

L'information matière première de l'intelligence

« Il est une chose qui coûte plus cher que
l'information, c'est l'ignorance »

J. F. Kennedy

Martial Morvan

Ligne 12

10 Janvier 2006

Tendances lourdes au niveau des entreprises

- ✓ Logiques sectorielles: concentrations continues et spécialisation des territoires
- ✓ Externalisation en interne: services que l'on va rationaliser et centraliser (Doc, Compétences...)
- ✓ Partenariats multiformes simultanés
- ✓ L'image comme élément de l'actif immatériel

Observations marquantes et contradictoires

- ✓ Montée en puissance des communautés de pratiques, ET difficulté de penser et d'agir sur mode collectif
- ✓ Proliférations des modèles ET persistance des difficultés d'intégration de la culture d'entreprise
- ✓ DRH proposent services sur-mesure aux salariés ET fidélité reste corrélée indicateurs marché emploi
- ✓ Individualisme, gestion personnalisée des carrières ET gestion de projet et le travail en équipe

Observations marquantes

Interrogations pour l'organisation

- ✓ Quelles sont nos valeurs ?
- ✓ Faut-il être leader ou suiveur ?
- ✓ Quel est le cœur de notre savoir-faire ?
- ✓ Que disent nos clients, nos concurrents ?
- ✓ Comment prenons-nous nos décisions ?

Observations marquantes

Interrogations pour l'individu

- ✓ Comment naviguer entre ces extrêmes, saisir ces forces internes, les liens qu'elles entretiennent ?
- ✓ Alors...choisir son camp ? Agir au nom d'une éthique personnelle ou collective ? Suivre les autres ?
- ✓ Que pense et fera mon voisin ? Comment rendre son comportement prédictible, voire l'influencer ?
- ✓ Sur quels critères serai-je évalué ? Le regard des autres ? Qu'est-ce que je gagne et perd ?
- ✓ Que vaut mon expérience ? Comment l'enrichir ?

Les outils pour comprendre

Historique et définitions



Historique de la fonction renseignement

- **500 ans avec JC, le chinois Sun Tsu** jette les bases pragmatiques de la stratégie militaire par un ouvrage majeur : « L'art de la guerre ».
- **Plus tard, Napoléon** s'appuie sur la fonction renseignement pour conquérir l'Europe en utilisant au mieux les ressources de ses ambassadeurs.
- **Vidocq (1775-1857)**, après avoir dirigé la brigade de sûreté, l'ancien bagnard exploite les méthodes du renseignement d'état dans un but commercial.
- Durant la **deuxième guerre mondiale**, les alliés percent le secret d'« Enigma », la machine de la cryptographie ennemie et prennent un avantage stratégique décisif.
- Après la **chute du mur de Berlin (1989)**, les espions de la guerre froide, jusque-là centrés sur le renseignement militaire, se reconvertissent dans le renseignement d'entreprise.
- En **1994, le rapport « Martre »**, pose les bases de la démarche française d'intelligence économique, préparant ainsi son intégration dans la culture d'entreprise.
- De **Tchernobyl** à la pollution engendrée par le naufrage du « l'Amoko Cadis », l'information prend une place croissante dans la gestion de crises environnementales.
- **Automne 2003 : Le rapport Carayon** lance les nouvelles bases françaises de la démarche.

APPARITION DES NOTIONS:

- ✓ **Gestion des Connaissances** : pratiquée depuis que l'homme est doté de capacités de perception
- ✓ **Renseignement militaire**: Chefs d'états et les Généraux ont toujours utilisé des agents de renseignement.
- ✓ **Renseignement économique** : dans les années 1990 après la chute du mur de Berlin
- ✓ **Développement du KM dans l'industrie**: retours d'expériences, FAQ, best practices, années 1990
- ✓ **Gestion stratégique de l'information** : après 1994 rapport martre

TYPOLOGIE ET CHAINE DE VALEUR

- ✓ **La donnée:** mesure de base, code, trace, symbole, enregistrement
- ✓ **L'information:** intervention humaine = donnée qui fait sens
- ✓ **La connaissance :** information «activable» en fonction d'une finalité
- ✓ **Le renseignement :** mode d'utilisation de l'information orienté action
- ✓ **Communication :** échange d'informations entre entités
- ✓ **Savoir :** part de connaissance détenue par une entité.

...Qu'est-ce que...

Le Knowledge Management ?

- *“Le KM est constitué d’un ensemble de processus technologies, permettant de collecter, d’organiser, diffuser, partager et faire vivre la connaissance”*
- *“Le KM est un ensemble d’actions organisées, afin d’utiliser la connaissance dans une organisation, en transformant sa capacité à la stocker et l’utiliser dans le but d’améliorer ses performances”*
- *“Le KM est l’introduction au sein des pôles traditionnels: Hommes, Technologies, Processus, d’un champ supplémentaire, celui des contenus”.*

.....Qu'est-ce que...
L'Intelligence Economique et Stratégique

Intelligence

vient de "**inter ligere**" = lier ensemble
relier des faits, des informations
et en déduire quelque chose...

.....Qu'est-ce que...

L'Intelligence Economique et Stratégique

"L'intelligence économique et stratégique 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. La notion d'IE implique le dépassement des actions partielles désignées par les vocables de documentation, de veille..."

Rapport du Commissariat Général du Plan. 1994.

.....Qu'est-ce que...

L'Intelligence Economique et Stratégique

« Une démarche organisée, au service du management stratégique de l'entreprise, visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion des connaissances utiles à la maîtrise de son environnement (menaces et opportunités) ; ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes. »

**« L'intelligence économique et stratégique dans les entreprises françaises »,
Frank BOURNOIS et Pierre-Jacquelin Romani, IHEDN, octobre 2000**

S'IL EN FALLAIT ENCORE DEUX...

« L'intelligence économique est la recherche et l'interprétation systématique de l'information accessible à tous, dans un objectif de connaissance des intentions et des capacités des acteurs. Elle englobe toutes les opérations de surveillance de l'environnement concurrentiel (protection, veille, influence). »

**Christian Harbulot,
Directeur de l'École de Guerre Économique**

« L'IE est un outil de connexion entre l'action et le savoir de l'entreprise »

Philippe Baumard Professeur des Universités Aix

Définition Veille :

"Activité continue, en grande partie itérative visant à une surveillance active de l'environnement au sens large... pour en anticiper les évolutions.

Norme expérimentale XP X 50-053 Afnor, 1998

DISCIPLINES EMBOITEES



Une matière première l'information



INFORMATIONS POUR QUOI FAIRE ?

- ✓ L'information permet de représenter son univers
- ✓ L'information permet de lutter contre l'entropie d'un système
- ✓ L'information permet de choisir ses contextes d'actions ou d'orienter ceux de ces partenaires
- ✓ L'information permet de faire des choix
- ✓ L'information permet d'utiliser les moyens à sa disposition

**L'information permet de se relier aux autres :
c'est de la communication !...**

Typologie de l'information :

Brute : dans sa forme à la production, n'ayant subi aucune modification

Elaborée : à déjà fait l'objet d'interprétation du point de vue de sa signification par rapport au contexte, de sa crédibilité et validité, de son importance par rapport à l'objectif visé....

Primaire : émane de sa source première, de son producteur d'origine (livre, article...)

Secondaire : souvent sous une forme différente de la forme primaire avec fidélité (résumé, synthèse, biblio, catalogue....)

Traitement de l'information

- ✓ Qualification des sources et des contenus d'informations
- ✓ Évaluation des informations
- ✓ Le tri des informations
- ✓ Identification des signaux faibles

Sources

- A- FIABLE
- B- EN GENERAL FIABLE
- C- ASSEZ FIABLE
- D- PAS TOUJOURS FIABLE
- E- PEU SURE
- F- NON EVALUABLE

Contenus

- 1- CONFIRME
- 2- PROBABLE
- 3- VRAISEMBLABLE
- 4- DOUTEUX
- 5- IMPROBABLE
- 6- NON EVALUABLE

Typologie de l'information

L'information formelle :

- cela concerne tout ce qui a un support papier, filmographique, numérique : presse généraliste et spécialisée, ouvrages, banques de données, brevets, sites Web, film, rapports de sociétés d'études, etc....

Sources formelles :

La presse

Avantages

- Publique, libre accès.
- Bon marché.
- L 'information est exhaustive.

Inconvénients

- Une multitude de titres (difficile de s'y retrouver).
- L 'information publiée est obsolète (événement déjà passé).*
- Information mise en scène (objectif de vente).

Sources formelles :

Les livres

Avantages

- Publique, libre accès.
- Bon marché.
- L'information est exhaustive.

Inconvénients

- Une multitude de titres (difficile de s'y retrouver).
- L'information publiée est encore plus obsolète (événement déjà passé).
- Ne pas compter découvrir un scoop dans un livre.

Sources formelles :

Les autres médias télévision, radio...

Avantages

- L'information est intéressante lorsque ce sont des films de relations publiques (présentation de produits ou d'installation).

Inconvénients

- Peu intéressants (publicité et support de communication).
- Contenu succinct.
- L'information a été obtenue bien avant par les autres sources.

Sources formelles :

Les banques de données et CD-ROM

Avantages

- Une exhaustivité remarquable.
- Faible coût.

Inconvénients

- Information rarement nouvelles.
- Difficultés d'accès.

Sources formelles :

Les brevets

Avantages

- Une source de richesse inestimable.
- 80% des informations techniques utiles se trouvent dans les brevets.

Inconvénients

- La publication intervient avec beaucoup de retard (18 mois après le dépôt).
- La compréhension des brevets est souvent difficile.
- Il existe des biais : certains secteurs ne sont pas du tout couverts par des brevets (service, informatique).

Sources formelles :

Les études réalisées par des prestataires

Avantages

- L'information de qualité est traitée, en vue de répondre à une question précise (le plus souvent un état de l'art sur une technologie, ou une étude de marché).
- Possibilité de personnaliser l'étude par des questions complémentaires auprès de l'auteur (fourniture d'intelligence).

Inconvénients

- Le coût de ces études peut parfois être très important (jusqu'à 75 K€).
- L'initiative est prise par le vendeur. Elles sont loin d'être disponibles sur tous les sujets au moment où on en a besoin.

Typologie des informations

L'information informelle

- cela concerne le reste : concurrents, fournisseurs, missions, salons, conférences, stagiaires, forum et groupes de discussion. Communication orale.

Sources informelles: Les concurrents

Ils peuvent être une source d'informations :

- par leur communication commerciale et financière.
- par leur journée portes ouvertes.
- par leur presse interne.

Sources informelles: Les fournisseurs et les sous traitants

Ils représentent une source d'information inestimable

- Quand ils sont également les fournisseurs des concurrents.
- Très réceptifs aux évolutions du marché.

Sources informelles:

Les missions et voyages d'étude

Ce sont des sources extrêmement riches , mais très onéreuses. Des règles de bon sens sont à respecter pour les rendre plus fructueuses :

- Préparer la mission avant de partir.
- Être professionnel pendant la mission, à la japonaise. Être à l'affût du moindre élément d'intérêt.
- Exploiter et diffuser correctement les informations rapportées. Ne pas remettre cela au lendemain lors de votre retour.

Sources informelles: Les expositions et les salons

Ce sont des sources très riches pour qui sait y faire.

- Préparer la mission avant de partir (recenser les contacts, localiser les exposants pour ne pas perdre de temps).
- Être réactif lors de la visite (durée brève : un ou deux jours).

Autres sources informelles :

- **Les colloques, congrès et clubs** : Les communications qui y sont faites sont riches en information. Mais il faut avant tout se concentrer sur les contacts que vous pouvez avoir.
- **Étudiants, stagiaires, thésards** : Bien encadrés, ces personnes peuvent vous apporter de riches informations (thésards, qui sont formés à la recherche), ou vous servir à en apporter (stagiaire envoyé chez un concurrent).
- **Les candidats à l'embauche** : Durant un entretien, on peut avoir des informations de grande valeur sur leurs anciens employeurs.
- **Les prestataires extérieurs** : agents de recherche (détectives), les cabinets spécialisés, les journalistes en free lance.
- **Le réseau relationnel en interne et en externe** : votre carnet d'adresse s'étoffera tout au long de votre vie professionnelle.

Statut de l'information

- ✓ **L'information blanche** : cela représente **80%** de l'information existante, elle est légalement disponible (gratuit ou payant).
- ✓ **L'information grise** : environ **15%**. informations jugée sensible, n'émanant pas de sources ouvertes. Elle est acquise de manière informelle mais légale.
- ✓ **L'information noire** : **5%**. information jugée très sensible, pouvant compromettre les intérêts de l'organisation si elle est dévoilée, elle est acquise par le vol, l'espionnage et autres méthodes illégales (chantage, piratage, etc.).

Statut de l'information

	Information	Déontologie	Renseignement
Codes couleurs	Blanc	Gris	Noir
Qualification	Ouverte	Sensible	Fermée
Accès	Libre	Sous conditions	Non autorisé
Infractions	Non	Selon jurisprudence	Lois civiles et commerciales
Sources	Organismes publics, privés, médias, conf...	Doct interne, personnel de l'Ent., réseaux	Sources internes

La gestion stratégique de l'information



Les enjeux : optimiser la gestion de l'information

- Problèmes économiques de plus en plus complexes.
- Environnement polymorphique et mouvant.
- Nécessité de maîtriser les flux d'information.
- Travailler en réseau interne et externe.
- Diffuser l'information en temps réel pour rester réactif et compétitif.
- Être proactif sur les marchés à venir afin d'anticiper les stratégies des concurrents.

Cohérence dans le cadre de l'IES

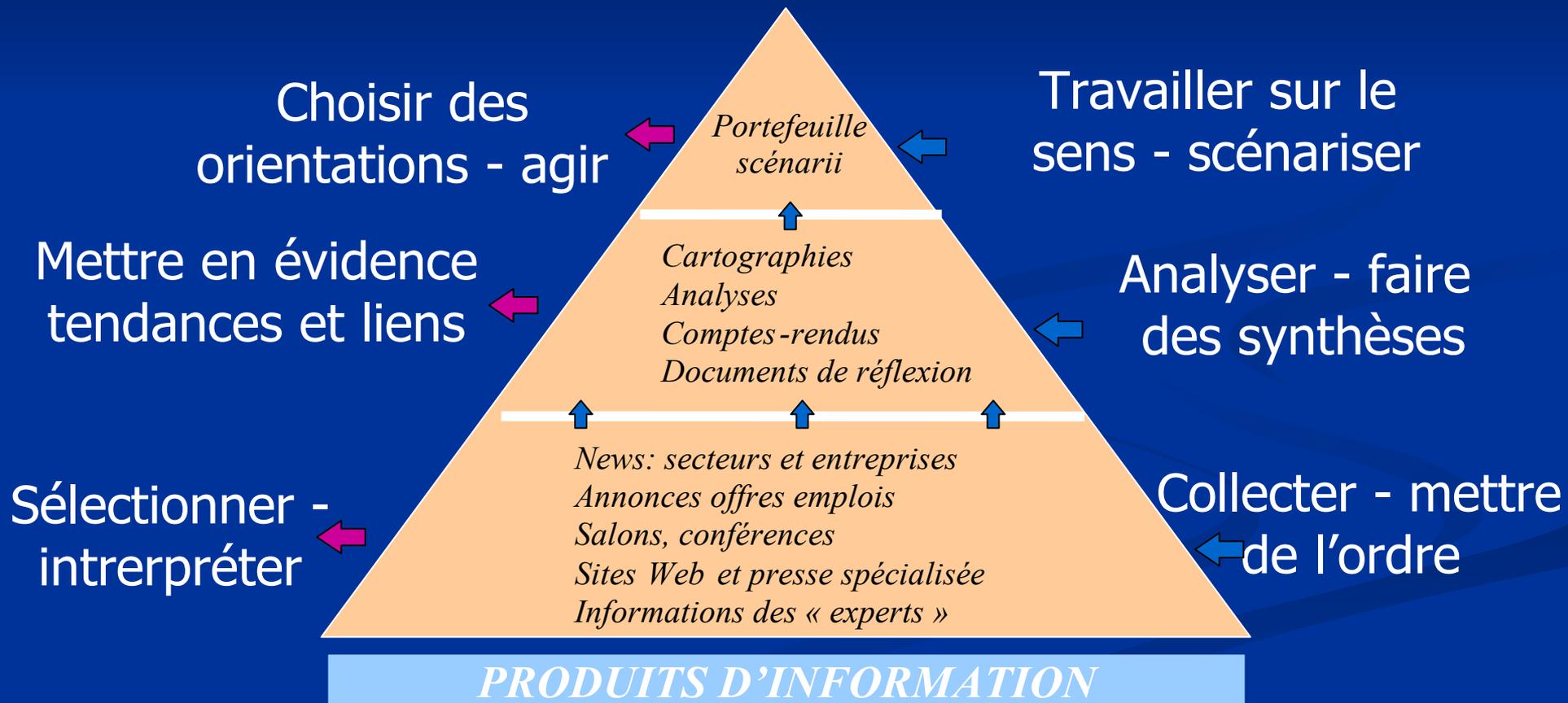
Afin d'assurer la cohérence dans la gestion de l'information il convient de se poser les bonnes questions :

Comment l'information...

- ✓ Est-elle **collectée** ?
- ✓ Est-elle **protégée** ?
- ✓ Est-elle **gérée** ?
- ✓ Est-elle **diffusée** ?

INTELLIGENCE ECONOMIQUE : UNE DEMARCHE ET SES PRODUITS

Un objectif : restreindre l'information...



Objectifs d'une gestion maîtrisée

Mot d'ordre :

«Savoir pour comprendre et comprendre pour agir»

Sur le plan défensif :

- ✓ la gestion stratégique de l'information consiste à prévenir et anticiper.

Sur l'aspect offensif :

- ✓ il s'agit d'optimiser l'exploitation des flux d'informations

Types de gestionnaires

- **Le dormeur** : son mode d'action est inexistant, il est sujet à un aveuglement total. Il juge donc la veille inutile et ne craint pas la concurrence.
- **Le réactif** : son mode d'action est seulement opportuniste, il réagit uniquement aux attaques extérieures et dispose d'un budget très limité.
- **L'actif** : il dispose de moyens classiques : presse généraliste, quelques journaux spécialisés; mais limités, cela s'inscrit dans le démarrage d'une cellule de veille. Quand il emploie l'observation des bonnes pratiques concurrente, c'est du benchmarking.
- **L'offensif** : ce sont en général les anciens de services d'état, il opère un traitement pointu des données. Il dispose de moyens importants, il est caractérisé par un professionnalisme exacerbé.
- **Le guerrier** : son mode d'action est orienté vers la guerre des brevets, il est positionné dans une situation très offensive. S'il cherche avant tout à exercer une influence sur son environnement, c'est un lobbyiste.

Guerre de l'information

Ou l'art de créer le risque informationnel...



Dans un contexte...

- ... ou le renseignement permet la création de valeurs, **l'information** devient une **richesse** qu'il faut valoriser et protéger, mais elle est également une **arme** qu'il faut savoir utiliser.

Définition militaire

- La guerre de l'information recouvre l'ensemble des champs conflictuels où l'information est utilisée comme une **arme offensive** pour affaiblir, déstabiliser ou détruire un adversaire. Les techniques offensives de la guerre de l'information peuvent prendre la forme de la désinformation, de la manipulation, de la rumeur, de la propagande

Définition civile

- “L’infoguerre revêt cependant un sens particulier puisqu’on la définit comme l’ensemble des opérations visant à contrôler ou neutraliser la capacité informationnelle d’un adversaire économique.”

L'Infoguerre *

- Né dans un contexte militaire au moment de la guerre du Golfe, le concept d'infoguerre a glissé peu à peu dans le domaine concurrentiel.
- Il vient ainsi à recouvrir les pratiques opérationnelles de ciblage des informations et des fonctions informationnelles d'un concurrent tout en cherchant à protéger son propre système.

* traduction de l'américain Infowar, contraction de « Information Warfare »

La mutation des techniques d'attaque

Espionnage industriel

- connaître l'autre
- devancer ses initiatives
- pirater son savoir
- capter ses marchés
- détourner ses clients
- débaucher ses cadres

Guerre de l'information

- empêcher l'autre d'agir
- identifier ses failles
- parler à sa place
- influencer ses alliés
- fragiliser son image
- démoraliser son personnel

L'évolution du risque informationnel

Hier	Aujourd'hui
<ul style="list-style-type: none">■ Médiatisation des rumeurs■ Action ponctuelle■ Dégâts limités■ Désinformation■ Frappes ciblées	<ul style="list-style-type: none">■ Multimédiatisation■ Campagne durable■ Dégâts illimités■ Orchestration de polémiques■ Frappes tous azimuts

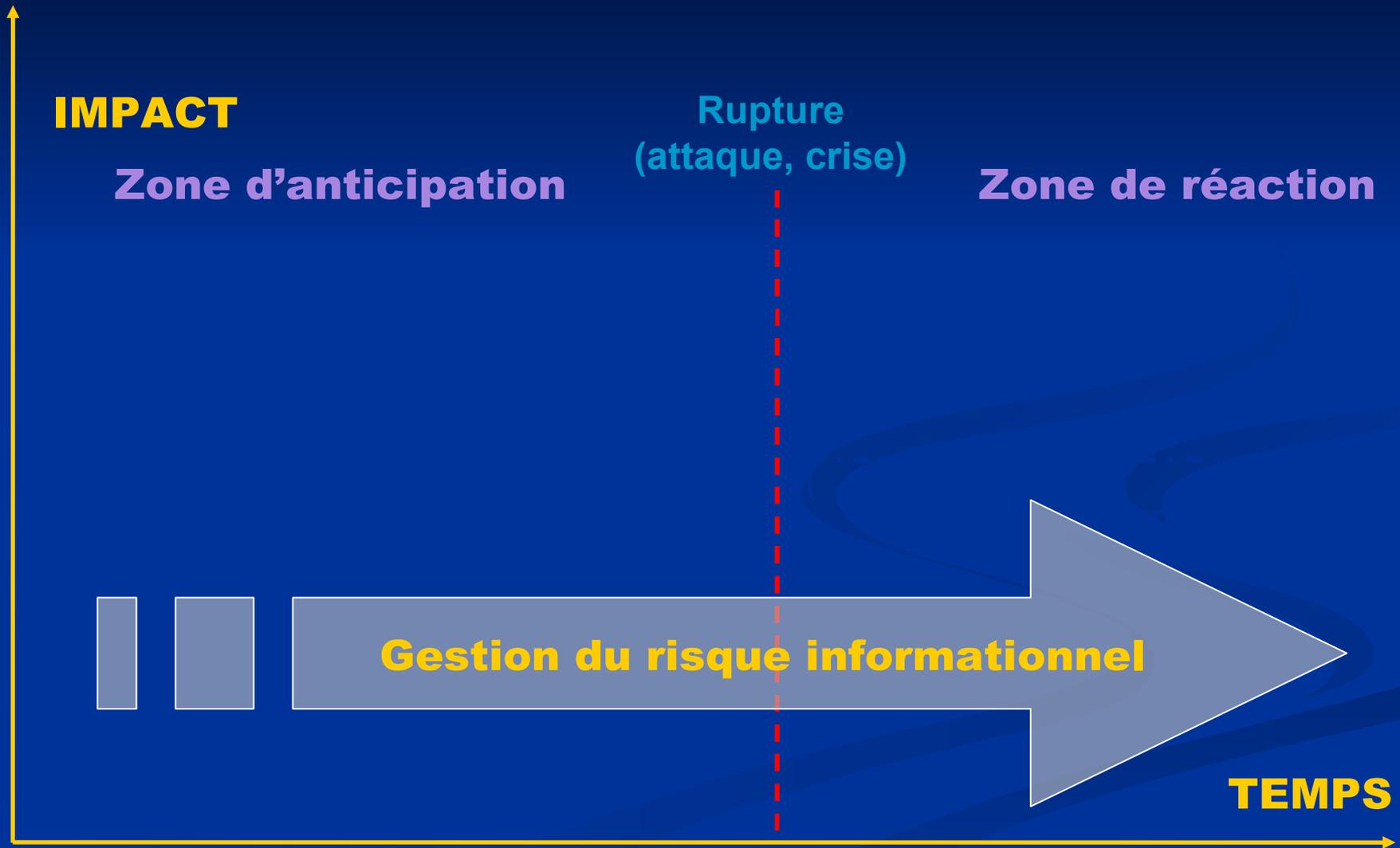
Définition du risque informationnel

Le risque informationnel est la probabilité d'une information avérée ou pas, susceptible de modifier ou d'influencer l'image, le comportement et la stratégie d'une entreprise

Le cadrage du risque

- La nature
- L'origine
- Les conséquences
- La détectabilité
- La contrôlabilité
- La gravité
- La probabilité d'occurrence

Développement du risque informationnel



Trois échiquiers

❑ L'échiquier géoéconomique

Nations

Hommes états

Institutions internationales

❑ L'échiquier concurrentiel

Partenaires

Concurrents

Clients

❑ L'échiquier de la société civile

ONG

Associations

Individus

Deux champs d'affrontement concurrentiel

Occuper le terrain par la connaissance

- mieux parler que l'autre
- se faire mieux entendre
- ne pas se faire diaboliser

Fragiliser l'autre en soulignant ses points faibles

- par la polémique
- par l'orchestration des caisses de résonance
- par une prise de conscience de l'opinion publique

Méthodologie d'évaluation d'un secteur d'activité :

Objectifs :

- Identifier les forces en présences
- Établir la cartographie exhaustive des acteurs
- Evaluer les rapports de forces
- Mesurer les interactivités
- Identifier les risques informationnels potentiels.
- Evaluer les sources d'informations possibles
- cibler les manques informationnels et relancer une dynamique

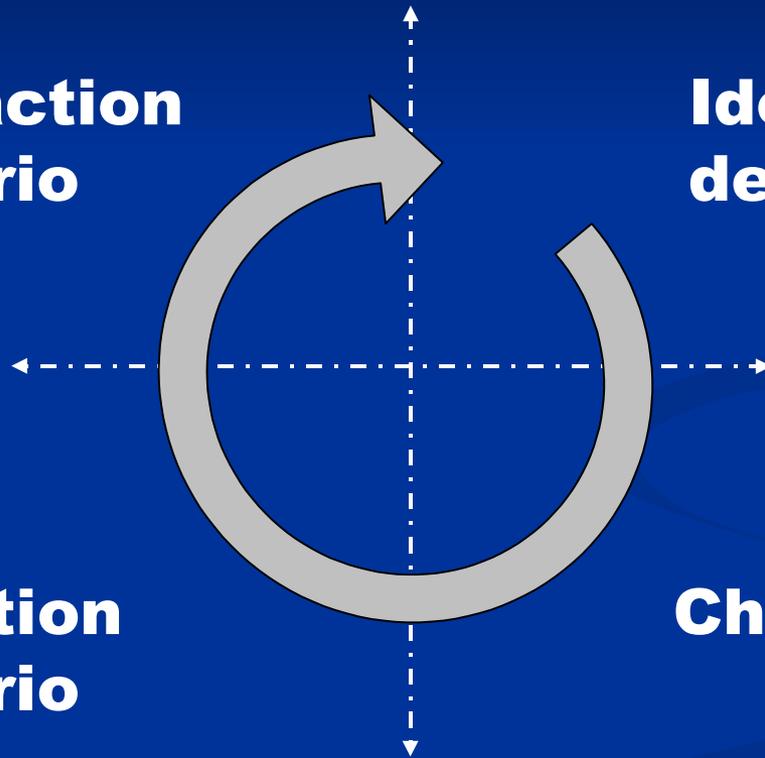
Le cycle d'attaque informationnelle

**Mise en action
du scénario**

**Identification
des failles**

**Construction
du scénario**

Choix des failles



Les principes

- La guerre **PAR** l'information : influencer le comportement de l'adversaire par les informations volontairement mises à sa disposition
- La guerre **Pour** l'information : prendre possession des canaux d'informations de l'adversaire et véhiculer les informations choisies.
- La guerre **Contre** l'information : détecter les informations émises et qui peuvent porter préjudice au déroulement de l'action, afin d'en limiter la diffusion.

Guerre par l'information

- **Communication active**
- **Propagande, rumeurs**
- **Désinformation,**
- **Surinformation, sous information**
- **Mésinformation**
- **Lobbying**

Quelques principes de désinformation

- Attaquer l'adversaire par surprise
- Tromper l'adversaire
- Manipuler les systèmes de connaissance adverses
- Discréditer l'image de l'entreprise
- Pousser l'autre à la faute
- Contre-attaquer avec les mêmes armes que l'attaquant

La contre-information

- Ne pas se justifier
- Utiliser à son profit les contradictions de l'adversaire
- Frapper ses points faibles
- Discréditer systématiquement ses points forts
- Influencer ses alliés

Guerre pour l'information

Les Applications au monde civile ou économique des technologies Echelon ou carnivore à l'origine développées pour la défense sont nombreuses, de multiples exemples liés au système Echelon ont été déclassifiés.

Guerre pour l'information

- Veilles...
- Benchmarking
- Réseaux d'informateurs
- Espionnage...

Guerre contre l'information

- Elle concerne les techniques visant à priver un adversaire de son accès à l'information et se rapporte à deux types de risques: d'une part la destruction des données et des programmes qui permettent leur traitement; de l'autre, le sabotage peut passer par le "deni de service"* et entraîner une paralysie des réseaux de transmission.

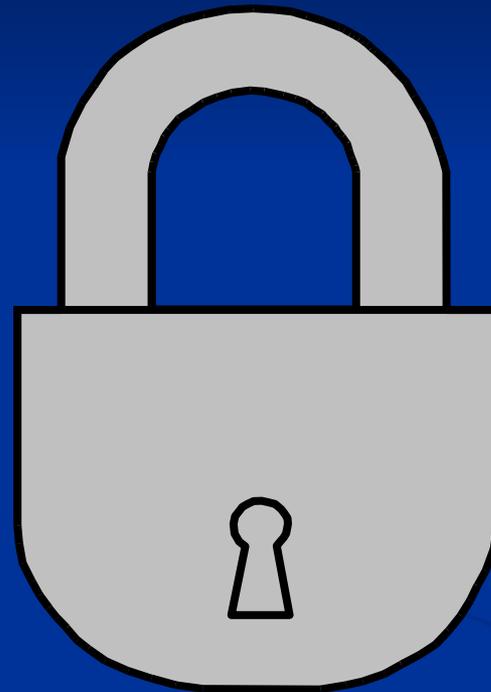
Facteurs d'échec en guerre de l'information

- Saturation informationnelle
- Idées préconçues
- Incompréhension culturelle
- Mauvaise analyse du jeu des acteurs
- Mauvaise analyse de la situation
- Absence de mémoire sur les phénomènes antérieurs
- Mauvaise évaluation des moyens à mettre en œuvre
- Mauvaise évaluation des priorités
- Mauvaise gestion de l'information
- Manque maîtrise des moyens de communication
- Mauvaise chronologie de l'action
- Absence de mesure de résultats
- Manipulation
- Mauvaise protection de l'action

Facteurs clés de succès en guerre de l'information

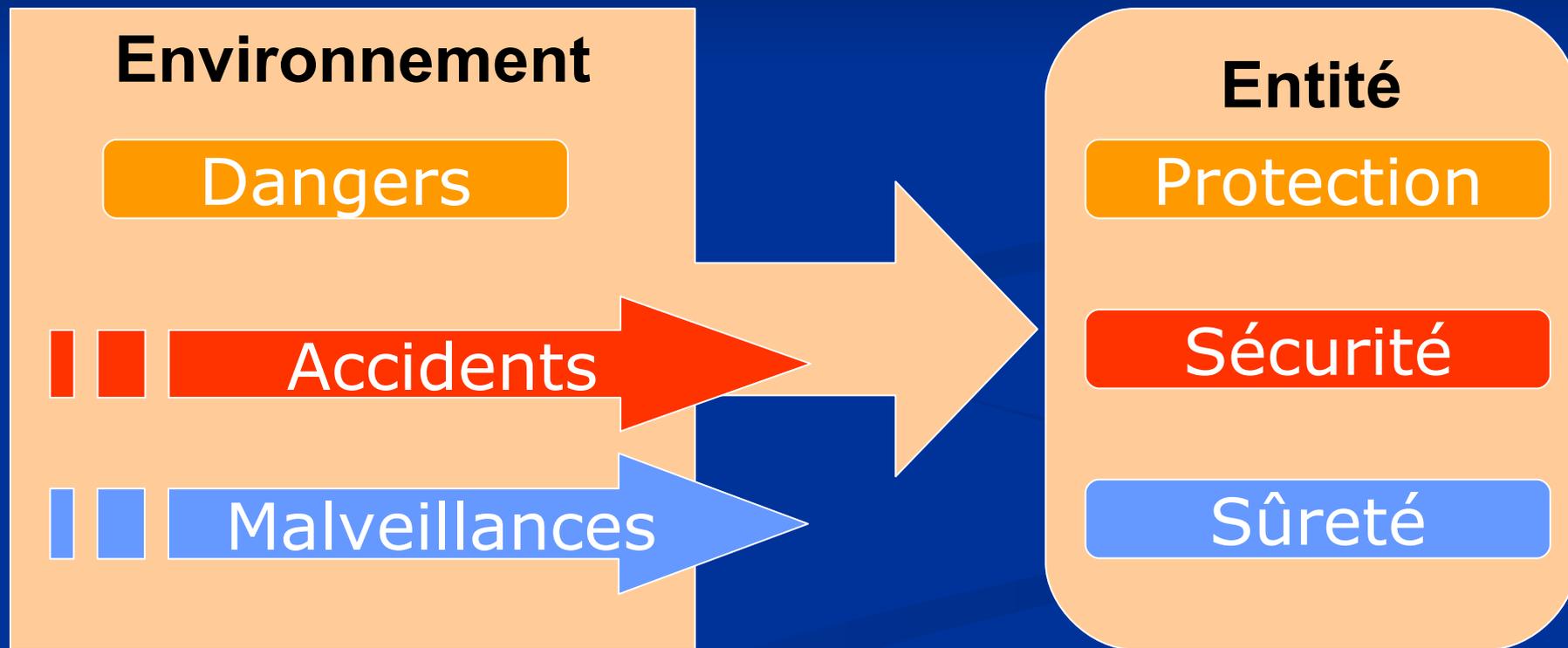
- Motivation et niveau d'engagement collectif, grande confiance entre les individus
- Compétences individuelles et collectives ; et expériences des opérateurs
- Définition claire des objectifs
- Soutien de la hiérarchie
- Déontologie et loyauté de l'action
- Simplicité de la mise en œuvre
- Mix de communication : produit, politique de communication, moyens de diffusion
- Ciblage des réseaux et des bons interlocuteurs
- Economie des forces et des moyens
- Qualité de la logistique
- Démarche indirecte et camouflée
- Maîtrise de la prise de risque
- Capacité d'ajustement de la mission
- Pro-activité
- Optimisation de l'attaque sur les points faibles
- Bonne application des règles de protection

Protection de l'information

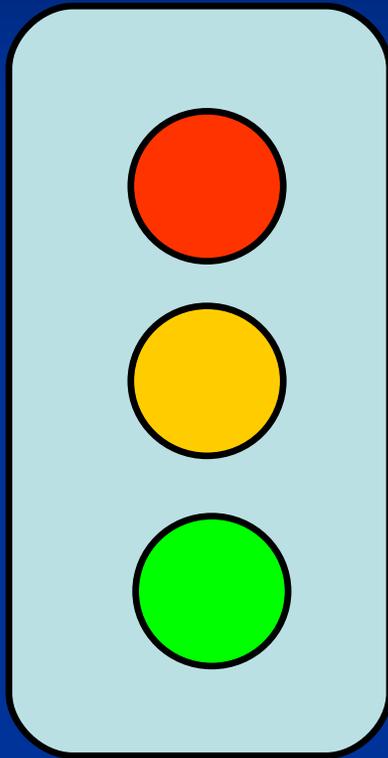


Notions essentielles :

Le risque zéro n'existe pas !



PROTECTION DE L'INFORMATION



Très sensible : Pouvant directement porter atteinte à la pérennité de l'Entité.

Sensible : seule, ne peut pas empêcher l'Entité de fonctionner mais pourrait grandement la ralentir.

Peu sensible : Information ouverte.

GRADATION DANS LA POSTURE

Prise en compte des niveaux de protection

l'exemple du garde du corps.

Prévention : Organisation de la mission gilet de protection et l'oreillette

Dissuasion : les lunettes noires, nombre des personnels...

Réaction : l'entraînement au tir et sports de combats ou la conduite sportive...

Etapes d'une démarche de protection

Diagnostic

- **Effectuer** un inventaire précis des données à protéger selon leur niveau de confidentialité et de sensibilité pour l'entreprise. Lister les matériels permettant de transporter l'information : lecteurs de disquette, graveur CD, scanner, micros, caméra, connexions au Web...

Etapes d'une démarche de protection

Conseil :

- **Définir** les « points d'accès » à ces informations et les personnes habilitées à y accéder en consultation, en modification et en suppression.
- **Choisir** les différents logiciels spécialisés dans la sauvegarde, la protection contre les virus, contre les intrusions de prise de contrôle à distance, de surveillance de l'activité du réseau, gestion d'accès...

Etapes d'une démarche de protection

Accompagnement :

- **Attribuer** des mots de passe UNIQUES ET CONFIDENTIELS pour chacun et les sensibiliser à l'importance de la confidentialité.
- **Garantir** la maintenance logicielle et matérielle du parc informatique en planifiant des tests d'intégrité du matériel et le nettoyage des disques notamment.
- **Prévoir** les procédures à suivre en cas d'atteinte aux données et former les différents acteurs afin de pouvoir anticiper sur une crise informationnelle.

CONCRETEMENT QUE DOIT-ON FAIRE ?

- ✓ **Etude des failles utilisables par la concurrence**
- ✓ **Etude des contre-mesures déjà en place**
- ✓ **Modélisation et validation de scénarii potentiel de crise**
- ✓ **Propositions de contre-mesures**
- ✓ **Sensibilisation du personnel**
- ✓ **Suivi des prestataires**

Protection logique :

Les dangers liés à l'informatique:

- ✓ La perte de données.
- ✓ La corruption des données.
- ✓ L'accès non sécurisé aux données.
- ✓ Le blocage des moyens d'accès aux données.
- ✓ La diffusion incontrôlée des données.

Menaces les plus courantes: hoax, mailbombing, crossposting, flooding, nuke, virus, intrusion, imposture, portscanning, vol, spoofing, keylogger

Et les écoutes téléphoniques...

Protection Physique

Les Locaux :

Gardiennage, télésurveillance, contrôle d'accès

Les déplacements :

Discussions, chambre d'hôtel, portable

Protection intellectuelle

Sur l'image :

- Marques

Sur les produits :

- Brevets
- Enveloppe solo

Sur les hommes :

- Contrats de travail
- Prestataires, stagiaires, partenaires

L'être humain maillon faible de la chaîne de protection

M.I.C.E

- ✓ L'argent
- ✓ L'idéologie
- ✓ La compromission
- ✓ L'ego

■ Questions ?..



Merci de votre attention...

"Il est très triste qu'il y ait si peu
d'informations inutiles de nos jours."
O.Wilde

m.morvan@ligne12.com