, comme par le passé, protégée dans un coffre-fort, ou bien dans une zone de sécurité d'un ordinateur central (Martinet & Marti, 1995). Désormais tout le monde y a théoriquement accès, à condition d'utiliser un ordinateur individuel connecté à un même réseau que celui de la cible. C'est pour cette raison que les systèmes de stockage (serveurs, ordinateurs individuels) possédant de l'information sensible ou privée bénéficient d'accès restreints, généralement protégés par un couple login/mot de passe.

Pour une entreprise ayant couplé son processus d'intelligence économique avec les Tic, le risque est donc grand puisque les informations sensibles stockées dans leurs serveurs sont théoriquement à la portée de tous : les ordinateurs individuels destinés à la collecte d'informations font le lien entre les réseaux externe (internet) et interne (intranet, réseau local) auxquels sont connectés les serveurs.

2.1. Le piratage informatique

Le piratage informatique est apparu au début des années 80 et n'a cessé d'évoluer en s'adaptant régulièrement aux progrès des Tic. Selon Guichardaz & al (1999), la première vague de la délinquance informatique est liée à l'apparition des micro-ordinateurs et à leur banalisation dans les entreprises, la seconde à l'émergence des réseaux locaux et étendus, tandis que la troisième vague correspond à la croissance du nombre d'entreprises connectées à l'internet. La quatrième vague, que nous subissons actuellement, ajoute une composante supplémentaire, les dérivés de l'internet que sont les intranets et les extranets.

Dans le même temps, les motivations des pirates informatique ont elles aussi évolué : du piratage de logiciels de la part d'amateurs dont la motivation essentielle consistait à voler pour

leur usage personnel, nous sommes passés à un piratage « professionnel »[1] dont les motivations sont aussi bien d'ordre économique (détournements d'argent) que par orgueil (afin de démontrer sa supériorité). Depuis l'apparition des intranets et des extranets, l'information se diffuse plus rapidement et plus largement hors des frontières de l'Entreprise, acquérant ainsi une telle valeur stratégique que l'enjeu est désormais de se l'approprier (Guichardaz et al, 1999) ; c'est le piratage industriel, proche de l'espionnage.

Parmi les techniques de piratage couramment utilisées depuis une vingtaine d'années, notons les divinations de mots de passe, « force brute », « denials of services » (DoS), « portes dérobées », « sniffing » et « spoofing » (Guichardaz et al, 1999). Tout responsable Ssi (Sécurité des Systèmes Informatiques) d'une entreprise connaît le fonctionnement de ces techniques et leurs faiblesses. Des diplômes universitaires spécialisés dans ce domaine existent et forment les futurs responsables à l'application des règles de la profession afin de protéger les serveurs dont ils auront la charge plus tard.

Le risque du piratage informatique est donc bien connu des entreprises, car les attaques de systèmes d'information sont souvent médiatisées et les hackers sont le plus souvent mis en scène (Guichardaz et al, 1999). Rares sont les entreprises qui ne prennent pas de mesures de protection contre cette délinquance numérique. En réalité, le piratage informatique tel que nous le connaissons n'est que la partie submergée d'un iceberg de techniques destinées au vol d'informations par le biais des réseaux.

Le problème essentiel des Tic réside ailleurs, sous deux formes : d'une part, une autre délinquance virtuelle peu médiatisée, donc peu connue et issue de technologies créées dans un but autre que le piratage, mais détournées à cette fin ; cette caractéristique non belliqueuse, ajoutée à une médiatisation quasi-nulle, est à l'origine de sa discrétion et de son succès. Nous l'appellerons *technologie du Web*. D'autre part, un comportement et des actions déjà connues du monde du renseignement, mais qui ont pris de l'ampleur avec l'apparition des Tic. Le tableau 2 récapitule ces éléments.

Nous rencontrons ces risques en particulier lorsqu'un processus d'intelligence économique est en partie ou entièrement effectué aux travers de Tic et lorsque celles-ci ont, à un moment ou un autre, accès aux réseaux externes à l'entreprise (internet, mails, documents électroniques, etc.).

2.2. Les nouvelles technologies du Web

Parallèlement au développement géographique de l'internet sont apparues des technologies destinées à le rendre plus accessible au grand public en améliorant l'interactivité des outils proposés en ligne (sites, forums, chats, etc.). Mais la facilité d'utilisation gagnée d'un côté se paie de l'autre, un peu à la manière du revers d'une médaille : de par la nature même de leurs fonctions, ces technologies récupèrent de nombreuses informations sur les internautes, le plus souvent à leur insu afin de ne pas perturber leur fonctionnement.

De plus, le développement de l'aspect commercial du Web, amplifié par les principes de sponsoring et de « B to C [2]», a joué un rôle de *mécène* dans le développement de techniques de récupération d'informations personnelles sur les internautes, dans le but de mieux les connaître et de leur proposer, à domicile, des produits correspondants à leurs goûts et à leurs budgets. Le profilage de l'internaute est une activité en forte expansion. Le profilage est conduit par les moteurs de recherche et par les sites Web surtout marchands qui sont désireux de mieux identifier les besoins de leurs clients afin de leur apporter une réponse personnalisée. Le profilage s'appuie sur des outils informatiques qui peuvent être détournés de leurs fonctions premières.

Ainsi donc, la technologie Web repose sur l'idée de traçabilité : il devient possible pour toute personne qui a des droits d'administration sur un site Web d'accéder aux fichiers log de ses serveurs. Ce fichier texte comporte la trace laissée par les internautes qui ont visité son site et en particulier des informations relatives à l'adresse IP permettant de localiser géographiquement l'ordinateur connecté, la date de connexion, la page chargée, la requête posée éventuellement au moteur de recherche avant d'arriver sur cette page. Les techniques de fouille de données de

[1] Le terme de « hacker » est apparu à ce moment

[2] B to C : business to consumer (relation vendeur-client)

type Web usage mining établissent des classifications de pages Web à partir des comportements de navigation des internautes tels qu'ils peuvent être appréhendés à travers des sources d'information telles que les fichiers log par exemple (Säuberlich F. et al, 2001, Fu Y. et al, 2000).

La technique la plus connue des spécialistes de l'intelligence économique est le « cookie », un petit fichier texte déposé et stocké sur le disque-dur d'un ordinateur par un site désireux de mieux connaître son propriétaire, un peu à la manière d'une carte de fidélité. Ainsi Revelli (2000) préconise-t-il de désactiver à tout moment les cookies, ou de faire en sorte d'être alerté à chaque fois qu'un site essaye d'en envoyer un.

Mais il ne s'agit pas là de la seule façon dont disposent les sites Web pour ficher (nous emploierons plutôt le terme de profiler) les internautes. En effet, d'autres techniques aussi discrètes que méconnues sont bien plus efficaces : variables d'environnement envoyées automatiquement par les navigateurs vers les serveurs distants afin d'établir et de synchroniser la connexion ; fichiers registres contenant pour certains des informations sur les logiciels installés sur un ordinateur et pour d'autres des informations relatives aux connexions internet ; lignes de code insérées dans les pages Web permettant d'accéder à certaines données des disques-durs, voire toutes, (applets Java, ActiveX, javascript) ; bannières de publicité de sociétés tierces établissant une connexion invisible vers leurs serveurs (Webbugs) ; logiciels-espions inventoriant les disques-durs ou spécialisés dans la récupération de certaines données (spywares, keyloggers, programmes de mises à jour automatiques) ; ou encore lignes de commandes permettant d'accéder à des informations personnelles sur les internautes (Finger, Whois).

Technologies du Web
Variables d'environnement
Fichiers-registres, ou logs (proxies Web & logiciels)[3]
Contenus Actifs (applets Java et ActiveX)
Scripts (javascript, VBscript)
Cookies[4]
WebBugs
Spywares, keyloggers
Commandes Finger et Whois
Comportements exacerbés par les Tic
Social engineering
Interception des communications (e-mails)
Vols de documents (Photocopieuses en réseau)
Désinformation (Re-routage selon IP)
Autres
Piratage non conventionnel (trojans, back doors)[5]
Virus

Tableau 2 : Risques, autres que le piratage, liés aux Tic lors d'un processus d'intelligence économique axé sur le Web

[3] Nous distinguons les fichiers-registres enregistrant les connexions Internet (IP, date, durée, URLs visitées) de ceux diagnostiquant les logiciels (état de fonctionnement, options, numéro de série).

[4] Les cookies servent à la fois à faciliter le commerce en ligne (caddies des sites commerciaux) et à établir le comportement et le profil des internautes.

[5] Ces techniques sont hybrides dans ce sens où ce sont bien des hackers qui les utilisent pour voler de l'information, mais leur principe est proche des techniques de récupération commerciale de données (spywares).

Ces techniques combinées aux techniques classiques d'exploitation des fichiers log permettent à leur détenteur de récolter de nombreuses informations précieuses : adresse IP permettant de localiser géographiquement l'ordinateur connecté, nom et coordonnées du propriétaire, date et heure système, langage utilisé, mémoire totale disponible, liste des logiciels installés sur les disques-durs, contenu des disques-durs, numéros de série des logiciels, du micro-processeur et de la carte-réseau, numéros d'identification Guid[6] des documents, service mail utilisé ainsi que les informations inhérentes (adresse mail, carnet d'adresse), sites précédemment visités, temps passé sur ces sites, liste des achats en ligne, mots-clés tapés dans les moteurs de recherche et dans les formulaires, mots de passe tapés et toute information personnelle entrée dans un formulaire (nom, prénom, âge, adresse mail et/ou postale, hobbies, numéro de Sécurité Sociale, numéro de carte de crédit, Csp, revenus, situation maritale, etc.).

2.3. Des techniques de renseignement améliorées grâce aux Tic

Ces listes ne sont pas exhaustives, elles ne sont qu'un aperçu des moyens et des informations disponibles sur le Web au travers des Tic. Mais ces dernières n'ont pas seulement permis d'inventer indirectement de nouvelles techniques de renseignement, elles ont également amplifié d'autres techniques déjà bien connues de la profession. En effet, malgré les multiples barrières technologiques destinées à sécuriser les systèmes d'information, les hackers continuent à pénétrer les ordinateurs et les réseaux (Guichardaz et al, 1999).

Les hackers utilisent par exemple le « social engineering », ou ingénierie sociale, qui leur permet d'obtenir des informations confidentielles telles que des mots de passe ou des numéros d'accès aux réseaux (Guichardaz et al, 1999). La technique consiste par exemple à se faire passer, le plus souvent par téléphone, pour un technicien informatique qui a rapidement besoin d'un accès (un mot de passe) à un ordinateur ou un réseau pour y effectuer une maintenance. L'apparition du mail dans les entreprises a considérablement augmenté ce type de requête, à tel point que les responsables informatiques des entreprises doivent désormais systématiquement signer numériquement leurs mails afin d'en prouver l'authenticité. Au-delà donc des risques techniques qu'imposent les Tic, la sécurisation des données informatiques commence par la sécurisation et la sensibilisation des ressources humaines.

Les interceptions de communications ont elles aussi évoluées, des écoutes téléphoniques nous sommes passés aux interceptions des messages électroniques : lorsqu'un mail est envoyé de façon habituelle, il n'est pas crypté et peut transiter par une dizaine de proxies[7] qui jalonnent le parcours vers sa destination. Or, ces derniers conservent, pour des raisons techniques mais aussi légales, une copie des messages reçus ; les informations contenues dans le corps du message et dans les fichiers joints peuvent donc être lues par autant de responsables de proxies que nécessite le trajet.

De plus, les Etats-Unis ont mis en place, dans les années cinquante avec la collaboration de pays anglo-saxons[8], un réseau baptisé Echelon destiné à intercepter toutes les communications mondiales par fax, téléphone et, plus tard, par messages électroniques. Ce système a été développé durant la guerre froide pour espionner les pays de l'Est ; depuis, il s'est transformé en instrument d'espionnage économique. Le système Echelon est non pas dédié aux communications militaires mais, au contraire, cible tout type d'entreprises, d'organisations ou de gouvernements : chacun des pays partie prenante dans le dispositif peut récupérer ainsi des informations intéressantes pour son gouvernement ou ses entreprises (Guichardaz et al, 1999).

Les vols de documents ne se produisent pas seulement en accédant, à distance ou non, à un ordinateur ou un serveur, mais également de la façon la plus inattendue : par les photocopieuses. Chaque fois que l'on copie un document sur un copieur moderne, une copie est enregistrée sur le disque dur de la machine. Elles sont ainsi devenues de véritables centres

[6] Global Unique Identifier : des sociétés telles que Microsoft et Real Networks tatouent leurs logiciels éditeurs d'un numéro de série leur permettant de retrouver aisément la personne à l'origine d'un document.

[7] Ordinateur qui s'intercale entre un réseau privé et l'Internet pour faire office de Firewall ou de Cache. Désigne également les ordinateurs par lesquels transitent les données sur le Web.

[8] Grande-Bretagne, Nouvelle-Zélande, Canada et Australie.

de stockage informatisés, et cela très souvent à l'insu des dirigeants et salariés des entreprises. Les copieurs et les machines multifonctions les plus modernes stockent les informations avant de les imprimer, des experts en informatique peuvent donc ensuite très facilement récupérer ces informations (Guillemin, 2003), d'autant plus que la plupart d'entre elles sont généralement connectées à un réseau d'entreprise, soit via un PC (imprimante partagée), soit grâce à une adresse IP propre.

En outre, lorsque la période de location du matériel arrive à son terme, la machine est louée à une autre société avec les informations sensibles qu'elle contient poursuit Guillemin (2003), rappelant que ce type de machine est le plus souvent louée par l'entreprise, et que chaque année 25.000 copieurs changent de mains.

La désinformation est une information fausse ou, de manière plus pernicieuse, l'utilisation spécifique d'un corpus d'informations en vue d'orienter un éventuel observateur sur de fausses pistes (Achard et al, 1998). Elle fait partie, historiquement, des conflits entre grandes puissances, mais avec l'internet, elle a acquis ses lettres de noblesse. Sur ce réseau, non seulement n'importe qui peut publier n'importe quoi en toute impunité (Guichardaz et al, 1999), mais une société peut également orienter un adversaire ou un concurrent particulier vers des pages spécifiquement créées à son intention afin de le désinformer: il suffit pour cela de réorienter de façon automatique les connexions entrantes des plages d'adresses IP appartenant aux concurrents.

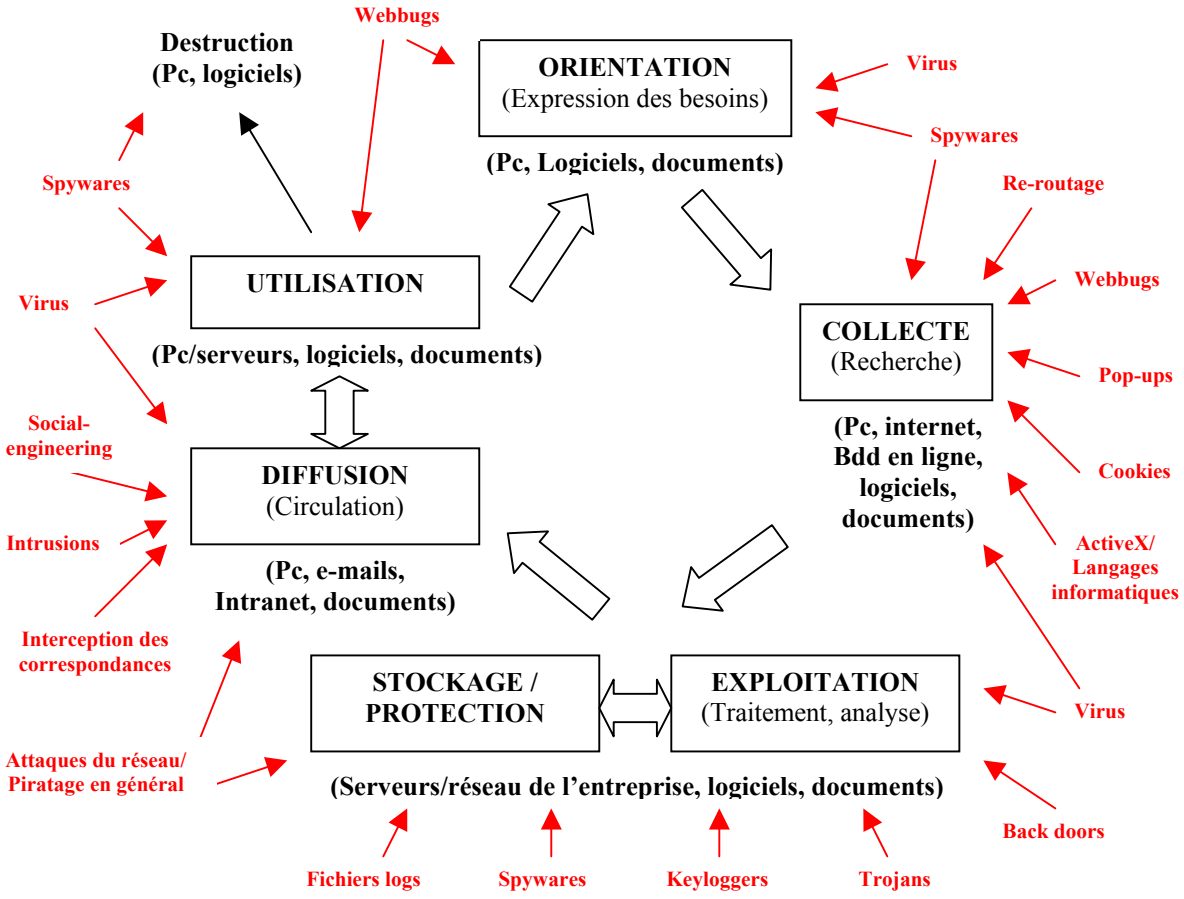

Figure 4 : Risques liés aux Tic dans le processus d'intelligence économique

Enfin, il ne faut pas oublier les virus informatiques qui ont considérablement évolué avec l'internet. Les hackers ont également pu améliorer des techniques de piratage que nous qualifierons de non conventionnelles en ce sens où désormais ils ne cherchent plus à forcer l'entrée d'un réseau privé, mais diffusent sur le Net des logiciels piégés qui, une fois exécutés sur un ordinateur, ouvrent des ports et établissent une liaison cachée avec le pirate. Ces logiciels-virus, parmi lesquels les « Trojans » (chevaux de Troie), utilisent le même principe d'extraction furtive de données privées que les logiciels de certaines grandes sociétés, les spywares cités plus haut.

3. LE PROCESSUS D'INTELLIGENCE ÉCONOMIQUE MENACÉ

En associant l'ensemble de ces techniques au processus de l'intelligence économique, nous nous rendons compte qu'elles en deviennent des risques. Etablir le profil des internautes dans un but commercial est une chose, mais la frontière vers l'utilisation de ces mêmes techniques dans le seul but d'identifier, d'espionner ou de désinformer un concurrent est proche. Si les Tic permettent d'améliorer sensiblement le processus d'intelligence économique, elles livrent de nombreuses informations aux sites visités, notamment le nom de l'entreprise veilleuse et les informations recherchées, atténuant en cela leur avantage.

La figure 4 permet d'avoir une vue d'ensemble, certes incomplète mais éloquente, de la situation du processus de l'intelligence économique si ce dernier est en partie ou totalement dirigé au moyen de Tic. Si la figure 3 nous a permis de constater que les Tic se sont imposés dans l'ensemble du processus d'intelligence économique au point de le rendre inefficace si l'un d'entre eux venait à faillir, la figure 4 démontre que les risques liés à ces mêmes Tic submergent le processus à tel point que si l'un d'entre eux est négligé, il rendrait tout autant inefficaces les efforts entrepris dans l'opération.

L'implantation des Tic dans un processus de l'intelligence économique rappelle les problèmes bien connus de confidentialité de l'information : social engineering consistant à obtenir la collaboration de personnels disposant d'accès privilégiés et reconstitution d'information à partir d'éléments supposés détruits ou inexistants. En effet, outre l'approche des personnels chargés du nettoyage, les services de renseignements collectaient, lors de la guerre froide, des sacs destinés à la poubelle pour en extraire et reconstituer les documents qui ont été déchiquetés (Guichardaz et al, 1999).

CONCLUSION

L'objectif de cette recherche est de faire prendre conscience aux entreprises mettant en œuvre les Tic dans leur processus d'intelligence économique que ce dispositif, s'il augmente considérablement leur potentiel de développement à long terme, comporte des risques : non seulement ils peuvent livrer à leurs concurrents des informations permettant de déduire leur stratégie de recherche, mais, outre le piratage conventionnel ils exposent leur réseau informatique aux techniques et technologies de récupération automatique de données via l'internet. Ces risques introduits par les nouvelles technologies renforcent donc le rôle d'une sensibilisation des acteurs de l'intelligence économique non seulement à une meilleure connaissance et une meilleure maîtrise des outils, mais également à une « culture » de la sécurité qui suppose des comportements et des habitudes adaptées à l'utilisation de ces outils.

BIBLIOGRAPHIE

Achard, P., Bernat, J.P. (1998), *L'intelligence économique : mode d'emploi*, ADBS Editions, Paris

Allain-Dupré, P., Duhard, N. (1997), *Les armes secrètes de la décision, La gestion de l'information au service de la performance économique*, Gualino éditeur, Paris

Baud, J. (2002), *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Paris

Bulinge, F. (2001), *PME-PMI et Intelligence compétitive : les difficultés d'un mariage de raison*, Actes du colloque VSST 2001, Barcelone

Carayon, B. (2003), *Intelligence économique, compétitivité et cohésion sociale*, La Documentation Française, Paris

de Guerny, J., Delbès, R. (1993), *Gestion concurrentielle. Pratique de la veille*, Delmas, Paris

de Vasconcelos, C. (1999), *L'intelligence économique et la stratégie de développement de la PME*, Thèse pour le doctorat en Sciences de Gestion, Grenoble.

Fu Y., Sandhu K., Shih M. (2000), *A generalization-based approach to clustering of Web usage sessions* , In Proceedings of the 1999 KDD Workshop on Web Mining, San Diego, CA, vol. 1836 of LNAI, pag 21 – 38, Springer

Fuld, L.M. (1995), *The new competitor intelligence: the complete resource for finding, analysing and using information about your competitors*, John Wiley, New-York

Guichardaz, P., Lointier, P., Rosé, P. (1999), *L'info guerre. Stratégies de contre-intelligence économique pour les entreprises*, Dunod, Paris

Guillemin, C. (2003), *Photocopieur : attention au risque de captation de données*, Zdnet France

Jacobiak, F. (1992), *Exemples commentés de veille technologique*, Les éditions d'organisation, Paris

Jacobiak, F. (1998), *L'intelligence économique en pratique*, Les éditions d'organisation, Paris

Jacobiak, F. (2001), *L'intelligence économique en pratique*, 2ème édition, Les éditions d'organisation, Paris

Juillet, A. (2005), *Le référentiel de formation à l'intelligence économique, état des lieux et perspectives*, Conférence à l'IHEDN, Paris

Lesca, H. (1994), *Veille stratégique.L'intelligence de l'entreprise*, Aster, Lyon-Villeurbanne

Martinet, B., Marti, Y.M. (1995), *L'intelligence économique. Comment donner de la valeur concurrentielle à l'information*, Editions d'organisation, Paris

Martre, H. (1994), Rapport sur *L'intelligence économique et stratégique des entreprises*, La Documentation Française, Paris

Massé, G., Thibault, F. (2001), *Intelligence économique. Un guide pour une économie de l'intelligence*, Editions De Boeck Université, Bruxelles

Oberson, P. (1997), *L'internet et l'intelligence économique*, Editions d'organisation, Paris

Pateyron, E. (1998), *La veille stratégique*, Economica, Paris

Revelli, C. (2000), *Intelligence stratégique sur internet*, Dunod, Paris

Rouach, D. (1996), *La veille technologique et l'intelligence économique*, Collection Que sais-je ?, Presses Universitaires de France, Paris

Säuberlich, F., Huber, K.-P. (2001), *A framework for Web usage ming on anonymous logfile data*, SAS Institute GmbH

Simon, H.A. (1980), *Le nouveau management*, Economica, Paris