On distingue habituellement quatre grands types de veille :
- la veille commerciale
- la veille concurrentielle
- la veille technologique
- la veille environnementale

Présentation des différents types de veille

l'IE est à la fois compliquée et complexe.

plusieurs personnes assistant au même événement le décrivent de façons très différentes.

-des perceptions biologiquement différentes.

Des interprétations de ces perceptions qui sont élaborées dans notre cerveau -à partir de nos expériences précédentes, de nos apprentissages, de nos cultures.

-Un nécessaire filtrage sur la partie de la réalité qui va être analysée

-Il est matériellement impossible à chacun de percevoir la totalité des événements quise passent dans l'Univers à chaque instant.

-Chacun de nous passe plusieurs fois par jour par des états de conscience variés:veille, sommeil, rêve.

L'intelligence économique consiste, pour une large part, à mettre en pratique ces nouvellesfaçons d'appréhender le monde. Il ne s'agit pas de comprendre tout ce qui se passe, maisseulement ce qui est accessible. Il ne s'agit pas de regarder les choses avec un seul point devue, mais de les faire varier pour comprendre pourquoi les intérêts divergent, quels outils etquelles armes peuvent être utilisées par les différents acteurs en train d'évoluer dans lecontexte observé.

Les grandes phases du cycle de renseignement:

-On commence le cycle en identifiant et précisant son « besoin desavoir »

Cette étape se termine par l'élaboration d'un Plan de renseignement on sait alors ce que l'on ne sait pas).

-On continue le cycle en cherchant les sources d'information. On procèdera à leur inventaire ainsiqu'à l'évaluation des coûts d'accession à l'information

Cette étape débouchera sur l'élaboration d'un Plan de recherchequi répond à la question « comment s'organiser pour trouver ? »

la troisième étape du cycle consiste à exploiter les résultats des recherches. Elle se décomposeenquatre sous-étapes : la validation des informations collectées (généralement par recoupement dessources), le traitement (notation et démarquage des informations pour les découpler de leurssources afin de ne pas influencer l'étape suivante), analyse des informations pour leur donner dusens en fonction des objectifs suivis, et enfin synthèse pour les mettre sous une forme acceptablespar leur destinataire final. Les deux premières sous-étapes se réalisent dans une logique decloisonnement (notamment pour effectuer le recoupement) alors que les deux dernières s'effectuentdans unelogique de transversalité (pour replacer les informations dans le paysage ou dans le futurrecherché).

- la quatrième étape du cycle consiste à diffuser l'information traitée vers ses destinataires : lecommanditaire (celui qui a demandé l'information), la mémoire de l'organisme (pour améliorer les évaluations ultérieures, pour garder trace de la recherche), les autres destinataires jugés utiles (desentreprises partenaires, l'adjoint du commanditaire qui sera parfois plus opérationnel que lecommanditaire, etc.) Il faut que le renseignement parvienne « à temps » (avant la clôture de l'appeld'offre) et « sous la bonne forme » (une cadre dirigeant ne lira pas un épais rapport technique car iln'en a pas le temps).

- le bouclage du cycle se fait, sur les questions suivantes : est-ce que le renseignement a permisd'agir ? la réorientation de l'action a-t'elle apporté quelque chose à l'entreprise ? est-ce que les questions qui ont déclenché le cycle de renseignement étaient les bonnes ?est-ce que lerenseignement est arrivé à temps et auprès des bonnes personnes ?

L'activité d'IE est un cycle qui doit fonctionner en permanence.

On distinguera deux grandes façons d'organiser les réseaux de surveillance :

Les réseaux « cybernétiques »(agentbête) auront des capacités de réaction généralement

plus rapides mais lesréseaux « managériaux »(agentpensant) ont une meilleurecapacité à produire d e l'information stratégique etpeuvent être exploités dans une gamme plus large d'actions de renseig nement.

Les rumeurs:
Ces déformations des informations se produisent notamment sous la forme
--de simplifications
--d'accentuations
--de transformations
Propagande, désinformation, communication biaisée:
Historiquement,le terme « propagande » est associé à des modes de communication mis en œuvrepa r des régimes totalitaires en direction des populations qu'ils dominent.. La propagande est un discou rs de vérité, souvent paranoïaque et fermé sur lui-même.
Il s'exprime principalement dans des formulations figées, aphorismes et néologismes servant àdésig ner les amis, les ennemis ou les concepts directeurs.
Le terme « désinformation » désigne une autre forme de discours. Présentant également l'apparence d'un discours de vérité, il porte un message opposé au discours qui est sa cible.
Le terme de « communication biaisée » désigne une troisième forme de discours. La différenceprinc ipale avec les deux précédents est que ceux qui l'émettent savent sans ambiguïté qu'ils necroient pa s dans ce qu'ils disent
Première approche de la sécurité informatique:
a) les risques individuels: antivirus et firewall pour se protéger lors des connexions sur internet. dup lication des données sur des supports mémoire externes (disques dur amovibles)
b) risques professionnels:Connaissant la négligence généralisée en matière de sécurité personnelle, certaines entreprisesorganisent la sécurité professionnelle de façon coercitive : tout agent qui est sur pris à ne pasrespecter une procédure de sécurité est considéré comme ayant commis une faute profe ssionnelle.
-- que la grande majorité des causes est humaine (défaillances ou attaques intentionnelles)
-- qu'elles sont parfois d'origine externe mais le plus souvent d'origine interne (non respect desproc édures de travail, défaillances physiques ou psychiques, vengeance d'un ancien salarié,désaccord d' un salarié avec les objectifs de l'organisation dans laquelle il travaille, conflit syndical). Lerecours à la sous--traitance ou au travail temporaire, qui ont pour effet d'introduire dans l'entreprisedes salarié s « externes », est un facteur de risque supplémentaire.
Protéger une entreprise, c'est donc d'abord procéder à un examen systématique des risques, puiscal culer les conséquences potentielles.
On voit que, dans ces différentes étapes, les mesures d'ordre technologique (alimentationsredondant es, firewall, sauvegardes etc.) viendront seulement après que l'audit de sécurité ait définila politique .
Une façon simple d'identifier une entreprise défaillante en matière de sécurité est de constater quele s équipements de sécurité ont été installés en l'absence d'un audit préalable. Il est alorsextrêmement probable que des « trous » existent dans la ligne de défense de l'entreprise.

La pédagogie inversée:
La mise en place un réseau d'information très simple:
a) création du canal de communication
b) ouverture et validation du canal de communication par mail
c) Ouverture et validation du canal de communication téléphonique par SMS
d) On peut remarquer que le canal e--mail n'est pas seulement un canal enseignant-étudiants mais peut également être utilisé en tant que canal étudiants--étudiants. Il suffit pour cela que l'enseignant laisse visible à tous la liste des destinataires.
Le processus qui enchaîne les phases de création, ouverture, validation, actualisation est un processus général de mise en place d'un dispositif de communication. Oublier une des

étapes (souvent l'étape de validation) peut avoir pour effet de rendre le dispositif moins sûr, voire inefficace. Il est donc nécessaire de s'astreindre à la discipline du respect de ce processus.

L'évolution parallèle de la théorie des firmes et de la théorie de l'information

En regroupant les étapes de la spirale de la vigilance, remarquons que cet enchaînement peut se simplifier dans le schéma suivant :

S'adapter -> connaître -> utiliser -> rentabiliser

Et que ce schéma, à son tour peut se résumer en :

Processus cognitif -> processus économique

Des façons différentes de concevoir et pratiquer l'intelligence économique :