« *L'Intelligence Economique et stratégique, les apports à la gestion des risques* » par Claude Delesse

Bordeaux Ecole de Management

Synthèse de la communication présentée aux rencontres AMRAE Lille 2002

En se plongeant dans l'histoire, on découvre que l'homme a toutes les capacités pour évoluer dans un environnement hostile et que l'utilisation de l'information à des fins stratégiques n'est pas nouvelle. Guerriers, politiques, marchands, banquiers se renseignaient ou gardaient le secret dans des pratiques offensives et/ou défensives leur permettant de saisir des opportunités ou d'évincer des menaces. Aujourd'hui le monde s'avère un système ouvert, multiacteurs, multirisques, donc instable, difficilement prévisible. Il se caractérise par l'accélération des mutations, par des interactions géopolitico-économiques, sociales, financières, par l'affirmation de contre-pouvoirs, par l'expansion de la criminalité organisée. L'économie de l'immatériel donne au savoir un statut de richesse. L' information, objet de toutes les convoitises, s'affirme comme une ressource, une arme ou une cible. Si les NTIC sont des autoroutes de l'information, elles véhiculent aussi de la désinformation et agissent comme caisses de résonance à l'opinion publique et consumériste. Le virtuel est un monde de transparence et d'opacité. De plus, de nouvelles lignes de fracture comme alimentation, santé, environnement, mode de vie, suscitent une vigilance protectrice ou opportuniste.

Le recours à de nouvelles grilles de lecture et un mode de raisonnement adapté deviennent indispensables pour appréhender cette complexité créée par le visible et l'invisible, la coexistence et l'imbrication de réseaux licites et illicites, par le brouillage entre information et désinformation. Ils favorisent un décodage et une analyse en profondeur. La question se pose alors : « Comment la « Gestion des Risques » et « l'Intelligence Economique et Stratégique » (IES) agissent-elles en tant que ressources ? ».

En se référant à de nombreuses définitions, tout en prenant en compte celle du rapport Martre de 1994, l' IES peut se résumer comme l'art concerté de la maîtrise de l'information dans une perspective de gestion stratégique et tactique. Cette approche globale mêle une perception vigilante, une compréhension de l'environnement, des stratégies relationnelles réseaux, une gestion des ressources technologiques « Techint » et humaines « Humint », des stratégies d'influences et met en place une stratégie de contre-intelligence.. Au service des décideurs, elle est un instrument de management, de savoir, d'actions offensives ou protectrices. Elle vise à déceler, provoquer et exploiter des opportunités, ou à anticiper et neutraliser des menaces. Transdisciplinaire et multiactorielle, l 'IES s'impose comme mode de pensée, de réflexion et d'action collective. L'information est omniprésente dans tous les comportements : questionner, écouter, observer, organiser, analyser, mémoriser, diffuser, communiquer, influencer, persuader, décider, agir ou plus globalement, Vouloir, Savoir, Pouvoir.

La Gestion des risques a évolué de la notion de sécurité pure à celle de sûreté. A l'origine « gérer le risque », consistait à « vivre dans l'éventualité qu'un événement futur provoque un préjudice ». Aujourd'hui, étant donné « les pressions accrues que subissent les décideurs, les gestionnaires ont besoin de nouvelles certitudes concernant les bons et les mauvais côtés de leurs décisions »..., « la gestion du risque » fonctionnant comme « un système de garanties et de contrôles » pouvant « mener l'entreprise à la réussite »[1]
D'autres définitions font apparaître les notions de gestion intégrée et de prise de risque[2]
« Tout élément qui peut avoir un impact sur la capacité de l'entreprise à atteindre ses objectifs »… «L'état de l'art semble se situer à la charnière des pratiques dont l'objectif est d'assurer la protection de la continuité des activités et de celles qui visent à intégrer la gestion des risques dans la gestion stratégique et opérationnelle »…« l'identification des risques et la diffusion de l'information sur les risques seront en phase avec les autres processus de gestion»

L'IES et la Gestion des risques se caractérisent par une hétérogénéité de définitions les érigeant au statut de concepts en construction. Activités transversales, elles se positionnent au niveau de la stratégie, ont pour préoccupations de détecter risques, menaces, vulnérabilités, opportunités. Leur finalité est d'anticiper et non pas de subir (état induit par un manque d'estimation proactive des risques), dans le but de préserver un patrimoine matériel et

[1] Ben Hunt.(2001) "L'irrésistible ascension de la gestion du risque" pp.326-330 in : *L'art de gérer les risques*, Financial Times Limited , Editions Village mondial/Pearson Education France, 370p.

[2] Pascal Beaurain, Patrick Frotiée, Brian Towhill.(2001) "Nouvelles perspectives pour les entreprises" p. 168 in *L'art de gérer les risques*, Financial Times Limited , Editions Village mondial/Pearson Education France,

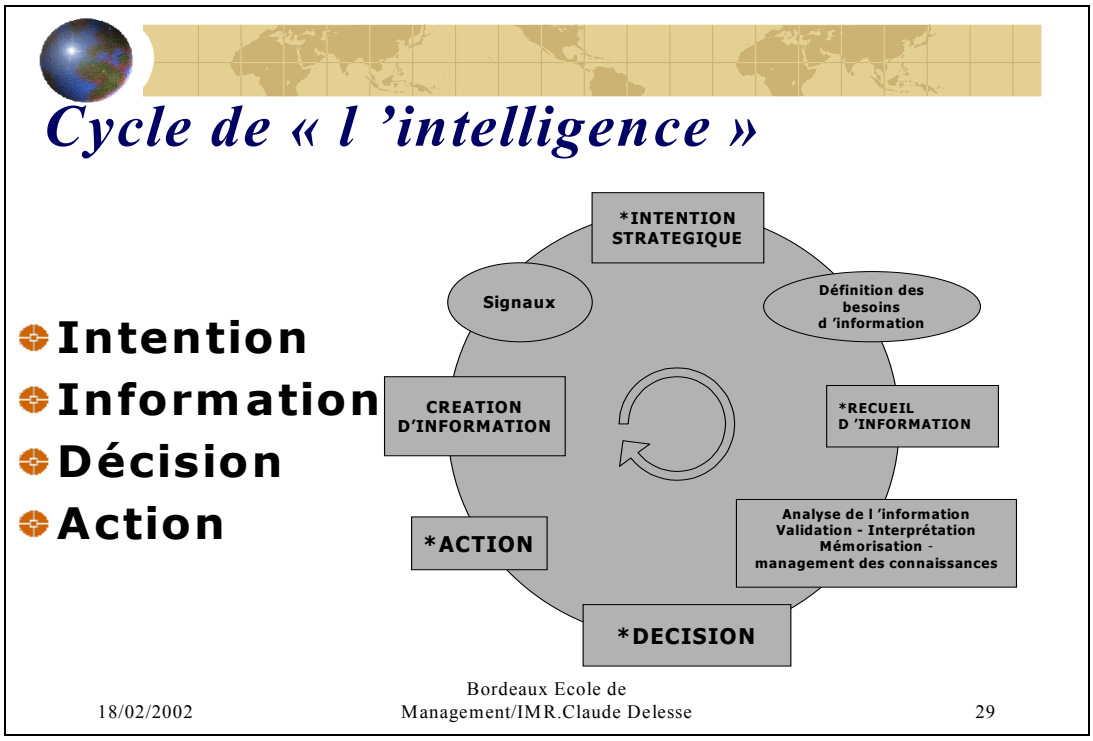
immatériel, l'entreprise devant survivre et se développer en créant de la valeur pour les actionnaires, les salariés, les clients et la société (développement de l'individu et collectif).

Les apports de l 'IES sont perceptibles à différents niveaux. Elle stimule l'anticipation, élargit la vision. Permettant une lisibilité globale qui intègre acteurs et signaux, elle éclaire la décision stratégique. De plus elle contraint à prendre en compte les différentes facettes de la guerre de l'information, sans oublier son rôle incitatif dans la dynamique d'intelligence collective au sein d'une organisation ou entre différents acteurs comme Etats, pouvoirs locaux, entreprises, laboratoires de recherches, universités, associations.

1. Dans la volonté d'anticiper, l'IES manifeste l'intention d'exercer une d'influence sur les rapports de force : Elle développe une capacité d'écoute, de détection du latent (exploration des possibles), de facilitation de l' émergence de liaisons inattendues, de construction des corrélations éclairantes, d' élaboration des scénarios. Elle accepte la prise de conscience de l'ignorance, préalable à la construction de sens. Comment rechercher des données sensibles, comment les analyser, comment établir des connexions intellectuelles entre des phénomènes et des situations a priori étrangers les uns aux autres ? Il convient au préalable de rappeler que l'information n'a de valeur que dans la décision qu'elle éclaire et que l'information utile est une addition d'intention et d'attention. Une observation interrogative constante intercepte, accepte et exploite les signaux émis, pour échafauder et transformer les informations en renseignements stratégiques. Une règle d'or de l'IES est d'être curieux, créatif et de poser ou susciter les bonnes questions.

2. Les fondations et le ciment de la construction de sens se matérialisent dans un questionnement permanent. Il n'y a aucune limite à l'étendue et au champ des interrogations. Il convient toutefois de veiller à la pertinence du questionnement, de distinguer ce qu'il est agréable de savoir, de ce qu'il est nécessaire de connaître. Les réponses permettant la balance entre opportunités et menaces influenceront la décision de prise de risque.

Les réponses ne sont bonnes et pertinentes que si les questions sont de qualité, opportunes et adéquates. Précisons que le questionnement doit rester discret et s'entourer de précautions. L'habileté est requise pour ne pas être repéré ou ne pas dévoiler ses préoccupations à travers ses questions.



L'analyse des informations (pièces du puzzle) doublée d'un ressenti donne une lisibilité et cartographie une cible dans un environnement dynamique. Elle prend en compte les informations tangibles (réalité économique de l 'acteur comme taille, part de marché, capacités d 'investissement, d 'autofinancement, technologies…), mais principalement les informations intangibles comme potentialités de développement, ressources immatérielles, savoir-faire non codifiables, compétences, valeurs, pensées, cultures, intentions des acteurs, ressources relationnelles...

Elle identifie les réseaux d 'influence comme les segments politiques, administratifs financiers, industriels, scientifiques et d 'expertises, criminels… Elle complète par des informations sur les organisations et les hommes, fait apparaître les circuits d'influence, les réseaux licites et illicites. La volonté de vision globale, systémique facilite le décodage. Des grilles de lecture sont d'une aide précieuse comme celle proposée par Bernard Sionneau[3] dans sa théorie du risque pays. « Les logiques d'action (souverainetés, marchés, innovation-technicité, idées) » s'appréhendent plus facilement à travers « un modèle de risque pays, expliquant ce dernier en termes de dé-ajustement des logiques et dysfonctionnement des systèmes d'action structurant le monde et la vie des collectivités nationales ». Les

[3] Bernard Sionneau. « Une théorie du risque pays (1)" *Revue française de géoéconomie*, n° 18, été 2001, pp. 142-176 et (2), n°19, automne 2001

compréhensions des interactions s'inspirent directement des réponses à : Qui fait quoi ? ou qui est susceptible de faire quoi ?, où ?, quand ?, comment ?, pourquoi ?, avec qui ?, jusqu'à quand ? Avec quel impact ? Sur qui ? dans quel délai ?…

La lisibilité se complète d'une grille de lecture interne, sachant que plus de 8O% de l'information utile est dans l'entreprise. Un audit des processus et flux d'information cherchent à savoir : Qui a, peut avoir de l'information ? Comment circule l'information ? Quelles sont les informations à valeur ajoutée sensibles ? Qui sont les personnes à risque? Qui a accès à l'information sensible ? Où sont les zones d'interfaces, d'interactions avec l'extérieur ? Quels peuvent être les scenarii de rupture ? Quelles sont les compétences, expertises individuelles et collectives ? Qui est en relation avec qui ?

La cartographie des acteurs internes et externes recherche l'appartenance à des réseaux, établit les liens et relations. Tout acteur est un vecteur source d'information et d'expertise ; un vecteur stratégique se révélant comme un appui interne, externe (Qui ? neutre ? hostile ? partenaire ? pour quelle stratégie ?) ; un vecteur relais dans le cadre d'une stratégie d'influence.

L'intelligence des situations s'enrichit d'un tel mode de pensée et d'analyse. Comprendre de l'intérieur, ce qui se passe à l'extérieur et quels sont les impacts possibles sur la vie de l'organisation, permet de construire la compréhension de l 'espace général du champ d'action ou d'influence : détecter les menaces et les opportunités, tout en identifiant ses propres forces et vulnérabilités, jauger les comportements ami-ennemi, les attitudes de variabilité dans le temps (ponctuel ou durable), soupçonner les stratégies indirectes (influence, accoutumance, perception management[4]…). La représentation des forces en présence, des ressources, des facteurs favorables ou défavorables, éclairées en l'occurrence par les jeux passés des divers acteurs, laissent présager des rapports de forces et des interactions possibles. Les estimations du risque et de la prise de risque s'ajustent ainsi avec plus de pertinence.

3. L'Intelligence collective agit comme dynamique de forces. Elle débride un management cloisonné en activant une dynamique de réseaux, inculque une culture du partage, met en place des capacités et des flux de réflexion et d'appui, élargit la marge de

[4] « Actions consistant à fournir et/ou à camoufler une information sélectionnée et des indices à des audiences étrangères de façon à influencer leurs émotions, leurs motivations et leurs raisonnements objectifs » Christian Harbulot

manœuvre. Au lieu de la hiérarchie et de ses règles, s'affirme la transversalité avec des corollaires comme adhésion, implication, mobilisation, connivence, confiance, respect des normes. Cependant, elle représente une menace à travers les décisions et les ressorts psychologiques (argent, ego, idéologie, vice caché…) de ses acteurs.

4. Sachant qu'il est facile de devenir victime face à un adversaire qui met en œuvre des moyens comme bases de données, logiciels, cabinets spécialisés, officines de renseignements, utilise les armes de l 'intelligence économique voire des méthodes moins licites, l'approche de la gestion des risques par l'IES inciterait à prendre en compte un cycle de la contre-intelligence qui s'amorce sur une triple intention stratégique :

- Protéger l'information stratégique : empêcher l'autre de (Protection de l'information et des systèmes)
- Diriger l'information, faire partager sa vision : influer sur l'autre (protéger par l'information)
- Annihiler (fausse information, propagation de rumeur…) : contre-attaquer l'autre (protection contre l'information)

L'Information numérique facilite le « jeu » obtenir, détruire, manipuler. Il faut prendre au sérieux les menaces de récupération de données sur site, les risques encourus inhérents à la nomadisation (portables et voyages), les vulnérabilités accentuées par les interconnexions (EDI, Intranet, e-management (clients, fournisseurs,...), se maintenir informé sur les agissements de la cybercriminalité.

L'avantage va à l'attaquant. Il focalise sur un point faible. La cible est dans l 'ignorance, doit protéger tout son système, sans forcément connaître les points vulnérables faute de les avoir tous identifiés. N'importe qui peut attaquer, on ne sait pas qui est attaqué, par qui, on ne sait ce qui est réel (désinformation), on ne sait pas qui est l 'adversaire (intentions, moyens). La cible est sous la menace. Elle risque le vol d'information ou la destruction, la paralysie des données et des systèmes. Et personne ne peut affirmer, ne pas posséder d'information sensible en matière d' axes de développement, plan de recherche, brevets industriels, données financières, prix, fichiers clients, business plans, secrets de fabrication.

Face à ces menaces, certaines précautions et actions s'imposent. Un benchmarking de

ses sinistres et de ceux des autres aident dans la compréhension des défaillances, des habitudes. Il s'agit d'identifier les points faibles qui ont facilité les fuites d'information, des personnes ou des dénominateurs communs à plusieurs sinistres, des personnes à risque (intrusions humaines, embauches, stagiaires, salariés influençables, corruptibles, insatisfaits).

La protection des intrusions et indiscrétions obligent à sécuriser les sites sensibles (équipes de nettoyage, visiteurs, employés, stagiaires, « faux »fournisseurs), à instaurer des règles (instructions, procédures: distribution du courrier, photocopies, fax, poubelles et prototypes, utilisation d' ordinateurs, télécommunications, transports, voyages), à cloisonner l'information sensible, à limiter le secret aux éléments très sensibles. Il faut choisir les priorités, car il est utopique de vouloir tout protéger.

Etre renseigné pour choisir ses partenaires (sous-traitance, fournisseurs, commerciaux, experts, consultants) est élémentaire, surtout dans les pays aux risques de corruption et criminalité élevé Il convient aussi de sélectionner ses clients à l'international en fonction de l'évaluation inhérent au transfert de technologie.

Dans un contexte mondial, le recours à la propriété industrielle ou au droit, la présence en amont dans les comités de normalisation ou de certification, la pratique du lobbying prennent une place accrue comme armes et ressources offensives ou défensives.

Un équilibre doit être trouvé entre la transparence et le secret. Comment parler de son entreprise, d'un nouveau produit, d'une innovation technologique sans tout dévoiler. Il y a un risque évident à communiquer à travers les rapports financiers, les compte-rendus aux actionnaires, les annonces sur support presse, les documentations techniques, les discussions commerciales ou dans les salons professionnels, les conférences dans les congrès scientifiques. Les demandes de certification, les questionnaires se remplissent aussi en pesant ses réponses.

Surveiller les propos, les discours médiatiques ne suffit pas, il est prudent de suivre aussi les discussions sur Internet. De nouveaux affrontements sont induits par le virtuel, car l'attaque par l'information se révèle moins chère que l'activité de renseignement. Internet agit comme amplificateur de crise, de type instantané. Les effets démultiplicateurs de la résonance accélèrent la rumeur, le bruit ambiant de diffamation, de confusion. La net-économie est très sensible à l'information, à l'hypermédiatisation du fait de la banalisation des outils et des procédures d'attaque. Le résultat est vérifiable en temps réel. Une entreprise perd rapidement son image et peut voir sa réputation entamée. Dans ce monde virtuel, à la fois transparent et opaque, les menaces et les opportunités peuvent prendre naissance en n'importe quel lieu de la planète . La défense est plus encore étroitement dépendante d 'une

certaine connaissance (Qui est « l 'ennemi » ?, Quels sont les méthodes qu 'il utilise ?), et de la capacité à utiliser les informations disparates pour reconstituer le puzzle cadre de la compréhension. Dans le jeu stratégique, la contre-intelligence n'est jamais sûre de gagner, jamais sûre de perdre, mais elle ne doit pas être surprise !

5. L'adhésion et la sensibilisation des acteurs sont les incontournables du programme de contre-intelligence

L'acteur est averti qu'il est une cible possible ou un capteur potentiel. La confidentialité de l'information est présentée comme une contrainte pour chacun. Les rôles et responsabilités doivent être clairement définis à travers des procédures, des règlements, les contrats d'embauche et de confidentialité… Ces contraintes s'accompagneront de systèmes de valorisation et de récompense des salariés. Des formations diverses sont indispensables, visant à sensibiliser à la sécurité, mais plus encore à la prévention. Initier à la collecte et à la transmission d'information (rapports d'étonnements, rapports de sinistres, rédaction de contrats, discrétion de recherches). Insister sur l'environnement géopolique, le risque-pays, le management interculturel, sans oublier de sensibiliser aux vulnérabilités humaines en apprenant à se mettre dans la peau de l'autre : qui est qui? qui peut faire quoi ? avec qui… ? pourquoi ?… Créer des réflexes, sensibiliser à l'éthique, aux valeurs, créer une culture « pouvoir avec » innovante et stimulante. L'IES et la gestion des risques ne se conçoivent pas dans un cadre individualiste.

Il semblerait donc que les apports de l'IES se concrétisent dans la création anticipative. La gestion des risques gagnent en sûreté, l'immatériel est mieux protégé, mieux partagé, mieux rentabilisé. Le développement d'une intelligence stratégique optimise les ressources internes et externes. Il élabore et protège image et réputation. Les règles du jeu modifiés, les acteurs s'affichent « socialement responsables » et adhèrent à une « logique de l'au-delà » en oeuvrant comme force de changement pour le développement de systèmes durables. Il devient dès lors réalisable de faciliter l'émergence d'une gestion stratégique des risques, partagée, créative et progressiste tenant compte à l'échelle planétaire, mais aussi locale et institutionnelle des équilibres économiques, politiques, sociaux, technologiques, écologiques et culturels.

12 mars 2002.
claude.delesse@bordeaux-bs.edu