Intelligence économique

Résumé du cours du 21 octobre 2015

Le cycle de l'IE

Les grandes phases du cycle de renseignement

Ce cycle du renseignement s'applique, avec des moyens différents, aussi bien à l'échelle de l'individu qu'à l'échelle de la très grand de entreprise ou de l'Etat.

- On commence le cycle en identifiant et précisant son « besoin de savoir ». Une entreprise aura notamment besoin de savoir (ou besoin d'en savoir plus) à propos de ses clients, de ses fournisseurs (sont ils fiables, ont-ils des problèmes juridiques ou financiers, etc.), ses technologies (et celles qui émergent ou sont utilisées par les concurrents), de son environnement juridique et fiscal (quelles évolutions en cours ou à prévoir ?), etc.

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 ainsi qu'à l'évaluation des coûts d'accession à l'information. On identifiera ainsi les sources les plus pertinentes et les moins coûteuses. Cette étape débouchera sur l'élaboration d'un Plan de recherche qui répond à la question « comment s'organiser pour trouver ? ».

- la troisième étape du cycle consiste à exploiter les résultats des recherches. Elle se décompose en quatre sous-étapes : la validation des informations collectées (généralement par recoupement des sources), le traitement (notation et démarquage des informations pour les découpler de leurs sources afin de ne pas influencer l'étape suivante), analyse des informations pour leur donner du sens en fonction des objectifs suivis, et enfin synthèse pour les mettre sous une forme acceptables par leur destinataire final. Les deux premières sous-étapes se réalisent dans une logique de cloisonnement (notamment pour effectuer le recoupement) alors que les deux dernières s'effectuent dans une logique de transversalité (pour replacer les informations dans le paysage ou dans le futur recherché).

- la quatrième étape du cycle consiste à diffuser l'information traitée vers ses destinataires : le commanditaire (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 (des entreprises partenaires, l'adjoint du commanditaire qui sera parfois plus opérationnel que le commanditaire, etc.) Il faut que le renseignement parvienne « à temps » (avant la clôture de l'appel d'offre) et « sous la bonne forme » (une cadre dirigeant ne lira pas un épais rapport technique car il n'en a pas le temps). Pour cela, il faut connaître les circuits de diffusion officiels (pour respecter la voie hiérarchique) mais aussi savoir utiliser les circuits officieux (pour rendre la diffusion plus efficace). Il est préférable d'établir des relations de confiance avec les destinataires (pour qu'ils exploitent le renseignement) et il faut veiller au fuite (pour que le renseignement ne soit pas exploité par d'autres).

- le bouclage du cycle se fait, sur les questions suivantes : est-ce que le renseignement a permis d'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 le renseignement est arrivé à temps et auprès des bonnes personnes ?

Conclusion

L'activité d'IE est un cycle qui doit fonctionner en permanence. Sinon, on perd facilement les réflexes et les savoir-faire. Le réseau d'informateurs non utilisé se délite. Les dirigeants qui ne reçoivent plus d'information perdent l'habitude d'en demander ou se tournent vers d'autres dispositifs. La sécurité des informations n'est plus régulièrement testée et des fuites apparaissent.

Le cycle qui vient d'être décrit présente des défauts :

- le temps de traitement fait que l'information traitée peut avoir évolué pendant le délai entre la captation et l'exploitation.
- La déconnexion du dispositif d'analyse avec la réalité quotidienne d'où proviennent les informations (les « villages ») peut provoquer des interprétations erronées.

Différentes méthodes existent pour limiter les effets de ces défauts mais il faut bien garder en tête qu'en matière d'IE, ce qui compte n'est pas tant d'être parfait que d'être meilleur que les concurrents.

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

- l'approche « cybernétique » dans laquelle les agents recherchent les informations sans savoir à quoi elles serviront et sans les interpréter. On est dans une logique de stricte hiérarchie. Les agents sont dirigés soit pas la force (par exemple, on obtient d'eux les informations par le chantage), soit par une mise en condition qui les conduit à intérioriser une idéologie et la nécessité pour eux d'obéir aveuglément aux instructions qui leurs sont données (modèle fanatique).
- L'approche « managériale » dans laquelle les agents « pensent », cherchent la meilleure source, pré-interprètent les données collectées, ont un pouvoir d'expertise. La relation hiérarchique dans ces réseaux est basée sur le choix (ou en tout cas le respect) du leader.

Les réseaux « cybernétiques » auront des capacités de réaction généralement plus rapides mais les réseaux « managériaux » ont une meilleure capacité à produire de l'information stratégique et peuvent être exploités dans une gamme plus large d'actions de renseignement.

Les rumeurs

Un des effets du dysfonctionnement d'un réseau est la production de rumeurs.

Ces déformations des informations se produisent notamment sous la forme

- de simplifications
- d'accentuations
- de transformations

Les phénomènes de rumeurs peuvent avoir des effets catastrophiques car elles entraînent des prises de décisions inappropriées dans les chaînes de commandement renseignées par le réseau d'information.

Propagande, désinformation, communication biaisée

Historiquement, le terme « **propagande** » est associé à des modes de communication mis en œuvre par des régimes totalitaires en direction des populations qu'ils dominent (régime nazi en Allemagne, régimes communistes en URSS et en Chine, etc.). Les dirigeants sont présentés de façon héroïque et toujours positive. Les orientations politiques sont répétées et déclinées sous de multiples formes. Les opposants sont présentés comme des ennemis de la liberté, des sous-hommes, des malades ou des « terroristes ». La propagande est un discours de vérité, souvent paranoïaque et fermé sur lui-même. Il s'exprime principalement dans des formulations figées, aphorismes et néologismes servant à désigner les amis, les ennemis ou les concepts directeurs. Ceux qui le créent, le prononcent ou le diffusent y croient, ou du moins semblent y croire. Principalement destiné à la population gouvernée, il s'adresse également au-delà des frontières, aux pays étrangers, opposants ou du même bord.

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. Il a pour objet de contrer le discours cible, au minimum en introduisant le doute dans les esprits et, si possible, en installant une croyance dans une autre vérité. Il peut être émis de façon préventive, avant même que le discours cible n'ait été communiqué. Tout comme le discours de propagande, ceux qui le créent, le prononcent ou le diffusent y croient, ou du moins semblent y croire.

Le terme de « **communication biaisée** » désigne une troisième forme de discours. La différence principale avec les deux précédents est que ceux qui l'émettent savent sans ambiguïté qu'ils ne croient pas dans ce qu'ils disent. Ils déforment ou transforment délibérément ce qu'ils pensent être la vérité. C'est un discours de mensonge.

Il est souvent difficile de distinguer, vu de l'extérieur, les trois formes de discours. En effet, comment savoir si l'orateur croit dans ce qu'il dit. Est-il un militant ou un cynique manipulateur ? Et comment déterminer si un discours est « vrai » dans l'absolu ? Aucune de ces deux questions n'a de réponse autre que relative : pour qualifier les discours, il faut soi-même se positionner comme adhérent (croyant) ou comme opposant (sceptique).

Dans la guerre de l'information, l'ensemble des systèmes de références est sans cesse en évolution.

En termes d'Intelligence économique, cela n'est pas sans poser de nombreux problèmes car les informateurs eux-mêmes sont les cibles des actions de propagande, de désinformation ou de communication biaisée. Cela peut parfois les amener à changer de croyances et donc à changer de

camps. C'est pour cela que, dans les réseaux de surveillance, il existe de nombreuses procédures visant à recouper les informations collectées, mais aussi à vérifier régulièrement la fiabilité des informateurs.

Le fait de ne pas accorder d'importance à ces phénomènes peut provoquer des effets catastrophiques pour les entreprises.

Cas d'école : en 2007, l'Inde lance un appel d'offre international pour acheter des hélicoptères de combat. L'entreprise européenne Eurocopter est en concurrence avec l'entreprise américaine Bell. C'est la première qui l'emporte, avec une proposition basée sur un excellent appareil. Mais, quelques semaines après l'annonce de la victoire, la presse indienne publie l'information selon laquelle l'entreprise indienne avec laquelle Eurocopter s'est associée pour répondre à l'appel d'offre est dirigée par le frère du principal responsable de l'évaluation des offres au ministère de la défense indien. Malgré les dénégations d'Eurocopter, un fort soupçon de corruption se répand et le gouvernement indien finit par casser sa décision puis réinitialise le marché. Peu importe que la rumeur soit vraie ou fausse, elle a produit ses effets et la société initialement éliminée, Bell, se retrouve en position favorable dans le marché réinitialisé.

Première approche de la sécurité informatique

a) les risques individuels

Petit sondage afin que les étudiants décrivent les procédures de sécurité informatique qu'ils utilisent effectivement. Ils évoquent les méthodes suivantes :

- antivirus et firewall pour se protéger lors des connexions sur internet

- duplication des données sur des supports mémoire externes (disques dur amovibles)

Il apparaît que, dans leur immense majorité, les étudiants n'ont pas réfléchi et organisé leur protection. Ils n'ont pas analysé leurs risques ni construit des procédures adaptées à leur situation personnelle. Lorsqu'ils utilisent les méthodes ci-dessus, ce n'est en général pas de façon systématique. Ils ne sont pas protégés contre certaines familles de risques (captation, croisement et utilisation de leurs profils individuels, vol de leurs équipements portables, vols de leurs identifiants et mots de passe, destruction simultanée des données et des sauvegardes, vols d'identité bancaire, etc.).

De façon interactive, l'enseignant effectue un examen systématique des risques auxquels un étudiant est soumis et les différentes mesures de protection sont indiquées. Pour conclure, les étudiants sont invités à procéder à leur mise en sécurité…tout en sachant que peu d'entre eux le feront !

b) risques professionnels

Connaissant la négligence généralisée en matière de sécurité personnelle, certaines entreprises organisent la sécurité professionnelle de façon coercitive : tout agent qui est surpris à ne pas respecter une procédure de sécurité est considéré comme ayant commis une faute professionnelle. Dans certaines entreprises, c'est un motif de licenciement immédiat. Dans d'autres entreprises, il y aura des procédures graduées allant du simple avertissement au licenciement en cas de récidive, en passant par l'obligation d'aller récupérer chez le directeur général la clé USB que l'on avait laissé traîner sur son bureau en partant le soir. Il existe, bien entendu, des entreprises ou des administrations qui négligent leur sécurité ou bien qui, ayant édicté des procédures, ne vérifient pas sans cesse leur bonne application.

L'examen des statistiques en matière d'accidents informatiques en milieu professionnel fait apparaître :

- 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 des procédures 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). Le recours à la sous-traitance ou au travail temporaire, qui ont pour effet d'introduire dans l'entreprise des salariés « externes », est un facteur de risque supplémentaire.

Protéger une entreprise, c'est donc d'abord procéder à un examen systématique des risques, puis calculer les conséquences potentielles (pertes financières, pertes de temps, pertes de compétences ou de connaissances, pertes d'archives, etc.) et ainsi déterminer l'ordre de priorité des protections qui doivent être installées. Ensuite, on examine les différentes façons de se protéger contre chacun des risques et on peut définir une politique de sécurité. La mise en œuvre de cette politique se concrétise par des investissements (achats d'équipements de sécurité, modification de la configuration des locaux, définition et rédaction des procédures, déploiement des équipement, maintenance, surveillance et validation régulière du dispositif).

On voit que, dans ces différentes étapes, les mesures d'ordre technologique (alimentations redondantes, firewall, sauvegardes etc.) viendront seulement après que l'audit de sécurité ait défini la politique.

Une façon simple d'identifier une entreprise défaillante en matière de sécurité est de constater que les équipements de sécurité ont été installés en l'absence d'un audit préalable. Il est alors extrêmement probable que des « trous » existent dans la ligne de défense de l'entreprise.