

Ecole Doctorale de Sciences de Gestion

ED 275

Thèse pour l'obtention du Doctorat en Sciences de Gestion

Conforme au nouveau régime défini par l'arrêté du 30 Mars 1992

**Veille anticipative stratégique
pour réduire le risque des agressions numériques**

Présentée par

Moufida SADOK

JURY :

Directeurs de recherche : Monsieur **Humbert LESCA**

Professeur à l'UPMF de Grenoble

Madame **Zeineb BEN AMMAR MAMLOUK**

Professeure à l'Université de Tunis

Suffragants:

Monsieur **Etienne KARMAZSIN**

Professeur à l'Université de Lyon

Madame **Sihem GUEMARA EL FATMI**

Maître de conférences à l'Université 7 Novembre

Monsieur **Jean-Fabrice LEBRATY**

Professeur à l'Université de Nice

Dédicace

Remerciements

Je remercie tout d'abord mes deux directeurs de recherche : Mme Zeineb BEN AMMAR MAMLOUK, pour ses précieuses remarques, ses conseils constructifs et pour la confiance dont elle a fait preuve à mon égard ; et M. Humbert LESCA pour l'orientation qu'il a su donner à mon travail, et qui n'a ménagé aucun effort pour me permettre de progresser dans ma recherche. Je leur exprime ma gratitude et mon grand respect.

Je tiens à remercier M. Etienne KARMAZSIN et Mme Sihem GUEMARA EL FATMI pour avoir consacré leur temps et leurs compétences à l'évaluation de ce travail, et pour avoir accepté d'en être rapporteurs.

Je remercie également M. Jean-Fabrice LEBRATY pour avoir accepté de faire partie du jury de soutenance.

Je tiens à exprimer ma profonde reconnaissance au Professeur Noureddine BOUDRIGA pour ses réflexions judicieuses qui m'ont été d'une extrême importance tout au long de cette recherche, et qui ont été généreux de son temps et de ses compétences pour orienter et recadrer mon travail.

Je me dois aussi de remercier tout particulièrement tous les experts qui ont participé dans l'étude empirique de cette recherche pour leur aide efficace et leurs commentaires précieux. Un grand merci aussi à Beyrem TRIKI qui a conçu et développé le logiciel supportant la méthode proposée dans cette recherche. Une pensée aussi à Nejoua BEN ROMDHANE, mon amie d'enfance, pour ses encouragements et son soutien moral dans les moments les plus difficiles.

Merci enfin, et surtout, à ma mère qui ne cesse de prier pour moi et pour son soutien inconditionnel, à ma sœur pour ses encouragements, à mon beau frère pour son extrême gentillesse. J'espère vous faire honneur à travers ce travail de recherche.

TABLE DES MATIERES

Liste des figures.....	8
Liste des tableaux.....	9
Introduction générale	10
1^{ière} Partie : Aspects théoriques de la problématique de recherche et état des connaissances face à notre question de recherche	20
Introduction de la première partie.....	21
Chapitre 1 : Enjeux stratégiques des agressions numériques pour l'entreprise	22
1.1 Aspects théoriques de la problématique de recherche	23
1.1.1 Définition de l'environnement	23
1.1.2 Concept d'incertitude de l'environnement	24
1.1.3 Relations entre l'incertitude et le risque	26
1.1.4 Veille anticipative stratégique : définitions et caractéristiques.....	26
1.1.5 Problématique de la phase d'exploitation des informations de la veille anticipative stratégique.....	29
1.2 Application des concepts théoriques de la problématique au contexte des agressions numériques	32
1.2.1 Les hackers : nouveaux acteurs de l'environnement externe de l'entreprise.....	32
1.2.2 La définition d'un système d'information	33
1.2.3 Les avantages de se mettre en réseau	34
1.2.4 Les risques de se mettre en réseau.....	36
1.2.5 Quelques chiffres significatifs décrivant l'ampleur du risque des agressions numériques.....	38
1.2.6 Les sources et la typologie des agressions numériques.....	40
1.2.7 Les pertes financières engendrées par les agressions numériques	42
1.2.8 L'incertitude liée aux agressions numériques.....	44
1.2.9 L'adaptation de la Veille anticipative stratégique dans le cas de réponse aux agressions numériques.....	45
1.3 Objectifs, intérêt et pertinence de la question de recherche	48
1.3.1 Délimitation du sujet de la recherche	48
1.3.2 Objectifs de la recherche.....	49
1.3.3 Pertinence du point de vue des praticiens.....	50
1.3.4 Pertinence par rapport aux publications académiques disponibles	52
Conclusion Chapitre 1.....	54
Chapitre 2 : État des connaissances actionnables disponibles dans les publications et dans les pratiques des entreprises par rapport à notre question de recherche	55
2.1 Apports et limites des techniques d'analyse du risque, dans les publications.....	56
2.1.1 Les techniques d'évaluation du risque.....	57
2.1.1.1 L'approche réductionniste.....	57
2.1.1.2 L'approche holistique	58
2.1.2 Apports et limites des techniques d'évaluation du risque	59
2.2 Apports et insuffisances des méthodes de traitement des informations de type signal et/ou signe faible.....	60
2.2.1 Définitions et caractéristiques des cartes causales	61
2.2.2 Limites des cartes causales par rapport à notre question de recherche	63
2.2.3 Traitement des informations de type signal et/ou signe faible au moyen d'un processus mettant en œuvre l'intelligence collective.....	64
2.2.4 Insuffisances constatées par rapport à notre question de recherche	65

2.3 État des pratiques dans les entreprises, à l'échelon international et d'après les rapports disponibles	67
2.3.1 Etude du risque encouru par une entreprise en cas d'agressions numériques	68
2.3.2 Définition d'une politique de sécurité face au risque numérique.....	70
2.3.3 Choix des solutions de sécurité, suite à la politique de sécurité retenue	73
2.3.4 La mise en place d'une ERI	76
2.4 État des lieux : rôle et activités d'une ERI	78
2.4.1 Aperçu historique de l'apparition des ERI.....	79
2.4.2 Activités et domaines d'intervention des ERI.....	80
2.4.3 Organisation et structure des ERI.....	81
2.4.4 Cas de l'ANACE de Tunis	83
Conclusion Chapitre 2.....	87
Chapitre 3 : Emprunts aux travaux antérieurs de l'équipe de recherche Veille Stratégique en relation avec la question de recherche.....	88
3.1 Présentation de la méthode L.E.SCAnning®.....	89
3.1.1 Modèle conceptuel de la méthode L.E.SCAnning®.....	89
3.1.1.1 Le ciblage	90
3.1.1.2 La traque des informations.....	91
3.1.1.3 La sélection des informations.....	92
3.1.1.4 La remontée des informations	93
3.1.1.5 La Mémorisation.....	94
3.1.1.6 La création collective de sens.....	94
3.1.1.7 La diffusion/Accès.....	95
3.1.1.8 L'action	97
3.1.1.9 L'animation	97
3.1.2 Les innovations de la méthode L.E.SCAnning® (en amont de la présente recherche)	98
3.2 Enrichissements escomptés de la méthode L.E.SCAnning® dans le cas considéré par la présente recherche.....	100
3.2.1 Enrichissements escomptés par rapport à la phase de création collective de sens	100
3.2.2 Enrichissements escomptés par rapport à la phase de mémorisation.....	102
3.2.3 Enrichissements escomptés par rapport à la fonction de médiation.....	103
3.2.4 Apport de l'Internet comme support à la méthode proposée.....	105
3.2.5 Exemple d'application : « <i>French Connection</i> »	107
3.3 Comparaison entre groupe de création collective de sens (méthode LESCAnning) et le travail de l'ERI dans le cas considéré	109
3.3.1 Création collective de sens dans les cas les plus fréquents d'application de la méthode L.E.SCAnning®	109
3.3.2 Description du travail de l'ERI dans la cas considéré.....	111
Conclusion Chapitre 3.....	116
Conclusion de la première partie	117
2^{IEME} PARTIE : Conception, construction, expérimentation de la MARRAN et évaluation des résultats.....	118
Introduction de la deuxième partie	119
Chapitre 4 : Conception de la méthode proposée pour assister les ERI.....	120
4.1 Modèle conceptuel de la méthode proposée pour assister le travail d'une ERI	121
4.1.1 Les trois phases du modèle conceptuel.....	121
4.1.2 La représentation du modèle conceptuel	122
4.1.3 La construction d'un chemin de raisonnement	124
4.1.4 Exemple illustratif	126

4.2 Utilisation du modèle conceptuel dans les travaux des ERI.....	127
4.2.1 Adaptation de la terminologie	128
4.2.2 Cas d'application.....	129
4.3 Raisonnements basés sur l'ensemble des liens présentés dans le modèle conceptuel .	131
4.3.1 Les opérations sur les noeuds et sur les liens.....	131
4.3.2 Le processus de médiation.....	133
4.3.3 La prise de décision, en aval du travail (<i>stricto sensu</i>) de l'ERI.....	135
4.4 La médiation dans les travaux de l'ERI	137
4.4.1 Rôle du médiateur	137
4.4.2 Rôle espéré de la technologie Internet dans le processus de création collective de sens ainsi que de médiation	138
4.4.3 Conception des heuristiques pour assister l'activité du médiateur	141
4.5 Construction d'indicateurs de mesure des progrès permis par l'application de la méthode proposée	142
4.5.1 Critères classiques utilisés en Systèmes d'Information.....	143
4.5.2 Les critères proposés pour l'évaluation de la méthode d'aide au travail d'une ERI	145
Conclusion Chapitre 4.....	147
Chapitre 5 : Expérimentation de la méthode sur des cas réels d'agressions numériques	148
.....
5.1 Mise en œuvre de la méthode sur des cas réels d'agressions numériques en vue d'expérimenter la méthode.....	149
5.1.1 Cas n°1 : Scanning du réseau de l'ANCE.....	149
5.1.2 Cas n°2 : "A Thousand Razors"	152
5.1.3 Cas n°3: "The Parking Lot"	154
5.1.4 Cas n°4: "Injection Indigestion".....	157
5.2 Spécification des conditions d'expérimentation de la méthode.....	160
5.2.1 Existence d'une politique de sécurité	161
5.2.2 Caractéristiques des informations utilisées.....	162
5.2.3 Possibilité de détection de signaux/signes faibles.....	162
5.2.4 Examen de cas d'agressions numériques non répétitives à l'identique.....	163
5.2.5 Face à face et possibilités d'interaction rapides à distance.....	164
5.2.6 Possibilités d'accéder rapidement à des informations appropriées et disponibles dans des bases de données internes et/ou externes à l'entreprise	165
5.2.7 Existence d'un animateur/médiateur	166
5.3 Conception et mise en œuvre d'un outil informatique pour assister la méthode d'aide à la création collective de sens	167
5.3.1 Objectifs et caractéristiques de l'outil informatique	167
5.3.2 Réalisation de l'outil.....	168
Conclusion Chapitre 5.....	171
Chapitre 6 : Évaluation de la méthode et analyse des résultats	172
6.1 Méthodologie de collecte de données	173
6.1.1 Conditions de la recherche et choix d'une méthode de collecte des données	173
6.1.2 Canevas des entretiens et description des informations à recueillir.....	175
6.1.3 Dispositif de recherche	177
6.1.4 Méthode d'analyse des données collectées lors des entretiens.....	178
6.2 Exploitation des données recueillies lors des entretiens auprès des experts	179
6.2.1 Analyse des résultats concernant l'utilité perçue de la méthode.....	179
6.2.1.1 Enseignements tirés concernant le traitement des signaux/signes faibles	179
6.2.1.2 Enseignements tirés concernant le rôle du médiateur.....	180

6.2.1.3 Enseignements tirés concernant la mémorisation des raisonnements	181
6.2.2 Analyse des Résultats concernant la facilité perçue d'utilisation de la méthode..	182
6.2.3 Analyse des résultats par rapport à l'état des pratiques des experts rencontrés....	182
6.2.3.1 Enseignements tirés concernant la structure de l'ERI	182
6.2.3.3 Enseignements tirés concernant le fonctionnement de l'ERI.....	183
6.2.3.4 Enseignements tirés concernant les outils de collecte des signaux faibles	184
6.2.4 Analyse des résultats concernant les indicateurs de mesure (dans la durée) que nous avons proposé pour l'évaluation de la méthode.....	184
6.3 Contributions théoriques et pratiques de la recherche	185
6.3.1 Apports théoriques de la recherche par rapport aux connaissances académiques	185
6.3.1.1 Risque en général versus risque des agressions numériques	185
6.3.1.2 Nouveau type d'acteurs de l'environnement de l'entreprise : les « hackers »	186
6.3.1.3 Transposition et adaptation de la phase de création collective de sens de la méthode L.E.SCanning®	186
6.3.1.4 Proposition de nouveaux indicateurs de mesure	187
6.3.2 Apports pratiques de la recherche	187
6.3.2.1 L'organisation du travail de l'ERI.....	187
6.3.2.2 La gestion des ressources humaines liée à l'ERI.....	188
6.3.2.3 La génération des connaissances à partir des constructions des scénarios d'attaques	190
6.3.2.4 La formation des médiateurs	191
6.3.2.5 Apports pratiques de l'usage de la technologie Internet.....	191
Conclusion Chapitre 6.....	193
Conclusion de la deuxième partie.....	194
Conclusion Générale.....	195
BIBLIOGRAPHIE.....	199
GLOSSAIRE.....	212
ANNEXE.....	217

LISTE DES FIGURES

Figure 1 : Démarche générale de la recherche	16
Figure 2: Le processus d'évaluation du risque d'après White (1995)	56
Figure 3: Les sept étapes de la réponse à une agression, d'après Bort et Cummings (2003) ..	81
Figure 4: Composition de l'ERI à l'ANCE de Tunis.....	86
Figure 5: Modèle référentiel de la méthode L.E.SCAnning®.....	89
Figure 6: Les innovations de la méthode L.E.SCAnning®.....	99
Figure 7: Représentation graphique des relations entre C1, C2 et C3	124
Figure 8: Chemin de raisonnement de longueur 3.....	127
Figure 9: Représentation du raisonnement de l'ERI dans le cas considéré	130
Figure 10: Opération de remplacement d'un noeud	132
Figure 11: Opération de réécriture d'un réseau de noeuds	133
Figure 12: Le modèle de DeLone et McLean (1992)	144
Figure 13: Représentation graphique du scénario de l'attaque à l'ANCE	151
Figure 14: Représentation graphique de l'agression "A Thousand Razors".....	154
Figure 15: Représentation graphique de l'agression "The Parking Lot".....	157
Figure 16: Représentation graphique de l'agression "Injection Indigestion".....	160
Figure 17: Description du logiciel	170

LISTE DES TABLEAUX

Tableau 1 : Plan de la recherche	19
Tableau 2 : Évolution du nombre de vulnérabilités reportées auprès du CERT	39
Tableau 3 : Évolution du nombre d'incidents reportés auprès du CERT	39
Tableau 4 : Les points d'attaques identifiés entre 2000-2003	41
Tableau 5 : Typologie des agressions les plus fréquemment rencontrées entre 2000-2004	42
Tableau 6 : Pertes financières occasionnées par les agressions numériques entre 2000-2003	43
Tableau 7 : Principaux moyens de sécurité employés entre 2000-2004	74

Domaine et question de recherche

Aujourd'hui, l'utilisation des TIC, et notamment l'Internet, est généralisée dans les entreprises pour gérer plusieurs activités à distance avec leurs différents partenaires et même avec leurs employés. Les entreprises se mettent en réseau pour accéder rapidement à des informations, améliorer la communication en réduisant les coûts, fournir de meilleurs services aux clients ou pour développer le commerce électronique.

Cependant, l'ouverture et l'extension du réseau de l'entreprise expose celle-ci à un nouveau type de risque lié à la sécurité de ses ressources informationnelles : le **risque des agressions numériques**.

Dans cette recherche, notre intérêt porte sur les nouveaux acteurs de l'environnement de l'entreprise utilisatrice des TIC, les **hackers** qui, à travers leurs actions, peuvent compromettre la sécurité informationnelle d'une entreprise. Ces actions sont de plus en plus complexes, dangereuses et renforcent l'**incertitude** de l'entreprise. Dans notre cas, l'incertitude est liée au fait que la visibilité des agressions numériques n'est clairement possible que lorsqu'elles sont terminées, mais aussi au fait qu'une entreprise peut être victime d'une agression sans en avoir conscience. La complexité s'accroît dans la mesure où les hackers sont de plus en plus inventifs. Les enjeux stratégiques des agressions numériques pour une entreprise ne se limitent pas à des pertes financières. Ils peuvent concerner également son image de marque ou son capital clients, ainsi que l'efficacité et la continuité de son activité.

Face à ce nouveau changement au sein de l'environnement, l'entreprise devrait développer une capacité d'anticipation afin de réduire le risque des agressions numériques et réduire le temps de réponse face à celles-ci. La veille anticipative stratégique semble pouvoir permettre à l'entreprise de réduire l'incertitude et le risque se traduisant par un manque, une abondance ou l'ambiguïté des informations pertinentes à la prise de décision. Ce dispositif est susceptible

également de réduire le temps de réponse face aux changements de l'environnement voire même de les anticiper.

Cependant, la veille anticipative stratégique est appréhendée comme étant un système d'interprétation (Daft et Weick, 1984) et un processus de construction de sens (Weick, 1995) à partir d'informations. Dans notre cas il s'agit d'informations susceptibles d'annoncer des ruptures ou des discontinuités dans l'environnement. Les informations de la veille stratégique peuvent être des signaux faibles (Ansoff, 1975) : elles ont alors pour caractéristiques d'être incertaines, qualitatives, ambiguës, fragmentaires (Gorry et Scott-Morton, 1971 ; Argyris, 1976 ; Lesca, 1986), fugaces (Marmuse, 1992), rapidement obsolètes (Bourgeois et Eisenhardt, 1988), incomplètes, imprécises et de fiabilité fragile (Lesca, 2003). Le traitement de ces informations est de type « interprétation et induction », et requiert la création d'une **intelligence collective** nécessitant la mobilisation d'expériences et d'expertises diverses au sein de l'entreprise, voire extérieures à celle-ci (Lesca, 2003).

Notre application, dans le domaine de réponse aux agressions numériques, concerne une **solution particulière** pour la réduction du risque des agressions numériques à travers le travail des **équipes de réponse aux incidents (ERI)** de sécurité. La réponse aux agressions numériques est une activité où le processus d'interprétation collective des informations de type signal et/ou signe faible est fondamental pour agir vite ou par anticipation.

Ainsi, **la question de recherche** s'énonce comme suit :

Est-il possible d'aider les ERI à **réduire** le risque des agressions numériques sur les réseaux d'entreprises en les **anticipant**, et partant réduire le délai de réaction ?

Intérêt et pertinence de la recherche

D'un point de vue managérial, la question de recherche soulève un problème crucial, dont l'ampleur ne cesse de croître, et vise donc à répondre à une **demande de terrain**. L'insuffisance des solutions techniques et physiques de sécurité face à la complexité et l'imprévisibilité croissantes des agressions numériques, de même que l'absence de réelle

formation de spécialistes dans ce domaine, obligent les entreprises à valoriser le rôle des ERI dans une perspective de réduction du temps de réponse aux agressions numériques voire même l'anticipation de leurs occurrences.

Cependant, les ERI **manquent de méthodes** adéquates pour :

- assister l'activité de réponse aux agressions numériques et particulièrement l'étape d'interprétation collective des informations collectées de type signal et/ou signe faible,
- capitaliser les expériences et les connaissances qui pourraient émerger de ce processus d'interprétation.

Le retour sur investissements, évalué en termes de valorisation des compétences acquises et du savoir faire des membres de l'ERI, pourrait justifier des investissements engagés pour la **recherche de méthodes** appropriées afin de soutenir leur travail, et pour la mise en place de **formation**.

D'un point de vue académique, peu de travaux dans la littérature ont proposé des **connaissances actionnables** et des méthodes pour assister l'activité d'interprétation des informations d'anticipation de type signal et/ou signe faible afin de réduire le risque des agressions numériques. La méthode que nous proposons dans cette recherche intègre divers éléments susceptibles de participer à la réflexion sur la conception d'outils, de méthodes, d'heuristiques et de formation pour soutenir l'intelligence collective dans le domaine de réponse aux agressions numériques.

Le modèle conceptuel de la méthode proposée permet de dégager des enrichissements théoriques qui font l'objet d'une **étude exploratoire** au sein d'une entreprise et dont les résultats permettront de produire des connaissances nouvelles sur le processus de création collective de sens.

Dans ce cadre, la méthode proposée dans ce travail constitue une transposition et une adaptation de la méthode L.E.*SCanning*® dans un domaine nouveau à savoir la sécurité informationnelle à l'égard des agressions numériques. De ce fait, la présente recherche représente un prolongement de travaux de recherche de l'équipe du Professeur LESCA

(CERAG, CNRS UMR 5820 UPMF) dans le domaine de la Veille Anticipative Stratégique (www.veille-strategique.org).

Plusieurs membres de l'équipe ont travaillé à produire des connaissances actionnables et des méthodes pour le traitement/interprétation de signaux/signes faibles captés sur l'environnement de l'entreprise (Valette, 1993 ; Caron-Fasan, 1997 ; Rouibah, 1998 ; Lesca N., 2002). Leurs résultats nous sont très utiles et nous servent de point de départ et d'appui pour nos propres recherches. Mais ces chercheurs ne se sont pas intéressés à cette autre variété de signaux et/ou signes qui sont ceux liés aux agressions numériques. Nous prenons donc la suite des recherches pour aborder ce **domaine nouveau**. Nous proposons en outre une méthode faisant appel à des outils mathématiques et informatiques que ces travaux de recherche n'avaient que peu utilisés jusqu'ici.

Ainsi, **les objectifs de la recherche** peuvent être articulés autour des quatre points suivants :

1. Construction de **connaissances actionnables**, au sens de Argyris (ou encore procédurales, au sens de Simon), qui prendront la forme notamment d'une **Méthode d'Analyse et de Réduction du Risque des Agressions Numériques (MARRAN)**, assistée par une utilisation innovante de la technologie Internet.
2. Test de **validation** du fonctionnement de la méthode sur des cas réels d'agression numérique.
3. **Evaluation**, en termes managériaux, de la méthode proposée. Ceci nous conduira à proposer des « indicateurs d'évaluation » qui permettront de préciser dans quelle mesure la réponse à la question de recherche est satisfaisante, c'est-à-dire si la méthode proposée permet effectivement d'aider une ERI à analyser et à réduire le risque des agressions numériques.
4. **Spécification des conditions** sous lesquelles la méthode serait applicable sur d'autres cas similaires et dans d'autres entreprises.

Cadre méthodologique de la recherche

Etant donnés les objectifs de notre travail, notre démarche pour répondre à la question de recherche s'inscrit dans le cadre d'une **recherche ingénierique**. Dans ce type de recherche, le

chercheur possède un statut de « *chercheur ingénieur qui conçoit l'outil support de sa recherche, le construit, et agit à la fois comme animateur et évaluateur de sa mise en œuvre dans les organisations, contribuant ce faisant à l'émergence de représentations et de connaissances scientifiques nouvelles* » (Chanal et al., 1997).

En effet, la recherche ingénierique s'intéresse à l'étude de **problèmes d'origine terrain** mal structurés, perçus comme complexes et sans réponse connue. Pour répondre à ces problèmes, les connaissances théoriques disponibles sont souvent peu adaptées, éparpillées et/ou ne sont pas actionnables.

Ainsi, le chercheur opère, d'abord, une modélisation à travers une articulation et une extension de certaines connaissances disponibles. Ensuite, il conçoit un outil (artefact au sens de Koenig) qui sera validé sur le terrain permettant ainsi la construction de nouvelles connaissances actionnables allant jusqu'à la phase de maturité d'un prototype. Les retours d'expérience sont alors de précieuses « données » pour le chercheur.

Dans notre cas, l'activité de réponse aux agressions numériques à travers le travail d'une ERI est complexe, faisant intervenir en grande part des **connaissances tacites**, et révèle beaucoup de difficultés surtout lors du processus d'interprétation des signaux et/ou signes faibles détectés. De même, peu de connaissances actionnables et de résultats liés à notre question de recherche sont disponibles dans les publications.

De ce fait, notre recherche est de nature **exploratoire** visant d'abord à concevoir et à réaliser une méthode d'aide à la réduction du risque des agressions numériques, supportée par certaines potentialités techniques de l'Internet. Nous procédons ensuite à une expérimentation de la MARRAN sur des cas réels d'agression numérique.

Dans l'étude empirique, pour collecter les observations « ou données » relatives à l'évaluation de l'**utilité perçue** et la **facilité perçue** d'utilisation de la MARRAN, nous avons choisi les entretiens semi directifs auprès des experts en sécurité informatique. Nous avons cherché également à partir des entretiens à savoir dans quelle mesure notre méthode représente une amélioration par rapport à l'état des pratiques dans le domaine de réponse aux agressions numériques.

Indiquons aussi que nous avons choisi de faire une **étude longitudinale** dans notre étude empirique. Ce choix découle directement de la nature de notre recherche, qui est en elle-même un **processus** constitué de plusieurs étapes qui s'enchaînent dans le temps. Ces étapes comprennent des phases suivantes :

- imprégnation, par le chercheur, des pratiques dans une entreprise de référence servant de terrain dans le but de s'approprier des pratiques, de s'en inspirer pour construire la future méthode,
- appropriation des exemples d'agression numérique par le chercheur,
- formalisation des exemples,
- validation des exemples par le chercheur (effet de miroir)
- validation des démarches formalisées par le chercheur
- construction d'un artefact
- élaboration d'un canevas d'entretiens
- entretiens individuels et collectifs (enquête participative)

La figure 1 expose les différentes étapes de la démarche générale de la présente recherche.

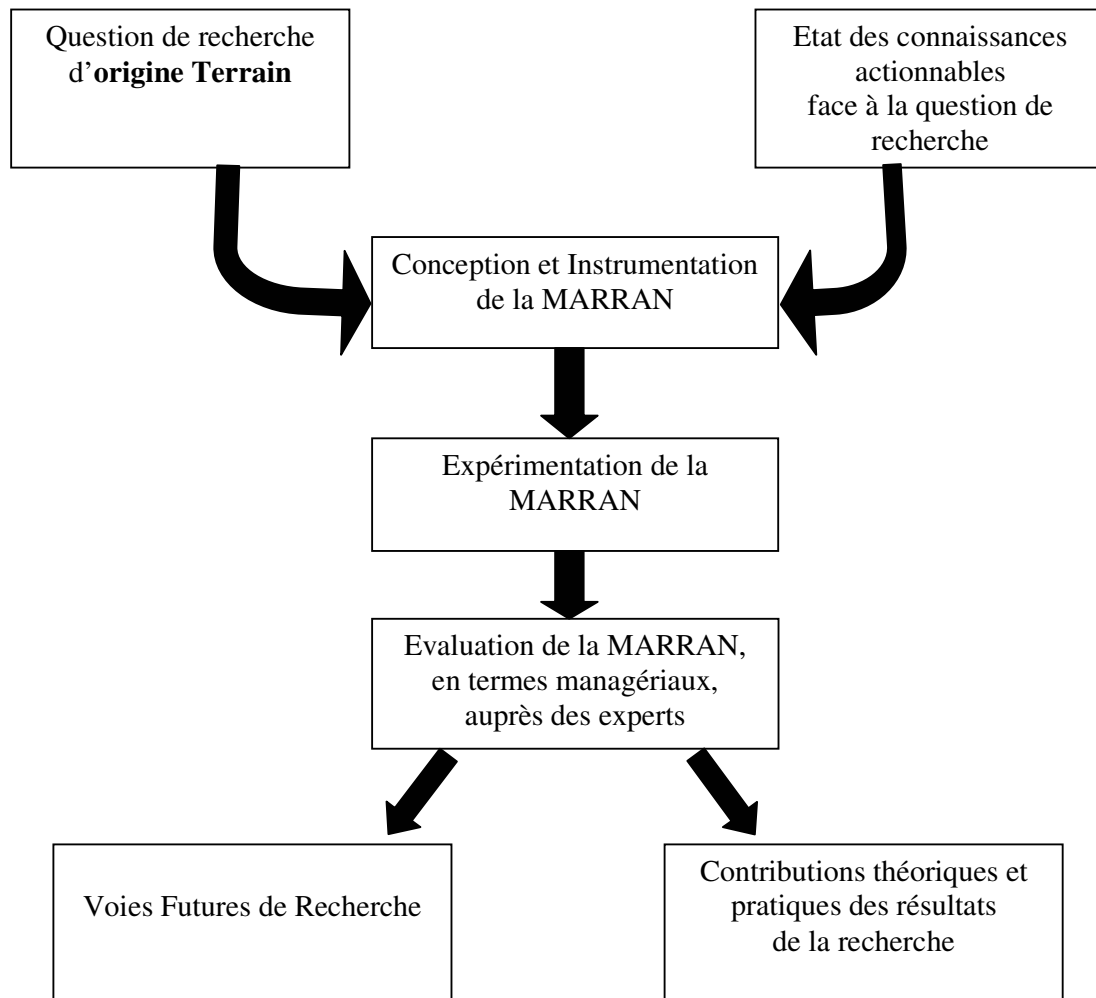


Figure 1 : Démarche générale de la recherche

Présentation du plan

Le présent travail est organisé en deux parties. La première partie comprend trois chapitres consacrés à la délimitation du sujet de la recherche, à la présentation de ses aspects théoriques et pratiques, et l'établissement de l'état des connaissances disponibles dans les publications.

Dans le premier chapitre, nous procédons à une adaptation des concepts clés de la veille anticipative stratégique au domaine de réponse aux agressions numériques. Nous choisissons par la suite de focaliser notre travail de recherche sur une solution particulière pour réduire le risque des agressions numériques à travers le travail d'une ERI. Nous terminons par expliciter

davantage l'intérêt et la pertinence de notre question de recherche d'un point de vue managérial et académique.

Dans le deuxième chapitre, nous rassemblons un ensemble de connaissances disponibles en nous y prenant de deux façons :

- Dans les publications en relation avec notre question de recherche dans le but de pouvoir les utiliser dans la conception et la construction de notre méthode.
- Dans les entreprises. Nous avons cherché à avoir une idée sur l'état des pratiques dans les entreprises en matière de réduction du risque des agressions numériques et ce, en nous référant à des documents de travail et des rapports publiés par des organismes internationaux spécialisés ainsi que dans l'entreprise tunisienne l'Agence Nationale de Certification Electronique (ANCE). Cette dernière a servi de terrain pour réaliser notre étude empirique.

Dans le troisième chapitre, notre intérêt a porté sur la méthode *L.E.SCAnning*® et spécifiquement sur trois phases de cette méthode qui apportent des éléments de réponse à notre question de recherche. Nous avons, par la suite, mis l'accent sur les enrichissements escomptés de la méthode *L.E.SCAnning*® concernant ces trois phases. Sur le plan de l'instrumentation de notre méthode proposée, nous avons montré l'intérêt de l'utilisation de l'Internet comme support.

La deuxième partie comprend également trois chapitres consacrés à la présentation du cadre conceptuel de la MARRAN, à son expérimentation et à l'analyse des résultats obtenus lors de son évaluation auprès des experts en sécurité informatique.

En réponse à la question de recherche, nous développons dans le quatrième chapitre le modèle conceptuel de la MARRAN qui représente une articulation et une extension des différentes connaissances actionnables pertinentes par rapport au domaine de la réponse aux agressions numériques. A travers le modèle conceptuel de la MARRAN, nous montrons la nécessité de l'activité de **médiation** (facteur humain qui se révélera essentiel) dans le processus de création collective de sens à travers le travail d'une ERI ainsi que le rôle des TIC pour soutenir une telle activité. Nous terminons le chapitre par la proposition des **critères de**

mesure en amont et en aval de l'expérimentation de la méthode proposée permettant son évaluation.

Le cinquième chapitre est consacré d'abord à l'**expérimentation** de la MARRAN sur des cas réels d'agression numérique en vue de tester son fonctionnement. Ensuite, nous spécifions les **conditions d'expérimentation** en vue de la réplication de la méthode pour d'autres cas et dans d'autres entreprises. Enfin, nous proposons **un logiciel** qui a été conçu et développé pour supporter la MARRAN.

Nous consacrons le sixième chapitre à l'évaluation de la MARRAN en précisant et justifiant la méthode de collecte des données choisie, les observations à collecter et la méthode d'analyse utilisée. Nous visons à travers l'exploitation des informations recueillies lors des entretiens auprès des experts en sécurité, à apprécier principalement l'utilité perçue et la facilité perçue d'utilisation de la MARRAN. Nous récapitulons dans la dernière section de ce chapitre les contributions théoriques et pratiques de notre recherche.

INTRODUCTION GENERALE	
1^{IERE} PARTIE	Aspects théoriques de la problématique de recherche et état des connaissances face à notre question de recherche
CHAPITRE 1	Enjeux stratégiques des agressions numériques pour l'entreprise
CHAPITRE 2	Etat des connaissances actionnables disponibles, par rapport à notre question de recherche
CHAPITRE 3	Emprunts aux travaux antérieurs de l'équipe de recherche Veille Stratégique, en relation avec la question de recherche
2^{IEME} PARTIE	Conception, expérimentation de la MARRAN et évaluation des résultats
CHAPITRE 4	Conception de la méthode proposée pour assister les ERI
CHAPITRE 5	Expérimentation de la MARRAN sur des cas réels d'agression numérique
CHAPITRE 6	Évaluation de la MARRAN et analyse des Résultats
CONCLUSION GENERALE	

Tableau 1 : Plan de la recherche

1^{ière} Partie :

Enjeux stratégiques des agressions numériques pour l'entreprise et état des connaissances face à notre question de recherche

Introduction de la première partie

La première partie a un double objectif. Il s'agit premièrement de présenter les aspects théoriques liés à la problématique posée dans cette recherche ainsi que les limites de notre sujet de recherche à travers l'étude d'une solution particulière de sécurité dans le domaine de réponse aux agressions numériques. Deuxièmement, nous étudions l'état des connaissances face à notre question de recherche afin de cerner les éléments de réponse qui lui sont liés.

Ainsi, dans le premier chapitre nous définissons les concepts théoriques clés de la veille anticipative stratégique et nous proposons leur adaptation dans le domaine de réponse aux agressions numériques. Par rapport au dispositif de la veille anticipative stratégique, nous délimitons notre étude au niveau du processus de création collective de sens qui trouve une application pertinente à travers le travail d'une ERI. La question de recherche est énoncée par la suite en mentionnant sa pertinence d'un point de vue managérial et théorique.

Le deuxième chapitre est consacré à l'étude des divers domaines susceptibles de fournir des connaissances actionnables en relation avec notre question de recherche. Dans ce cadre, l'étude a concerné les techniques d'évaluation du risque en général, les cartes causales ainsi que le processus d'intelligence collective. L'étude a également concerné l'état des pratiques dans les entreprises, notamment au sein d'une entreprise tunisienne, pour réduire le risque des agressions numériques.

Le troisième chapitre traite plus spécifiquement des apports de la méthode *L.E.SCA*ning® par rapport à la question de recherche ainsi que des enrichissements escomptés théoriques et pratiques de cette méthode.

Enjeux stratégiques des agressions numériques pour l'entreprise

Ce premier chapitre pose la problématique générale de ce travail, ses enjeux, ainsi que ses aspects théoriques et empiriques. Il sera consacré à décrire le contexte stratégique des agressions numériques afin de mettre en évidence la nature du risque encouru par l'entreprise en absence d'une réaction rapide et au bon moment. Ce contexte se caractérise principalement par l'incertitude, et par conséquent par la difficulté de détecter et d'anticiper les agressions numériques. Avec l'utilisation et l'intégration de plus en plus importante des technologies de l'information et de la communication et notamment l'Internet dans les systèmes de gestion et de production, l'entreprise est amenée à gérer et à réduire le risque des agressions numériques à travers une approche proactive dans la mesure où les informations constituent l'une des ressources les plus importantes à protéger dans une entreprise.

Ainsi, la première section de ce chapitre est consacrée à la présentation des aspects théoriques de la problématique générale de ce travail de recherche. Ces aspects concernent essentiellement la définition de l'environnement externe de l'entreprise, l'incertitude perçue de l'environnement, le risque perçu et la veille anticipative stratégique. La deuxième section démontre la validité de ces aspects théoriques dans le domaine des agressions numériques. Nous mettons l'accent dans cette section sur les hackers comme étant des nouveaux acteurs de l'environnement agissant sur la continuité et la croissance de l'activité d'une entreprise. Les actions des hackers sont incertaines et difficilement imprévisibles, et présentent un risque énorme pour les ressources informationnelles de l'entreprise. La mise en place d'un dispositif de veille anticipative stratégique susceptible de permettre à l'entreprise de réduire le risque des agressions numériques s'avère nécessaire. La troisième section présente les objectifs, l'intérêt et la pertinence de notre recherche en délimitant le sujet au niveau de l'étude d'une solution particulière pour réduire de risque des agressions numériques à travers le travail des **équipes de réponse aux incidents** de sécurité (ERI).

1.1 Aspects théoriques de la problématique de recherche

L'objectif de cette première section est de définir l'environnement externe de l'entreprise, l'incertitude perçue de l'environnement ainsi que de caractériser la relation entre l'incertitude et le risque. Cette relation nous amène à présenter le processus de la veille anticipative stratégique permettant à l'entreprise de réduire l'incertitude et de se préparer le plutôt possible aux changements susceptibles de se produire dans son environnement extérieur.

1.1.1 Définition de l'environnement

Nous adoptons, dans notre recherche, la définition de l'environnement externe de l'entreprise comme étant constitué par un ensemble d'acteurs agissant d'une façon directe ou indirecte (Martinet, 1984) sur la survie et la croissance de l'entreprise, et intervenant dans l'élaboration de sa stratégie (Koenig, 1996). Ces acteurs peuvent être actuels ou potentiels (Lesca, 1986).

Les principaux acteurs classiques sont les concurrents, les clients, les fournisseurs, les groupes de pression et les pouvoirs publics, auxquels viennent s'en ajouter de nouveaux. Les actions et les manœuvres de ces acteurs impliquent des changements fréquents et imprévisibles de l'environnement externe de l'entreprise (Huber et Daft, 1987 ; Weick, 1995).

De plus, ces acteurs peuvent appartenir à l'environnement spécifique dont l'influence est plutôt directe sur l'organisation ou à l'environnement général pouvant l'affecter indirectement (Daft *et al.*, 1988).

Plusieurs théories de l'organisation se sont intéressées à situer l'impact des changements de l'environnement externe sur la structure (Burns et Stalker, 1961 ; Minzberg, 1982), la stratégie (Miller, 1988), le processus décisionnel (Simon, 1991) et la performance de l'organisation (Miles, *et al.*, 1974). Cet intérêt est surtout justifié par la relation d'interaction réciproque entre l'organisation comme étant un système ouvert et son environnement externe.

Ainsi, l'environnement est considéré comme étant hétérogène, complexe, dynamique (Duncan, 1972), turbulent (Emery et Trist, 1965 ; Tung, 1979), volatile (Bourgeois, 1985), discontinu et surprenant (Ansoff, 1975) et incertain (Kefalas, 1980 ; Marmuse, 1992 ; Elenkov, 1997).

Dans ce cadre, des modèles théoriques ont été proposés pour caractériser la variation de l'environnement externe selon trois dimensions indépendantes à savoir la fréquence, l'amplitude et la prévisibilité (Wholey et Brittain, 1989) ou de l'appréhender selon deux approches de mesure objective et subjective (Boyd, *et al.*, 1993).

1.1.2 Concept d'incertitude de l'environnement

Les changements de l'environnement sont considérés comme étant une source majeure d'incertitude surtout avec l'évolution de plus en plus rapide et imprévisible des actions des acteurs pertinents ce qui est de nature à retarder une réponse appropriée et à temps de l'entreprise. Ce qu'il faut noter c'est que le changement n'implique pas forcément un état d'incertitude car l'environnement peut varier d'une façon prévisible. Nous nous intéressons aux changements de type **discontinuités et ruptures**, au sens de Ansoff, qui sont très difficiles à prévoir ou à anticiper.

L'incertitude est une notion centrale et fondamentale dans les développements théoriques décrivant particulièrement les relations d'interface de l'organisation avec son environnement (Burns et Stalker, 1961 ; Thompson, 1967 ; Lawrence et Lorsch, 1967).

Cependant, plusieurs problèmes et difficultés liés à la conceptualisation et à la mesure de l'incertitude ont entraîné des propositions et des modèles théoriques parfois contradictoires (Jauch et Kraft, 1986).

Dans une revue bibliographique de la théorie organisationnelle consacrée à l'incertitude, Buchko (1994) a montré que, malgré l'importance du concept, peu d'études et de recherches ont proposé des échelles de mesure. Ceci est expliqué en grande partie par le fait que les études et les recherches sur la question ont essayé d'étudier et de mesurer la perception de l'incertitude plutôt que d'identifier une mesure objective.

Ainsi, la **perception** de l'incertitude peut varier avec le temps et peut être facilement influencée par le changement et l'évolution des variables de l'environnement ce qui est de nature à diminuer la validité de l'échelle de mesure dans le temps (Buchko, 1994). De même, les différences et les caractéristiques individuelles, comme les biais et les processus cognitifs, introduisent des variations dans les mesures de l'incertitude. Au niveau de l'organisation, la carrière et la période passée dans le poste sont également deux critères qui influencent le processus perceptuel d'un manager (Hambrick et Mason, 1984 ; Milliken, 1990). La

perception de l'incertitude politique et macroéconomique peut être différente également et d'une façon significative d'un pays à un autre (Miller, 1993 ; May et al., 2000 ; Ebrahimi, 2000 ; Sawyerr et al., 2000). Dans ce cadre, la **culture nationale** influence la perception des crises et des menaces (Elenkov, 1997) et donc le comportement et la réponse stratégiques des organisations.

Par ailleurs, la perception de l'incertitude de l'environnement est reliée à plusieurs actions de management comme l'activité de scanning (Milliken, 1987 ; Daft *et al.*, 1988 ; Boyd et Fulk, 1996), la réponse stratégique des managers (Miles, Snow et Pfeffer, 1974), la formulation de la stratégie (Priem, *et al.*, 1995), la prise de décision (Child, 1972 ; Daft et Weik, 1984), l'alignement organisationnel (Kohberg, 1987) et les tactiques politiques et de gestion (Galaskiewicz et Bielefeld, 1998).

Trois sources d'incertitude sont identifiées dans la littérature et qui semblent représenter des points communs entre les différentes définitions formulées :

- le manque d'informations pertinentes à la prise de décision (Duncan, 1972 ; Milliken, 1987 ; Huber et Daft, 1987) d'où la nécessité de rechercher de nouvelles informations complémentaires,
- la surcharge d'informations et la difficulté de sélectionner des informations (Gifford, Bobbitt & Slocum, 1979) d'où la nécessité de bien cibler les informations,
- l'ambiguïté des informations disponibles (Weber, 1984) d'où la nécessité d'interpréter d'une façon inductive les informations.

Pour Daft *et al.* (1988) la perception de l'incertitude varie en fonction de la qualité et de la valeur de l'information détenue par une organisation concernant son environnement, ainsi que de la nature du support de l'information. De ce fait, la recherche d'informations s'avère de faible importance dans le cas d'un environnement complexe car il contient des signaux et des stimuli peu familiers aux preneurs de décision qui recourent plutôt à leur expérience passée ou à leur intuition pour situer les effets et les implications de la complexité de l'environnement sur leur organisation (Daft et Macintosh, 1981).

La perception de l'incertitude est liée d'une façon significative à la perception du risque. Dans ce qui suit, nous explicitons cette relation en mentionnant certains travaux de recherche dans ce domaine.

1.1.3 Relations entre l'incertitude et le risque

La littérature démontre une forte relation entre l'incertitude et le risque. Ce qu'il faut préciser c'est que les auteurs parlent plutôt de risque perçu et d'incertitude perçue. Dans ce cadre, l'existence d'incertitude conduit inéluctablement à la perception d'un risque faute de disposition de l'information nécessaire pour choisir (Jacoby *et al.*, 1994).

La perception du risque est susceptible d'engendrer des coûts. Cependant, les coûts liés à la perception du risque sont intangibles (Grewal *et al.*, 1994), incertains et potentiellement financiers (Wood et Sheer, 1996).

Dans la littérature marketing, les deux construits sont même traités d'une manière équivalente (Volle, 1995 ; Perrouy et d'Hauteville, 2000). La relation entre les deux concepts est très utilisée comme étant un élément d'une importante capitale dans le mécanisme de recherche d'information (Dowling et Staelin, 1994). Ce mécanisme constitue une étape cruciale dans le processus de prise de décision d'achat du consommateur.

En management stratégique, la perception du risque est évaluée en termes d'estimations probabilistes du degré d'incertitude situationnelle, du degré de contrôlabilité de l'incertitude et de la confiance en ces estimations (Sitkin et Weingart, 1995). De plus, le risque managérial est associé à l'incertitude des résultats (Palmer et Wiseman, 1999).

Par ailleurs, la théorie des coûts de transaction (Williamson, 1991) présente un cadre conceptuel pour tenter de réduire le risque lié à l'incertitude des transactions et au comportement opportuniste des personnes impliquées dans le contrat.

1.1.4 Veille anticipative stratégique : définitions et caractéristiques

La perception de l'incertitude de l'environnement est reliée à plusieurs actions de management comme l'activité de scanning (Milliken, 1987 ; Daft *et al.*, 1988 ; Boyd et Fulk, 1996; Elenkov, 1997). La montée de l'incertitude constitue un antécédent clé pour la pratique de la veille anticipative stratégique qui vise en premier lieu à réduire l'incertitude et améliorer la réactivité et le temps de réponse de l'organisation face à son environnement changeant et évolutif. En effet, la veille stratégique s'intéresse à l'environnement externe de l'organisation

pour analyser et anticiper son évolution de façon à donner le maximum de marge de manœuvre aux managers, afin de réduire le temps de réponse et assurer ainsi l'adaptation de l'organisation à son environnement.

De nombreux travaux théoriques et empiriques dans le domaine du management stratégique ont montré l'importance de l'existence d'un dispositif d'observation et de surveillance de l'environnement (Lawrence et Lorsch, 1973; Thiétart, 1984; Lesca, 1986 ; Marmuse, 1992 ; Koenig, 1996). L'acquisition de l'information concernant l'environnement est une activité importante pour l'entreprise (Aguilar, 1967) permettant aux décideurs d'identifier les menaces et les opportunités stratégiques relatives à son évolution (El Sawy et Pauchant, 1988).

En effet, l'information peut aider à réduire l'incertitude (Ginzberg, 1980), le risque dans la prise de décision (Gilad, 1996) et constituer un important input dans le processus de formulation de la stratégie (Lozada et Calantone, 1996).

Les entreprises utilisent plusieurs moyens pour s'informer au sujet de l'environnement et plusieurs sources d'information, qui peuvent être personnelles, impersonnelles, internes ou externes (Aguilar, 1967 ; Culnan, 1983). Plusieurs recherches ont démontré que les sources personnelles ont un contenu plus riche, permettent plus de détecter des signaux faibles (Ansoff, 1975 ; Daft et Lengel, 1984) ainsi qu'une meilleure compréhension et interprétation des problèmes dans une situation d'incertitude stratégique perçue élevée (Daft et Weick, 1984 ; Daft *et al.*, 1988). Par contre, les sources impersonnelles sont beaucoup plus appropriées lorsque les événements de l'environnement sont analysables et discrets. Cependant, la fréquence d'utilisation d'une source externe est conditionnée également par la qualité de l'information et l'accessibilité de la source (O'Reilly, 1982 ; Culnan, 1983).

Ainsi, il est important dans le cadre de la surveillance de l'environnement d'explicitier les secteurs de l'environnement spécifique ou général à surveiller en relation directe ou indirecte avec l'activité de l'entreprise (Yasai-Ardekani et Nystrom, 1996), dégager les principales tendances, changements et événements caractérisant l'environnement (Stoffels, 1982 ; Narchal *et al.*, 1987; Milliken, 1990) et qui peuvent représenter pour l'entreprise autant de menaces que d'opportunités affectant son activité et sa performance à moyen ou à long terme.

La surveillance de l'environnement et le recueil continu d'information devraient permettre à l'entreprise de développer une capacité appréciable d'anticipation des phénomènes et des ruptures de son environnement (Baumard, 1991).

La veille stratégique signale bien ce fait en permettant à l'entreprise de réduire son incertitude, notamment en aidant à anticiper les ruptures pouvant se produire dans l'évolution de son environnement socio-économique et technologique (Lesca, 1994). En effet, la formulation efficace de la stratégie d'une entreprise suppose une vision prospective de son environnement extérieur afin de lui permettre d'anticiper (Thiéart, 1991).

L'écoute anticipative de l'environnement traduit une attitude proactive de l'entreprise lui permettant d'acquérir l'information (Subramanian *et al.*, 1993) lui permettant d'avoir un avantage informationnel important et nécessaire pour améliorer la capacité d'adaptation de l'organisation aux changements de son environnement (Hambrick, 1981). En effet, la survie et la pérennité de l'entreprise dépendent de plus en plus de sa capacité d'adaptation à son environnement changeant et incertain (Miles et Snow, 1978 ; Lesca 1989 ; Doty *et al.*, 1993).

Dans ce cadre, Lesca (2003) définit la veille anticipative stratégique comme étant «le processus volontariste par lequel un individu ou bien une entreprise traque de façon active et utilise des informations à caractère anticipatif concernant les changements et les ruptures de son environnement socio-économique dans le but de réduire l'incertitude, de se créer des opportunités d'affaires, et d'agir au bon moment et vite »

La veille anticipative stratégique est une expression générique qui inclut plusieurs types de veilles spécifiques, telle la veille technologique, la veille concurrentielle, ou la veille commerciale. La veille commerciale, par exemple, a pour but de mieux connaître les clients actuels, leurs besoins exprimés et non satisfaits ainsi que leurs attentes latentes. La veille commerciale vise aussi l'identification des clients potentiels.

En se référant au modèle I.D.C (*Intelligence - Design - Choice*) du processus de décision de Simon, la veille anticipative stratégique correspond à la première étape de ce processus à savoir, l'identification dans l'environnement des facteurs clés en étroite relation avec la survie et la pérennité de l'entreprise. Ainsi, la veille stratégique doit contribuer à la phase d'intelligence du processus de décision stratégique (Thiéart, 1984; Marmuse, 1992).

Par ailleurs, le terme stratégique désigne ici le fait que la décision à prendre est de nature non répétitive, non programmable, dont l'enjeu peut être important pour l'entreprise et prise dans un contexte d'incertitude.

En réalité, la pratique de la veille stratégique s'avère comme étant un exercice difficile, complexe et soulève beaucoup de problèmes à cause notamment de la diversité et de la complexité des variables de l'environnement et de la capacité cognitive limitée des managers pour comprendre son évolution (Cyert et March, 1963). De plus, la nature des informations de la veille stratégique rend les activités de leur exploitation et traitement difficiles à mener.

Dans ce cadre, peu de travaux de recherche ont proposé des méthodologies et des connaissances actionnables pour assister cette phase fondamentale pour la veille anticipative stratégique.

1.1.5 Problématique de la phase d'exploitation des informations de la veille anticipative stratégique

Plusieurs auteurs en management stratégique caractérisent les informations de la veille stratégique de signaux et/ou signes faibles (Martinet et Petit, 1982; Martinet, 1983; Joffre et Koenig, 1985; Lesca, 1986; Narchal *et al.*, 1987 ; Marmuse, 1992) qu'il peut être vital de savoir détecter, amplifier, interpréter et traiter.

En effet, la surveillance des environnements incertains et turbulents à travers la détection anticipative des menaces et des opportunités se fait par la collecte d'informations anticipatives et de faits ambigus (Ansoff, 1975 ; Daft et Weick, 1984). L'**ambiguïté** se traduit par la possibilité de donner plusieurs interprétations à une information de type signal et/ou signe faible, comme elle peut se traduire par l'impossibilité de ne donner aucune interprétation (Weick, 1995).

Les signaux et/ou signes faibles sont des informations susceptibles d'avoir un caractère anticipatif, dont l'interprétation peut permettre d'éclairer un événement qui ne s'est pas encore produit, qui « se développent et s'améliorent avec le temps....augmentent progressivement en intensité à mesure que les signaux et et/ou signes de l'environnement deviennent plus forts » (Ansoff, 1975).

De plus, les informations qui ont un caractère anticipatif, annoncent un événement potentiellement en cours de formation, et peuvent contenir les prémises des ruptures ou des discontinuités stratégiques dans l'environnement de l'entreprise et à conséquences importantes sur sa compétitivité durable.

Les informations de type signal et/ou signe faible sont incertaines, qualitatives, ambiguës, fragmentaires (Gorry et Scott-Morton, 1971 ; Argyris, 1976 ; Lesca, 1986) et peuvent avoir plusieurs représentations, formes ou supports (Blanco et al., 2003). Comme elles peuvent être peu ou pas familières et se caractériser par une visibilité, et une pertinence faibles (Lesca et Blanco, 2002). Ces informations peuvent être aussi fugaces (Marmuse, 1992), rapidement obsolètes (Bourgeois et Eisenhardt, 1988), incomplètes, imprécises et de fiabilité fragile (Lesca, 2003).

Ces différentes caractéristiques soulignent les difficultés rencontrées par les preneurs de décision lors de la détection et du traitement de ce type d'information. Peu de travaux dans la littérature proposent des connaissances actionnables et méthodes pour gérer l'activité de collecte des informations d'anticipation (Gibbons et Prescott, 1996). De plus, Le traitement des informations ambiguës est considéré comme étant une opération difficile (March et Feldman, 1981 ; Weick, 1995).

Les traitements de ces informations sont de type « interprétation et induction ». L'interprétation des informations annonciatrices des changements de l'environnement, qui sont souvent ambiguës, (Pfeffer et Salancik, 1978 ; Ford et Baucus, 1987) joue un rôle important dans les actions futures et de l'efficacité continue de l'organisation (Chattopadhyay *et al.*, 2001) et devrait améliorer sa capacité d'adaptation (Daft et Weick, 1984; Lesca 1989 ; Hambrick et Mason, 1984 ; Thomas *et al.*, 1993).

Dans ces conditions, la veille anticipative stratégique est comprise comme étant un système d'interprétation (Daft et Weick, 1984) et un processus de construction de sens (Weick, 1995 ; Lesca N., 2002) qui se situe en amont de la prise de décision et vise à informer les décisions à prendre (Le Moigne, 1979) et orienter les actions à mener.

La théorie du « *sensemaking* » ou de construction de sens de Weick (1979, 1995) décrit le processus au cours duquel le décideur se construit une représentation anticipative, signifiante

et plausible de son environnement à partir d'informations fragmentaires et de sources diverses et qui est déterminante pour la prise de décision et l'action stratégique de l'entreprise.

Ainsi, l'interprétation anticipative des événements de l'environnement, à partir d'informations potentiellement anticipatives, s'apparente à une activité organisée d'intelligence (Frishammer, 2002) et suppose le ciblage, la traque, la sélection, l'évaluation et l'analyse des informations (Gilad et Gilad, 1986; Lesca, 1986; Huber, 1990; Lackman et al., 2000). En effet, l'intelligence vise à créer des représentations et des connaissances intéressantes pour assister le processus de prise de décision et orienter l'action (Bartoli et Le Moigne, 1996).

C'est dans ce cadre que la mise en place d'une veille anticipative stratégique requiert la création d'une intelligence **collective** nécessitant la mobilisation d'expériences et d'expertises diverses (Lesca, 2003). Au sein de l'entreprise, l'intelligence collective traduit la capacité d'un groupe d'individus (experts, responsables de l'entreprise) à se procurer des informations à caractère anticipatif, à sélectionner certaines d'entre elles selon des critères, à créer et à manipuler des liens de raisonnement entre ces informations (Lesca et Caron, 1995) en vue de construire une vision intelligible de l'environnement et de créer des champs possibles pour l'action ultérieure des opérationnels. L'intelligence d'une organisation est ainsi mesurée par rapport à sa capacité de se procurer, d'analyser et de retrouver les informations pertinentes à la prise de décision au bon moment (Feldman et March, 1981).

L'importance de la dimension **collective** de ce processus réside dans la réduction des biais cognitifs individuels et l'importance de la synergie des connaissances. En effet, l'interprétation des informations de la veille anticipative stratégique devrait se faire d'une manière collective à cause de la capacité cognitive limitée de l'individu pour rechercher et interpréter l'information (Cyert et March, 1963; Simon, 1991).

Le processus de l'intelligence collective est également un processus d'**apprentissage** dans lequel les connaissances acquises dans l'action évoluent dans le temps en permettant à l'entreprise de mieux anticiper son environnement incertain et d'y faire face.

1.2 Application des concepts théoriques de la problématique au contexte des agressions numériques

Dans cette section, nous mettons l'accent essentiellement sur les changements induits par l'évolution considérable des technologies de l'information et de la communication (TIC) et les conséquences de leur exploitation comme moyens de travail, de communication et de production. Cette exploitation est de nature à apporter des avantages notamment en termes de flexibilité et de réduction des coûts, mais engendre des inconvénients liés surtout à la **dépendance** de plus en plus accrue des entreprises à ces technologies et leur exposition à un risque affectant la sécurité de leur système d'information, et plus généralement leur **sécurité informationnelle**.

1.2.1 Les hackers : nouveaux acteurs de l'environnement externe de l'entreprise

Parmi les acteurs de l'environnement agissant d'une façon directe ou indirecte sur la compétitivité durable d'une entreprise apparaissent maintenant des « nouveaux venus » : les pirates informatiques ou les hackers (le terme en anglais), au centre de la présente recherche.

Les hackers sont des personnes qui peuvent compromettre la sécurité du système d'information d'une entreprise et/ou perturber ou arrêter son activité. Deux types de hackers, par mégarde ou intérêt, représentent une source de menace ou/et de perte. Il s'agit des hackers externes à l'entreprise et des hackers internes (Smith et Rupp, 2002) qui sont parmi les employés de l'entreprise et qui peuvent être des administrateurs du réseau, des techniciens ou des simples utilisateurs.

Les hackers sont également répartis en deux sous-classes : les curieux et les malins. Les actions des curieux sont surtout liées à la collecte des informations concernant le système alors que celles des malins sont beaucoup plus dangereuses et ont pour objectif la destruction ou le vol d'une ressource afin d'en tirer profit.

Les actions des hackers ont des conséquences qui ne se limitent pas à des pertes financières et matérielles mais aussi des pertes immatérielles et indirectes qui peuvent concerner la réputation et l'image de marque d'une entreprise, la perte de certaines opportunités d'affaires ainsi que la dégradation de la performance et de la productivité du système d'information.

En effet, la connectivité de plus en plus importante des entreprises et la dépendance accrue à l'égard des réseaux dont la maîtrise leur échappe en grande partie (partie d'ailleurs variable en fonction de leur proactivité) font des actions des hackers, qu'ils soient internes ou externes, des sources extrêmes de menaces pour l'efficacité et la continuité de l'activité de l'entreprise.

A cet égard, les actions des hackers ont largement contribué à des changements rapides de l'environnement externe de l'entreprise qui devient de plus en plus turbulent au sens de Emery et Trist. En effet, les hackers comme les événements le prouvent et les journaux en témoignent chaque jour sont toujours plus inventifs, toujours plus nombreux et leurs agressions sont en nombre sans cesse croissant. Ainsi, une notion d'**accélération** du changement de l'environnement **dans le temps** s'impose à l'entreprise sans cesse croissante.

Nous avons choisi de focaliser notre étude sur les hackers externes et les méthodes qu'ils utilisent pour attaquer le système d'information et de communication d'une entreprise. Les approches que nous développons dans ce travail s'appliquent néanmoins aux agressions d'origine interne sans modifications majeures.

Dans les paragraphes suivants, nous décrivons le contexte dans lequel les hackers agissent en explicitant les avantages et les risques de l'utilisation des TIC.

1.2.2 La définition d'un système d'information

Un système d'information est défini ici selon quatre niveaux nécessaires pour soutenir le flux, l'organisation et l'exploitation de l'information au sein d'une entreprise, et entre l'entreprise et son **environnement planétaire**.

Le premier niveau désigne le réseau de communication adopté. Le deuxième niveau définit l'infrastructure en équipements informatiques. Le troisième niveau précise l'ensemble des applications et des programmes mis en œuvre pour le traitement de l'ensemble des informations qui sont accessibles à travers le réseau. Le quatrième niveau détermine l'ensemble des services offerts par le système d'information à des utilisateurs en précisant les règles et les contrôles des accès.

Le terme réseau désigne le support d'information et de communication de l'entreprise (Petit, 2002). Un réseau d'entreprise peut être défini par ses composants, ses utilisateurs, ses applications, ses services ou ses gestionnaires (Montagnon, 2001) rendant possibles communications et partage d'informations et de ressources à travers des transmissions asynchrones ou en temps réel (Woodcock, 1999). Les composants comprennent les différents équipements informatiques qui font partie du réseau (tels que les modems, les logiciels, commutateurs de message). Les réseaux peuvent être classés également selon leur étendue :

- Les réseaux locaux dont la taille est relativement limitée. C'est l'exemple de l'Intranet dont la couverture et les applications sont limitées au périmètre d'une entreprise.
- Les réseaux étendus qui couvrent une zone géographique importante (il est souvent constitué de plusieurs réseaux locaux reliés). Dans ce cadre, l'Internet est un réseau étendu public dans cette catégorie en utilisant le protocole TCP/IP qui permet de connecter plusieurs ordinateurs indépendamment de leurs systèmes d'exploitation d'une façon facile et efficace.

A l'heure actuelle, les entreprises sont obligées d'ouvrir leurs réseaux notamment à l'Internet pour soutenir plusieurs activités avec leurs clients, leurs fournisseurs, leurs différents partenaires et même avec leurs employés.

En effet, les réseaux ont révolutionné le monde des affaires et deviennent inévitables pour la gestion des entreprises en permettant d'accéder rapidement à des informations, améliorer la communication en réduisant les coûts, de collaborer avec des acteurs distants, fournir de meilleurs services aux clients ainsi que de développer le commerce électronique.

1.2.3 Les avantages de se mettre en réseau

Les entreprises se mettent en réseau pour tirer profit de plusieurs avantages sur un plan opérationnel, organisationnel et stratégique.

Sur un plan opérationnel, les entreprises installent des réseaux essentiellement afin de :

- partager des ressources (qui peuvent être matérielles comme les imprimantes, le disque dur, un lecteur de CD-ROM, un modem,...etc., ou logicielles comme les progiciels, une base de données, une banque d'images,...etc.),
- permettre la communication en ligne. Certaines entreprises investissent dans les réseaux pour échanger des informations par l'utilisation des logiciels de messagerie électronique et d'agendas de groupe ce qui permettrait, par conséquent, de faciliter la gestion et l'organisation de l'entreprise,
- rendre disponible en temps réel certaines ressources de l'entreprise.

Dans ce cadre, l'évolution remarquable des TIC a augmenté l'ouverture des systèmes d'information (site Internet, messagerie électronique, Extranet, achat et vente sur Internet, accès distant pour les salariés mobiles, accès Internet) et amélioré d'une façon remarquable la connectivité des entreprises au niveau interne et externe. Mais en contrepartie, elles sont exposées à un nouveau type de risque d'une importance considérable.

Les développements importants en matière des TIC ont permis à l'entreprise de se disposer d'un ensemble de nouveaux moyens pour augmenter la flexibilité des processus par une réduction des temps et des coûts du changement ainsi que par la facilitation de la communication, de la coordination et de la coopération entre les acteurs (Prax, 1997 ; Reix, 1999). L'introduction des TIC a également favorisé la réorganisation et la reconfiguration de la chaîne de valeur (Porter, 1986) notamment par la mise en place d'une chaîne virtuelle capable de créer de la valeur tout autant que la chaîne de valeur physique (Rayport et Sviokla, 1996; Venkatraman et Henderson, 1998). De plus la chaîne de valeur peut être partiellement externe à l'entreprise.

Par ailleurs, la complète diffusion de l'Internet a largement favorisé le traitement et la transmission de données notamment texte, son et image. Ceci est de nature à permettre des possibilités d'interfaces directes entre clients et producteurs ce qui a permis le développement du commerce électronique qui devient un vecteur de croissance privilégié (Bitouzet, 1999 ; Hervier, 2001) par les entreprises en permettant la réduction des coûts, l'amélioration de la qualité de service, l'attraction de nouveaux clients et la création de nouveaux modes de vente des produits existants (Boyle, 2001 ; Grandon et Pearson, 2003). L'utilisation de l'Internet

comme un outil important et efficace de gestion de la relation client (Bradshaw et Brash, 2001 ; Ab Hamid et Kassim, 2004) dans une optique de personnalisation des produits et des services pour des clients exigeants, qui demandent de plus en plus des solutions globales adaptées à leurs besoins spécifiques et des qualités de services plus élevées.

Cependant, les avantages de se mettre en réseau mondial ouvre les « murs » de l'entreprise à une multitude de risques nouveaux dont seule une partie commence à être clairement entrevue. Notre présente recherche s'intéresse particulièrement au risque des agressions numériques.

1.2.4 Les risques de se mettre en réseau

Les entreprises se mettent en réseau soit parce qu'elles sont obligées soit parce qu'elles souhaitent en tirer des avantages sur un plan opérationnel et stratégique. Cependant, l'ouverture de leur réseau les expose à des agressions de plus en plus complexes, imprévisibles et dangereuses.

En effet, l'ouverture et l'extension du réseau d'entreprise ne sont pas sans risques. Les attaques ou les agressions numériques représentent un risque énorme pour la sécurité d'un système d'information d'une entreprise en termes de pertes en coût et de temps de réparation, de productivité, de clients, de continuité du service, d'image de marque et de réputation ainsi que de part de marché. En effet, en cas d'agression grave, l'enjeu n'est plus la seule continuité d'un service informatique mais bien la pérennité de l'activité de l'entreprise.

De plus, la menace pèse également sur les équipements physiques (ordinateurs et périphériques, ainsi que les équipements de production liés à l'informatique), les ressources logiques et virtuelles (vol de fichiers, altération ou duplication de logiciels, destruction de données par infections informatiques ou sabotage manuel) et les réseaux (moyens de liaison entre les équipements informatiques).

D'une façon générale, une **agression** est toute action compromettant la sécurité de l'information d'une organisation (Stallings, 2000). La sécurité réseau concerne la protection des ressources en informations (notamment les informations personnelles et financières des

utilisateurs, projets de recherche, prototypes virtuels de produits,..etc.) de l'entreprise. La sécurité se fonde sur trois aspects :

- la confidentialité,
- l'intégrité, et
- la disponibilité (Canavan, 2001 ; Vermeulen et Solms, 2002).

De ce point de vue, une attaque de sécurité réside dans toute atteinte à l'un de ces aspects. La confidentialité doit assurer l'accès aux ressources pour les personnes autorisées. L'intégrité de l'information concerne l'authenticité des données qui ne peuvent être modifiées que par les personnes autorisées. La disponibilité est le concept garantissant l'accès à l'information quand un utilisateur autorisé en a besoin.

Dans notre recherche, nous nous intéressons aux agressions numériques qui peuvent toucher une ou les trois facettes. Le terme numérique désigne le fait que l'information est traitée par un ordinateur local ou à distance. L'échange de l'information ainsi que le contrôle du réseau se font à travers des programmes représentés par des numéros (0 ou 1) et transportés par un signal électrique.

Les exemples les plus classiques d'agression numérique sont les virus qui, d'un mois à un autre, ne cessent de se diversifier avec des impacts de plus en plus néfastes. Voici quelques exemples.

En janvier 2004, le virus informatique très puissant Mydoom de type ver, a infecté des millions de courriels dans le monde en exploitant les carnets d'adresses des boîtes aux lettres des ordinateurs infectés pour se propager. Ce virus était programmé aussi pour attaquer les sites Web de l'éditeur de logiciels américain SCO et de Microsoft (sur le site www.solutions.journaldunet.com, des informations sur les nouveaux virus sont disponibles et actualisées)

Ou encore :

Yahoo, Amazon.com, e-Bay, et beaucoup d'autres sites populaires ont été la cible d'une agression numérique de type **déni de service**. Cette agression se manifeste par le blocage du fonctionnement du serveur, pendant une durée de temps, qui se trouve incapable de répondre à un ensemble de requêtes dépassant de loin ses capacités ce qui engendre son arrêt (source le site www.solutions.journaldunet.com, où nous trouvons aussi les agressions les plus sévères détectées).

Ce qu'il faut signaler c'est que certaines propriétés des systèmes de communication rendent les agressions numériques plus difficiles à détecter, à analyser et à répondre que les agressions usuelles. Ces propriétés incluent notamment :

- le caractère automatique des tâches
- la possibilité d'effectuer des actions à distance
- la possibilité de faire propager les techniques d'attaques
- le fait que l'identité de l'attaquant soit facilement dissimulable puisqu'il s'agit généralement d'une adresse.

1.2.5 Quelques chiffres significatifs décrivant l'ampleur du risque des agressions numériques

Dans le contexte des agressions numériques, il est important de distinguer entre les menaces, les vulnérabilités et les agressions (Canavan, 2001). Une **menace** se traduit par n'importe quelle action de nature à perturber l'exploitation, la fonctionnalité, l'intégrité ou la disponibilité d'un réseau ou d'un système d'information. Les menaces peuvent être environnementales (tels que les incendies, les séismes ou les inondations), humaines involontaires (qui sont liées à des mauvaises utilisations ou des erreurs commises par les programmeurs ou les administrateurs), et humaines volontaires (qui sont dues à des intrus internes ou externes à l'entreprise et qui accèdent sans avoir l'autorisation aux ressources du système d'information). Une **vulnérabilité** est une faiblesse inhérente au design, à la configuration, à l'implémentation ou à la gestion d'un système ou d'un réseau qui peut être exploitée par une ou plusieurs menaces, et de nature à affecter la confidentialité, l'intégrité ou la disponibilité des informations critiques du système d'information. De ce point de vue, une agression est définie par une menace et l'ensemble des vulnérabilités correspondantes.

Selon les statistiques du CERT (Computer Emergency Response Team), une agence fédérale chargée de la surveillance de la sécurité informatique des Etats-Unis, le nombre de vulnérabilités susceptibles d'être exploitées pour mener une agression numérique est en croissance accélérée. Le tableau suivant trace l'évolution du nombre de vulnérabilités reportées auprès du CERT entre 1999 et 2003.

Année	1999	2000	2001	2002	2003
Nombre de vulnérabilités reportées	417	1090	2437	4129	3784

Tableau 2 : Évolution du nombre de vulnérabilités reportées auprès du CERT

Le huitième rapport annuel réalisé par le Computer Security Institute (CSI) conjointement avec le FBI (Richardson, 2003) sur l'état de sécurité dans plusieurs entreprises américaines opérant dans plusieurs secteurs d'activité (finance, santé, éducation, télécommunication, commerce, industrie, etc.) indique que plus de 90% des 356 entreprises interrogées reconnaissent avoir été victimes, au moins une fois, d'une attaque de l'extérieur ou de l'intérieur.

Dans une étude similaire réalisée en Australie en 2003 par le AusCERT, 96% des 200 entreprises interrogées reconnaissent avoir été victimes, au moins une fois, d'un incident de sécurité (annexe 2). Pour l'an 2002, le CERT a recensé plus de 82000 incidents de sécurité, soit quatre fois plus qu'en 2000. Ce chiffre est passé à plus que 135000 incidents pour l'année 2003. Le tableau suivant trace l'évolution remarquable du nombre d'incidents reportés auprès du CERT entre l'année 1999 et l'année 2003.

Année	1999	2000	2001	2002	2003
Nombre d'incidents reportés	9859	21756	52658	82094	137529

Tableau 3 : Évolution du nombre d'incidents reportés auprès du CERT

De même, le rapport publié en 2003 par la firme Symantec, l'éditeur de Norton Antivirus, montre que les agressions exploitent maintenant des failles relativement récentes puisque 64% des invasions tirent profit de failles découvertes il y a moins d'un an.

En effet, des analyses effectuées récemment par le CERT ont montré que les outils utilisés lors des agressions numériques ont beaucoup évolué en devenant de plus en plus sophistiqués notamment pour les rendre difficilement identifiables dans les phases d'investigation sur les incidents. La rapidité dans la découverte des vulnérabilités rend de plus en plus difficile la conservation d'un niveau de sécurité satisfaisant sur un système d'information hétérogène et géographiquement dispersé.

1.2.6 Les sources et la typologie des agressions numériques :

Les entreprises peuvent être attaquées de l'intérieur, et/ou de l'extérieur. Le huitième rapport du CSI/FBI (Richardson, 2003) indique que les agressions numériques venant de l'extérieur représentent la proportion la plus élevée. Ce résultat est confirmé également dans le rapport de AusCERT de l'année 2003 avec 94% des entreprises qui reconnaissent avoir été attaquées de l'extérieur.

En pourcentage très élevé les agressions venant de l'extérieur sont menées par des hackers indépendants externes, soient 82% des 488 entreprises répondantes affirment avoir été victimes des actions de hackers indépendants selon le rapport du CSI/FBI de l'année 2003.

Ce même rapport signale trois types de points à travers lesquels les agressions peuvent être menées : les connexions via l'Internet, les systèmes internes, et les connexions à distance. Les entreprises consultées ont rapporté que l'Internet est le point d'attaque le plus fréquent comme le montre le tableau suivant, qui retrace les points d'attaque identifiés par les entreprises entre 2000 et 2003. L'Internet est également le point d'attaque le plus fréquent cité dans l'étude réalisée par l'AusCERT pour l'année 2003.

Le tableau suivant indique les trois sources d'attaques les plus rencontrées par les entreprises qui ont participé à l'étude menée par le CSI/FBI entre l'année 2000 et l'année 2003.

Sources des agressions	Pourcentage des entreprises en 2000	Pourcentage des entreprises en 2001	Pourcentage des entreprises en 2002	Pourcentages des entreprises en 2003
Internet	59	70	74	78
Connexion à distance	22	18	12	18
Systèmes internes	38	31	33	30

Tableau 4 : Les points d'attaques identifiés entre 2000-2003

Par ailleurs, la connectivité croissante des entreprises et l'extension de leurs réseaux exposent ces entreprises à de multiples agressions qui sont de plus en plus complexes, imprévisibles et dangereuses.

Les études réalisées par le CSI/ FBI sur plusieurs années, et par l'AusCERT pour deux années consécutives (2002 et 2003), signalent que les agressions détectées les plus sévères sont : les virus, l'accès réseau et abus de service Internet, le déni de service, la pénétration des systèmes d'information de l'entreprise et l'accès non autorisé par des utilisateurs internes.

D'après une étude sur la sinistralité informatique en France réalisée par le Club de la Sécurité des systèmes d'Information Français pour les années 2002 et 2003 (www.clusif.asso.fr) auprès de 600 entreprises de six secteurs d'activités et de 100 collectivités publiques, les virus sont les agressions les plus rencontrées par les entreprises qui ont participé à cette étude.

Le tableau suivant nous donne une idée sur les agressions numériques les plus sévères et reportées entre 2000 et 2004 dans l'étude du CSI/FBI.

Types d'agression	2000	2001	2002	2003	2004
Déni de service	27	36	40	42	17
Virus	85	94	85	82	78
Abus de privilèges de l'accès Internet	79	91	78	80	59
Pénétration dans le système de l'extérieur	25	40	40	36	39
Vol d'information	20	26	20	21	10

Tableau 5 : Typologie des agressions les plus fréquemment rencontrées entre 2000-2004

Insistons sur le fait que la plupart des agressions ne sont visibles que lorsqu'elles se terminent et que les entreprises peuvent ne pas se rendre compte de leur occurrence, et de ne pas les détecter. Cet état des faits implique des pertes qui peuvent être financières ou immatérielles comme la perte de la confiance des clients.

1.2.7 Pertes financières engendrées par les agressions numériques

Chaque attaque est caractérisée par sa probabilité, sa difficulté technique, le coût de sa réalisation et de son impact. Des chiffres importants témoignent de l'ampleur de ce risque encouru par les entreprises impliquant des pertes notamment financières et matérielles considérables.

Cependant, il faut signaler les difficultés de mesure des pertes financières occasionnées par les agressions contre la sécurité du système d'information. D'après le rapport du CLUSIF pour l'année 2002, seulement 14% des entreprises impactées procèdent à une évaluation financière, ce qui reste encore très marginal. De plus, de nombreux incidents de sécurité ne sont pas comptabilisés, car non détectés. Ce constat est également présent dans l'étude réalisée par le CSI/FBI (2003), puisque 75% des entreprises répondantes indiquent des pertes financières mais 47% seulement sont capables de les quantifier.

Le rapport du CLUSIF pour l'année 2002 précise que l'impact financier des attaques comprend :

- les coûts de réparation ou de remplacement du matériel informatique endommagé ou manquant,
- les coûts de reconstitution de données, de logiciels ou des procédures endommagés ou perdus,
- les coûts liés à la perte d'exploitation,
- les coûts de renforcement des protections,
- les coûts liés à la responsabilité encourue par l'entreprise et aux pertes de patrimoine.

Le tableau suivant indique le montant des pertes financières engendrées par les plus sévères agressions numériques détectées entre 2000 et 2003 selon le huitième rapport annuel de CSI/FBI (Richardson, 2003).

Type d'agression	Pertes Totales Annuelles			
	2000	2001	2002	2003
Vol d'information	66708	151230,1	170827	70195,9
Sabotage des informations du réseau	27148	5183,1	15134	5148,5
Pénétration du système par un outsider	7104	19066,6	13055	2754,4
Abus de privilèges de l'accès Internet	27984,74	35001,65	50099	11767,2
Fraude financière	55996	92935,5	115753	10186,4
Déni de service	8247,5	4283,6	18370,5	65643,3
Virus	29171,7	45288,15	49979	27382,34
Accès interne non autorisé	22554,5	6064	4503	406300
Pertes annuelles	244914,44	359052,7	437720,5	599378,04

Tableau 6 : Pertes financières occasionnées par les agressions numériques entre 2000-2003

Dans ce même cadre, l'étude réalisée par l'AusCERT révèle que les pertes financières ont doublé de 2002 au 2003 en passant de 6 millions à 12 millions de dollars.

Ce qu'il faut noter par rapport à ces études, c'est que le vol des informations, le déni de service, et les virus sont les agressions numériques qui ont enregistré les pertes financières les plus élevées.

1.2.8 L'incertitude liée aux agressions numériques

Le risque des agressions numériques est très lié à l'incertitude de leurs occurrences. Cette relation est traduite par les pertes financières engendrées par ces agressions ainsi que par la diversité de leurs types et de leurs sources comme en témoignent les rapports des organismes spécialisés officiels internationaux.

Dans notre cas, l'incertitude des agressions numériques est liée à deux principales causes :

- leur visibilité n'est clairement possible que lorsqu'elles sont terminées, et qu'il est alors trop tard (dans la plupart des cas) ;
- une entreprise peut être victime d'une agression sans en avoir conscience.

La première cause montre, d'abord, que l'entreprise se trouve dans une situation de manque d'information (et spécialement en temps voulu) qui peut empêcher de détecter à temps les agressions et d'y répondre d'une façon appropriée.

Dans ce cadre, il est nécessaire de collecter des informations d'un certain type relatives à des **alertes précoces** liées à des problèmes potentiels de sécurité. Ces informations doivent avoir un caractère anticipatif « *early warning* » dont l'interprétation est susceptible de réduire le risque des agressions et de minimiser les coûts de réparation (Killcrece *et al.*, 2003).

Ceci suppose la mise en place d'un système de captage, de sélection et de remontée des informations, au sein de l'entreprise, rapportées à une agression numérique ainsi que des mécanismes pour tracer l'historique de tous les flux informationnels entrant et sortant. Sans ces mécanismes de repérage, la détection d'une agression va gérer une quantité surabondante d'informations ce qui est de nature à augmenter l'incertitude.

De plus, en absence d'une politique de sécurité qui détermine d'une façon claire et précise les règles, les limites et les autorisations assignées aux utilisateurs du système d'information, la détection et la réponse sont très difficiles à cause de l'**ambiguïté** des informations.

La deuxième raison relative à l'incertitude de l'occurrence des agressions numériques réside dans le fait que les entreprises ne s'aperçoivent pas toujours des agressions dont elles sont

victimes ou sont incapables de détecter les sources qu'elles soient internes ou externes de ces agressions.

En effet, le rapport du CSI/ FBI (Richardson, 2003) révèle que 26% des 356 entreprises interrogées sont incapables d'identifier la source de l'agression. De plus, 22% des 503 entreprises interrogées signalent qu'elles sont incapables de savoir d'une façon précise si elles ont subi un accès non autorisé.

A cet égard, le vol des informations est considéré comme étant une des agressions numériques les plus dangereuses et les plus coûteuses à une époque où l'information constitue un levier important de l'activité d'une entreprise et donc de sa compétitivité.

Ainsi, le contexte dans lequel les entreprises détectent, analysent et répondent aux agressions numériques se caractérise par l'incertitude. Les sources d'incertitude identifiées dans la littérature sont également valables dans ce contexte. Les responsables de sécurité se trouvent souvent dans une situation de manque d'information, de surabondance des informations et d'ambiguïté des informations. Cette incertitude est de nature à handicaper le processus de prise de décision dans ce domaine et expose les entreprises à des risques tangibles et intangibles considérables.

Il est donc impératif de détecter le plus tôt possible une agression numérique ou d'**anticiper son occurrence**.

1.2.9 L'adaptation de la veille anticipative stratégique dans le cas de réponse aux agressions numériques

Dans le cadre de notre recherche, la pratique de la veille anticipative stratégique est confrontée à une activité fondamentale et vitale pour l'entreprise à savoir la sécurité de son système d'information contre les agressions numériques.

L'essor de la société numérique et le développement important des réseaux, et plus particulièrement de l'Internet, devraient faire de la sécurité du système d'information une priorité absolue pour les entreprises. Les enjeux financiers importants ajoutés au nombre

croissant et complexe des agressions numériques, poussent les entreprises à développer des approches proactives, puissantes et efficaces de sécurité afin de maintenir un niveau de sécurité optimal et de réagir le plus rapidement possible.

En effet, la rapidité avec laquelle une entreprise détecte, analyse et répond à une agression contre son système d'information limite d'une façon significative les dommages occasionnés par celle-ci et réduit considérablement les coûts de son recouvrement (Killcrece *et al.*, 2003).

Cependant, les agressions numériques sont imprévisibles, complexes et **ne sont détectées qu'après coup**. L'incertitude liée aux agressions numériques augmente le risque encouru par l'entreprise suite à l'extension ou à l'ouverture de son réseau pour des besoins de développement de ses relations ou de ses activités avec ses clients ou ses partenaires.

Il devrait être donc impératif, dans ce cas, d'anticiper les agressions numériques le plus tôt possible pour pouvoir se protéger à temps et aux moindres coûts. Dans la plupart des cas, l'anticipation des agressions numériques s'effectue à travers la détection des informations de type signal et/ou signe faible générées par le réseau de l'entreprise et dont les caractéristiques ont été explicitées dans les paragraphes précédents.

Ce qu'il faut noter c'est que la détection de ces signaux et/ou signes générés par le réseau est difficile et complexe, ce qui explique en grande partie le nombre croissant des agressions numériques.

De même, la prise de décision, tout comme l'analyse des agressions, nécessite une activité d'interprétation **collective** des informations à caractère anticipatif selon un processus de création de sens afin d'élaborer des réponses techniques et managériales appropriées. De plus, ces agressions ainsi que les liens générés lors du processus d'interprétation devraient être mémorisés pour enrichir le processus de réponse aux incidents de sécurité et pour constituer un processus d'apprentissage efficace.

Ainsi, la mise en place d'un dispositif de veille anticipative stratégique pour réduire le risque lié à l'incertitude des agressions numériques nous paraît trouver une application prometteuse dans le domaine de la sécurité des réseaux d'entreprise. En effet, la veille anticipative

stratégique est un dispositif d'**attention** permettant de réduire le risque lié à l'incertitude et de sécuriser ou amélioré dans le futur la position de l'organisation (Choo, 1997). Dans notre cas, la veille anticipative stratégique est un dispositif qui porte l'attention sur des nouveaux acteurs particuliers dont les actions représentent un risque énorme pour l'efficacité et la continuité de l'activité de l'entreprise dans le contexte des TIC.

Dans le domaine de la sécurité des réseaux, la veille anticipative est un système d'information dédié à l'aide à la protection des ressources informationnelles de l'entreprise. Elle permet la détection :

- des agressions numériques qui ont été préalablement répertoriées (et largement commentées dans des sites destinés à leur analyse) et la prise de décision relative à la réponse à ces agressions compte tenu de leur impact sur l'activité de l'entreprise.
- Ce même processus permet de caractériser les agressions non encore répertoriées à travers l'analyse de certains signaux et/ou signes faibles collectés par des systèmes de détection, d'évaluer les dégâts potentiels occasionnés et de préparer une réponse appropriée et rapide à ces attaques.

Sur le plan stratégique, les agressions numériques sont essentiellement de nature à nécessiter la génération des décisions d'un certain type : de nature non répétitives, non programmables, dont l'enjeu peut être grand pour l'entreprise et prises dans un contexte d'incertitude.

Par ailleurs, la réaction générée face à une agression oblige à revoir la **politique de sécurité**, les mécanismes de captage et de contrôle pour remédier à leurs insuffisances constatées ainsi que l'organisation de l'activité de l'entreprise. De plus, le caractère variable, complexe et imprévisible des menaces et donc des vulnérabilités pousse les entreprises à mettre en place des approches et méthodes de sécurité dynamiques et adaptatives.

Notre application dans le domaine de la sécurité des réseaux d'entreprise concerne une **solution particulière** de sécurité où le processus d'interprétation collective des informations de type signal et/ou signe faible est une activité fondamentale pour agir vite ou par anticipation.

1.3 Objectifs, intérêt et pertinence de la question de recherche

Dans cette section, nous énonçons, d'abord, la question de recherche en délimitant le sujet au niveau de l'étude d'une solution particulière de sécurité pour réduire le risque des agressions numériques à travers le travail des **équipes de réponse aux incidents (ERI)** de sécurité. Ensuite, nous exposons les objectifs de la recherche. Enfin, nous explicitons l'intérêt et la pertinence de la question de recherche, selon nous, sur les plans académique et pratique.

1.3.1 Délimitation du sujet de la recherche

La présente recherche s'inscrit dans le cadre de développement d'un dispositif de Veille Anticipative Stratégique au sein de l'entreprise afin de réduire l'incertitude et le risque des agressions numériques.

Les développements précédents ont montré la gravité, la complexité et le caractère sournois des agressions numériques ce qui est de nature à remettre en cause la pérennité et la compétitivité durable de l'entreprise. Les enjeux importants des agressions numériques mettent en évidence la nécessité de réagir à temps et de développer une capacité d'anticipation.

Dans le domaine de la sécurité des réseaux, la veille anticipative stratégique est un système d'information susceptible d'aider à la détection des agressions numériques et la prise de décision relative à la réponse à ces agressions compte tenu de leur impact sur l'activité de l'entreprise. Ce même processus permet l'analyse de certaines informations potentiellement anticipatives collectées par des systèmes de détection, afin de se préparer par anticipation face à ces agressions.

Les entreprises mettent en place plusieurs solutions en matière de sécurité. **Nous avons choisi** de nous intéresser à une solution particulière pour réduire le risque des agressions numériques à savoir la **composition d'une Equipe de Réponse aux Incidents (ERI) de sécurité** (l'expression en anglais est *Incidents Response Team*).

Les ERI se chargent des activités de détection, d'analyse et d'élaboration de réponse rapide à partir d'informations de type signal faible et/ou signe. Ces activités sont effectuées dans un

contexte d'incertitude et supposent la mise en place d'un processus d'intelligence **collective** afin de réduire le risque des agressions numériques et aider à la prise de décision dans ce domaine. Cette décision à prendre dans le contexte des agressions numériques est de nature non répétitive dont l'enjeu est très grand pour l'activité de l'entreprise utilisatrice des TIC.

Ainsi, le présent travail s'intéresse principalement à la question de recherche suivante :

Est-il possible d'aider les ERI à **réduire** le risque des agressions numériques sur les réseaux d'entreprises en les **anticipant** et partant réduire le délai de réaction ?

L'hypothèse centrale de cette recherche découlant de cette question est de tester si la méthode proposée permet d'aider efficacement une ERI à réduire le risque des agressions numériques.

1.3.2 Objectifs de la recherche

Dans le cadre de ce travail, nous avons choisi de proposer une connaissance actionnable au sens d'Argyris sous forme d'une méthode dans le but d'améliorer l'efficacité et la réactivité d'une ERI. Cette connaissance actionnable (ou méthode) devrait aider le travail quotidien des ERI. Elle se base sur certains aspects de la méthode *LESCanning*® et vise à faire des apports sur le plan conceptuel et pratique. De plus, la méthode proposée est susceptible d'être supportée par certaines potentialités de la technologie Internet.

Etant donné que la question de recherche se pose autour de la proposition de connaissances actionnables pour aider les ERI à réduire le risque des agressions numériques, les objectifs du présent travail s'articulent autour des quatre points suivants :

- Proposer une méthode qui pourra être assistée par une utilisation de la technologie Internet afin de réduire le délai d'action face à une agression et d'agir par anticipation.
- Expérimenter le fonctionnement de la méthode sur des cas réels d'agressions numériques.

- Evaluer le progrès réalisé par rapport à la réduction du risque numérique, apporté par l'expérimentation de la méthode dans les cas considérés. Des indicateurs d'évaluation seront proposés à cet effet.
- Présenter les conditions d'expérimentation sous lesquelles la méthode serait répliquable.

Ainsi, la réponse à la question de recherche se base sur la conception et la construction d'une méthode d'interprétation des informations spécifiques de la veille anticipative afin de créer du sens et de connaissances nécessaires à la réduction du risque des agressions numériques. La méthode proposée devrait permettre un enrichissement de la typologie des liens créés entre les informations ainsi que le raisonnement de type heuristique de la méthode *LESCanning*®.

Ceci nous conduira à proposer des indicateurs d'évaluation qui permettront d'apprécier dans quelle mesure la réponse à la question de recherche est satisfaisante, c'est-à-dire si la méthode proposée permet effectivement de réduire le risque des agressions numériques.

Cependant, les conditions d'expérimentation doivent être indiquées de façon précise afin de permettre la réplification de l'expérimentation sur d'autres cas, à des fins de validation.

Par ailleurs, il est opportun de signaler que la dimension temporelle a une importance capitale dans notre recherche. La conception et l'expérimentation de la méthode proposée ont nécessité un certain temps pour l'apprentissage et ce dans le **cadre d'une étude longitudinale**.

1.3.3 Pertinence du point de vue des praticiens

Le choix de la question de recherche a pour origine une « demande de terrain », qui présente une importance considérable, et sans doute croissante dans les années qui vont venir. Dans cette recherche, le risque des agressions numériques est considéré comme étant un risque et un **problème de gestion** et non pas uniquement un risque technique.

L'étude portant sur un problème d'origine terrain doit apporter une réponse significative pour les praticiens. Ceci est particulièrement important dans le domaine de la **recherche en sciences de gestion**, option systèmes d'information (Ganesh *et al.*, 2003).

Dans ce cadre, la sécurité des ressources informationnelles à l'ère numérique constitue un levier important d'efficacité et de croissance pour l'entreprise utilisatrice des TIC. Les enjeux stratégiques des agressions numériques poussent l'entreprise à développer des solutions de plus en plus sophistiquées en matière de sécurité.

Cependant l'utilisation des solutions techniques et physiques de sécurité s'avère insuffisante vu la complexité et l'imprévisibilité croissantes des agressions numériques. Les rapports des organismes spécialisés officiels internationaux (CERT, AusCERT, CLUSIF) montrent que l'utilisation massive des antivirus, des *firewalls* et des systèmes de détection d'intrusion est d'une efficacité limitée dans le cas des agressions compliquées ou inconnues.

La constitution d'une ERI comme étant une solution complémentaire de sécurité se trouve largement justifiée afin de détecter et d'interpréter des **signes précoces** d'intrusion ou des tentatives d'intrusion. Cette interprétation nécessite une véritable intelligence au sein d'une ERI et devrait permettre de réduire et d'anticiper le risque des agressions numériques.

Toutefois, les ERI **manquent de méthodes** (Killcrece *et al.*, 2003) adéquates pour assister cette étape d'interprétation des informations collectées de type signal et/ou signe faible.

Ainsi, l'intérêt managérial réside dans la conception, la construction, l'expérimentation et l'évaluation d'une méthode pour détecter et analyser les agressions numériques afin d'y répondre d'une façon appropriée et en minimisant les pertes. La méthode proposée devrait développer également un système d'aide à la décision collective.

Dans cette perspective, la présente recherche s'oriente vers la conceptualisation de nouveaux problèmes issus de l'exploitation des informations de la veille anticipative stratégique de type signal et/ou signe faible dans le domaine de la sécurité des ressources informationnelles de l'entreprise et la production de **connaissances actionnables validées** et appropriées à ce type d'informations.

De plus, la méthode proposée devrait déboucher sur une utilisation innovante de la technologie Internet. L'assistance de la méthode proposée par un outil informatique exploitant certaines potentialités de la technologie Internet est susceptible de faciliter l'utilisation de la méthode ainsi que la réplique de celle-ci sur d'autres cas d'agressions numériques.

1.3.4 Pertinence par rapport aux publications académiques disponibles

L'intérêt académique apparaît dans la mesure où des réponses n'ont pas été publiées dans des revues académiques sur notre question de recherche. Notons qu'à notre connaissance, aucune recherche dans le domaine des **sciences de gestion** n'a proposé et validé empiriquement une méthode formalisée d'intelligence collective pour réduire le risque des agressions numériques.

L'ampleur du risque des agressions à l'ère numérique devrait relancer des recherches en sciences de gestion afin de cerner toutes les problématiques liées à ce nouveau type de risque. Notre travail de recherche s'intègre bien dans cette perspective et vise à produire des connaissances actionnables pour aider à analyser et à réduire le risque des agressions numériques.

En effet, les méthodes et les techniques d'évaluation du risque en général recensées dans la littérature ne semblent pas être appropriées à la nature du risque des agressions numériques ni aux spécificités du contexte d'analyse et de réduction de celui-ci. Les informations de type signal et/ou signe faible ne sont pas aussi prises en considération dans ces méthodes et techniques d'évaluation du risque en général.

La méthode proposée dans cette recherche assiste le processus de création collective de sens à partir d'information de type signal et/ou signe faible devant aider les ERI à réagir vite ou par anticipation face au risque des agressions numériques. Elle se base sur certains aspects de la méthode *LESCanning*® orientée davantage vers l'anticipation et qui a été conçue, réalisée et validée en prenant en compte la nature des informations anticipatives et en utilisant l'intelligence collective pour l'interprétation de ces informations.

Par rapport à la méthode *LESCAnning*®, nous visons réaliser des apports sur le plan conceptuel et théorique, spécifiques au domaine de réponse aux agressions numériques.

Les apports théoriques du modèle conceptuel résident au niveau de l'enrichissement de la typologie des liens créés entre les informations de veille anticipative de nature à permettre un raisonnement de type heuristique nécessaire à un processus d'intelligence collective.

Dans ce travail, nous utilisons une extension des cartes causales pour la représentation et la manipulation des liens dynamiques et probabilistes dans un contexte d'incertitude de nature à ouvrir le champ à un **raisonnement non déterministe**. Nous visons à travers cette extension à assister le raisonnement, de nature complexe, lors du processus de création collective de sens.

L'enrichissement de la typologie des liens est réalisé dans notre travail en intégrant la **probabilité** et l'approximation dans la création de relations entre les informations et la **pression du temps** comme étant des facteurs très significatifs dans le domaine d'analyse et de réponse aux agressions numériques. L'enrichissement de la typologie des liens est très important à cause de la complexité et de la diversité des raisonnements dans ce domaine.

De même, notre apport se situe aussi au niveau de la **formalisation de la fonction de médiation** qui supporte le processus de création collective de sens et qui apparaît sans une méthodologie explicite appropriée dans le travail développé par Chaib-draa, (2002) ainsi que dans la méthode *LESCAnning*® (Lesca, 2003).

Ainsi, nous ambitionnons à travers ce travail de recherche de contribuer plus spécifiquement au domaine de la veille anticipative stratégique en adaptant les concepts clés de cette discipline au contexte de réponse aux agressions numériques.

Conclusion Chapitre 1

Nous avons montré dans ce chapitre que les concepts théoriques clés de la veille anticipative stratégique trouvent une application pertinente dans le contexte de réponse aux agressions numériques.

En effet, ce contexte se caractérise par l'incertitude et la turbulence du fait que les agressions numériques sont de plus en plus imprévisibles, complexes et les hackers sont de plus en plus inventifs. Cet état de faits implique un risque énorme pour les entreprises utilisatrices des TIC, d'où la nécessité de développer des approches proactives en matière de sécurité des ressources informationnelles.

Nous avons choisi une solution particulière de sécurité à travers le travail d'une ERI et avons montré que le processus de création collective de sens à partir d'informations de type signal/signe faible présente un intérêt particulier par rapport aux activités d'une ERI.

La question de recherche posée dans ce travail répond à une problématique de terrain à travers la conception et la réalisation d'une Méthode d'Analyse et de Réduction du Risque des Agressions Numériques (MARRAN) afin d'aider une ERI à réagir vite ou par anticipation.

Chapitre 2

État des connaissances actionnables disponibles dans les publications et dans les pratiques des entreprises par rapport à notre question de recherche

Ce chapitre a pour but d'étudier l'état des connaissances utiles et disponibles pour notre proposition, et qui devra tenir compte du travail des ERI. Il s'agit d'identifier des éléments de réponse à notre question de recherche qui s'articule autour de la réduction du risque des agressions numériques à travers la conception et la mise en pratique d'une méthode (à construire) de traitement d'informations de type signal et/ou signe faible. Cette méthode devrait être susceptible d'aider et d'assister les ERI dans leur travail quotidien de protection du réseau de l'entreprise.

Pour cela, nous nous intéressons aussi bien à l'état des connaissances dans les publications qu'à l'état des pratiques dans les entreprises, ainsi que les solutions techniques ou autres adoptées par celles-ci pour réduire le risque des agressions numériques.

S'agissant des publications, nous nous intéressons à des domaines distincts mais complémentaires comme les techniques d'analyse du risque, les cartes causales en tant que cadre conceptuel pour la représentation et l'interprétation des informations ainsi qu'à d'autres méthodes d'exploitation collective des informations de type signal et/ou signe faible. La revue de littérature dans ces domaines devrait nous permettre de situer les apports d'ordre conceptuel et théorique de notre proposition.

Concernant l'état des pratiques dans les entreprises, il est important de voir les meilleures pratiques de protection au sein des entreprises. Dans ce cadre, nous nous référons à des documents de travail et des rapports publiés par le CERT/CC ainsi que l'état des lieux dans une entreprise tunisienne fortement concernée par notre sujet, l'Agence Nationale de Certification Electronique, et qui fera l'objet de nos investigations empiriques.

Ainsi, la première section exposera les différentes techniques d'analyse du risque. La deuxième section s'intéressera à l'apport des cartes causales et de l'intelligence collective lors de la phase du traitement des informations. La troisième section sera réservée à l'état des pratiques dans les entreprises en matière de sécurité afin de réduire et de gérer le risque des

agressions numériques. La quatrième section décrira plus en détail les pratiques des ERI dans les entreprises selon une étude réalisée dans ce but.

2.1 Apports et limites des techniques d'analyse du risque, dans les publications

A travers la revue de la littérature réalisée par White (1995), trois phases communes sont identifiées dans un processus d'évaluation du risque encouru par une entreprise : une phase d'identification du risque, une phase d'estimation du risque et une phase d'appréciation du risque. Chaque phase implique certaines actions pour évaluer le risque. La figure suivante illustre le processus d'évaluation du risque à travers la description de chaque phase et de ses implications.

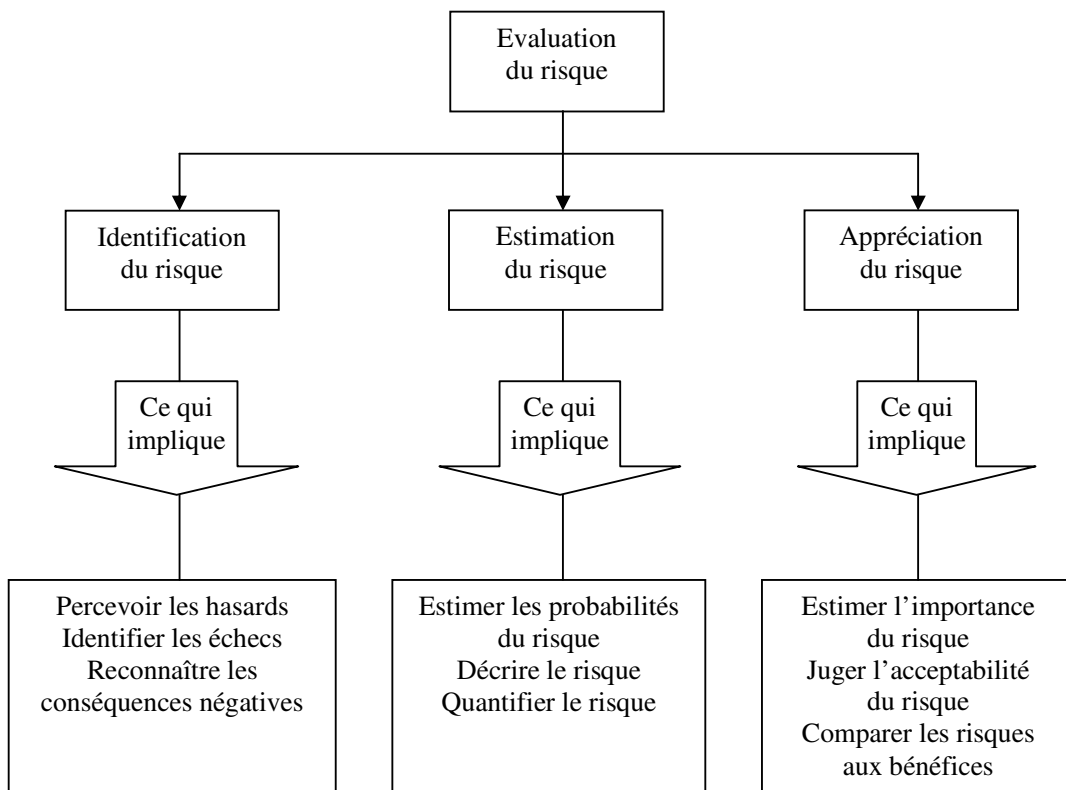


Figure 2: Le processus d'évaluation du risque d'après White (1995)

Nous rapportons dans ce qui suit certaines techniques d'évaluation et d'analyse du risque telles que avancées par White (1995) dans une revue de la littérature sur le sujet. Nous soulignons par la suite les apports et les insuffisances de ces techniques par rapport à notre question de recherche.

2.1.1 Les techniques d'évaluation du risque

Nous avons choisi de nous rapporter au travail de synthèse de White (1995) qui a pour objet l'étude comparative des différentes techniques d'évaluation et d'analyse de risque avancées dans la littérature. Dans cette revue de la littérature, la notion de probabilité apparaît comme étant un point central dans les techniques d'évaluation du risque alors que l'interprétation de cette probabilité peut varier selon un point de vue objectif ou subjectif.

Par ailleurs, l'auteur distingue entre deux types d'approches selon lesquelles les techniques développées dans la littérature peuvent être classées. Il s'agit de l'approche réductionniste et de l'approche holistique.

2.1.1.1 L'approche réductionniste

Selon cette approche, les techniques d'évaluation du risque se limitent à l'étude isolée d'un élément du système ou du processus à analyser pour estimer les probabilités de défaillance de cet élément et les implications de cette défaillance sur la performance globale du système ou du processus.

Parmi ces techniques figure la **méthode FMEA** (*Failure Mode and Effect Analysis*) qui se base sur un brainstorming systématique pour évaluer la performance d'un système ou d'un processus. Elle consiste à lister, pour chaque composant du système, toutes les possibilités de défaillance et évaluer leurs impacts sur le reste du système. Le concept de base de cette méthode est d'analyser le système en le divisant en ses composants élémentaires, et d'assigner une probabilité d'échec à chaque élément composant le système. Cependant, les systèmes sont complexes et les possibilités d'interaction et de complémentarité entre les différents éléments du système sont importantes à considérer lors de l'évaluation d'une défaillance. De plus, le fonctionnement et la performance d'un système dépendent aussi de l'impact de certains facteurs de l'environnement externe de celui-ci .

La méthode CBA (*Cost Benefit Analysis*) est également utilisée pour estimer et quantifier le risque selon une approche réductionniste. La prémisse de base de cette méthode est que les

alternatives sont sélectionnées en comparant les avantages et les inconvénients qui peuvent résulter des conséquences estimées d'un choix. Ceci suppose la disponibilité des options alternatives. Cette technique implique de combiner les bénéfices attendus ou les coûts attendus ou des conséquences adverses. A chaque bénéfice et conséquence est attribuée une valeur monétaire. Cette méthode connaît plusieurs limites, comme le non prise en compte de l'incertitude et des spécificités du contexte dans lequel le risque est considéré.

De plus, durant la phase d'évaluation du risque, le degré d'acceptabilité du risque doit être considéré. Dans ce cadre, plusieurs techniques d'évaluation du risque se sont développées pour mesurer les attitudes envers le risque notamment en se basant sur la perception qui est déterminée par les capacités cognitives des individus. Parmi ces techniques figurent la méthode DELPHI et les systèmes experts. La méthode DELPHI se caractérise par l'utilisation des questionnaires auprès d'un panel d'experts qui répondront **individuellement** tout en illustrant leurs réponses. La démarche se termine par une analyse consensuelle entre les experts. Les systèmes experts se basent sur des modèles assistés par ordinateur et utilisent l'intelligence artificielle pour imiter le processus de raisonnement d'un expert. Ceci implique la nécessité d'une base de connaissances et de règles actualisées.

Le mérite de l'approche réductionniste est de garantir l'efficacité intrinsèque de chaque élément d'un système. Toutefois, lors de l'assemblage des différents éléments d'un système cette approche ne permet pas d'identifier les propriétés émergentes de l'interaction entre ces éléments. Ainsi, cette approche ne permet pas de déterminer le comportement global du système qui dépend aussi bien de ses mécanismes internes que des variables caractérisant son environnement externe.

2.1.1.2 L'approche holistique

Dans cette approche, le système est évalué dans sa globalité tout en prenant en considération l'influence de ses variables contextuelles. Cette approche est particulièrement pertinente dans le cas de traitement des problèmes difficilement structurables.

La théorie culturelle « *culture theory* » (Thompson, 1980) s'intègre dans cette approche du risque et propose comme hypothèse la construction sociale du risque selon laquelle les individus ont des attitudes différentes envers le risque (aversion ou acceptation) compte tenu de leur culture ou de la spécificité du contexte social. Les résultats obtenus en utilisant une

perspective subjective varient en fonction de l'état de l'information et les suppositions des analystes qui peuvent amener à différentes réponses pour un même problème (Vesely, 1984). Ainsi, le résultat de l'évaluation du risque dépend de l'approche utilisée et les points de vue des analystes.

Le concept de construction sociale du risque est également évoqué à travers la notion de la confiance qui est considérée comme étant un processus social et cognitif pour réduire le risque et augmenter les chances de succès des futures décisions (McLain et Hackman, 1999). Ceci est d'autant plus important que s'accroît la prolifération des contrats interentreprises comme moyens pour saisir des opportunités de développement d'activité sur le plan national ou international.

2.1.2 Apports et limites des techniques d'évaluation du risque

La revue de la littérature montre plusieurs techniques et concepts liés à l'identification, l'évaluation et l'estimation du risque et qui peuvent se différencier selon un point de vue réductionniste ou holistique.

Les apports de cette revue de la littérature se situent essentiellement au niveau de l'importance d'assigner une probabilité lors des phases d'identification, d'évaluation et d'estimation du risque. Cette probabilité concerne aussi bien la réalisation d'une action que la relation de cette action avec les autres éléments d'analyse. De ce point de vue, la méthode d'évaluation du risque doit être holistique et reconnaître l'influence des facteurs internes et externes au système étudié. Les relations probabilistes sont de plus en plus importantes à prendre en considération face à l'incertitude et aux changements de diverses natures de l'environnement externe ainsi que la difficulté de traiter des problèmes flous ou difficilement structurables.

Les limites des différentes techniques présentées dans cette revue de la littérature se situent principalement au niveau de la non spécification de la **nature des informations** utilisées pour l'identification et l'évaluation du risque. Certaines techniques se basent sur l'utilisation des bases de données constituées par des statistiques et des informations quantitatives. Le traitement de ces informations est, dans la plupart des cas, assisté par ordinateur. Seulement la technologie « ne peut pas se substituer à l'intelligence humaine lorsque l'interprétation, les

savoirs tacites, et peut être aussi l'intuition, sont au cœur des raisonnements » (Lesca N., 2003).

Ces informations n'ont pas de caractère anticipatif, les auteurs parlent même d'informations « historiques ». On peut se demander si de telles informations sont appropriées pour faire des anticipations autres que des projections qui reproduisent le passé dans le futur. Pour ce qui nous concerne, ce n'est pas ce type d'information qui retiendra notre attention dans la suite de ce travail.

Notre intérêt est tourné vers les informations à caractère anticipatif de **type signal et/ou signe faible** de nature à permettre, sous réserve d'être correctement interprétées, de détecter un risque pour l'entreprise et dont le traitement requiert un processus de création collective de sens.

Notre position est située dans une approche proactive et anticipative pour réduire le risque. Notre recherche porte sur un risque particulier encouru par l'entreprise : le **risque numérique** engendré par l'usage de l'Internet.

2.2 Apports et insuffisances des méthodes de traitement des informations de type signal et/ou signe faible

Le traitement des informations sur l'environnement s'apparente à une activité de « *sensemaking* » (Feldman, 1989 ; Weick, 1995), à de l'interprétation (Daft and Weick, 1984 ; Smircich et Stubbart, 1985 ; Koenig, 1996) et qui fait appel à un processus de créativité (Winkler, 1982 ; Fontenot, 1993) afin de créer des possibilités d'action pour l'entreprise (Choo, 2001; Ashmos et Nathan, 2002).

Cependant, des études (Caron-Fasan, 1997 ; Lesca, 2001, par exemple) ont signalé un vide dans les méthodes à mettre en œuvre ainsi que dans les techniques à utiliser pour le traitement des informations de type signal et/ou signe faible à cause notamment de la difficulté de cette opération étant donné la nature des informations de type signal et/ou signe faible.

Nous nous référons, dans cette section, aux apports des cartes causales qui présentent certaines fonctionnalités intéressantes lors du traitement des informations dans une optique de

construction de représentations signifiantes de l'environnement. De même, le modèle conceptuel du processus d'intelligence collective (Lesca et Caron-Fasan, 1995 ; Blanco *et al.* 2003) présente un intérêt particulier par rapport à notre question de recherche en apportant des éléments de réponse qui peuvent être intégrés dans notre conception et construction de la méthode proposée.

2.2.1 Définitions et caractéristiques des cartes causales

Huff (1990) a identifié cinq familles génériques de cartes cognitives. Parmi les cartes cognitives les plus intéressantes et les plus utilisées, figurent les cartes de causalité ou causales. Les recherches sur les cartes cognitives constituent un point de départ important pour la conception d'une méthodologie adaptée à l'étude des processus cognitifs.

Etant donné que la construction de sens est un processus cognitif, il est essentiel de s'interroger sur la pertinence de la cartographie cognitive comme outil pour l'étude des processus cognitifs de construction du sens à partir des informations de la veille anticipative stratégique. Nous focalisons notre recherche sur l'étude de l'opportunité de l'utilisation des cartes causales dans l'activité de construction de sens.

Les cartes causales offrent une base théorique pour représenter plusieurs perspectives en matière de prise de décision et une aide, pour un individu ou les membres d'un groupe, pour interpréter et organiser leur environnement tout en facilitant la communication et la négociation de leurs idées. Dans le cas d'un groupe, le raisonnement de type causal permet de prévoir certains événements, expliquer des événements passés, prendre une décision, analyser et expliquer les différentes représentations des membres d'un groupe (Chaib-draa, 2002).

Dans le domaine d'aide à la prise de décision, la représentation cognitive est un élément déterminant dans les choix et les actions des preneurs de décision (Fiol et Huff, 1992).

En effet, une carte se présente comme étant un réseau constitué de nœuds et de liens (Eden, 1989), un agrégat d'informations inter-reliées (O'Keefe et Nadel, 1978), un ensemble de concepts et de relations (Laroche et Nioche, 1994) permettant la représentation visuelle et holistique de la perception des faits et de leur contexte. Les nœuds qualifiés par Komocar (1994) par les objets de la pensée peuvent également désigner des événements ou des concepts employés par un individu pour construire une représentation d'une certaine situation

sociale. Les nœuds peuvent être soit des variables traduisant l'idée que se fait le sujet d'un phénomène donné et la façon dont il l'exprime, soit des construits définis à priori par le chercheur (Komocar, 1985; Jenkins, 1994).

Par ailleurs, les cartes causales impliquent des relations de cause à effet et permettent de relier différents éléments cognitifs par des liens de causalité (Huff, 1990 ; Barr et al., 1992). Elles permettent de décrire les liens entre les informations et de les interpréter (Narayan et Fahey, 1990), elles sont utilisées surtout comme un moyen de prédiction des événements futurs (Huff, 1990).

Le point fort des cartes causales réside dans la possibilité de représenter les concepts et les relations entre eux par un graphe orienté donnant une vue globale du processus cognitif d'un individu, ou d'un groupe d'individus, en permettant une meilleure représentation des informations. La représentation graphique permet aussi d'identifier un manque d'information ou démontrer l'intérêt à regarder certaines informations en particulier (Fiol et Huff, 1992). De même, le graphe peut être transposé sous la forme d'une matrice.

Trois relations fondamentales caractérisent les cartes causales. Il s'agit des :

- relations positives désignées par {+} indiquent un effet positif entre deux concepts.
- relations négatives désignées par {-} indiquent un effet négatif entre deux concepts
- relations nulles désignées par {0} indiquent aucun effet entre deux concepts.

Un ensemble plus complet de relations causales se présente sous la forme de huit valeurs résultantes de toutes les combinaisons logiques possibles du positif, du négatif et de zéro : {+, -, 0, \oplus , \ominus , \pm , ?, a}(Axelord, 1976 ; Nakumara et al., 1982 ; Buede et Ferrell, 1993).

où :

- \oplus non négatif {0, +}
- \ominus non positif {0, -}
- \pm non zéro {+, -}
- ? universel {+, -, 0}
- a ambivalent, ensemble vide ; lorsque deux (ou plus) affirmations sont en conflit

Ces relations sont issues de quatre opérations mathématiques de base nécessaires pour manipuler les cartes causales qui sont : l'addition (l), la multiplication (*), l'intersection (\cap) et

l'union (U). Ces différentes opérations mathématiques soutiennent le calcul matriciel des cartes causales.

2.2.2 Limites des cartes causales par rapport à notre question de recherche

Les cartes causales fournissent une première réponse au besoin d'outils de représentation et de formalisation des structures et des processus cognitifs.

Les cartes causales constituent un outil d'aide à l'interprétation des informations et de prédiction des événements futurs mais leur construction est basée sur des informations **rétrospectives et disponibles**, alors que dans le domaine de la veille anticipative stratégique les raisonnements reposent sur des **informations incomplètes, fragmentaires, ambiguës et incertaines** (Caron-Fasan, 1997).

De plus, elles sont limitées à des liens de causalité qui déterminent la nature des chemins de raisonnements. Ceci est de nature à ne pas permettre une véritable analyse et une représentation des situations qui se caractérisent par une multiplicité de variables et une abondance de relations entre elles, ainsi que par une multitude de boucles (Steinbruner, 1974 ; Axelrod, 1976 ; Weick, 1979).

Conscients de la nécessité de créer de nouveaux liens et codes, à cause de la diversité des raisonnements (Fletcher et Huff, 1990), **notre apport** se situe au niveau de la conception d'une méthode qui tient compte de la probabilité de la relation entre deux concepts pour faire face à l'incertitude, ajouter des relations de dépendance entre informations disponibles ou actions à entreprendre, et fournir des nouvelles opérations pour manipuler les approximations entre les informations. L'enrichissement de la typologie des liens est très important à cause de la complexité et de la diversité des raisonnements. Les liens approchés, sémantiques, et probabilistes sont utiles pour supporter un processus de construction de sens.

Notre apport se situe encore au niveau de l'intégration de **la variable temps** comme étant une composante principale de raisonnement et d'analyse. Les liens doivent être dynamiques et adaptatifs en fonction d'un certain nombre de paramètres non figés pour tenir compte du contexte temporel, de l'évolution des problèmes traités et de l'interprétation suite à de nouvelles informations sur l'environnement ou suite à l'évolution des contraintes imposées à l'entreprise.

Par ailleurs, la technique de la carte causale ne permet pas d'appréhender le processus de construction de sens dans sa continuité qui apparaît comme une suite continue de cartes causales qu'il est important de mémoriser chacun de ses états transitoires (Lesca, N. 2000)

Dans ce cadre, nous ambitionnons de concevoir et de mettre en œuvre un outil adapté à l'étude des processus cognitifs relatifs au contexte de la veille anticipative stratégique et de construction du sens à partir des informations de type signal et/ou signe faible. Cet outil exploite principalement les potentialités offertes par la **technologie Internet** et l'intelligence collective.

2.2.3 Traitement des informations de type signal et/ou signe faible au moyen d'un processus mettant en œuvre l'intelligence collective

Le modèle conceptuel de (Lesca et Caron-fasan, 1995 ; Blanco *et al.* 2003) montre trois phases importantes à suivre pour créer du sens à partir d'informations fragmentaires, incomplètes, incertaines et ambiguës.

En premier lieu, il est important de regrouper les informations suivant certains thèmes afin d'améliorer les possibilités de recoupement et de classement des nouvelles informations. Ensuite, la création de liens significatifs entre les informations appartenant au même groupe ou à des groupes différents. La troisième phase consiste à laisser une trace des raisonnements utilisés. Ces trois phases soutiennent le processus d'intelligence collective au sein de l'entreprise afin d'améliorer sa réactivité et sa capacité d'anticipation.

S'agissant de la première phase, le regroupement des informations permet d'avoir un stock informationnel plus riche, plus synthétique et plus générique. Le classement d'une nouvelle information dans un regroupement déjà existant autour d'un thème se fait, généralement, selon trois types de critères :

- Critère de similitude : les informations peuvent être regroupées par similitude lorsqu'elles expriment la même idée ou lorsqu'elles traitent d'un même thème (Weber, 1984 ; Conklin, 1987 ; Moles, 1990).
- Critère de proximité : qui signifie que l'information est proche du thème auquel on va la rattacher comme le fait d'avoir une caractéristique commune (Moles, 1990) par exemple.

- Critère d’analogie : les informations peuvent être regroupées par analogie (directe ou symbolique) lorsqu’elles sont associées sur la base de ressemblances constatées (Hofbauer *et al.*, 1994).

La phase de création collective de sens fait intervenir plusieurs acteurs (experts, responsables de l’entreprise) et suppose leur capacité à créer et à manipuler des liens de raisonnement entre informations éparses stockées à un moment donné et sélectionnées (Lesca, H. et Caron, M-L. 1995) afin de créer des champs possibles pour l’action ultérieure des opérationnels.

Les liens proposés par le modèle sont des liens de confirmation, des liens de contradiction, et des liens de causalité. Ces mêmes liens peuvent être également de nature hypothétique demandant à être validés ou invalidés au cours du processus d’amplification des informations.

La création et la manipulation des liens entre les informations peuvent être induites :

- soit d’une façon automatique suite à une consultation de la base des connaissances et à travers des interactions de mémoires individuelles et collectives,
- soit par des raisonnements collectifs et créatifs sur les liens.

Par métaphore, ce processus peut être comparé à un jeu de puzzle consistant à regrouper des pièces incomplètes et en désordre, avec la différence cependant qu’il ne s’agit pas de reconstituer quelque chose qui existerait déjà et que certaines pièces peuvent manquer. L’output de la co-construction du puzzle dépend de la capacité des acteurs d’ajouter du sens aux informations incomplètes, fragmentaires et incertaines en utilisant leurs connaissances **tacites**. Le rôle de l’animateur du groupe de travail est central dans ce processus d’intelligence collective qui consiste à faire converger les points de vue des participants au cours d’une séance de création de sens.

La troisième phase du processus d’intelligence collective prévoit de laisser une **trace** des raisonnements utilisés. Cette phase est nécessaire pour alimenter un processus d’**apprentissage** collectif au sein de l’entreprise.

2.2.4 Insuffisances constatées par rapport à notre question de recherche

Le modèle conceptuel de (Lesca et Caron-Fasan, 1995 ; Blanco *et al.*, 2003) apparaît se baser sur des liens statiques qui ne prennent pas en considération plusieurs aspects importants, dans

notre contexte de recherche. Le raisonnement dans ce modèle conceptuel apparaît comme étant un processus collectif, dans lequel la prise de décision est basée sur une vue établie à la fin de la première phase et analysée par intelligence collective durant la deuxième phase. Cependant, la complexité et la diversité des événements externes requièrent une formulation dynamique des liens et l'établissement de variables paramètres dépendant du temps et du contexte. En effet, le processus d'interprétation est dynamique (Drazin et al., 1999), et le travail d'une équipe de « *sensemaking* » (Ashmos et Nathan, 2002) est plutôt continu et dynamique.

Ainsi, les facteurs « temps » et « contexte organisationnel » doivent être explicitement incorporés au modèle conceptuel pour permettre une interprétation collectivement acceptable. La prise en considération de la **variable temps** dans un modèle devrait permettre de proposer une théorie de création de sens, et probablement des décisions plus robustes; et dans laquelle l'intelligence collective continue de jouer un rôle important.

De plus, la création de sens devrait intégrer un raisonnement non linéaire, ainsi que c'est déjà le cas dans le modèle Lesca, Caron Blanco, essentiellement lorsque le groupe d'intelligence collective est face à des situations difficilement structurables, avec un degré élevé d'ambiguïté des informations et/ou des informations incomplètes.

Pour ces raisons, les liens doivent intégrer explicitement l'**approximation**, la nature incomplète des informations, la probabilité au raisonnement. De plus, ce raisonnement doit être itératif pour permettre des approximations successives. Nous proposons une extension de du modèle Lesca et Caron-Fasan (1995) et Blanco *et al.*, (2003), composé également par trois phases, pour amplifier les signaux et/ou signes faibles détectés, les interpréter et répondre d'une façon appropriée au risque d'agression numérique.

Le modèle conceptuel que nous proposons a pour objectif de soutenir la prise de décision collective pour répondre au risque d'agression numérique en assurant une optimisation des moyens en termes de coûts, et de temps. La prise de décision collective requiert d'organiser et de **formaliser la fonction de médiation** qui apparaît sans une méthodologie explicite appropriée dans le modèle de Lesca et Caron-Fasan (1995) et Blanco *et al.*, (2003).

Notre recherche vise à satisfaire ces besoins de formalisation, d'organisation et d'assistance tout en gardant au médiateur un rôle central. L'ajout d'heuristiques apparaît comme un

possible outil de convergence (et de formalisme) pour supporter la prise de décision collective dans le domaine qui nous concerne ici.

En effet, notre apport se situe aussi au niveau de la construction d'une carte cognitive collective ou de groupe et la conception et la mise en place d'un mécanisme de médiation à travers des heuristiques et des règles de travail pour faire converger des points de vue différents. Notre approche constitue dans ce cadre une extension du travail développé par (Chaib-draa, 2002) sur la fonction de médiation dans la prise de décision collective, ainsi que de la méthode *LESCanning*® (2003).

Ainsi, nous ambitionnons un enrichissement de la typologie des liens par rapport aux cartes causales et une conceptualisation, appropriée à notre contexte, de la fonction de médiation dans le processus de prise de décision collective.

2.3 État des pratiques dans les entreprises, à l'échelon international et d'après les rapports disponibles

La sécurité des ressources informationnelles/du système d'information d'une entreprise est devenue un élément vital pour le développement et la pérennisation de son activité avec l'évolution notable de son contexte économique et technologique, notamment la forte évolution de l'informatique et de l'Internet ainsi que de leurs usages. Le besoin de l'entreprise de demeurer ouverte à ses employés, à ses partenaires et à ses clients l'expose à des menaces et à des agressions qui ne cessent de se multiplier et dont les conséquences tangibles et intangibles sont néfastes.

Les entreprises mettent en place des politiques de sécurité pour réduire le risque à un niveau acceptable par l'utilisation des solutions de sécurité adaptées à leurs besoins et en fonction des caractéristiques de leurs services offerts. La mise en place suppose l'utilisation de méthodes et de techniques pour réaliser une détection et une analyse du risque afin de choisir par conséquent des solutions et des pratiques appropriées en matière de sécurité. C'est dans ce cadre que la composition d'une ERI apparaît comme étant une solution complémentaire et adoptée de plus en plus par les entreprises.

2.3.1 Etude du risque encouru par une entreprise en cas d'agressions numériques

La mise en place d'une politique de sécurité efficace et appropriée nécessite l'étude préalable du risque afin d'optimiser les investissements en matière de solutions et de mesures de sécurité.

En effet, **la sécurité absolue n'existe pas en soi** d'où la nécessité d'évaluer l'opportunité d'investir en fonction de l'importance des informations à protéger et en fonction de la probabilité de l'occurrence d'une agression, tout en se concentrant sur la réduction du risque en optimisant les coûts. Ainsi, l'entreprise détermine le niveau de risque qu'elle est prête à accepter sur ses ressources en comparaison avec le coût induit par les menaces qu'elle encourt (Brenton et Hunt, 2003 ; Llorens et Levier, 2003).

L'analyse du risque s'impose et permet d'identifier les informations, les plus importantes et critiques de l'entreprise, à protéger ainsi que de déterminer les conséquences, les menaces et les vulnérabilités du système d'information. Les éléments qui doivent être considérés dans la gestion des risques sont les suivants :

- l'identification des menaces qui peuvent affecter les ressources critiques qui doivent être classées selon un ordre d'importance,
- l'estimation de la probabilité de l'occurrence de ces menaces, en se basant par exemple sur des données historiques collectées par l'entreprise et sur les appréciations de certains experts dans le domaine de la sécurité informatique,
- l'estimation de la perte potentielle relative à chaque ressource en cas de réalisation de la menace,
- l'estimation du coût des actions d'audit et de surveillance des systèmes afin de réduire le risque. Ces actions peuvent concerner l'implantation de nouvelles politiques de sécurité, des mesures préventives ou la réalisation de contrôles techniques ou physiques.

Ainsi, l'analyse du risque évalue la relation entre la gravité de l'agression, la fréquence ou la probabilité de son occurrence et le coût de l'implémentation des mécanismes de protection appropriés (Hassler, 2001). La gravité peut être mesurée par les coûts de réparation des dommages occasionnés par une agression réalisée, notamment en termes de temps perdu entre le chômage technique et la réparation des systèmes impactés. De ce fait, plus l'agression est

grave et susceptible de se reproduire souvent, plus les coûts de couverture des dégâts seront élevés et plus l'implémentation d'une protection appropriée est nécessaire.

Sur un plan pratique, les entreprises peuvent recourir à la sous-traitance à travers la réalisation d'un audit externe, comme elles peuvent mobiliser du personnel interne assisté par des outils et des techniques d'analyse et de gestion de risque.

Plusieurs approches de gestion de risque ont été développées pour assister les entreprises. Parmi ces outils de gestion de risque figure la **méthode OCTAVE[®]** (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) développée par le SEI (*Software Engineering Institute*) avec la collaboration de CMU (Carnegie Mellon University), la **méthode MEHARI** (MEthode Harmonisée d'Analyse de Risque Informatique) développée par le CLUSIF et la **méthode NETRAM[©]** (Network Risk Analysis Method) développée par le laboratoire de recherche tunisien CN&S (Communication Network & Security) pour les besoins de l'Agence Nationale de Certification Electronique (l'ANCE).

La méthode OCTAVE[®] peut être utilisée par des petites ou grandes entreprises et se base sur un ensemble d'activités agencées selon trois phases permettant l'identification et la gestion de risque afin de mettre en place une stratégie de sécurité (Alberts et Dorofee, 2003). L'évaluation des risques selon cette méthode se focalise sur les pertes qu'ils engendrent en considérant qu'ils sont équiprobables et qu'ils ne diffèrent que par leur impact.

La première phase inclut un examen des menaces pesant sur les ressources de l'entreprise afin de situer les failles procédurales. La deuxième phase comprend une étude des vulnérabilités des ressources utilisées. Dans la troisième phase, la stratégie et la politique de sécurité sont élaborées. Chaque phase est détaillée selon un ensemble de processus.

Le **point faible** de cette méthode est l'absence de la gestion des imprévus, qui représente une activité essentielle afin de prendre des mesures de sécurité convenables en cas d'agression avant d'étudier l'origine du problème. Ceci est lié entre autre à l'absence de mécanismes de surveillance continue du système d'information.

La méthode MEHARI est utilisée pour classer les informations et les ressources du système d'information, réaliser des audits de sécurité, analyser le risque lors du développement d'une nouvelle application de sécurité. Cette méthode comprend des guides, des bases de connaissances et des processus d'évaluation quantitative et décrit le risque suivant un scénario selon lequel elle précise qui attaque quoi et comment. Ainsi, les risques sont classés selon deux paramètres à savoir la potentialité et l'impact.

La méthode NETRAM© tient compte de certaines insuffisances constatées dans les deux méthodes précédentes et propose un ensemble cohérent et automatisé de tâches organisées selon dix processus. L'apport de la méthode NETRAM© réside dans l'ajout de quatre nouveaux processus par rapport aux autres méthodes (Hamdi, *et al.*, 2003). Ces nouveaux processus concernent la proposition d'une gamme de contre-mesures pour chaque scénario de risque, le monitoring (la surveillance continue), le calcul de l'effort de sécurisation des systèmes d'information, et la réponse aux incidents.

Pour chacun de ces processus, la méthode NETRAM© offre des outils plus appropriés pour mieux gérer les imprévus, comparer les scénarios de risque selon plusieurs critères, et estimer la durée et le coût de sécurisation d'un système d'information. Cette méthode précise également le nombre d'intervenants qui peuvent être engagés dans le processus d'analyse de risque.

L'adoption d'une approche ou d'une autre de gestion de risque s'avère d'une extrême importance comme étant une phase préparatoire à la mise en place d'une politique de sécurité. Cette gestion de risque est une activité continue en fonction de l'évolution de l'activité de l'entreprise et en prenant en considération les décisions stratégiques de diversification des services *on line* et les choix technologiques de support.

Ces méthodes présentent l'intérêt d'aider à effectuer un audit pour identifier les vulnérabilités d'une entreprise à l'égard du risque numérique. En revanche, au regard de notre question de recherche elles n'apportent **pas de connaissances actionnables** répondant à notre question de recherche concernant l'anticipation des risques numériques et/ou de la réduction du temps de réponse aux menaces ou agressions.

2.3.2 Définition d'une politique de sécurité face au risque numérique

La définition d'une politique de sécurité vise tout à la fois à définir les besoins de l'entreprise, à élaborer des stratégies de sécurité afin de protéger les biens les plus critiques et à définir le référentiel des contrôles de sécurité (Llorens et Levier, 2003).

La mise en place d'une politique de sécurité découle de l'analyse du risque. La politique de sécurité tient compte de la taille de l'entreprise, de la nature et de ses besoins d'activité, du

degré d'ouverture du réseau de l'entreprise et de l'organisation de ses services. Elle prend en compte aussi les contraintes stratégiques et opérationnelles de l'entreprise et les coûts générés par la sécurité comparés aux gains de sécurité engendrés.

De ce point de vue, la politique de sécurité fait partie intégrante de la stratégie globale de l'entreprise dans la mesure où la stratégie de l'entreprise détermine les objectifs de la politique de sécurité. Par exemple, les choix stratégiques en matière d'adoption du **commerce électronique**, ou les besoins d'interconnexions réseau entre les différents sites géographiques de l'entreprise, ou avec les fournisseurs, sont autant de facteurs qui doivent être intégrés dans la politique de sécurité.

La politique de sécurité est constituée d'une suite de règles et de principes répondant aux besoins de sécurité de l'entreprise et explicités dans un document écrit. Elle comprend des documents et des guides décrivant de manière formelle les principes ou les règles auxquels se conforment les personnes qui ont le droit d'accès au système d'information de l'entreprise. Elle est également décrite selon un certain nombre de procédures à caractère opérationnel et technique et explicitant d'une manière concise les étapes à suivre pour atteindre un objectif de sécurité donné.

Une politique de sécurité comprend trois bases : la prévention, la détection et la réponse (Canavan, 2001). La prévention consiste à implémenter des mesures nécessaires et suffisamment décourageantes pour limiter l'exploitation des vulnérabilités du réseau de l'entreprise. La détection implique la mise en place d'un ensemble de procédures pour identifier des problèmes potentiels. Plus la détection est rapide plus la correction et la réponse seraient faciles. La réponse est développée au sein d'un plan approprié qui spécifie les actions à entreprendre et les responsabilités.

Une politique de sécurité doit couvrir les éléments relatifs à la sécurité de l'infrastructure (la sécurité logique et physique des équipements et des connexions réseau, aussi bien internes que celles fournies par des fournisseurs réseau), la sécurité des accès (la sécurité logique des accès locaux et distants des ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès au système d'information de l'entreprise) et la sécurité du réseau intranet face à Internet ou aux tierces parties (la sécurité logique des accès aux ressources de l'entreprise par Extranet et l'accès aux ressources extérieures via Internet).

En conséquence, la prévention et la détection dans le cadre d'une politique de sécurité supposent l'implémentation des mécanismes appropriés de détection, d'exploitation et de

supervision permanents des **signes** d'intrusions ou des tentatives d'intrusion contre les ressources les plus critiques à protéger pour évaluer en temps réel les vulnérabilités, et contrôler d'une façon permanente l'intégrité des services offerts en ligne par l'équipe de sécurité (ERI éventuellement) au sein d'une entreprise.

Afin de maintenir un niveau continu de vigilance, il est important de prendre des actions appropriées pour découvrir et détecter des activités non autorisées, inattendues ou suspectes. L'identification **précoce** de ces activités est une condition nécessaire pour protéger le système d'information d'autant plus qu'elles peuvent réapparaître et présenter un risque considérable dans le futur. Dans ce cadre, il est indispensable de stocker les données relatives à ces actions anormales ou suspectes pour pouvoir les utiliser ensuite pour comprendre plus rapidement et plus précisément des nouvelles agressions, ainsi que pour investiguer des agressions inconnues.

Si les **signes** liés à la détection des intrusions, ou des tentatives d'intrusion, ne sont pas collectés et étudiés, il est impossible de déterminer les violations ou les infractions contre l'intégrité, la disponibilité ou la confidentialité des informations critiques.

L'incapacité de détecter ou d'identifier ces signes à temps est due à l'absence de mécanismes d'**alerte précoce** nécessaires et des procédures d'étude, à l'absence d'un état d'information attendu pour le comparer à l'état actuel opérationnel. Les différences entre l'état attendu et l'état actuel peuvent fournir une indication sur l'occurrence d'une intrusion. L'incapacité de détecter les intrusions ne permet de déterminer ni l'ampleur de l'intrusion ni les dommages occasionnés. Le temps de réparation augmente et l'entreprise peut perdre des opportunités d'affaires et même de remettre en cause sa réputation.

Ainsi, la mise en place de politiques et de procédures de détection de signes permet de limiter l'exposition de l'entreprise à un risque d'intrusion et les dommages possibles d'une telle agression.

De plus, la politique de sécurité doit spécifier les actions à entreprendre, suite à la découverte des activités anormales, inattendues ou suspicieuses, exiger que les actions prescrites soient habituellement exécutées, identifier les responsabilités et les autorités des administrateurs du système ou du personnel de sécurité pour exécuter les actions prescrites.

Tout comme l'analyse de risque, la politique de sécurité doit évoluer au fur et à mesure de la croissance de l'entreprise (son implantation géographique) ou de ses choix stratégiques (son développement à l'international) ou technologiques (extension de son réseau local, interconnexion de sites distants par VPN).

L'élaboration d'une politique de sécurité et sa mise en œuvre sont loin d'être un exercice facile pour les entreprises. Le rapport annuel 2002 de CLUSIF montre que **64% des entreprises n'ont toujours pas défini de politique de sécurité des systèmes d'information** ce qui est fort inquiétant vu la dépendance de plus en plus forte de ces systèmes et leur ouverture **sur le réseau Internet** en progression.

2.3.3 Choix des solutions de sécurité, suite à la politique de sécurité retenue

Le choix d'une solution de sécurité est en interdépendance avec les exigences explicitées dans le cadre de la politique de sécurité. De nombreux outils techniques et complémentaires peuvent être utilisés en parallèle, en fonction des objectifs de sécurité fixés.

En se référant au rapport CSI/FBI (Richardson, 2003), les entreprises participant à l'étude utilisent des équipements hardware et software qui analysent les flux d'information entrant et sortant. Les résultats montrent une grande utilisation des logiciels antivirus, des *firewalls*, des systèmes de contrôle d'accès et de la sécurité physique (la sécurité physique consiste essentiellement à se protéger contre les vols, les incendies, les coupures d'électricité, etc).

A un niveau moins important, les entreprises interrogées emploient un système de détection d'intrusion (et des tentatives d'intrusion) qui est réparti au niveau des services informatiques, des systèmes d'autorisation et d'authentification. Le système de détection d'intrusion est un système d'alerte qui permet la surveillance du trafic réseau en temps réel et l'identification de toute anomalie ainsi que l'arrêt immédiat des activités non autorisées. Les entreprises emploient également la technique de cryptographie et des mots de passe.

Le tableau suivant expose les solutions de sécurité les plus fréquemment adoptées par les entreprises qui ont participé à l'étude réalisée par le CSI/FBI entre 2000 et 2004.

Principaux Moyens de sécurité utilisés	Pourcentage des entreprises en 2000	Pourcentage des entreprises en 2001	Pourcentage des entreprises en 2002	Pourcentage des entreprises en 2003	Pourcentage des entreprises en 2004
<i>Firewalls</i>	78	95	89	98	98
Antivirus	100	98	90	99	99
Contrôle d'accès	92	90	82	92	71
Sécurité physique	90	92	84	91	-
Détection d'intrusion	50	61	60	73	68

Tableau 7 : Principaux moyens de sécurité employés entre 2000-2004

Une étude similaire réalisée en 2003 en Australie sur plus de 200 entreprises révèle les mêmes pratiques avec :

- le recours au antivirus qui est préconisé par 98% des entreprises interrogées
- l'installation des *firewalls* qui est adoptée par 95% des entreprises interrogées
- le contrôle d'accès qui est réalisé par 93% des entreprises interrogées
- le système de détection d'intrusion par 45%

De même, le rapport du CLUSIF de 2002 marque également les mêmes tendances avec l'utilisation au premier rang des solutions antivirus, puis par ordre décroissant les techniques des mots de passe, les pare-feux, le système de détection d'intrusion, les moyens d'authentification renforcée et le chiffrement de données. Les entreprises françaises qui ont participé à cette étude emploient également des moyens de plus en plus importants pour renforcer la sécurité physique.

Ce qu'il faut signaler c'est que les mesures de sécurité doivent être sans cesse révisées et actualisées pour s'assurer de leur conformité avec la protection requise au bon fonctionnement du système d'information et pour tenir compte des avancées technologiques ainsi que de la multiplicité des vulnérabilités et des menaces.

Ces constatations autour de l'utilisation des solutions techniques et physiques de sécurité donnent lieu à trois remarques importantes.

La première remarque dérive de la comparaison entre le tableau des principaux moyens de sécurité utilisés entre 2000 et 2003 et le tableau mentionné au premier chapitre, relatif aux types d'agressions numériques les plus rencontrées pendant la même période. Cette comparaison montre une **corrélation négative** entre l'utilisation massive des antivirus et des firewalls et les agressions par virus ou à travers la pénétration du système d'information de l'extérieur qui sont les agressions les plus rencontrées par les entreprises. Les entreprises installent de plus en plus des antivirus et des *firewalls* mais elles sont de plus en plus attaquées par des virus. Cet état des faits est également confirmé dans le cas des études récentes réalisées en Australie ou en France.

Ceci s'explique principalement par l'augmentation de la perméabilité des *firewalls* suite à une évolution des protocoles et objets utilisés sur Internet ainsi que par le fait que les antivirus installés sont efficaces pour stopper des virus déjà programmés alors que les réseaux sont attaqués par des virus de plus en plus sophistiqués et de type **inconnu**. De plus, les mises à jour permanentes des bases de signatures des virus confirment que la détection des virus est loin d'être prévisible (Llorens et Levier, 2003).

La deuxième remarque est reliée à l'implémentation de plus en plus préconisée par les entreprises des systèmes de détection d'intrusion et des tentatives d'intrusion et qui s'avère également insuffisante vu le nombre élevé des agressions liées au vol d'informations et qui représentent les agressions dont les conséquences sont les plus coûteuses et les plus néfastes. En effet, l'efficacité d'une telle implémentation est conditionnée par un effort de sélection, de traitement et d'analyse des informations captées ou des **signes précoces** "*early warning*" relatives à des intrusions ou à des tentatives d'intrusion.

La détection suppose l'implémentation de capteurs des signes d'intrusion ou des tentatives d'intrusions qui nécessitent par la suite un traitement et une analyse pour y répondre d'une façon adéquate. La détection des signes nécessite la présence d'une équipe capable d'interpréter, d'analyser et de traiter ces signes car la seule implémentation des outils et techniques software et hardware est insuffisante.

Ceci peut illustrer en grande partie l'opportunité d'investir dans une solution complémentaire à savoir la constitution d'une ERI selon une approche de sécurité à plusieurs niveaux.

La composition d'une ERI s'avère une solution nécessaire et complémentaire à l'analyse de risque, la définition d'une politique de sécurité et l'implémentation d'un ensemble de solutions techniques et physiques.

En effet, dans plusieurs cas d'observation d'une indication initiale d'un comportement suspect, les responsables de sécurité manquent d'informations pour déterminer ce qui se produit et évaluer la situation de sécurité. Il est important dans ce cas de voir les occurrences passées d'un comportement similaire et étudier les résultats de cette investigation. L'investigation consiste à formuler et à poser des questions différentes pour mieux identifier les données qui peuvent mieux révéler ce qui se passe. Par conséquent, il est opportun de modifier la configuration des mécanismes de sélection et de collecte des **signes** afin de collecter des informations complémentaires, mieux filtrer et sélectionner les données existantes. Il est également possible d'ajouter de nouveaux mécanismes pour collecter des signes d'intrusion ou des tentatives d'intrusion.

La troisième remarque découle des deux précédentes et consiste à reconnaître le caractère éventuellement itératif de l'analyse et de l'investigation des agressions numériques, ce qui nécessite une véritable intelligence au sein de la fonction de sécurité dans l'entreprise et requiert un processus d'apprentissage délibérément organisé. Ceci nécessite une **intervention humaine** qui nous amène à parler des équipes ERI.

2.3.4 La mise en place d'une ERI

Dans la plupart des cas, les agressions numériques sont de plus en plus complexes et **inhabituables**. Les hackers recherchent toujours de nouvelles façons et développent des programmes sophistiqués pour s'introduire rapidement dans un système d'information. Même en cas d'implémentation des mesures de protection et de sécurité, il est essentiel de surveiller de près les ressources en informations et les transactions faites sur ces ressources afin de détecter des signes d'intrusion ou des tentatives d'intrusion. La surveillance peut être compliquée car les hackers cachent souvent ou camouflent leurs manœuvres en changeant les moyens d'introduction au système d'information.

En effet, une intrusion peut avoir déjà lieu sans qu'on puisse s'en apercevoir car l'état du système paraît opérer normalement. Dans ce cas, il serait difficile et même impossible de

déterminer plus tard si le système a été compromis ou d'évaluer les conséquences d'une telle agression.

Les vulnérabilités des réseaux, l'accroissement des agressions et des menaces montrent clairement que le niveau de sécurité informatique est bien en deçà de ce qu'il devrait être et témoignent de l'insuffisance des solutions et de l'infrastructure techniques pour protéger les ressources informationnelles critiques de l'entreprise.

En effet, il est important d'identifier et de collecter les données qui caractérisent le système d'information (telles que les données générées par le réseau, les applications et les activités des utilisateurs) dans le but d'aider à la détection des **signes** des comportements suspects. A cet effet, l'implémentation des mécanismes de collecte et de surveillance des signes d'intrusion ou des tentatives d'intrusion pour enregistrer les données et les traiter est essentielle afin de maintenir un état d'**alerte continue**.

Ainsi, les ERI collectent des informations relatives à des incidents de sécurité, des faiblesses et/ou des vulnérabilités software du système. Ces informations sont très importantes pour évaluer, gérer et réduire le risque encouru par l'entreprise en cas d'agression numérique.

De ce point de vue, le travail des ERI s'intègre dans un processus de *business intelligence* devant permettre à l'entreprise une réduction du risque ainsi qu'une réaction rapide et appropriée (Killcrece *et al.*, 2003). Selon ces auteurs, ce processus de *business intelligence* suppose également la détection, la recherche et la création collective de liens entre des informations relatives à des alertes précoces et des problèmes potentiels de sécurité. Ces informations sont de nature anticipative « *early warning* » dont l'interprétation est susceptible de réduire le risque et de minimiser les coûts de réparation. Cette opération collective (« *this also allows the CIRT to link together events that may not have been seen to be related when looked at individually* » p.12 Killcrece *et al.*, 2003) de création de liens est très importante selon ces auteurs car certaines informations détectées individuellement ne peuvent avoir de la signification qu'à travers un traitement et une interaction collectifs. Les auteurs mettent l'accent également sur la nécessité de partager et de communiquer l'information à l'interne de l'entreprise avec d'autres départements et à l'externe avec d'autres équipes pour échanger et enrichir les expériences mutuelles.

En outre, il est également indispensable d'archiver, d'une façon structurée et réutilisable, les informations liées à des agressions numériques pour pouvoir s'en servir afin de reconnaître et

de construire des scénarios d'attaques (Moore *et al.*, 2001). Ceci est de nature à permettre, en réponse à des agressions, d'apprendre des actions réussies ou échouées et de réduire la probabilité de l'occurrence d'agressions similaires.

Ceci démontre bien le fait que le processus de détection, d'analyse et de réponse à une agression est un processus d'**apprentissage collectif**.

Dans ce cadre, les ERI offrent trois types de services (West-Brown *et al.*, 2003) :

- des services **réactifs** qui impliquent la diffusion d'informations décrivant des alertes, des mises en garde, des vulnérabilités du système d'information afin de fournir des orientations et des recommandations possibles pour améliorer le niveau de sécurité
- des services **proactifs** qui fournissent de l'information **pour anticiper** les agressions, les problèmes ou certains évènements. La performance de ces services est en relation directe avec la réduction du nombre d'attaques dans le futur.
- des services de gestion de la qualité qui ne sont pas spécifiques à un seul département mais qui concernent l'amélioration des pratiques actuelles et futures de sécurité dans toute l'entreprise.

Les services réactifs ne sont plus suffisants à cause de la rapidité et la complexité des agressions, il faut plutôt développer et gérer les services proactifs.

Cependant, l'efficacité d'une ERI dépend considérablement de sa **formation** et de ses compétences acquises dans le domaine de la sécurité. Sur une autre dimension, son efficacité est également liée aux pratiques et à l'état de la **culture de sécurité** dans l'entreprise (West-Brown *et al.*, 2003).

2.4 État des lieux : rôle et activités d'une ERI

L'ouvrage de Killcrece *et al.*, (2003) publié par le *Computer Emergency Response Team* (CERT) à l'université de Carnegie Mellon présente un intérêt particulier par rapport à l'état des pratiques dans les entreprises en ce qui concerne le travail des ERI. Cet ouvrage donne les résultats d'une étude importante, valables pour la période allant de juin 2002 jusqu'à août 2003, sur l'état des pratiques, des processus organisationnels et structurels des ERI dans 12

pays appartenant à des régions différentes (les Etats Unis, l'Europe, l'Amérique du Sud et l'Asie Pacifique) dans des entreprises opérant dans des secteurs d'activité différents (militaire, éducation, communication et information, organisations à but non lucratif, administrations publiques, commerciales,...etc.). Les principaux résultats de cette étude seront fournis dans les paragraphes suivants.

2.4.1 Aperçu historique de l'apparition des ERI

La nécessité de la création de la première ERI aux Etats-Unis a été ressentie suite à la détection d'un virus de type ver « Morris » le 2 novembre 1988, développé par un jeune étudiant de 23 ans. Ce ver autonome se propage d'un ordinateur à un autre en exploitant les vulnérabilités. À cette époque, il a infecté approximativement 10% des postes connectés à l'Internet. Les conséquences de cet incident étaient très néfastes au point que le Centre National de la Sécurité Informatique (*National Computer Security Center*) a initié une série de colloques pour discuter de la prévention et de la réponse à fournir à de tels incidents dans le futur ainsi que d'évaluer les enseignements tirés d'un tel incident.

Le problème d'origine était lié à l'**absence d'une méthode** formelle de coordination pour traiter une agression de cette catégorie et développer l'analyse et la réponse appropriées.

En reconnaissant ce problème, le CERT/Coordination Center (CERT/CC) a été créé à Carnegie Mellon University en décembre 1988. L'année suivante, plusieurs organisations ont adopté l'approche de ce centre comme le *National Aeronautics and Space Administration* (NASA) et créé leurs propres équipes.

En Août 1989, est créé le FIRST (*Forum of Incident Response and Security Teams*), qui constitue un réseau des membres enregistrés pour prévenir les incidents, partager l'information et coordonner les activités appropriées de réponse dans le cas d'une agression.

Avec l'utilisation de plus en plus répandue de l'**Internet** comme moyen de communication et de travail, le nombre des agressions ne cesse d'augmenter, la composition d'une ERI comme solution de sécurité est adoptée de plus en plus par les organisations à l'échelle internationale.

Le FIRST compte en septembre 2003, 151 organisations appartenant à plusieurs régions (l'Europe, l'Asie Pacifique, l'Amérique Latine, l'Amérique du Nord).

Aujourd'hui, il y a beaucoup de ERI qui sont opérationnelles dans le monde, et plusieurs projets sont en cours pour faciliter la coordination et le partage d'informations entre les équipes et standardiser leurs processus de travail.

2.4.2 Activités et domaines d'intervention des ERI

Les ERI sont chargées d'identifier les agressions en analysant les signaux et/ou signes faibles collectés par les systèmes de détection, afin de réduire leur impact et de prendre la décision appropriée pour protéger les ressources critiques de l'entreprise. La réaction des ERI est intégrée dans le cadre d'une politique de sécurité. Les activités les plus importantes accomplies par les ERI sont les suivantes :

1. la notification (mémorisation temporaire): chaque incident doit être identifié à temps et communiqué aux personnes concernées ou aux départements appropriés,
2. l'analyse qui détermine les causes et les conséquences de l'incident de sécurité ainsi que les éventuels liens avec les précédents incidents,
3. la réaction afin de stopper ou limiter l'impact de l'incident en tenant compte les spécificités et les contraintes de l'activité de l'entreprise. Cette réaction doit être rapide, efficace et réalisée collectivement,
4. la documentation et la traçabilité (la mémorisation): chaque incident de sécurité doit être documenté selon un format spécifique et publié des sites Web de façon d'être accessible à tout moment,
5. l'investigation qui vise la détection précoce de problèmes de sécurité ou la détection précoce des intrusions ou des tentatives d'intrusions.

La figure suivante présente les activités d'une ERI telles que présentées dans la littérature ou par rapport à l'état des pratiques dans les entreprises qui ont participé à l'étude.

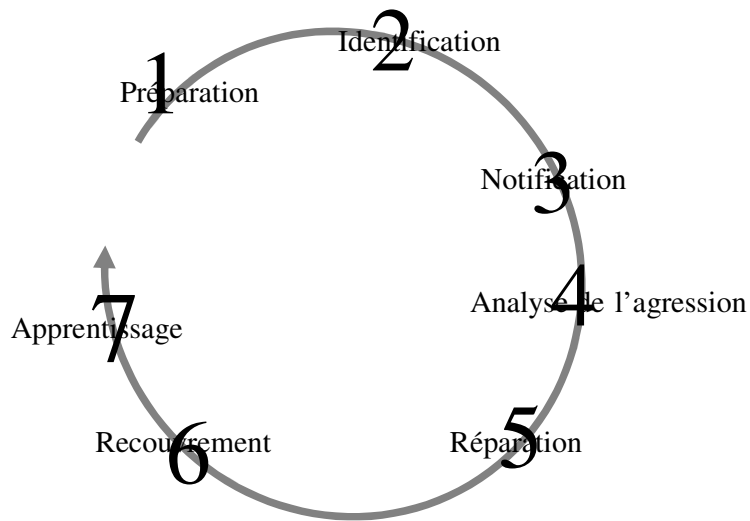


Figure 3: Les sept étapes de la réponse à une agression, d'après Bort et Cummings (2003)

Dans leur travail quotidien, les ERI sont confrontées à plusieurs problèmes signalés par cette étude.

En effet, ces équipes ne disposent pas, jusqu'à la publication de ce rapport, de méthodes appropriées au traitement de ce type d'informations (contenues dans les *log files*) tout en reconnaissant la difficulté d'une telle activité et recherchent encore des outils utiles pour la coordination et le partage de ces informations (Killcrece *et al.*, 2003, Moore *et al.*, 2001).

De plus, une ERI se trouve souvent dans une situation de surabondance d'information. Il est crucial d'ajouter des outils de détection plus adéquats pour une analyse ultérieure. Ces outils permettront de mieux cibler l'information à capter en fonction de l'importance des ressources à protéger et de l'ouverture des services offerts.

2.4.3 Organisation et structure des ERI

Toutes les ERI ne sont pas forcément organisées et structurées de la même manière. La structure la plus répandue dans cette étude (34%) est celle d'une équipe interne, qui a une localisation géographique ou physique unique, responsable de toute l'organisation et chargée à plein temps des problèmes de sécurité.

Pour l'exercice de l'autorité, trois cas se présentent :

- autorité totale pour prendre les décisions sans approbation des managers pour répondre et prendre des actions correctives (déconnecter le système en cas d'intrusion). Cet état est signalé par 34% des entreprises.
- autorité partielle ou partagée : l'ERI participe à la prise de décision et peut influencer les actions à prendre pendant une attaque. 24% des entreprises.
- pas d'autorité : l'ERI ne prend pas la décision, il avance des suggestions ou des recommandations ou propose des stratégies pour réduire le risque et elle ne peut faire valoir ou appliquer aucune action. 24% des entreprises.

La taille des équipes dépend de la **compétence** et de **la formation** du staff, la charge de travail et le type des services fournis :

- 1 à 5 membres plein temps (31%)
- 6 à 10 membres plein temps (31%)
- plus que 10 membres (21%).

Une équipe est composée, dans la plupart des cas étudiés, comme suit :

- le manager de l'équipe, qui peut être le coordinateur ou le chef technique, qui coordonne, supervise et oriente les activités de l'équipe
- le staff technique, qui fournit un support à la manipulation d'un incident grâce à son expertise dans le domaine de la sécurité (le staff peut être interne ou externe).
- les assistants au bureau ou le staff en garde qui sont les premiers à reporter des informations relatives à une agression
- les experts en sécurité informatique, spécialistes en plateforme ou en réseau, qui peuvent fournir des conseils ou des orientations lors du traitement de l'incident
- les autres professionnels qui peuvent appartenir à plusieurs départements comme le département informatique, ressources humaines, relations publiques ou des responsables en management qui assistent l'ERI
- le personnel administratif de support.

Le nombre d'incidents manipulés par jour par les ERI varie considérablement d'une équipe à une autre. Celles qui ont participé à l'étude signalent :

- 1 à 3 incidents par jour (38%)
- 4 à 8 incidents par jour (18%)
- plus que 15 par jour (18%).

Les ERI coordonnent leur travail avec les départements internes et avec des équipes externes, des experts en sécurité et les autorités légales. Les résultats de l'étude montrent que :

- 66% coordonnent leur travail avec le *CIO* et les départements de télécommunications ou les autorités légales
- 58% avec d'autres ERI
- 41% avec leur département juridique

De même, les ERI partagent l'information avec :

- 66% avec le *CIO*
- 58% avec le département des technologies de l'information ou de télécommunications
- 58% avec les autorités légales
- 55% avec d'autres ERI

Dans ce qui suit, nous focalisons notre étude sur le cas d'une entreprise tunisienne l'Agence Nationale de Certification Electronique (ANCE) et sur l'état de ses pratiques en matière de sécurité. Cette entreprise a servi de terrain à nos investigations empiriques.

2.4.4 Cas de l'ANCE de Tunis

L'ANCE est une entreprise publique tunisienne à caractère non administratif, oeuvrant dans le domaine des TIC. Les principaux objectifs de sa création s'articulent essentiellement autour de :

- La régulation de l'activité de certification et la promotion des échanges électroniques.
- La définition des normes techniques des systèmes de création et de vérification de la signature électronique en Tunisie.

- La veille technologique et la participation aux activités de recherche, de formation et d'études afférentes aux échanges et commerce électroniques.
- L'homologation, l'étude et l'audit des systèmes de cryptage électronique.

L'ANACE offre quatre types de service. Il s'agit de :

- Service d'assistance aux activités de certification : Ce service organise l'activité d'offre de services de certification, assiste et contrôle les fournisseurs dans leurs procédures.
- Service de certification : ce service vise à organiser l'activité de certification (en accord avec la réglementation en vigueur) et à répondre aux besoins d'identification et d'authentification nécessaires aux agents publics dans l'exercice de leurs activités dans le cadre d'une administration électronique. Ce service fera l'objet d'une étude plus détaillée dans le paragraphe suivant.
- Service d'homologation : ce service vise à garantir la protection des échanges électroniques, à protéger les utilisateurs des systèmes de cryptage contre toute forme de cyber-attaque et à sécuriser les infrastructures des systèmes d'information des entreprises.
- Service d'audit : ce service vise à aider les entreprises à analyser les menaces et les risques de sécurité qu'elles encourent dans la réalisation de leur chaîne de valeur, lorsque celles-ci utilisent les TIC, et à proposer des solutions de sécurité.

Quatre situations sont considérées comme des incidents de sécurité au sein de l'ANACE. La perte de la disponibilité, de l'intégrité, de la confidentialité de l'information et la violation des règles de sécurité. Un plan de réponse doit être mis en œuvre pour chacune de ces situations pour éviter la prise de décisions improvisées, prises sur le champ. Un plan de réponse définit les activités que doit effectuer l'ERI et comprend :

- la notification de l'incident par des mécanismes automatisés ou manuels
- la limitation des dégâts
- la restauration
- les enseignements tirés

L'ERI de l'ANCE comporte sept personnes. Une personne est chargée de la **Médiation**/coordination et trois sous équipes comprenant chacune deux personnes réparties selon le type d'incident à gérer en relation avec la sécurité physique, la sécurité des réseaux, et la sécurité des services.

En effet, la détection et l'analyse d'une agression sur les services (exemple d'une agression de type de **déni de service**) peuvent avoir des origines qui peuvent toucher des aspects de la sécurité des réseaux ou la sécurité physique.

Chacune des sous équipes, composée de deux personnes, est chargée, en ce qui la concerne, de l'audit et de toute intervention nécessaire d'où le respect de la confidentialité de trois fonctions, que l'ANCE considère comme étant séparables.

La politique de sécurité au sein de l'ANCE détermine pour chaque sous équipe sa mission, son champ d'activité et avec quelles entités elle peut interagir. La mission de chaque sous équipe consiste à effectuer des contrôles périodiques (et à l'occasion de l'occurrence d'un incident potentiel) dans le but de vérifier l'état de sécurité, amplifier, et analyser les signes d'intrusion ainsi que de contribuer à l'élaboration d'une réponse. Le champ d'activité délimite les attributions en précisant ce qui est peut être accessible ou modifiable par chaque sous équipe et en spécifiant les règles associées. Pour l'interaction, il s'agit d'indiquer les entités (qui peuvent être des administrateurs informatiques, des administrateurs réseau, des administrateurs serveurs) avec lesquelles chaque sous équipe peut collaborer en tenant compte de la spécificité des tâches effectuées par celle-ci.

La figure ci-dessous présente la composition de l'ERI au sein de l'ANCE de Tunis.

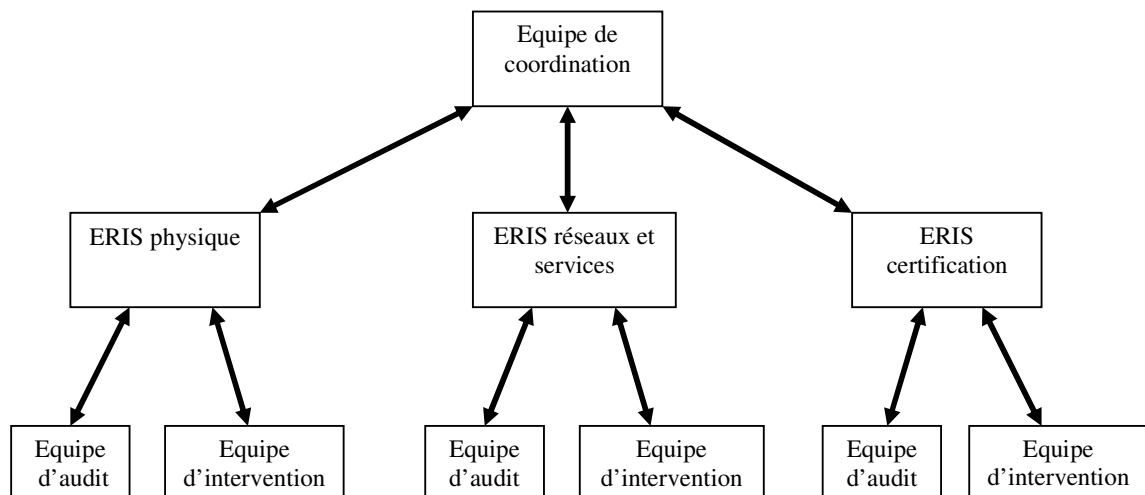


Figure 4: Composition de l'ERI à l'ANCE de Tunis

Conclusion Chapitre 2

Nous avons cherché dans ce chapitre à situer dans les publications académiques des connaissances disponibles et qui nous seront utiles dans la conception et la réalisation de notre méthode en fournissant des éléments de réponse à notre question de recherche.

Par rapport aux techniques d'évaluation du risque en général, nous avons retenu la nécessité d'assigner une probabilité relative à la réalisation d'une action ou à ses relations avec d'autres éléments d'analyse. Les relations probabilistes sont appropriées à un contexte d'incertitude ou dans le cas de problèmes flous ou difficilement structurables. Cependant, ces techniques ne spécifient pas la nature des informations utilisées pour l'identification et l'évaluation du risque.

Par rapport aux méthodes de traitement des informations de type signal et/ou signe faible, nous avons fait référence aux cartes causales et au modèle conceptuel de Lesca et Caron-Fasan (1995) et Blanco *et al.* (2003) qui décrit un processus mettant en œuvre l'intelligence collective. Nous avons montré que les liens devraient être étendus en intégrant la probabilité, l'approximation et la variable temps afin de couvrir la complexité des raisonnements dans des situations d'incertitude.

Au cours de ce chapitre, nous avons cherché également à recenser l'état des pratiques des entreprises en matière de sécurité. Nous avons souligné l'insuffisance des moyens techniques et physiques de sécurité face à la complexité et l'imprévisibilité accrues des agressions numériques. La composition d'une ERI s'avère de plus en plus comme étant une solution complémentaire et nécessaire pour réduire le risque des agressions numériques. Cependant, nous avons noté le manque de méthodes et outils appropriés pour aider une ERI dans l'activité de réponse aux agressions numériques.

Chapitre 3

Emprunts aux travaux antérieurs de l'équipe de recherche Veille Stratégique en relation avec la question de recherche

Ce chapitre est consacré à l'étude d'une méthode particulière, L.E.*SCAnning*®, qui représente un dispositif de Veille Anticipative Stratégique et d'Intelligence Collective (VAS-IC®) issue de nombreux travaux théoriques et empiriques de l'équipe de recherche du professeur Lesca. Cette équipe a déjà consacré plus d'une douzaine de thèses à ce domaine, sans cesse en évolution, notamment du fait du développement de l'Internet. Cette méthode présente des spécificités importantes dont on pense qui devraient permettre de notre point de vue de développer un support original et approprié pour le travail des ERI.

Le modèle conceptuel de la méthode L.E.*SCAnning*® présente un ensemble de phases en boucles rétroactives. Notre intérêt à travers ce travail porte particulièrement sur trois phases de son modèle conceptuel à savoir la création collective de sens, la mémorisation et l'animation. Dans ce chapitre, nous présentons certains enrichissements escomptés de la méthode L.E.*SCAnning*® concernant ces trois phases. Sur un plan pratique, nous démontrons l'intérêt de l'utilisation des TIC et particulièrement la technologie Internet pour la mise en application de la méthode proposée dans ce travail de recherche.

Dans ce chapitre, nous réalisons également une comparaison entre le travail d'une ERI et d'une équipe de création collective de sens. Cette comparaison nous permet de mettre en relief les spécificités des conditions et des méthodes de travail de chaque équipe.

Ainsi, ce présent chapitre est organisé en trois sections. La première section décrit les différentes phases de la méthode L.E.*SCAnning*® ainsi que les innovations apportées par cette méthode au niveau du traitement des informations de type signal et/ou signe faible. La deuxième section présente les enrichissements escomptés de la méthode L.E.*SCAnning*® dans notre domaine d'étude afin de proposer une extension de la méthode sur le plan conceptuel et sur le plan de la mise en application. La troisième section évoque les points de ressemblance et les points de différences entre le groupe de création collective au sens de la méthode L.E.*SCAnning*® et le travail des ERI.

3.1 Présentation de la méthode L.E.SCanning®

Dans cette section nous décrivons les différentes étapes du modèle conceptuel de la méthode L.E.SCanning® ainsi que ses innovations dans le domaine de la veille anticipative stratégique. Cet exposé, nous permettra ultérieurement de situer nos propres apports théoriques et empiriques en tenant compte des spécificités de notre terrain de recherche.

3.1.1 Modèle conceptuel de la méthode L.E.SCanning® :

Le modèle conceptuel présente des fonctions essentielles pour un dispositif de Veille Anticipative Stratégique et Intelligence Collective comme étant un système avec boucles rétroactives.

La figure ci-dessous présente les fonctions essentielles d'un dispositif VAS-IC®. La fonction cruciale de la méthode, la création collective de sens, est placée au centre de la figure.

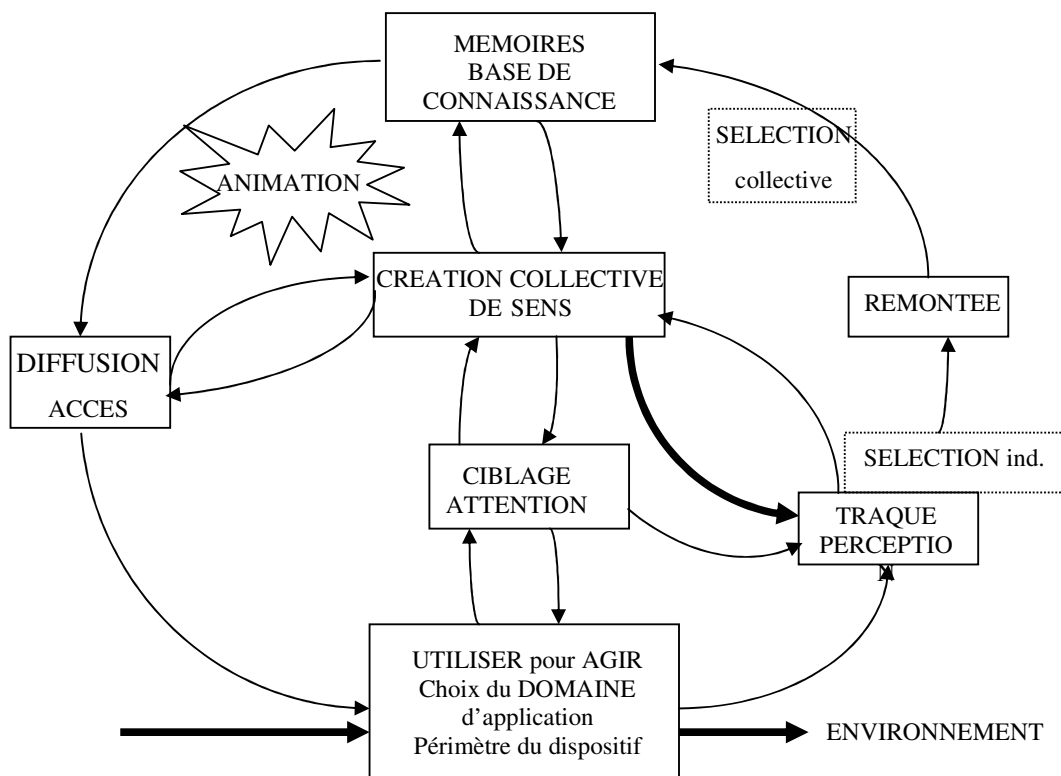


Figure 5: Modèle référentiel de la méthode L.E.SCanning®

3.1.1.1 Le ciblage

C'est l'opération qui vise à définir et à délimiter la partie de l'environnement externe de l'entreprise sur laquelle il faut cibler les efforts de la veille anticipative stratégique. Le ciblage permet de se concentrer sur les parties ou les acteurs clés de l'environnement et donc d'optimiser les coûts et le temps dédiés à l'activité de la veille anticipative. La définition de la cible doit se faire d'une façon dynamique en fonction des besoins des utilisateurs opérationnels.

En effet, la veille anticipative a pour objectif de capter des signaux et/ou signes annonciateurs d'évènements externes qui sont de nature à influencer la survie et la croissance de l'organisation. Il semble logique de remonter en amont des évènements pour se tourner vers les acteurs actuels et potentiels susceptibles d'engendrer les évènements en question.

Ainsi, le ciblage de la veille anticipative fait intervenir la notion d'acteur et la notion de thème. Un acteur pertinent pour la veille anticipative est toute personne, ou groupe de personnes, ou entreprise (ou autre organisation), dont les décisions et les actions sont susceptibles d'avoir, dans le futur, une influence positive ou négative, directe ou indirecte sur le devenir de l'entreprise. Les types classiques d'acteurs sont les clients, les concurrents, les fournisseurs, les partenaires et certains pouvoirs publics. Il est également important de bien identifier les acteurs actuels, potentiels, directs et indirects.

La phase précédente se termine par une liste nominale d'acteurs, aussi exhaustive que possible. Puis il serait question de hiérarchiser les acteurs selon certains critères.

Un thème désigne une activité de l'acteur ou une certaine caractéristique de l'acteur qui concerne la veille anticipative.

La phase du ciblage s'apparente également à définir les besoins en information et donc l'identification des sources à scruter susceptibles de fournir les informations ciblées.

Les sources d'information sont de deux types :

- Informelles (ou sources de « terrain ») : les contacts avec les clients, les concurrents, les fournisseurs, les distributeurs ; les participations aux colloques scientifiques et aux salons professionnels ; les missions à l'étranger et les contacts avec des experts, etc.
- Formelles : les publications scientifiques et techniques ; les bases de données ; les publications des entreprises ; les brevets et les dépôts légaux, etc.

Dans le contexte de la présente recherche, le ciblage soulève une difficulté spécifique. En effet, parmi les acteurs pertinents de l'environnement de l'entreprise figure une nouvelle catégorie : les hackers. Or les hackers, par définition, ne sont pas des acteurs que nous pouvons identifier individuellement a priori : nous ne pouvons pas les cibler individuellement.

3.1.1.2 La traque des informations

C'est l'opération par laquelle les informations de la veille anticipative sont procurées. On désigne par traqueur, ou capteur « *gatekeeper* », une personne qui a pour rôle d'aller au devant de ces informations. Les traqueurs sont de deux types :

- Les traqueurs « sédentaires (ou résidents) » qui travaillent dans leurs bureaux et qui sont au contact de sources documentaires et de bases de données.
- Les traqueurs « nomades (ou itinérants) », ou encore « traqueurs de terrain », qui se déplacent au contact de sources extérieures d'information. C'est le cas des commerciaux, par exemple.

La tâche de traque des informations est plus facile pour les traqueurs sédentaires que pour les traqueurs nomades. En effet, pour les traqueurs nomades, la tâche de traque des informations vient s'ajouter à leur tâche professionnelle principale.

Parmi les critères importants de choix d'une personne chargée de la mission de traque figurent le degré de familiarité avec les sources d'information avec lesquelles couramment elle est en contact, du fait de ses activités habituelles.

Ainsi, la traque est une activité différente de ce qui est habituellement écrit au sujet de la collecte ou bien de l'interrogation de bases de données. Il ne s'agit pas de recherches bibliographiques par mots clés. Il s'agit d'acquérir l'habileté cognitive à détecter des informations informelles d'un genre particulier dont les caractéristiques résultantes ont été mentionnées plus haut et susceptibles d'être interprétées et de livrer du sens utile pour l'anticipation des changements de l'environnement de l'entreprise. L'information n'est que le **stimulus** de l'action ultérieure du capteur. Le commentaire est la valeur ajoutée qui se révèle ensuite essentielle. Aujourd'hui, l'entreprise se trouve confrontée à une offre d'informations

en explosion. Elle doit faire donc preuve d'une capacité à donner du sens aux stimuli qu'elle reçoit (Baumard, 1997).

Dans le contexte de notre recherche, les traqueurs sont des traqueurs « sédentaires », non en contact avec le terrain mais en relation avec les TIC de l'entreprise et ses réseaux informatiques.

En outre, ce n'est pas le traqueur qui va au devant des signes et/ou signaux, mais au contraire ce sont eux qui font intrusion chez le traqueur qui, ici, est un membre de l'ERI. En fait il peut y avoir un autre cas, également possible : celui où le traqueur (ERI) détecte un signe en faisant ses tests de surveillance du réseau.

3.1.1.3 La sélection des informations

Il s'agit d'opérer une sélection méthodique, selon des critères précis et explicites, des informations traquées sur l'environnement externe de l'entreprise et susceptibles d'intéresser les utilisateurs potentiels. La sélection peut être faite à un niveau individuel par chacun des traqueurs et/ou à un niveau collectif. Les critères de sélection concernent essentiellement le caractère anticipatif de l'information et la pertinence de celle-ci.

Une information est anticipative « lorsque l'interprétation qui en est faite laisse entendre qu'un événement pourrait plausiblement se produire dans le futur, alors que cet événement n'est peut-être pas même amorcé au moment où est découverte l'information » (Lesca, 2003).

Les informations anticipatives sont de deux types : les informations de potentiel et les signes d'alerte précoces.

Les informations de potentiel (Porter, 1982 ; Thiétart, 1990 ; Ghoshal et Westney, 1991) concernent certaines caractéristiques de l'acteur ciblé (ses points forts et ses points faibles par exemple) afin de pouvoir analyser et évaluer sa capacité à agir dans le présent et le futur. Si l'acteur ciblé est un client ou concurrent, il est important de se renseigner sur sa capacité financière, ses alliances actuelles ou éventuelles, les valeurs qui sous-tendent ses choix, etc.

Ces informations peuvent être présentées de façon à exprimer une évolution au cours du temps (Thiétart, 1990). Sous cette forme, les informations de potentiel sont faciles à visualiser et plutôt facilement accessibles auprès de sources formalisées.

Les signes d'alerte précoces sont des informations dont l'interprétation donne à penser qu'un événement susceptible d'être important pour l'avenir d'une organisation pourrait se produire (Lesca, 2001). Elles peuvent concerner une manifestation, une annonce, ou un mouvement d'un acteur de l'environnement, etc. et fournit des indications sur ses intentions, ses motivations, ou sa situation interne (Lesca et Blanco 2002). Plus ces signaux sont précoces, plus la marge de manœuvre de l'entreprise est importante. Les signes d'alerte précoce résultent souvent de l'opération réalisée sur des signaux et/ou signes faibles à travers une amplification graduelle (Ansoff, 1975). Cette opération nécessite une formation adéquate et peut être assistée d'heuristiques appropriées.

La pertinence d'une information concerne son caractère approprié dans le temps ainsi que son utilité actuelle ou potentielle pour des preneurs de décision. La pertinence peut être évaluée à travers son degré de rattachement par rapport à un acteur cible, un thème, et/ou à un « puzzle » déjà en cours de construction. Comme pour découvrir l'éventuel caractère anticipatif d'une information, la découverte de la pertinence requiert une formation dans ce domaine.

3.1.1.4 La remontée des informations

La remontée des informations est l'opération par laquelle un traqueur fait parvenir les informations recueillies à la personne chargée de les stocker. Le dispositif de remontée nécessite que le traqueur dispose d'un moyen matériel approprié, pour transmettre les informations, facile d'accès et d'utilisation. Dans ce cadre, il est important de tester le caractère approprié du support de remontée et de communication, en terme de type d'information, avec les caractéristiques et exigences relatives aux différentes phases du dispositif de la veille anticipative stratégique.

Notons que, selon la théorie de la richesse des médias (Daft et Lengel, 1986 ; 1988), tout médium de communication n'est pas nécessairement approprié à l'échange de n'importe quel type d'information. Ainsi, et selon ces auteurs, le face-à-face est considéré comme étant le médium le plus approprié pour véhiculer une information riche en contexte, c'est-à-dire à une information ambiguë susceptible de plusieurs interprétations.

Dans le contexte de notre recherche, la **pression du temps** est considérable de telle sorte qu'un médium qui privilégie la rapidité de transmission pourra être préféré, alors que l'ambiguïté de l'information communiquée aurait justifié le choix d'un autre médium, en application de la théorie « *media richness* ».

3.1.1.5 La mémorisation

La mémorisation, désignée également par l'expression « stockage intelligent », est nécessaire pour valoriser et exploiter les informations collectées de la veille anticipative. Le stockage intelligent nécessite la mise en forme des informations et leur classement dans des bases de données pour pouvoir les retrouver à tout moment prêtes à être utilisées. Le plan de classement reprend les thèmes et les acteurs, qui sont les mots clés principaux, et affine les détails. L'affinage se fait en fonction de la liste des mots clés résultant du ciblage de la veille anticipative stratégique. Cependant, la liste des mots clés n'est pas définitive ni statique et peut évoluer en relation avec l'évolution du ciblage de la veille stratégique. Pour la mémorisation, il s'agit également d'une base de connaissances.

Notre recherche étant ancrée sur la **technologie Internet**, nous mettrons en évidence certaines de ses potentialités en ce qui concerne la fonction de mémorisation des informations, et nous montrerons l'usage qui pourra en être fait, en support de la méthode que nous proposons.

3.1.1.6 La création collective de sens

C'est la phase cruciale, du processus, qui consiste à traiter et à interpréter d'une façon **inductive** les informations de veille anticipative de façon à mettre en lumière des champs d'actions possibles pour l'entreprise. Il s'agit de l'opération collective au cours de laquelle sont créés de la connaissance et du « sens ajouté » par la création de liens significatifs entre informations fragmentaires, ambiguës et incertaines, au moyen d'interactions avec des

mémoires individuelles et collectives des participants, mémoires tacites ou formelles. Les liens peuvent être de nature hypothétique, de confirmation, d'opposition ou de causalité.

En effet, l'intelligence (**individuelle**) désigne la capacité d'un individu à discerner des éléments autour de lui, à choisir certains de ces éléments et à établir des liens entre eux en vue de créer une représentation globale qui donne du sens pour lui. Dans une entreprise, l'intelligence **collective** désigne le processus collectif volontariste par lequel des individus unissent délibérément leurs efforts pour discerner et acquérir des informations anticipatives et pour en tirer des anticipations utiles pour une action rapide et au bon moment.

Par analogie, ce processus peut être comparé à un jeu de puzzle consistant à regrouper des pièces incomplètes, ambiguës et en désordre, avec la différence qu'il ne s'agit pas de reconstituer quelque chose qui existerait déjà (comme c'est le cas dans le jeu du puzzle) et que certaines pièces manquent et/ou sont difficilement identifiables. L'output de la co-construction du puzzle dépend de la capacité des acteurs de créer du sens à partir des informations éparses, fragmentaires et incertaines en utilisant leurs connaissances tacites ou explicites stockées en mémoires.

Nous serons amenés à utiliser les **liens** déjà présents dans la méthode L.E.SCA[®], mais en introduisant plusieurs **extensions**, notamment pour prendre en compte **le temps**, par exemple, ou encore l'**approximation**.

Les calculs matriciels dont nous montrerons l'usage plus loin, dans la méthode que nous proposons, ont dû tenir compte de l'enrichissement des liens mentionnés ci-dessus.

Les potentialités de la technologie Internet seront également explorées, comme support à la création collective de sens.

3.1.1.7 La diffusion/Accès

La diffusion est l'opération qui consiste à mettre les informations élaborées et les conclusions de la création collective de sens à la disposition des utilisateurs potentiels finals autorisés, souvent des responsables opérationnels. La diffusion efficace signifie que les informations

seront prises en compte par les utilisateurs potentiels c'est à dire ceux qui peuvent transformer l'information en action.

De même, un utilisateur potentiel peut prendre l'initiative d'aller vers l'information s'il éprouve le besoin de disposer de certaines informations qu'il est capable de désigner ou bien qui lui ont été recommandées par d'autres utilisateurs. Dans ce cas de figure, il s'agit de la phase d'accès aux informations.

La phase de diffusion/accès pose également le problème de l'appropriation du support de communication à la nature et les caractéristiques des informations. La théorie de la richesse des médias (Daft et Lengel, 1986 ; 1988) devrait trouver aussi un intérêt particulier par rapport à l'efficacité de cette phase, cependant, l'ambiguïté des informations n'est qu'un aspect du problème.

Ici, à nouveau, la très forte **pression du temps** pousse à choisir des méthodes et des moyens de communication qui priorise cette contrainte.

La diffusion (et l'accès), dont il est question ici, ne sont pas uniquement internes à l'entreprise. La diffusion se fait également vers **l'extérieur** de l'entreprise car il s'agit d'alimenter des bases de données, à l'échelon international, gérées par des organismes spécialisés dans la sécurité informatique (CERT, par exemple www.cert.org, ou encore CLUSIF www.clusif.org).

Le défaut d'accès continu à de telles bases internationales, de la part de certaines entreprises, peut être précisément la cause d'occurrence d'agressions numériques. En effet, un hacker peut très bien se rendre compte qu'une entreprise n'a pas fait la démarche de mise à jour de ses protections et il peut être tenté d'exploiter cette vulnérabilité. De ce fait l'entreprise accroît elle-même le risque d'être agressée. Avec cynisme, on pourrait presque parler de pro-activité de l'entreprise dans l'augmentation de sa vulnérabilité.

3.1.1.8 L'action

Si les informations traitées sont suffisamment significatives, elles peuvent être intégrées dans le processus décisionnel. Si par contre, les informations traitées ne permettent pas une vision assez claire, elles peuvent être complétées en lançant une (nouvelle) requête des informations manquantes.

La **prise de décision** en conséquence de la détection d'un risque, ne relève pas de l'ERI (dans le cas le plus fréquent). L'ERI doit en référer à sa hiérarchie qui agit ensuite comme elle l'entend.

3.1.1.9 L'animation

L'animation est une fonction vitale pour un dispositif de VAS-IC® lors de sa mise en place initiale ainsi que pour garantir son fonctionnement et sa pérennisation. Les principales tâches assignées à un animateur sont les suivantes :

- La promotion pour faire connaître et reconnaître le dispositif de VAS-IC ce qui est de nature à aider à la compréhension et à la réalisation des objectifs de la veille.
- La création d'un environnement de communication facile, d'échange dynamique d'information et de partage des connaissances explicites et tacites.
- La coordination, vu le caractère transversal du dispositif VAS-IC qui nécessite la convergence des efforts et des flux d'informations descendantes, ascendantes et transverses.
- La **médiation**, notamment par l'intégration des différents fragments d'information et des points de vue des participants afin de converger les efforts vers une intelligence collective utile à l'action.

Ainsi, l'animateur devrait avoir un profil particulier de pédagogue, de communicant et d'extraverti pour motiver et convaincre les différents participants intervenant dans le périmètre de la veille stratégique.

Dans le **contexte de notre recherche**, l'animation (de la méthode L.E.SCA[®]) se ramène uniquement à la médiation focalisée sur les phases de création collective de sens et de prise de décision.

L'activité de médiation nécessite l'usage de certains outils, tel le calcul matriciel, par exemple. Le recours à de tels outils tient au fait que « l'animateur », médiateur, doit faire converger les jugements éventuellement en conflit, et cela de façon aussi objective que possible. Nous laissons ainsi entendre que l'animateur/médiateur doit posséder certaines compétences dans l'utilisation de tels outils, ainsi que des compétences de technicien. Donc il aura dû recevoir une **formation** appropriée.

3.1.2 Les innovations de la méthode L.E.SCA[®] (en amont de la présente recherche)

La principale caractéristique du système d'information appelé «Veille Anticipative Stratégique et Intelligence Collective (VAS-IC)» est d'être tournée vers le futur et par conséquent la compétitivité durable de l'entreprise. La méthode est orientée, notamment, vers l'anticipation et/ou l'identification des ruptures et des discontinuités.

En effet, cette méthode a été conçue, réalisée et validée pour supporter des décisions stratégiques prises dans un contexte d'incertitude, en utilisant des informations de type signal et/ou signe faible et en se basant sur un processus de création collective de sens pour des fins d'anticipation et/ou d'identification des ruptures et des discontinuités

La figure suivante montre les innovations de la méthode L.E.SCA[®].

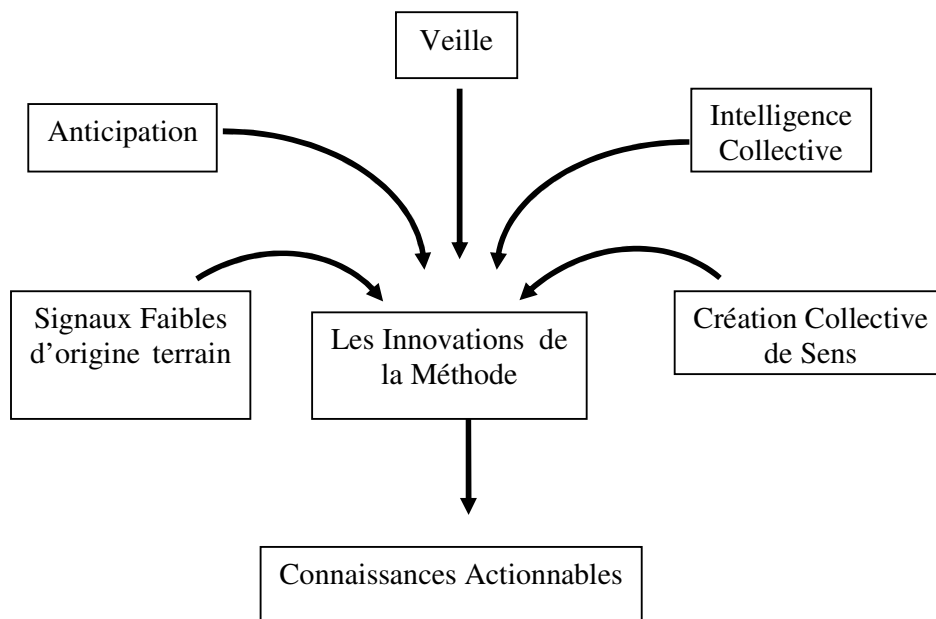


Figure 6: Les innovations de la méthode L.E.SCANing®

La méthode est orientée vers l'anticipation. Ceci implique l'utilisation des signes faibles et des informations de terrain. Toutefois, la détection, la perception et l'interprétation de ces informations constituent des opérations difficiles et délicates. Il en découle la nécessité d'une intelligence collective en formulant les hypothèses relatives à la réalisation d'une synergie « cognitive » entre les intervenants dans l'activité de création de sens et la réduction des **biais cognitifs** individuels. En sens inverse, l'existence de biais cognitifs collectifs ne peut pas être ignorée, ni réduite totalement comme on pourrait le souhaiter.

L'analyse du dispositif de la veille anticipative stratégique et d'intelligence collective fait apparaître qu'il s'agit d'un processus d'**apprentissage collectif**. L'apprentissage collectif renvoie à la fois au savoir qui se construit par l'action et aux connaissances nouvelles ou les transformations des connaissances qui résultent du processus d'apprentissage. Plus l'entreprise utilise ses informations et ses connaissances (tacites et formelles) pour l'action, plus elle apprend de la correction de ses erreurs afin d'être plus performante dans ses actions futures. Et plus, elle soutient sa compétitivité durable.

3.2 Enrichissements escomptés de la méthode L.E.SCAnning® dans le cas considéré par la présente recherche

Les phases du modèle conceptuel de la méthode L.E.SCAnning® qui intéressent particulièrement notre travail de recherche sont : la phase de construction collective de sens, la phase de mémorisation et l'animation comme étant une fonction de support pour la mise en place et la continuité du dispositif de veille anticipative stratégique et intelligence collective.

Par rapport à ces trois phases, nous apportons de nouveaux éléments d'analyse et de connaissance à travers une transposition et une adaptation de la méthode L.E.SCAnning® dans le domaine de gestion et d'anticipation des agressions numériques afin d'aider à la prise de décision dans ce domaine particulier.

Nous apportons aussi des éléments de méthode pour assister le travail en groupe d'une équipe de création de sens. Pour la mise en application, notre apport se place également au niveau de l'assistance active que peut fournir l'utilisation des TIC.

3.2.1 Enrichissements escomptés par rapport à la phase de création collective de sens

La diversité et la complexité du raisonnement dans un contexte fortement incertain requièrent une richesse de la typologie des liens ; de plus pour assister le processus de création de sens les acteurs ont besoin des mécanismes pour la représentation des liens, et des outils pour la manipulation des liens.

En effet, les liens considérés dans ce travail de recherche présentent des possibilités plus nombreuses et plus adaptés au contexte de la recherche, de nature à ouvrir le champ à un **raisonnement non déterministe**. Ces liens sont créés et manipulés avec une disponibilité limitée de tous les éléments de raisonnement tout en prenant en considération les objectifs et les contraintes de l'entreprise qui peuvent varier en fonction du temps.

L'enrichissement de la typologie des liens est réalisée dans notre travail en intégrant la **probabilité et l'approximation** dans la création de relations entre les informations et la **pression du temps** comme étant des facteurs très significatifs dans le domaine de prise de décision relative à la détection et à l'analyse des agressions numériques. En effet, les liens probabilistes permettent d'élargir le champ du raisonnement dans un contexte incertain et changeant. Les liens dynamiques, variables en fonction du temps, permettent d'adapter le

raisonnement au contexte et aux objectifs de la prise de décision. De plus, l'enrichissement de la typologie prend en compte des relations de nature diverse entre les éléments du raisonnement telles que les relations sémantiques, quantitatives, transactionnelles, etc.

Dans ce travail, nous utilisons une extension des cartes causales pour la représentation et la manipulation des liens dynamiques et probabilistes dans un contexte d'incertitude.

En effet, l'utilisation des cartes causales permet la représentation graphique des liens et des nœuds par un graphe et qui peut être transposé à une matrice de la représentation mentale que chaque membre se fait de l'ensemble des concepts relatifs à l'évaluation d'une situation.

De ce fait, les cartes causales présentent des fonctionnalités intéressantes pour une application à la problématique de traitement des signaux et/ou signes faibles, particulièrement l'appropriation de l'outil par rapport à une démarche heuristique qui prend en considération les schémas cognitifs permettant de résoudre des problèmes complexes avec une indisponibilité de certains types d'information. Ceci est susceptible de réduire la complexité du raisonnement qui risque d'affecter défavorablement la qualité de la prise de décision.

Nous proposons un ensemble d'opérations sur les liens qui sont importantes à manipuler dans le cadre du processus de création collective de sens. Ces opérations sont essentiellement des opérations de :

- Remplacement, qui consiste à remplacer ou substituer ou éclater un nœud par un réseau de nœuds et de liens afin de clarifier et d'analyser les sous implications du nœud et ce par équivalence, par approximation, par réduction, ou par restriction ;
- Réécriture, qui consiste à remplacer des éléments de raisonnement représentant une vue particulière par un sous réseau de nœuds et de liens représentant une autre vue plus pertinente pour plus de signification de la vision globale, pour offrir une alternative de raisonnement et pour affiner le processus de raisonnement. Les opérations de réécriture comprennent la réécriture, la suppression et la dissimulation de certains liens de raisonnement d'un sous réseau.

Ainsi, l'extension opérée sur l'utilisation des cartes causales permet une formalisation des vues collectives par une représentation sous forme d'un graphe ou d'une matrice en permettant de donner une sémantique aux éléments de raisonnement d'une vision collective.

Ceci est de nature à contribuer à une automatisation de construction des chemins de raisonnement d'une vue globale et collective par des opérations mathématiques de multiplication des matrices.

En conséquence, l'apport que nous proposons par rapport à cette phase met en œuvre un ajout sur la nature des concepts manipulés, l'extension des liens de causalité et l'enrichissement des mécanismes de raisonnement.

3.2.2 Enrichissements escomptés par rapport à la phase de mémorisation

Notre apport au regard de cette phase peut se positionner sur un triple plan :

- La conception de mécanismes de structuration des mémoires en base de données et base de connaissances à travers l'exploitation des potentialités offertes par les TIC.
- La conception de mécanismes de gestion des mémoires pour réaliser des enrichissements et des requêtes de la base des données et de la base des connaissances.
- La définition d'heuristiques permettant la convergence des raisonnements basée sur l'utilisation de la base de connaissances et la construction des vues alternatives afin d'assister l'activité de médiation ainsi que les opérations de manipulation des cartes causales associées.

Les mécanismes de structuration devraient contribuer d'une façon efficace et rapide à un stockage intelligent et dynamique des informations collectées avec la création de liens utiles à une structuration et une hiérarchisation significatives de celles-ci. Cette approche permet également une capitalisation des connaissances lorsque, en plus des informations proprement dites, sont stockées également les cartes causales formulées et construites par les membres d'un groupe de création de sens, ainsi que les validations éventuelles de celles-ci en cas de prise de décision. Ceci est de nature à permettre la traçabilité de l'évolution de la base des connaissances et par la suite la constitution d'un véritable catalyseur de l'apprentissage collectif.

L'instrumentation des liens de regroupement des informations collectées doit être capable d'appréhender et de tracer cette évolution avec la mise en œuvre d'une typologie de liens de raisonnement pour organiser les informations disponibles sous forme d'une connaissance signifiante. Ceci peut être accompli par la séparation entre la mémorisation des informations et le traitement des liens. Concernant la mémorisation des informations, une base de données peut être utilisée pour stocker les informations regroupées selon des liens statiques. Le

traitement des liens peut être activé à travers l'exploitation d'une base de connaissances opérant sur des liens dynamiques résultant des cartes causales de groupe déjà construites (ou des vues en cours de construction), des outils de représentation des liens et des outils heuristiques permettant ainsi la recherche des liens optimisés et la traçabilité de leur évolution.

Le regroupement classique des informations dans des bases de données présente plusieurs insuffisances. En effet, celui-ci se caractérise par l'existence de liens statiques et déterministes ce qui implique des possibilités limitées de recoupement et d'enrichissement des informations nécessaires pour générer de la signification. De plus, les mécanismes de recherche de type « recherche exacte » ne satisfont qu'à un pourcentage faible les critères de regroupement des informations mémorisées. Nous proposons d'inclure des mécanismes de recherche de type « **recherche approchée** » basée sur des relations diverses entre les éléments en mémoire incluant l'analogie, la similarité, la proximité, etc.

Par ailleurs, la définition d'heuristiques est importante pour assister la création et la manipulation des liens entre les informations. Ces liens peuvent être induits soit d'une façon automatique suite à une consultation de la base des connaissances ou des bases externes à l'entreprise réputées riches de références, en tenant compte de certaines variables déterminées par le processus de médiation et à travers des interactions de mémoires individuelles et collectives, soit par des raisonnements collectifs et créatifs sur les liens.

3.2.3 Enrichissements escomptés par rapport à la fonction de médiation

Puisque la création de sens est un processus collectif (dans le cas qui nous concerne ici) , il est important de définir des mécanismes de conciliation et d'intégration des différents points de vues.

Ainsi, notre intérêt par rapport à la fonction de l'animation se limite au périmètre du processus de création collective de sens et au processus de prise de décision. Nous proposons à ce propos des éléments de méthode et des heuristiques générales pour faire converger les points de vue et les différentes alternatives ainsi que pour aider à la prise de décision collective.

En effet, au cours de ce processus chaque membre présente ses propres éléments de raisonnement lesquels peuvent être représentés par un réseau de nœuds et des relations de dépendance. Cependant, des divergences ou des conflits entre les points de vue peuvent se produire durant le processus d'évaluation et d'analyse de la situation.

Pour l'intégration des vues, la médiation et la négociation sont des mécanismes nécessaires pour construire une vision globale, collective et intelligible.

La médiation cerne les zones de conflit, les analyse en vue de trouver des arrangements possibles pour plus de compatibilité entre les relations et les liens de raisonnement.

La négociation dans ce cadre se traduit, d'une part, par l'altération d'un point de vue vers un autre plus compatible avec le reste du graphe par persuasion et discussion. D'autre part, la négociation se traduit par l'enrichissement et la modification des vues en conflit à travers des mécanismes de raffinement des cartes causales.

La réconciliation des vues peut être visualisée à travers un graphe unique et global où nous pouvons voir :

- les zones de consensus
- les zones de désaccords partiels
- les zones de désaccords complets

La réconciliation est importante pour les deux derniers cas, et elle peut être accomplie par :

- la réalisation d'une définition commune et/ou partagée des tous les concepts pertinents pour l'évaluation de la situation
- la négociation et la médiation pour éliminer la vue unilatérale ou la faire rapprocher du reste du graphe.

Après le processus de réconciliation, tous les nœuds et toutes les relations sont représentés par un graphe unique en vue de l'analyser et de prendre la décision étant donné un certain nombre d'informations, d'hypothèses, de contraintes et d'objectifs.

Des heuristiques peuvent être employées pour aider à la prise de décision collective et à gérer des chemins de raisonnement alternatifs et qui consistent à :

- supprimer tous les segments composant un chemin particulier, qui ont une influence négative. Ainsi, l'objectif est évalué d'une façon relative
- supprimer les chemins positifs pour considérer l'impact d'une décision sans considérer l'influence positive
- compenser l'effet positif par un effet négatif

- choisir entre plusieurs alternatives compte tenu des contraintes, des objectifs stratégiques de l'entreprise.

Dans notre domaine d'application, l'objectif étant :

- premièrement de décider si une agression a été perpétrée,
- deuxièmement construire le scénario de l'agression
- et finalement l'anticiper en trouvant les mesures correctives.

Toutes ces techniques mettent en relief le **rôle important que peut jouer le médiateur** dans le processus d'intelligence collective en vue de construire une vision globale suffisamment pertinente pour la prise de décision. En effet, et compte tenu des objectifs de l'entreprise, les contraintes et les menaces, les compétences et le degré d'implication des acteurs du processus de création collective de sens, le médiateur accomplit les actions suivantes :

- valider les concepts qui sont représentés par les nœuds
- consolider, actualiser et manipuler les liens qui sont représentés par les arcs
- construire tous les chemins pertinents pour la prise de décision
- concevoir des heuristiques pour réduire la complexité du raisonnement
- contrôler le processus de raffinement pour une vision collective.

3.2.4 Apport de l'Internet comme support à la méthode proposée

D'une façon générale, la technologie Internet est caractérisée par quatre principaux outils qui peuvent être utiles aux différentes étapes d'un processus d'**intelligence collective** :

- un outil d'accès à une information interne et/ou externe distante (en termes de temps et d'espace) et quel que soit son support (texte, son, image) ;
- un mécanisme de structuration des informations (collectées et/ou déduites) dans des bases de données en utilisant des liens d'hierarchisation et de dépendance ainsi que des critères de regroupement à travers la création de liens hypertexte et d'adresses URL ;
- un mécanisme de recherche d'information par l'utilisation des moteurs de recherche (comme les opérateurs logiques) fonctionnant par mots clés ou des expressions et en opérant des liens sémantiques ;
- un mécanisme de contrôle d'accès qui permet de mettre en œuvre des politiques d'accès, d'authentification et d'autorisation aux ressources de l'entreprise et qui garantit la

traçabilité des accès, des actions opérées sur les ressources et de l'évolution des actions opérées sur les ressources.

Il nous paraît ainsi que l'utilisation de la technologie **Internet comme support au processus d'intelligence collective** répond aux besoins des preneurs de décision de disposer d'outils efficaces et rapides permettant :

- un regroupement systématique et dynamique des informations. En effet, le chapitre suivant montre l'apport d'une base des connaissances associée aux procédures de structuration et dont le rôle est de mémoriser les liens dynamiques pouvant être créés lors du processus d'Intelligence Collective et de tracer l'évolution du processus d'**induction** ;
- un traitement significatif des informations. En effet, un certain nombre de règles de recherche (de nature exacte, probabiliste, ou approchée) seront développées dans la suite permettant de créer des liens dynamiques, sémantiques et/ou probabilistes afin d'assister la phase de création collective de sens.

La technologie Internet permet de répondre à ces besoins par l'emploi des mécanismes de stockage de l'information en hypertexte (liens statiques, recherche exacte et approchée), et la manipulation de liens dynamiques à travers des moteurs d'inférence. Ceux-ci représentent des outils qui permettent de faire de la déduction automatique à partir d'hypothèses et de règles de déduction approchée à travers la création de liens sémantiques et/ou probabilistes. La technologie Internet permet également la gestion d'une base de connaissances implémentant des heuristiques de raisonnement appropriées aux liens stockés.

L'accent sera mis particulièrement sur l'apport des mécanismes de **recherche approchée** dans le processus d'intelligence collective qui permettent l'utilisation d'une base de connaissances associée à une grande variété et à une manipulation dynamique des de raisonnement créés à partir d'informations de type signal et/ou signe faible. Ils permettent également la définition d'une politique d'accès, en fonction de la contingence de la tâche de l'utilisateur (le médiateur, un membre de l'ERI par exemple), aux informations et connaissances stockées.

Les apports potentiels de la technologie Internet servent aussi à performer la fonction de la médiation : ils devraient représenter des outils et des supports efficaces pour la représentation et la manipulation des liens, la recherche d'informations internes et externes.

3.2.5 Exemple d'application : « *French Connection* »

Nous avançons dans ce paragraphe un exemple qui tente d'explicitier les concepts développés plus haut. Il développe les termes signal et/ou signe faible, création de liens, processus d'amplification, et donne des exemples d'apport de la médiation à travers la description de deux processus de prise de décision contradictoires.

Cet exemple est décrit dans l'ouvrage de Schiffman, (2001). Dans cet ouvrage, l'auteur expose 20 challenges à relever par les ERI afin de trouver le scénario de l'agression en donnant certaines informations techniques relatives aux circonstances de son occurrence.

L'**agression numérique** considérée dans cet exemple vise la dégradation de l'activité d'un site Web d'une entreprise de taille moyenne opérant dans le secteur du software. L'entreprise en question opère dans le domaine des technologies de l'information où l'Internet est un outil de production important. Toute agression visant cet outil peut remettre en cause la continuité de l'activité de l'entreprise.

La prise de conscience de l'agression a été effectuée suite à la réception d'un appel téléphonique un vendredi soir de la part d'un utilisateur final signalant une possible agression contre le site Web de l'entreprise.

Cet appel téléphonique n'a pas été considéré comme un **signal faible** car il était rapporté par une source externe au système d'information dont les compétences et les capacités d'analyse sont inconnues pour l'entreprise. Le signal n'a pas été traité à temps et le lundi l'agression est publiée par son auteur dans Yahoo, ce qui a engendré des pertes matérielles et immatérielles considérables pour l'entreprise.

Cependant, l'information contenue dans l'appel téléphonique n'a pas été ignorée et par conséquent l'ERI s'est réunie dès le lundi, a commencé à analyser le signal pour décider s'il s'agit bien d'une attaque sérieuse ou non, ou bien s'il s'agit d'une alerte concernant une faille possible dans le système d'information de l'entreprise.

L'ERI commence à construire le scénario de l'agression qui a détérioré le niveau d'activité du site Web de l'entreprise. Elle découvre effectivement une faille qui permet à l'auteur de l'agression de prendre le contrôle de la machine attaquée (i.e., un serveur). Le serveur étant à l'intérieur du réseau, le hacker peut ainsi utiliser une porte dérobée pour entrer dans le système et copier tous les fichiers sensibles en exécutant certaines commandes qui deviennent possibles après l'agression.

Pourtant, la visualisation des fichiers log du système, dont le rôle est de tracer les commandes exécutées, ne montre pas l'existence d'une attaque évidente. De plus, le log des événements dans le système d'exploitation (*NT event log*) ne montre aucune entrée dans les jours qui ont précédé l'agression ou durant l'agression. L'entreprise, sur proposition de l'ERI, décide alors d'ignorer le signal puisque il n'y a aucune évidence de l'occurrence d'une agression.

Ceci montre bien un problème au niveau des capacités d'analyse et de traitement des informations des membres de l'ERI de cette entreprise.

Le lien (de nature probabiliste pour nous) entre le signal faible et la conclusion d'une attaque non évidente n'a pas été bien estimé ou même a été écarté de l'analyse durant la phase d'exploitation/amplification du signal faible, en se basant sur les capacités d'analyse et les connaissances des membres de l'ERI. Par conséquent, la réconciliation et la médiation dans ce cas n'ont pas contribué à réaliser une vue pertinente durant la construction d'une vision globale.

En effet, après le week-end, l'ERI décide d'analyser plus en détails le problème et d'amplifier davantage le signal reporté par l'utilisateur final.

L'ERI commence à construire le scénario de l'attaque qui a causé la détérioration du niveau d'activité du site Web de l'entreprise. Elle découvre effectivement une faille qui permet le contrôle de la machine.

- a) Cette découverte constitue la première information qui peut être mémorisée dans la base des données.
- b) La deuxième information concerne le fait que le serveur est à l'intérieur du réseau et utilise un système d'exploitation contenant des failles.
- c) La troisième information découle de la création d'un lien de dépendance entre les deux informations incomplètes précédentes; elle montre que le hacker peut utiliser une porte dérobée pour entrer dans le système et copier tous les fichiers sensibles ainsi que les mots de passe en exécutant des commandes appropriées.

d) Une fois que l'ERI a connu la méthode probable d'entrée et identifié la faille, elle commence une construction collective du scénario de l'attaque.

e) L'ERI découvre qu'une faille particulière du système d'exploitation pouvait être utilisée. Le système, d'ancienne version, ne palliait pas à cette faille. Pour éviter cette agression, l'entreprise en question aurait gagné à utiliser une politique de mise à jour des versions de son système d'exploitation par l'installation de certains patches disponibles sur le marché.

3.3 Comparaison entre la démarche du groupe de création collective de sens (méthode *LESCanning*) et le travail de l'ERI dans le cas considéré

La comparaison entre le travail d'un groupe de création collective de sens et le travail des ERI relève des points de ressemblance mais aussi des points de différence. Nous commençons, d'abord, par faire une description d'une séance de création collective de sens. Ensuite, nous décrivons le travail d'une ERI pour analyser et répondre à une agression numérique.

3.3.1 Création collective de sens dans les cas les plus fréquents d'application de la méthode *L.E.SCanning*®

Il y a une douzaine de personnes dans une salle, qui sont des décideurs, dotés de compétences différentes et complémentaires, relativement faciles à identifier dans l'entreprise. Il y a aussi un animateur qui maîtrise la méthodologie de création de sens.

Le groupe dispose de quelques signes faibles qui ont été préalablement captés au cours des semaines précédant la séance et mis sur un support. Les informations sont généralement peu nombreuses et sont affichées au bord d'un tableau.

Le travail commence en prenant une information et en l'affichant au tableau. Le choix de cette première information est plutôt arbitraire. Chacun des participants exprime ses réactions, l'animateur doit veiller à gérer des interactions entre les participants et à ce que :

- tout le monde ne parle pas au même temps,
- Une personne « n'écrase pas » les autres,
- Chacun s'exprime.

Des associations d'idées, des « déclics » se produisent par :

- Rattachement de l'information affichée à des éléments tacites en mémoire d'un individu A.
- Rattachement du propos d'une autre personne B à quelque chose que A a tacitement dans sa tête.

La séance continue en prenant une seconde information et en l'affichant au tableau. Le choix cette fois-ci n'est plus arbitraire mais est induit par le résultat du premier rattachement. Il faut dans ce cas distinguer entre deux étapes qui sont confondues dans la pratique :

- Le rattachement d'une information à des éléments en mémoires implicite et explicite
- La création de liens entre les deux informations affichées et c'est là qu'apparaissent toutes les discussions et les réactions possibles au sujet du ou des liens entre les deux informations affichées. Des conflits sont susceptibles de se produire entre les participants concernant l'interprétation des liens et des informations. L'animateur doit veiller à ce que ces conflits ne dégénèrent pas mais en restent au stade de divergences d'interprétation. De plus, l'animateur ne doit pas imposer l'évolution vers un consensus. Les diverses interprétations divergentes doivent être écrites au tableau afin de garder une trace des raisonnements qui sont formulés de façon fugitive, car ils sont probablement plus importants que les informations elles-mêmes. Ces raisonnements sont en partie des heuristiques explicitées sur l'instant. S'il n'est pas possible de formaliser ces raisonnements, qui sont des connaissances provisoirement tacites provisoirement pas tacites, ils seront définitivement perdus. Au contraire si nous pouvons les stocker d'une façon formelle, ils deviennent une base de connaissances utiles pour d'autres séances de création collective de sens : d'où l'intérêt de voir du côté de toutes les technologies possibles qui permettraient de capter les réactions fugitives : visuelles, gestuelles, orales et de les mémoriser pour ensuite en faire des bases d'heuristiques réutilisables.

Le travail du groupe de création collective de sens se poursuit par prendre une troisième information et ainsi de suite.

L'animateur doit veiller à ce que ne se produisent pas de biais cognitifs collectifs qui conduiraient le groupe à ne plus chercher que des informations qui vont confirmer l'hypothèse qu'ils prennent comme certitude.

D'une façon récurrente l'animateur doit demander aux participants ce qu'ils peuvent faire avec le résultat des raisonnements : lister les actions à faire et les personnes chargées de les accomplir

Le but de la séance de création collective de sens n'est pas d'aboutir à la réponse qui serait la seule à être « juste ». Le but est d'aboutir à une construction d'une vision argumentable et qui peut déboucher sur des actions.

3.3.2 Description du travail de l'ERI dans le cas considéré

Les agressions numériques sont détectées dans la plupart des cas à travers des signaux et/ou signes faibles. Cette détection, difficile et complexe, suppose la mise en place d'un système de captage, de sélection et de remontée des informations à l'ERI rapportées au risque potentiel d'une agression. Vue la nature de ce type d'information, les phases de captage, de sélection et de remontée s'avèrent d'une extrême importance pour atteindre une conscience anticipative de l'occurrence d'une agression numérique.

Cependant, un fort pourcentage de ces signaux et/ou signes se révèlent insignifiants, ce qui est de nature à rendre le captage et la remontée de ces signes complexes et délicats.

La première étape dans le travail d'une ERI se réfère à la collecte d'un ensemble d'alertes à partir de métriques gérées par des systèmes de détection d'intrusion. Ces métriques sont en général définies conformément à une politique de sécurité interne, ainsi qu'une analyse des risques et des vulnérabilités.

La deuxième étape se réfère à l'amplification des signaux et/ou signes faibles captés. L'amplification se base sur l'analyse et l'interprétation des fichiers log associés aux signes captés, la traque des activités afférentes à ceux-ci et l'utilisation des fonctions multi objectifs pour calculer le degré de sévérité de l'alerte.

L'ERI procède ensuite à une collecte d'informations complémentaires qui devraient permettre de confirmer ou d'infirmer la possibilité d'une agression probable. Ces informations complémentaires peuvent être disponibles dans des bases de données situées dans des organismes spécialisées internationales (CERT, CLUSIF, etc....), comme elles peuvent être fournies par des entités à l'échelle internationale dont le rôle est de traquer les agressions

numériques et de collecter des informations liées aux nouvelles vulnérabilités et menaces des systèmes d'information. Ceci fournit un support adéquat pour la construction du scénario d'une agression. Cette collecte complémentaire permet une étude aussi systématique que possible du risque associé aux vulnérabilités du réseau de l'entreprise.

L'activité de création de liens entre les informations collectées est une activité fondamentale dans le travail d'une ERI dans le but de pouvoir construire le scénario de l'agression, réagir vite ou agir par anticipation. Ces liens peuvent être statiques comme les liens de causalité, de confirmation, et/ou d'opposition. Cependant, la complexité et l'évolution des variables de décision supposent une **typologie de liens plus riche**. En effet, l'ERI a besoin d'utiliser des règles de déduction dynamiques et des paramètres de décision non figés dans le temps et/ou dans l'espace. Ceci implique la création de **liens d'inférence** qui tiennent compte de l'évolution des contraintes imposées à l'entreprise et des actions opérées par les hackers.

Comme nous l'avons déjà signalé au deuxième chapitre, les ERI **manquent de méthodes** (et d'une **formation** appropriée) adéquates pour assister cette étape de création de liens entre les informations collectées de type signal et/ou signe faible. Nous ambitionnons de concevoir et de construire une méthode susceptible d'apporter un support adéquat à cette activité fondamentale pour le développement d'une capacité d'analyse et d'anticipation des agressions numériques afin de réagir vite, au bon moment et aux moindres coûts.

La création des liens statiques et d'inférence devrait contribuer à une construction collective du scénario de l'agression. L'ERI opère ensuite une évaluation des dégâts directs et indirects engendrés par l'agression ainsi que la définition des actions immédiates à accomplir pour y répondre, compte tenu de la nature d'activité de l'entreprise et des contraintes imposées à celle-ci. Cette étape est de nature à améliorer la visibilité de l'ERI par une identification du risque numérique ce qui est de nature à aider et à orienter la prise de décision par le choix des contre mesures appropriées.

Dans la dernière étape, comprenant la réparation des dégâts occasionnés par l'agression et l'anticipation des protections nécessaires pour réduire le risque d'être attaqué à nouveau dans le futur. En effet, l'ERI prend des mesures correctives nécessaires à la sécurité du système d'information de l'entreprise contre des agressions similaires susceptibles de se reproduire.

Cette étape devrait améliorer la capacité d'anticipation des membres de l'ERI par **apprentissage collectif** et par conséquent réduire le risque des agressions numériques.

Ainsi, le travail d'une ERI présente plusieurs ressemblances avec un groupe de création collective de sens tel que décrit dans le paragraphe précédent. Toutefois le **contexte spécifique** des agressions numériques présente certaines particularités qu'il est important de signaler.

1-La première particularité apparaît au niveau de la composition de l'ERI qui se caractérise par la présence d'un corps permanent technique outre les compétences managériales requises par la situation.

2-La deuxième est relative à la nature de l'agression numérique et à son signalement. Une ERI peut commencer parfois même son travail à partir d'un seul signe ou signal faible.

3-La troisième particularité est relative à la pression du temps imposée à la prise de décision dans le contexte des agressions numériques avec une urgence maximale pour analyser, construire le scénario et répondre.

En effet, dans le cas étudié, l'horizon temporel dans lequel les décisions doivent être prises par le comité de création collectif de sens est très court : de **l'ordre de quelques heures** au maximum. Au delà de ce délai une agression numérique peut avoir des conséquences négatives considérables pour les organismes agressés.

Une telle urgence est un cas plutôt extrême dans la prise de décision « stratégique » au sens où ce mot est défini dans la méthode L.E.SCA[®]. Souvent les délais sont plutôt de l'ordre de quelques semaines. Toutefois tout dépend du contexte. Ainsi pourrait-on dessiner un axe tel que :

Délai = 0 ←----- **curseur** -----→ délai = de l'ordre d'un an.

Cette particularité a plusieurs conséquences :

- Le face à face n'est pas une condition obligatoire vu l'urgence de la situation

- La pression très forte du temps justifie l'intérêt que nous portons pour les **TIC** susceptibles d'abrèger le plus possible les communications et les interactions entre les personnes chargées de la création collective de sens ERI.

Par ailleurs, dans le cas considéré, les personnes sont placées dans l'incertitude car elles doivent exploiter des informations de types signal et/ou signe faible. Elles ignorent qui est l'agresseur et la méthode qu'il a utilisée, et doivent tout de même prendre des décisions. De ce point de vue la situation ressemble aux situations rencontrées par une équipe de création collective de sens, du moins dans les cas les plus fréquents.

La différence c'est que l'agresseur, le metteur en scène de l'agression existe, il a un nom, une adresse et il est unique. Nous sommes dans un cas binaire : il existe ou il n'existe pas. Mais s'il existe il est unique : la solution finale est unique également. Il faut chercher à la reconstituer de la façon la plus **fidèle** possible.

Dans les autres cas habituellement rencontrés, les membres de l'équipe de création collective de sens doivent créer (inventer) une certaine vision de l'environnement avec lequel elles doivent interagir. Cet environnement n'existe pas en soi : il est le résultat d'une interprétation et d'une création (ceci est en accord avec la théorie de la contingence).

Sur la base des mêmes informations utilisées en input, une entreprise créera un sens S1 et prendra des décisions D1. Une autre entreprise, sur la base des mêmes in put créera un sens S2 et prendra des décisions D2. Une troisième entreprise... etc.

Rien ne permet de dire que l'une de ces entreprises a raison et qu'une autre a tort. Tous les choix peuvent se révéler mauvais après coup, ou bien tous les choix peuvent se révéler également bons, après coup. Il n'y a pas de réponse unique. Ceci a bien été traduit par la **théorie de la contingence** (Lawrence et Lorsch, 1967).

Les conséquences pour notre étude :

- Dans notre cas d'étude, nous avons l'espoir de tendre itérativement vers une connaissance actionnable de plus en plus satisfaisante et efficace, d'où l'importance du cumul des retours d'expériences et de la mémorisation des traces des

raisonnements effectués (traçabilité) pour améliorer toujours plus et de l'apprentissage collectif.

- Dans le cas de contingence cet espoir est sans fondement puisque une fois que l'entreprise a réalisé une analyse du risque numérique et mis en place une politique de sécurité, les scénarios d'attaques sont réduits et l'ERI se trouve devant l'obligation de construire le scénario le plus approprié, et ce, le plus rapidement possible.

Conclusion Chapitre 3

Le troisième chapitre a eu pour objectif de transposer et d'adapter la méthode L.E.SCA[®], qui représente un dispositif de Veille Anticipative Stratégique et d'Intelligence Collective (VAS-IC[®]), au domaine de réponse aux agressions numériques. Trois phases de cette méthode concernent particulièrement notre domaine de recherche à savoir la création collective de sens, la mémorisation et l'animation.

Dans ce chapitre, nous avons mis l'accent sur les enrichissements escomptés de la méthode L.E.SCA[®] concernant ces trois phases. Par rapport à la phase de création collective de sens, notre apport se situe au niveau de l'extension des liens, l'utilisation du calcul matriciel pour assister et formaliser la construction des chemins de raisonnement.

Au regard de la phase de mémorisation, nous avons montré l'intérêt de l'utilisation des TIC pour la conception de mécanismes de structuration et de gestion des mémoires en base de données et base de connaissances ainsi que les mécanismes de recherche de type « **recherche approchée** » en établissant des liens sémantiques, probabilistes entre les éléments en mémoire.

S'agissant de la fonction d'animation, notre intérêt se limite au périmètre du processus de création collective de sens et au processus de prise de décision en proposant des éléments de méthode et des heuristiques générales pour faire converger et concilier les points de vue ainsi que pour aider à la prise de décision collective.

Sur le plan pratique, nous avons montré l'intérêt de l'utilisation de certaines potentialités techniques de l'Internet comme support à notre méthode proposée. Ces potentialités intègrent les techniques d'accès et de contrôle d'accès, les mécanismes de structuration et de recherche des informations. Ceci est de nature à assister le processus d'intelligence collective et de garder la trace des raisonnements effectués lors de ce processus ainsi que des heuristiques pouvant émerger de celui-ci.

Conclusion de la première partie

Rappelons que le premier objectif de recherche est de répondre à une problématique de terrain à travers la conception et la construction d'une méthode d'aide à la réduction du risque des agressions numériques.

Le premier chapitre justifie cet objectif sur un double plan managérial et académique. Dans le deuxième et le troisième chapitre, nous avons rassemblé un ensemble de connaissances théoriques et/ou actionnables potentiellement pertinentes par rapport à notre question de recherche dans le but de les utiliser lors de la conception et de la construction de notre méthode.

2^{IEME} PARTIE

**Conception, construction, expérimentation de la MARRAN et
évaluation des résultats**

Introduction de la deuxième partie

La deuxième partie est consacrée à la conception, à l'expérimentation et à l'évaluation de la MARRAN.

Ainsi, le quatrième chapitre présente le cadre conceptuel de la MARRAN qui constitue une articulation et une extension des différentes connaissances théoriques et actionnables présentées en première partie. Nous montrons également l'intérêt du modèle conceptuel de la MARRAN dans le domaine de réponse aux agressions numériques à travers le travail d'une ERI.

Le cinquième chapitre propose quatre cas réels d'agressions numériques pour expérimenter la MARRAN tout en soulignant les conditions d'expérimentation de celle-ci, en vue de sa réplication pour d'autres cas. Nous présentons également dans ce chapitre un logiciel qui a été conçu et développée pour supporter la MARRAN.

Le sixième chapitre énonce les résultats d'évaluation de la MARRAN suite à l'exploitation des données recueillies lors des entretiens semi directifs auprès des experts en sécurité informatique en signalant les contributions théoriques et pratiques des résultats empiriques de la recherche.

Conception de la méthode proposée pour assister les ERI

Ce chapitre est consacré à la formulation du cadre théorique de la méthode proposée dans la présente recherche, pour assister le travail d'une ERI, à travers la présentation de son **modèle conceptuel**. Dans cette présentation, nous procédons par une utilisation et une extension des connaissances développées dans les chapitres précédents, particulièrement les connaissances théoriques concernant la création collective de sens.

Ainsi, la première section présente les **fondements théoriques** du modèle conceptuel de la méthode proposée dans le présent travail à travers notamment l'utilisation et l'extension des cartes causales pour la **représentation et la formalisation** du modèle conceptuel.

La deuxième section montre l'intérêt de l'utilisation de notre modèle conceptuel dans les travaux des ERI à travers une adaptation de la terminologie et une illustration par un exemple réel d'une agression numérique.

La troisième section expose les opérations de manipulation et de raisonnement sur les **liens** en se focalisant particulièrement sur le processus de **médiation**, d'une façon générale.

La quatrième section met l'accent sur le **rôle de la médiation** dans les travaux des ERI ainsi que le rôle des TIC pour soutenir cette activité fondamentale dans le processus de création collective de sens.

Dans la cinquième section, nous présentons des **critères pour mesurer le succès** des systèmes d'information, utilisés d'une façon générale. Nous proposerons, pour les transposer à notre domaine, certains critères disponibles dans les publications, que nous adapterons si nécessaire, et nous serons amenés à les compléter avec des critères supplémentaires.

4.1 Modèle conceptuel de la méthode proposée pour assister le travail d'une ERI

Le modèle conceptuel est structuré selon trois phases essentielles. Ces phases décrivent le processus collectif de raisonnement créatif à partir d'informations de type signal et/ou signe faible dans un contexte incertain et turbulent. Dans le cas du travail d'une ERI l'objectif d'un tel processus est de **construire le scénario de l'agression** numérique afin de réduire le risque, d'y **répondre** le plus rapidement possible et d'**anticiper** l'occurrence d'agressions similaires dans le futur. Nous définissons dans cette section la nature des noeuds et des liens qui soutiennent le modèle conceptuel ainsi que les opérations de création d'un chemin de raisonnement.

4.1.1 Les trois phases du modèle conceptuel

Phase 1. La première phase décrit l'activité de **création des liens initiaux**. Son objectif est d'amplifier le signal et/ou signe faible détecté et d'établir des liens capables de donner une première idée sur le risque potentiel encouru par l'entreprise. Il est nécessaire d'établir une typologie des liens de raisonnement pour organiser, d'une façon significative, les informations disponibles. Celles-ci proviennent des signaux et/ou signes faibles amplifiés, des sources internes ou externes, ainsi que de la contribution des acteurs du processus de création collective de sens. Les liens initiaux devraient être capables de tracer et d'appréhender l'évolution des variables critiques à l'analyse dans un contexte incertain et turbulent.

Phase 2. La deuxième phase, cruciale dans le processus, décrit l'activité de création des **liens d'inférence** par raisonnement itératif. Durant cette phase, des nouveaux liens sont inférés itérativement en utilisant les liens existants, les **connaissances tacites** des acteurs du processus de création collective de sens. Les acteurs peuvent également extraire des **informations documentaires** prélevées dans des archives structurées et actualisées tout au long du processus, afin d'aboutir à une vision plus intelligible de la situation. De plus, cette phase requiert :

- des heuristiques appropriées, et
- la transformation automatique des liens pour créer des nouveaux liens qui seront présentés ultérieurement dans ce chapitre.

Phase 3. Dans la troisième phase des critères de satisfaction (des membres de l'ERI et des responsables qui auront à prendre la décision finale) sont définis pour mettre fin au processus de raisonnement sur les liens. Cette phase a pour objectifs:

- la **vérification** si le processus itératif de raisonnement parvient à une connaissance claire du risque encouru,
- une bonne compréhension des mécanismes qui ont généré les signaux et/ou signes faibles détectés, et
- une estimation globale d'autres risques potentiellement liés à l'agression en cours d'examen.

A la fin de cette phase, un plan d'action peut être déclenché pour proposer, en cas de besoin, les réponses requises pour réduire le risque identifié et anticiper des décisions liées à celui-ci.

L'instrumentation du modèle conceptuel et la mise en œuvre peuvent être basées sur l'utilisation de la technologie Internet, qui peut fournir :

- Une **base de données** pour stocker des informations liées aux risques encourus par l'entreprise et **garder la trace** toutes les informations générées lors de la phase de raisonnement sur les liens
- Une base de connaissance qui stocke tous les **raisonnements** sur les signaux/signes faibles et la trace de tous les liens inférés lors du processus d'intelligence collective.

Les bases de données et de connaissances fournissent un support pour un processus de création collective de sens **dynamique**. Ces bases sont assistées par des mécanismes intelligents d'extraction permettant la **recherche approchée**, la recherche des heuristiques et la transformation automatique des liens stockés.

4.1.2 Représentation du modèle conceptuel

Le modèle conceptuel est représenté par un graphe orienté, composé d'un ensemble de nœuds et de relations liant ces nœuds entre eux. Une extension des cartes causales est employée pour la représentation du modèle conceptuel, ne se limitant pas aux seuls liens de causalité. D'autres types de liens seront utilisés.

Définition de « lien » : Nous définissons un lien par un graphe orienté et libellé comme suit :

$$LC: (N, E, f: E \rightarrow [0, 1], g: E \rightarrow \Delta) \quad (1)$$

Les composants de ce graphe sont un ensemble de N noeuds, un ensemble de E arcs, une fonction f qui associe à chaque label une valeur probable, et une fonction g qui indique une relation d'influence entre les labels.

Un noeud représente un concept (par exemple une hypothèse, un objectif), une action à entreprendre, ou une information de type signal et/ou signe faible pertinente pour le raisonnement lors du processus de création collective de sens. Un arc représente une relation de dépendance entre les actions ou bien une relation causale entre les concepts.

Nous considérons Δ un ensemble de relations incluant les trois relations causales classiques, des relations variables en fonction du temps, et des relations transactionnelles de type output/input. Nous supposons que Δ est définie comme suit:

$$\Delta : \{+, -, 0, \leq, OI\} \quad (2)$$

Où,

(+): signifie qu'un noeud i a un effet positif sur un noeud j ;

(-): signifie qu'un noeud i a un effet négatif sur un noeud j ;

(0): signifie qu'un noeud i n'a pas d'effet sur un noeud j ;

(\leq): signifie qu'un noeud i devrait précéder dans le temps un noeud j ; et

(OI): (relations de type output/input) signifie que l'output du noeud i est l'input du noeud j .

Les trois premières relations sont déjà étudiées par Chaib-draa (2002). Les deux dernières sont **ajoutées** pour couvrir une partie des raisonnements dans lesquels l'ambiguïté des informations, et l'incertitude sont des notions critiques.

En se basant sur la définition ci-dessus, les arcs représentent des relations causales ou de dépendance affirmant comment un noeud peut affecter un autre noeud avec une valeur qui mesure la probabilité de cette affirmation. Les probabilités associées à ces relations sont supposées **variables en fonction du temps**, dans la mesure où la valeur probable assignée à un label peut varier d'un moment à un autre.

A titre d'**exemple**, supposons que C_1 , C_2 et C_3 désignent trois concepts qui représentent respectivement une information, une action à entreprendre et un objectif à atteindre. Le concept C_1 influence positivement le concept C_2 signifie qu'une information détenue ou captée par une entreprise peut activer la mise en œuvre d'une certaine action afin de tirer profit de l'opportunité ou de diminuer le risque que peuvent révéler cette information. Cette action à entreprendre est de nature à précéder dans le temps un objectif à atteindre dans la mesure où la réalisation à court, à moyen ou à long terme de cet objectif (le concept C_3) dépend de cette action (concept C_2).

La représentation graphique de ces relations entre les trois concepts C_1 , C_2 et C_3 peut s'énoncer comme suit :

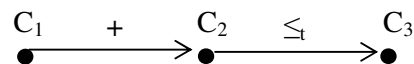


Figure 7: Représentation graphique des relations entre C_1 , C_2 et C_3

4.1.3 Construction d'un chemin de raisonnement

La connexion des nœuds avec les arcs libellés par les relations décrites plus haut constitue le résultat de base de la construction d'un chemin de raisonnement à partir du contenu des nœuds. Par conséquent, la connexion des nœuds conduit à la construction d'un chemin de raisonnement désignant un point de vue partiel ou intégral d'un acteur du processus de création collective de sens et par rapport à une situation donnée.

Un chemin de raisonnement P reliant un nœud n_1 à un nœud n_s dans un graphe est défini comme étant une séquence d'arcs libellés :

$$P: (n_1n_2), (n_2n_3), \dots, (n_s n_{s+1}) \quad (3)$$

Où $(n_i n_{i+1})$ est un arc caractérisé par son label tel que défini dans l'équation (2).

Comme les noeuds peuvent représenter des concepts, des actions ou des informations diverses, nous pouvons considérer qu'un nœud est une variable qui peut prendre des valeurs dans un domaine donné. Un modèle mathématique peut être développé pour déterminer la valeur d'un nœud dans un domaine donné et pour manipuler les chemins de raisonnement automatiquement au sein du même graphe. Les principales caractéristiques de ce modèle concernent :

- la représentation des liens: les liens peuvent être représentés à l'aide d'une matrice. Le $(i, j)^{\text{ième}}$ composant de la matrice décrit l'affirmation selon laquelle un nœud i exerce un effet sur un nœud j .
- la composition des liens: supposons C_1 et C_2 deux liens contenant respectivement n nœuds et p nœuds (avec $n \geq p$). Ainsi, la composition de C_1 et C_2 , représentée par $C_1 * C_2$, est le lien obtenu par la sommation/la collecte de tous les nœuds et les arcs ensemble. Les liens, qui désignent et montrent des associations de causalité et de dépendance, représentent le raisonnement qui soutient le processus de création collective de sens. Ils permettent la prévision des actions futures, l'explication des événements passés, et l'anticipation des effets. Les liens créés offrent également des moyens pour choisir entre des actions alternatives. Pour ce but, plusieurs opérations sur les liens peuvent être implémentées. Parmi les opérations les plus importantes, nous pouvons citer les opérations de remplacement et de réécriture. La prochaine section détaille en profondeur la nature et l'utilité de ces opérations.
- La construction d'un chemin de raisonnement : une opération mathématique classique basée sur la multiplication des matrices et la composition des relations, peut être développée. En effet, si C est un lien, donc:

$$C^2 = C . C$$

$$C^n = C^{n-1} . C \quad (4)$$

Où $(.)$ désigne la multiplication des matrices, qui une fois implémentée, utilise la composition des relations définies comme suit :

Si R et R' sont des relations entre des nœuds appartenant à l'ensemble Δ , alors le produit de R et R' ($R . R'$) indique spécifie toutes les paires de nœuds reliées les unes aux autres en

utilisant R et R'. Pour cette raison, nous disons que C^2 est un chemin de longueur 2 et C^n est un ensemble de chemins de longueur n.

4.1.4 Exemple illustratif

L'objectif de cet exemple fictif est de concrétiser les notions présentées dans cette section pour la représentation et la formalisation du modèle conceptuel de la méthode proposée dans ce travail de recherche.

Soient N_1 , N_2 , N_3 , et N_4 quatre nœuds représentant respectivement une information, une hypothèse, une action à entreprendre, un objectif à atteindre.

Nous pouvons imaginer un chemin de raisonnement reliant ces quatre nœuds. Supposons qu'une information captée par une entreprise incite à l'exploitation ou le traitement de cette information par la formulation d'une certaine hypothèse en relation avec cette information. Cette hypothèse de nature variable en fonction du temps peut contribuer à mettre en œuvre une certaine action. Cette même action peut être intégrée dans le raisonnement comme input afin de réaliser un objectif précis.

Une matrice (de dimension 4 x 4) appelée C, peut être utilisée pour représenter les relations entre les quatre nœuds.

$$C = \begin{matrix} & \begin{matrix} N_1 & N_2 & N_3 & N_4 \end{matrix} \\ \begin{matrix} N_1 \\ N_2 \\ N_3 \\ N_4 \end{matrix} & \begin{pmatrix} 0 & + & 0 & 0 \\ 0 & 0 & \leq_t & 0 \\ 0 & 0 & 0 & OI \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

Le chemin de raisonnement liant N_1 à N_4 peut être déduit et construit par multiplication de la matrice C par trois.

$$C^3 = \begin{matrix} & N_1 & N_2 & N_3 & N_4 \\ \begin{matrix} N_1 \\ N_2 \\ N_3 \\ N_4 \end{matrix} & \left(\begin{array}{cccc} 0 & 0 & 0 & (+, \leq, OI) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \end{matrix}$$

La matrice C^3 peut être transposée à travers la représentation graphique du chemin de raisonnement de longueur 3.

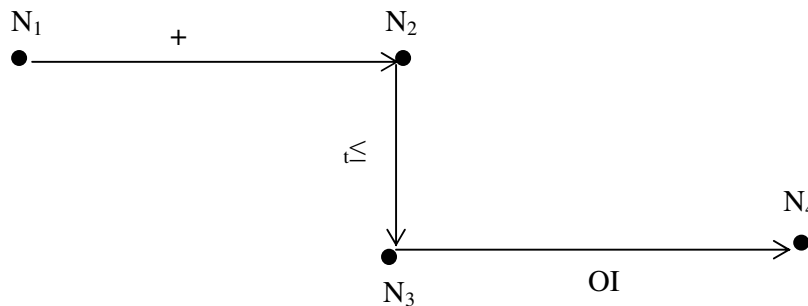


Figure 8: Chemin de raisonnement de longueur 3

4.2 Utilisation du modèle conceptuel dans les travaux des ERI

Nous avons montré que l'ensemble des liens (décrits plus haut) présente des fonctionnalités témoignant leur utilité potentielle par rapport à une démarche heuristique. En effet, une démarche d'essence heuristique prend en considération les schémas cognitifs permettant de résoudre des problèmes complexes en situation d'informations incomplètes.

Dans cette section, nous adaptons la terminologie utilisée dans la représentation du modèle conceptuel au niveau du travail d'une ERI. Puis, à l'aide d'un exemple d'une agression numérique réelle, nous appuyons cette adaptation.

4.2.1 Adaptation de la terminologie

L'utilisation des liens pour la représentation du modèle conceptuel se base sur un ensemble de nœuds et d'arcs. Les nœuds représentent des actions, des hypothèses, des informations, ou des objectifs. Dans le domaine de la sécurité informationnelle, les actions incluent, mais ne sont pas limitées à :

- Une intrusion ou un abus d'utilisation d'une action,
- Un accès non autorisé, et
- Une obtention de certaines informations non autorisées ou une exécution d'une opération non autorisée sur les ressources de l'entreprise.

Les hypothèses incluent des décisions ou des contre-mesures à entreprendre au niveau du système d'information afin de le protéger ou de limiter les dégâts occasionnés par une agression numérique. Les objectifs peuvent être par exemple :

- la ressource X est face à une agression spécifique,
- le système X est protégé d'une manière appropriée, ou
- l'agression X est identifiée

Les informations représentées par des nœuds sont des signaux et/ou signes faibles (détectés par les systèmes de captage au niveau du réseau de l'entreprise) ou toute autre information utile à la détection, à l'analyse ou à la réponse à une agression numérique potentielle. Les arcs indiquent le type d'influence entre deux nœuds. Comme nous l'avons déjà signalé, Il existe **cinq types de relations d'influence** entre les nœuds :

- une relation positive (+) qui indique que le nœud n_1 est nécessaire pour, rend possible, augmente, active, aide, ou améliore le nœud n_2 . Dans le domaine de sécurité réseau, une première information collectée peut indiquer un risque potentiel qui peut activer la réalisation d'une certaine action.
- une relation négative (-) qui indique que le nœud n_1 entrave, endommage, empêche, ou inhibe le nœud n_2 . Par exemple, si le nœud n_1 est une contre-mesure et le nœud n_2 représente une possible action, alors la relation (-) combine l'effet de la contre-mesure à l'action proposée.

- une relation neutre (0) qui indique l'absence d'influence entre les noeuds.
- une relation transactionnelle (de type Output/Input) entre n_1 et n_2 qui indique que l'output de n_1 est l'input de n_2 . Comme input, nous pouvons mentionner une adresse IP, un mot de passe, une information non autorisée, etc.
- une relation variable en fonction du temps (\leq_t) qui indique une relation dynamique entre la réalisation du contenu des deux nœuds en fonction du temps. Dans notre cas d'étude, le temps constitue une variable importante pour établir des relations significatives entre les informations collectées et mémorisées en vue de détecter une éventuelle agression.

Ces relations permettent une estimation qualitative de l'effet d'un concept sur un autre et répondent au besoin de quantifier ensuite cet effet. Ceci devrait permettre la construction du scénario définitif de l'agression et l'estimation de ses conséquences.

Pour réduire la complexité des raisonnements, la technologie Internet peut être utilisée pour accéder à des sites Web utiles connus par leur riche documentation en fournissant des informations sur toutes les agressions déjà connues et réalisées (par exemple des informations publiées sur le site Web du CERT). Dans ce cas, le recours à l'utilisation de la technologie Internet réduit d'une manière significative le nombre des agressions candidates et contribue à la convergence des points de vue des membres de l'ERI en cas de conflit.

4.2.2 Cas d'application

Nous reprenons dans ce paragraphe l'exemple que nous avons déjà avancé au troisième chapitre afin de représenter les nœuds et certaines relations d'influence, et de décrire l'opération de construction de deux chemins de raisonnement contradictoires à partir des informations relatives à cet exemple.

Rappelons qu'il s'agit d'une agression numérique qui a visé la **dégradation de l'activité d'un site Web** d'une entreprise opérant dans le domaine des TIC. La prise de conscience de cette agression s'est fait suite à la réception d'une information de type signal faible, rapportée par un utilisateur final, et alertant sur une possible agression numérique contre le site Web de l'entreprise.

Un premier chemin de raisonnement de longueur trois a été conduit par l'ERI de l'entreprise en question. En effet, l'ERI a commencé son investigation par la vérification des fichiers log et de l'état du système d'exploitation. La vérification des états d'entrées et de sorties au système d'exploitation n'a pas signalé l'existence d'un comportement suspect. Cette constatation a renforcé la conclusion de la non évidence d'une agression. Ces deux actions représentent des nœuds significatifs pour commencer le raisonnement. L'absence d'irrégularités dans l'état des entrées et des sorties dans le système d'exploitation et dans le réseau a favorisé la conclusion relative à la non évidence de l'agression numérique. Cette dernière hypothèse constitue un input significatif qui peut être intégré dans le raisonnement et qui conduit l'ERI à ignorer le signal faible. L'ignorance du signal renforce l'hypothèse de l'absence d'une agression.

Cependant, un autre chemin de raisonnement de longueur trois également pouvait être conduit dans cet exemple si l'ERI avait envisagé une relation positive probable entre le signal faible et l'existence d'une évidence d'agression.

La figure 6 montre les nœuds et les relations relatifs à l'analyse de la situation confrontée par l'entreprise suite à une alerte, signalée par un utilisateur final, sur une possible agression numérique contre le site Web de l'entreprise.

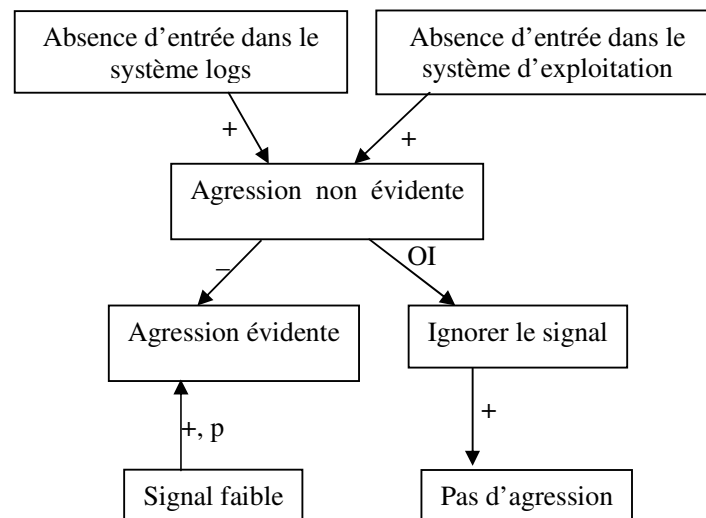


Figure 9: Représentation du raisonnement de l'ERI dans le cas considéré

Le raisonnement peut être facilement représenté par une première matrice C pour décrire les relations entre les nœuds. Le chemin de raisonnement qui a conduit l'ERI à ignorer le signal et l'inexistence d'une agression est de longueur trois. Il peut être obtenu à travers la multiplication de la matrice C par trois.

4.3 Raisonnements basés sur l'ensemble des liens présentés dans le modèle conceptuel

Plusieurs opérations, comme les opérations de remplacement ou de réécriture, sont appropriées dans le cas de la sécurité du réseau d'entreprise afin de construire le scénario de l'agression, réduire le risque et **anticiper** des agressions similaires. De plus, ces opérations peuvent intéresser également le processus de médiation et assister le processus de prise de décision.

4.3.1 Les opérations sur les nœuds et sur les liens

Certaines opérations sur les liens sont importantes à opérer lors d'un processus de création collective de sens dans un contexte qui se caractérise par l'**incertitude**. Ces opérations permettent d'**élargir le champ du raisonnement**, de choisir parmi plusieurs alternatives afin d'aboutir à une construction finale d'une vision collective.

Parmi ces opérations, nous proposons **deux types d'opérations** : de remplacement et de réécriture.

L'opération **de remplacement** est liée directement au contenu d'un nœud et consiste à remplacer (au sens strict du mot) mais aussi à substituer (de façon **approximative**), ou éclater, un nœud par un réseau de nœuds et de liens afin de clarifier et de mettre en évidence les sous implications du nœud. Plusieurs méthodes peuvent être utilisées pour accomplir le remplacement d'un nœud notamment en se basant sur l'équivalence, l'approximation, la réduction, ou la restriction.

Il est clair que le remplacement d'un nœud devrait être accompagné par une redéfinition des relations, des nœuds et des arcs qui prennent comme point d'arrivée ou de départ le nœud remplacé. La redéfinition procède par des méthodes de réduction, d'approximation, et d'ajout de concepts (comme l'ajout d'une information complémentaire).

Ainsi, le remplacement d'un nœud par réduction du concept représenté par ce nœud, par exemple, implique des modifications appropriées des labels et des liens engendrés par ce nœud.

Dans le domaine d'analyse et de réponse aux agressions numériques, supposons, par exemple, que le système de surveillance du trafic sur le réseau d'une entreprise ait détecté trois actions suspectes. Supposons qu'un des membres de l'ERI ait introduit un concept pour donner un point de vue décrivant un lien possible entre les trois actions. Un autre membre peut, lui, formuler un autre point de vue basé sur un ou plusieurs autres concepts qui n'ont rien à voir avec le premier concept introduit dans le raisonnement.

La figure 7 montre l'opération de remplacement d'un nœud D par un réseau de nœud ce qui est de nature à redéfinir les relations liées directement à ce nœud (c'est-à-dire les relations L₃, L₄ et L₅).

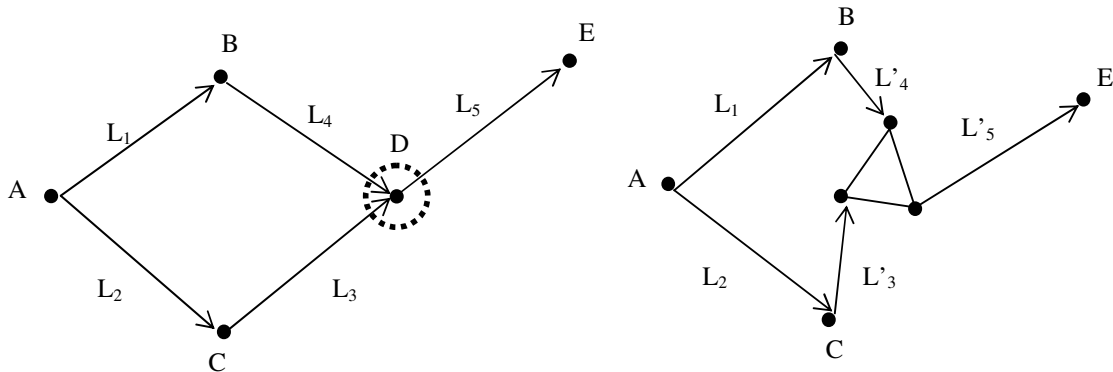


Figure 10: Opération de remplacement d'un nœud

L'opération **de réécriture** est liée directement à un sous réseau de nœuds et consiste à remplacer des éléments de raisonnement représentant un point de vue particulier par un sous réseau de nœuds et de liens représentant un autre point de vue plus pertinent et qui peut être intégré au reste du graphe. Cette opération améliore la signification de la vision globale, offre une alternative de raisonnement et **affine** le processus de raisonnement.

Plusieurs méthodes peuvent être utilisées pour accomplir cette opération comprenant notamment la réécriture, la suppression ainsi que la dissimulation de certains liens de raisonnement d'un sous réseau. La réécriture d'un sous graphe permet, par exemple, de **fournir plus d'alternatives** pour les différentes actions à mener afin d'atteindre un objectif donné.

La figure 8 montre l'opération de réécriture d'un réseau de nœuds par un autre au niveau du nœud D.

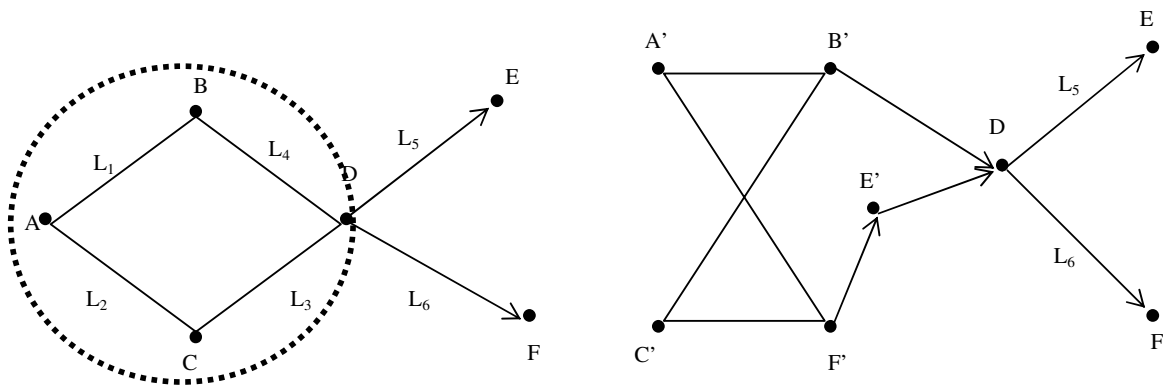


Figure 11: Opération de réécriture d'un réseau de noeuds

Seul le nœud D est partagé entre les deux points de vue c'est-à-dire que le remplacement supprime totalement les concepts A, B, C et les liens qui les concernent pour remplacer le tout par un autre point de vue.

Ces opérations (de remplacement et de réécriture) sont importantes à manipuler lors de la construction du scénario d'attaque, du processus de médiation et de prise de décision. Elles peuvent être transposées au niveau des matrices associées.

4.3.2 Le processus de médiation

Afin d'intégrer le raisonnement sur les liens qui soutient le point de vue subjectif de chaque membre, tous les concepts sont codés (comme les noeuds) dans le même graphe, donc tous

les points de vue peuvent être facilement transformés en une unique matrice M de taille n x n où n est le nombre de concepts. Dans cette matrice, chaque élément peut être représenté comme suit :

$$m_{ij} = \ell_1, \ell_2, \dots, \ell_v$$

Où v est le nombre des vues, et ℓ_k est un label placé par le $i^{\text{ième}}$ membre dans l'arc reliant le noeud i à j.

La matrice M permet l'étude des cas suivants:

- les zones de consensus où les membres perçoivent les mêmes relations d'influence. Ces aires se caractérisent par des multi labels de même forme. Dans ce cas, nous avons l'indice suivant:

$$m_{ij} = \ell, \ell, \dots, \ell$$

- les zones de désaccords partiels qui se caractérisent par des perceptions similaires des relations d'influence entre les nœuds. Toutefois, les valeurs probables assignées aux labels sont différentes.
- les zones de désaccords qui se caractérisent par des labels perçus en conflit par les membres.

Des multi labels particuliers sont désignés par des points de vue unilatéraux. Ils expriment une estimation unilatérale de l'effet entre deux noeuds, désignés respectivement par i et j. Dans ce cas, le multi label m_{ij} , est écrit comme suit:

$$m_{ij} = 0, \dots, 0, \ell, 0, \dots, 0 \quad \text{and} \quad \ell \neq 0$$

La **conciliation** des différences entre les points de vue des membres de l'ERI devrait se focaliser sur trois principaux objectifs suivants :

- la réalisation d'une définition commune et/ou partagée de tous les concepts, les actions et les informations pertinents pour l'évaluation et l'analyse de la situation
- l'élimination des désaccords partiels en utilisant la négociation ou encore l'investigation en s'appuyant sur les TIC
- la réduction du nombre des vues unilatérales et les zones de désaccords partiels visant à diminuer les différences.

Le **médiateur** peut contribuer à l'accomplissement de toutes ces activités. Une base de données documentaires et de connaissances formalisées mentionnées précédemment peuvent constituer des outils appropriés pour supporter ces issues et les problèmes concernant la médiation.

De plus, le modèle formel supportant la représentation des nœuds et des liens, la manipulation des relations, et l'intégration des vues subjectives, peut être instrumenté au moyen de la technologie de l'Internet afin d' « assister » les activités de médiation.

4.3.3 La prise de décision, en aval du travail (*stricto sensu*) de l'ERI

Rappelons qu'il faut distinguer deux cas de figure :

- celui où la pression du temps exige que l'ERI prenne une décision immédiatement, sans accord préalable de la hiérarchie ;
- celui où c'est la hiérarchie qui prend la décision, en tenant compte probablement des avis de l'ERI. C'est le cas le plus fréquent.

Après avoir concilié les différences entre les raisonnements des membres d'un groupe de création collective de sens à travers le processus de médiation, leurs vues peuvent être représentées par un graphe unique. Ce graphe va être visualisé afin d'aider à résoudre essentiellement les décisions indéterminées.

La prise de décision autour d'un problème **peut commencer comme suit** : étant donné un graphe pouvant inclure une décision, un objectif (ou plusieurs) (i.e., des informations ou des actions représentées par des liens et par des nœuds), il s'agit de déterminer quelle décision prendre, ou bien rejeter, en fonction de la réalisation de l'objectif.

Dans le **domaine de la sécurité**, plusieurs types de décisions sont à prendre :

- vérifier si un signal faible révèle effectivement une agression (par exemple une action malveillante sur des ressources protégées)
- choisir le meilleur chemin d'influence entre une hypothèse et une action ou un objectif
- construire le scénario d'attaque réalisé par le hacker (ceci inclut la reconnaissance de toutes les opérations, actions ou informations significatives pour l'attaque)
- sélectionner parmi les réponses possibles celle qui répond au mieux, compte tenu des contraintes, de la nature d'activité de l'entreprise ainsi que de ses objectifs stratégiques.

Le chapitre cinq montrera, à travers des exemples réels d'agressions numériques, l'utilisation de ces raisonnements.

Pour aboutir à une proposition de décision, le médiateur doit calculer la totalité des relations d'influence reliant les décisions à l'objectif (tous les chemins qui connectent les décisions à l'objectif). Généralement, les décisions qui contiennent seulement des effets positifs sont retenues et les décisions impliquant des chemins négatifs sont écartées.

Les chemins de raisonnement qui sont en conflit entre eux mènent à des décisions **indéterminées**. Résoudre cette situation est une activité difficile. Plusieurs techniques peuvent être utilisées pour assister cette activité, pouvant consister à :

- supprimer tous les segments composant un chemin de raisonnement particulier, qui ont une influence négative. Ceci signifie que l'objectif est évalué d'une façon relative compte tenu de certaines hypothèses,
- supprimer les chemins positifs afin d'analyser l'impact d'une décision sans considérer l'influence positive,
- **suggérer** une compensation possible. Nous supposons que l'impact d'une décision sur un objectif produit un effet positif qui a plus de valeur que son impact négatif. La décision est ainsi retenue,
- choisir entre plusieurs décisions alternatives. Ceci peut être aidé par la recherche d'informations complémentaires,

- affiner le raisonnement en ajoutant des concepts, des connaissances en mémoire ou des informations disponibles dans des bases de données internes ou externes à l'entreprise.

4.4 La médiation dans les travaux de l'ERI

Nous mettons maintenant l'accent sur l'importance de l'activité de médiation dans le travail d'une ERI ainsi que l'apport potentiel de la technologie Internet pour fournir un support éventuellement approprié à cette activité.

4.4.1 Rôle du médiateur

Nous avons déjà montré le rôle de la médiation dans le processus de création collective de sens. Le médiateur négocie avec chaque participant en conflit afin de parvenir à un arrangement mutuel satisfaisant. Le médiateur construit et analyse une nouvelle matrice qui représente tous les noeuds et toutes les relations qui sont pertinents à la situation afin d'identifier des conflits potentiels. La médiation, dans le processus de création collective de sens pour réduire le risque des agressions numériques, couvre un ensemble d'actions qui ont pour objectifs de:

- Aider les membres afin de construire des vues individuelles de la situation,
- Concilier les vues individuelles divergentes,
- Aider pour construire la représentation collective et pour interpréter celle-ci.
- Affiner les vues collectives.

L'activité de médiation est effectuée par un médiateur dont le rôle est l'**animation**, la convergence vers des actions collectives, la construction des alternatives en matière de décision, et l'extraction des concepts/informations si nécessaire. Le médiateur peut ajouter, réduire ou supprimer des liens construits et des sélections d'information.

Ainsi, le médiateur a besoin d'outils efficaces pour assister la représentation des noeuds et des liens ainsi que la manipulation des relations entre les noeuds. De plus, il a besoin des moteurs

de recherche efficaces (pour des raisons liées à la pression du temps) pour extraire des informations complémentaires stockées dans des bases de données internes ou externes.

Pour résoudre les problèmes et intégrer les différents graphes, le médiateur devrait avoir également certaines **compétences** pour accomplir ce rôle efficacement. Les principales compétences appropriées sont la **pédagogie**, la **crédibilité** (fondée sur l'expertise et l'expérience), la **confiance**, la **communication**, et la **coordination**. Ceci soulève les questions de la sélection et de la **formation** du médiateur.

Les activités de médiation dépendent de la nature d'activité de l'entreprise, de ses objectifs, des opportunités et des menaces de son environnement ainsi que des compétences et du **degré d'implication** des membres du processus de création collective de sens. Un ensemble d'actions devrait inclure:

- La validation des concepts qui sont représentés par les nœuds,
- La consolidation actualisée des liens qui sont représentés par les arcs,
- La construction de tous les chemins de raisonnement qui supportent la représentation collective après convergence des opinions des membres de l'ERI, puis éventuellement la prise de décision qui pourra en résulter.
- Le contrôle du processus d'affinement afin d'aboutir à une vision collective.
- La construction des heuristiques qui ont émergé au cours du travail de l'ERI

4.4.2 Rôle espéré de la technologie Internet dans le processus de création collective de sens ainsi que de médiation

Les publications spécialisées ont montré l'importance des TIC, d'une façon générale, dans le processus de prise de décision et de la formulation de la stratégie (Ackermann et Eden, 2001). Plusieurs études ont prouvé, par exemple, que certaines technologies d'aide au travail collectif peuvent fournir un support significatif à un groupe de créativité (Masseti, 1996; Wierenga et Bruggen, 1998) et améliorer la qualité de l'intelligence collective « *organizational intelligence* » au sein de l'organisation (Huber, 1990). Des modèles ont été

proposés pour décrire particulièrement l'impact de l'Internet sur la qualité du processus de « *competitive intelligence* » (Teo, 2000; Teo et Choo, 2001) ainsi que sur l'amélioration de la qualité et de la performance d'une équipe de travail (Elmuti, 2003).

En effet, l'Internet est de plus en plus considéré comme étant une source d'informations nombreuses et variées qui concernent divers domaines (Brabston et McNamara, 1998) et par la suite un possible accélérateur de l'intelligence stratégique (Marmuse, 1992-1996) définie comme étant la mise en œuvre “ des dispositifs efficaces afin de collecter, traiter et diffuser les informations pertinentes et fiables indispensables à la prise de décision ” (Revelli, 1998).

Chen et al. (2002) proposent un outil qui supporte certaines phases du processus de l'intelligence compétitive appelé, *Competitive Intelligence Spider*, et qui dépasse les insuffisances des moteurs logiques disponibles sur Internet en offrant des possibilités plus importantes pour une collecte en temps réel des pages Web spécifiées par l'utilisateur, une structuration et une indexation des documents collectés utiles pour l'analyse des sites Web dont le contenu et l'évolution intéressent le veilleur.

Plusieurs autres études se sont intéressées aux avantages des agents intelligents (Maes, 1994 ; Liu, 1998) pour les activités de scanning de l'environnement externe liées particulièrement à la recherche et à la diffusion des informations.

Rappelons que notre principal objectif à travers ce travail est de proposer une méthode qui devrait pouvoir être instrumentée au moyen de la technologie Internet. Cette instrumentation devrait permettre la constitution et l'exploitation d'une **mémoire collective** et **explicitant le fonctionnement du processus de création collective de sens**.

En effet, nous espérons que la technologie Internet puisse offrir des mécanismes avancés qui devraient fournir un support efficace au processus de création collective de sens et particulièrement à la médiation. Quatre principaux fonctionnements de l'Internet semblent potentiellement intéressants dans cette perspective (Sadok *et al.*, 2003):

- Des moteurs de **recherche approchée** en utilisant des liens sémantiques (Greenberg, 2003), des liens de dépendance et hiérarchiques, ainsi que des liens avancés, comme les

hyperliens, les adresses URL. Ces moteurs de recherche permettent de pallier aux insuffisances de la classification classique des informations dans les bases de données qui se caractérise par l'existence de liens statiques et déterministes ce qui implique des possibilités limitées de recoupement et d'enrichissement des informations nécessaires pour générer de la signification. De plus, les mécanismes de recherche de type recherche approchée se basent sur des relations diverses entre les éléments en mémoire incluant l'analogie, la similarité, la proximité. Ceci est de nature à permettre des possibilités étendues de recherche d'informations complémentaires ou de connaissances mémorisées afin de conduire et d'enrichir le raisonnement collectif.

- La **manipulation des liens dynamiques** en utilisant des moteurs d'inférence permettant de faire de la déduction automatique à partir d'hypothèses et de règles de déduction approchée en créant des liens sémantiques et/ou probabilistes. Ceci est de nature à contribuer à créer un stock intelligent et dynamique des informations collectées d'une façon efficace et rapide à travers la création de liens utiles pour structurer et organiser les informations disponibles d'une manière hiérarchique.
- Des mécanismes de **contrôle d'accès** qui impliquent l'implémentation au sein de l'entreprise des politiques de contrôle pour authentifier les utilisateurs, accéder aux ressources informationnelles, et autoriser la réalisation d'actions spécifiques sur ces ressources.
- Des mécanismes permettant de **garder les traces** de toutes les opérations réalisées sur les ressources informationnelles de l'entreprise. Dans notre contexte, ces mécanismes permettent la capitalisation de certaines connaissances au sein de l'entreprise à travers le stockage des représentations formulées et construites par les membres d'un groupe de création collective de sens, ainsi que les validations éventuelles de celles-ci en cas de prise de décision.
- La technologie Internet devrait permettre l'utilisation des heuristiques émergeant de la création collective de sens au sein de l'ERI : un support pour **manipuler plus commodément** les heuristiques et les capitaliser (en résultat de l'apprentissage collectif). Ceci devrait être de nature à accroître la réactivité de l'ERI.

Ces potentialités de la technologie Internet, comme support au processus de médiation et de création collective de sens, présentent des qualités susceptibles d'intéresser les preneurs de décision dans une optique de développer une **capacité anticipative**. Ces qualités incluent la fiabilité, la flexibilité et la rapidité en réponse à la très forte pression du temps.

En effet, l'utilisation de la technologie Internet comme support à ces processus devrait garantir une fiabilité acceptable dans la mesure où elle permet une **traçabilité des raisonnements** effectués à partir des informations. La flexibilité se traduit en termes d'adaptabilité aux modifications structurelles de l'information et aux modifications observées dans les règles de prise de décision.

Enfin, l'utilisation de la technologie Internet devrait faciliter la réplication des expérimentations, qui seront présentées au cinquième chapitre, en permettant d'utiliser la même technologie (condition technique inchangée) dans des conditions de contexte organisationnel choisies pour être analogues à celles des expérimentations déjà réalisées.

4.4.3 Conception des heuristiques pour assister l'activité du médiateur

Dans un environnement incertain et **turbulent**, les problèmes liés aux décisions stratégiques sont souvent des **problèmes difficiles à structurer**. Il semble approprié, dans ce cas, de concevoir des heuristiques pour assister **l'activité du médiateur**.

Dans ce cadre, nous annonçons des heuristiques qui émergeront au cours des expérimentations que nous présenterons au cinquième chapitre :

- Réduire la complexité du raisonnement par la dissimulation des nœuds, des liens ou sous graphes qui n'ont pas des effets significatifs sur le raisonnement conduit.
- Aider l'ERI à trancher lors du raisonnement contradictoire par l'ajout d'hypothèses qui peut impliquer la recherche des informations complémentaires.
- Réduire délibérément les champs de recherche de chemins de raisonnement par des techniques de seuillage par exemple en tenant compte des probabilités en labels.

- Mener des raisonnements utilisant des multi chemins (dans le cas de recherche de scénarios d'attaques, par exemple) en associant des relations sémantiques entre des labels aboutissant (ou émanant de) à un même concept (une action, par exemple).
- Mener un raisonnement contextuel dans le but de restreindre les concepts qui apparaissent potentiellement dans un raisonnement à un seul graphe par rapport à un contexte donné. Par exemple, l'exécution d'une procédure peut dépendre dans sa faisabilité, sa forme ou sa modalité du système d'exploitation (Windows, LINUX ou INUX) qui l'exécute. Tout ceci dans le but de réduire autant que possible la complexité du problème et limiter le nombre de scénarios d'attaque, pour pouvoir déboucher sur une action effective de limitations des dégâts et prendre les mesures nécessaires de réparation.

4.5 Construction d'indicateurs de mesure des progrès permis par l'application de la méthode proposée

L'évaluation de la performance de la méthode proposée par rapport à la question de recherche posée nécessite des indicateurs de mesure. Des auteurs ont proposé, en général, des indicateurs de mesure applicables aux systèmes d'information. Ces indicateurs avaient la **prétention de l'objectivité** mais, en réalité, ont suscité beaucoup de critiques de la part des chercheurs spécialisés.

C'est pourquoi des auteurs ont proposé, par la suite, des indicateurs de nature perceptuelle. Il s'agit alors d'évaluer des **perceptions** formulées par les utilisateurs de systèmes d'information « à mesurer ». Ainsi, ont été proposées les deux familles : « utilité perçue » et « facilité perçue », chacune des deux familles étant instrumentées par des indicateurs plus « ponctuels ». Ces indicateurs sont supposés applicables aux systèmes d'information en général.

Dans le domaine de la Veille Stratégique, lui aussi spécifique des systèmes d'information, Lesca (2003) a été amené à proposer des indicateurs spécifiques. Certains de ces indicateurs sont de nature objective, alors que d'autres sont de nature perceptuelle.

A notre tour, nous sommes amenés à adapter et à proposer des indicateurs spécifiques à notre contexte de recherche qui concerne, lui aussi, un aspect des systèmes d'information et de la Veille Anticipative Stratégique.

4.5.1 Critères classiques utilisés en Systèmes d'Information

Nous nous référons dans cette sous section au modèle de DeLone et McLean (1992) élaboré suite à une revue de la littérature sur les facteurs de succès des systèmes d'information. Les facteurs significatifs avancés selon ce modèle sont les suivants :

- la qualité du système d'information : qui signifie la **facilité d'utilisation**, la **convivialité** de l'interface, la **facilité d'apprentissage** (Doll et Torkzadeh, 1988), l'adéquation entre les fonctionnalités offertes par le système et les besoins des utilisateurs, la facilité avec laquelle les utilisateurs peuvent devenir compétents dans l'utilisation du système (Davis, 1989)
- la **qualité de l'information** : qui décrit le format de l'information dans la mesure de son adaptation à l'utilisation, la clarté de l'information fournie, le degré de satisfaction de l'exactitude des informations fournies, des informations actualisées pour la prise de décision, la disponibilité des informations nécessaires à temps (Doll et Torkzadeh, 1988).
- l'utilité qui s'interroge si l'utilisation du système permet d'effectuer le travail plus rapidement, plus facilement, et avec une plus grande valeur ajoutée (Davis, 1989).
- la satisfaction des utilisateurs qui se traduit par le degré d'adéquation du système aux besoins informationnels, à la réalisation des objectifs de travail tout en optimisant les efforts.
- l'impact individuel.
- l'impact organisationnel.

La figure ci-dessous illustre la composition du modèle de succès des systèmes d'information de DeLone et McLean (1992).

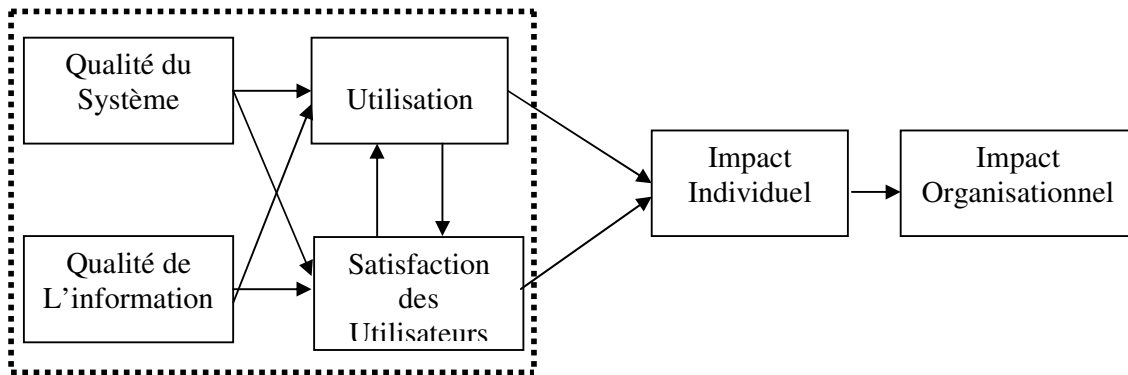


Figure 12: Le modèle de DeLone et McLean (1992)

Ce qu'il faut noter c'est que la **satisfaction des utilisateurs** est un construit central dans la plupart des travaux consacrés à l'élaboration des critères de succès des SI.

Dans ce cadre, Seddon et Kiew (1994) ont proposé un modèle de mesure de la satisfaction des utilisateurs, où ils ont ajouté par rapport au modèle de DeLone et McLean (1992) une autre dimension décrivant l'**implication** des utilisateurs.

Dans le domaine du management stratégique, il est important d'adapter les critères d'évaluation aux particularités des problèmes traités, des objectifs visés ou des décisions à prendre.

Les critères proposés par Lesca (2003), afin de mesurer les progrès réalisés suite à l'implantation d'un dispositif de **veille anticipative stratégique** et d'intelligence collective (la méthode L.E.SCA^{ning}®), présentent un intérêt particulier par rapport à notre travail de recherche.

En effet, l'auteur propose des critères susceptibles d'évaluer l'utilité, la praticabilité de la méthode L.E.SCA^{ning}® ainsi que la satisfaction des utilisateurs. Cette évaluation est essentiellement basée sur les perceptions exprimées par les utilisateurs de la méthode interrogés.

Le critère de l'**utilité perçue** permet de mesurer les résultats ou les progrès réalisés par l'entreprise dans l'activité de traitement des signaux faibles afin de supporter les décisions stratégiques.

Le **critère de la praticabilité** de la méthode est lié à son fonctionnement afin de mesurer la **facilité perçue** d'utilisation de la méthode, son organisation ainsi que l'efficacité de la technologie utilisée pour la supporter.

La qualité de l'information anticipative sur l'environnement est également un indicateur évoqué afin d'évaluer dans quelle mesure la méthode L.E.SCA^{ning}® a augmenté la valeur et la pertinence de celle-ci.

4.5.2 Les critères proposés pour l'évaluation de la méthode d'aide au travail d'une ERI

La lecture de certains indicateurs de mesure de succès d'un système d'information, nous amène à choisir et à adapter ces indicateurs en liaison avec la spécificité de notre terrain de recherche.

Nous retenons les critères avancés par Lesca (2003) liés à l'utilité et à l'efficacité perçues par les utilisateurs de la méthode proposée tout en opérant une adaptation par rapport à notre domaine de recherche.

En effet, dans le contexte de détection, d'analyse et de réponse aux agressions numériques le **facteur temps** est d'une extrême importance. Les critères proposés devraient prendre en considération cette variable critique et déterminante dans le travail d'une ERI et dans la prise de décision dans le domaine de la sécurité informatique.

Rappelons que notre recherche vise la conception et la construction d'une méthode pour assister le travail d'une ERI.

Notre approche se caractérise par l'élaboration des indicateurs de mesure en amont et en aval de l'expérimentation de la méthode proposée.

- **En amont**, nous procédons par des **entretiens semi directifs** effectués au moyen d'une grille de questions (présentée en annexe). Ces entretiens « amont » sont réalisés auprès des membres de l'ERI de l'ANCE (dans le contexte de notre étude exploratoire), de certains responsables de l'ANCE et de certains experts dans le domaine de la sécurité informatique.

En aval, nous utiliserons les critères quantitatifs suivants :

- le temps de traitement de chaque signal faible : il s'agit de mesurer la durée moyenne entre le moment de détection d'une alerte et le moment où l'agression est identifiée (ou la certitude d'une absence d'agression). La variation moyenne de ce critère indique si la méthode permet effectivement d'aider l'ERI en réduisant le temps de traitement.
- le ratio des fausses décisions sur le nombre total des décisions prises. Dans ce cas, deux types de fausses décisions peuvent être prises par l'ERI. Celle-ci peut décider qu'il s'agit d'une fausse alerte alors qu'il s'agit bien d'une agression. Ou bien, elle peut décider qu'il s'agit d'une agression alors, qu'elle ne l'est pas. Cet indicateur permet alors de voir si la méthode permet de réduire le nombre des fausses décisions prises dans le temps.
- le ratio des décisions incomplètes sur le nombre des attaques qui se répètent. Une décision incomplète montre si l'ERI est capable ou non à faire du raisonnement à partir d'un signal/signe faible détecté et par la suite anticiper l'occurrence d'agressions similaires. Cet indicateur permet de voir si la méthode aide l'ERI à construire le scénario d'une attaque et par la suite à prendre une décision.
- le temps de réactivité globale qui mesure le temps de détection, de traitement et de réponse à une agression numérique. Cet indicateur fait intervenir des composantes de gestion et d'organisation liées au travail d'une ERI. Le temps de détection est intimement lié aux mécanismes de collecte des signaux/signes faibles. Pour la réponse à une agression, l'ERI ne prend pas une décision de recouvrement sans recourir à la hiérarchie qui compte tenu de ses objectifs et ses contraintes prend la décision finale.

La liste de ces indicateurs « aval » n'est pas exhaustive, ni définitive. Elle pourra être enrichie en fonction de « l'apprentissage » résultant des expérimentations.

Ces indicateurs ne sont mesurables **qu'à partir du moment ou nous disposons d'un** historique suffisamment long.

Conclusion Chapitre 4

Nous avons présenté dans ce chapitre le cadre conceptuel de la MARRAN et ses fondements théoriques notamment à travers l'utilisation et l'extension des cartes causales ainsi que les connaissances théoriques concernant la création collective de sens. Nous avons proposé dans ce cadre conceptuel, trois phases pour assister le raisonnement créatif à partir d'informations de type signal et/ou signe faible. Le modèle conceptuel peut être représenté par un graphe orienté composé d'un ensemble de nœuds et de liens représentant des chemins de raisonnement et désignant un point de vue partiel ou intégral d'un acteur du processus de création collective de sens. Ces liens sont de cinq types, probabilistes et variables en fonction du temps. Deux types d'opérations : de remplacement et de réécriture sur les nœuds et sur les liens peuvent être manipulées pour aider à la construction des chemins de raisonnement.

Nous avons procédé par la suite à une adaptation de la terminologie du modèle conceptuel au domaine de réponse aux agressions numériques en mettant l'accent sur le rôle de la médiation dans les travaux d'une ERI. Les activités de médiation comportent la validation des concepts et des liens sur un graphe, la construction de tous les chemins de raisonnement, la convergence des points de vue formulés par les membres de l'ERI, l'affinement du raisonnement afin d'aboutir à une vision collective, et la construction des heuristiques qui ont émergé au cours du travail de l'ERI

Nous avons montré par la suite les apports potentiels de la technologie Internet pour l'instrumentation de la MARRAN à travers la constitution et l'exploitation d'une mémoire collective afin d'assister le processus de création collective de sens et particulièrement le processus de médiation.

Dans la cinquième section, nous avons proposé deux approches d'évaluation de la MARRAN. La première, en amont de l'implémentation de la MARRAN, se base sur des entretiens semi collectifs auprès des experts en sécurité informatique. La deuxième, en aval, se base sur des critères nécessitant un historique suffisamment long pour pouvoir les mesurer.

Expérimentation de la méthode sur des cas réels d'agressions numériques

Dans ce chapitre, notre objectif se situe sur un triple plan. Il s'agit premièrement d'expérimenter la méthode proposée pour assister le travail d'une ERI sur quatre cas réels d'agressions numériques. Cette expérimentation vise à valider les concepts théoriques développés dans le chapitre quatre et qui soutiennent le modèle conceptuel de la méthode proposée. L'accent sera mis particulièrement sur la représentation des nœuds et la manipulation des liens au sein d'un graphe afin d'assister les processus de médiation et de prise de décision. Le choix de ces exemples réels d'agressions numériques est principalement guidé par la volonté de couvrir les concepts théoriques formulés dans le chapitre précédent.

Deuxièmement, il s'agit de présenter une liste des conditions d'expérimentation de la méthode proposée dans le cadre de travail d'une ERI.

Troisièmement, nous visons à montrer l'aspect pratique de la méthode proposée qui réside dans la possibilité de l'assister par un outil informatique qui a été conçu et développé en exploitant certaines potentialités de la technologie Internet.

Ainsi, la première section avance quatre cas réels d'agression numérique déjà produits et ce dans le cadre d'une « expérimentation ex post » tout en justifiant le choix de ces cas.

La deuxième section spécifie les conditions d'expérimentation la méthode proposée, en vue de la répliation de celle-ci pour d'autres cas.

La troisième section présente un outil informatique qui a été conçu et développé afin d'assister la méthode proposée dans ce travail.

5.1 Mise en œuvre de la méthode sur des cas réels d'agressions numériques en vue d'expérimenter la méthode

L'expérimentation de la méthode se réalise sur des *challenges* qui reproduisent des situations réelles d'attaques dans lesquelles un signal faible est détecté. En effet, un **concours international** est organisé chaque mois et qui a pour but de mettre en compétition des ERI appartenant à des entreprises, opérant dans des domaines d'activité différents, sur des problèmes qu'elles doivent résoudre avec des contraintes de temps et de travail réelles. L'ERI de l'ANCE a participé plusieurs fois à ce concours international de challenges. L'expérience acquise par celle-ci lui a permis d'obtenir des classements remarquables dans ce concours (voir site Internet www.honeynet.org, les challenges 20, 23, 24, et 28).

L'ERI de l'ANCE a procédé à une série d'activités d'expérimentation et d'apprentissage de la méthode, réalisées à travers l'étude de trois challenges traités dans les ouvrages de Schiffman (2001) et de Schiffman *et al.*, (2003) et qui présentent des exemples réels d'agressions numériques. Elle a traité également le premier cas d'agression qui s'est produit réellement à l'ANCE.

L'expérimentation de la méthode sur chaque cas montre trois étapes essentielles pour construire le scénario de l'attaque et aider à la prise de décision. Pour chaque cas, nous décrivons les étapes suivantes :

- D'amplification progressive, des signaux/signes faibles détectés, par la recherche d'informations internes liées au trafic sur le réseau de l'entreprise afin de vérifier l'existence d'une agression numérique.
- De recherche d'informations complémentaires internes ou externes à l'entreprise afin de réduire l'ambiguïté des signaux/signes faibles détectés.
- De raisonnement itératif par l'ajout des concepts et la création de liens entre ceux-ci dans le but de construire le scénario de l'agression numérique.

5.1.1 Cas n°1 : Scanning du réseau de l'ANCE

Ce premier cas décrit une agression de type **scanning** à travers laquelle un hacker essaye de collecter le maximum d'informations relatives aux caractéristiques et au fonctionnement du

réseau d'une entreprise en vue de détecter les vulnérabilités et les points d'entrée possibles dans celui-ci. L'activité de scanning est dangereuse et présente un risque potentiel dans la mesure où elle peut constituer une première étape pour préparer une agression. Il est donc important de détecter les tentatives de scanning et de connaître leurs natures et leurs sources.

Dans le présent cas, l'ERI de l'ANACE a détecté un premier signal qui indique un nombre important de messages émis par une seule source excédant un certain seuil habituel. Cette émission de messages devient de plus en plus suspecte dans la mesure où elle a dépassé une durée de temps proche de trois heures.

Pour amplifier ce signal, qui peut déceler l'existence d'une attaque probable, l'ERI de l'ANACE a été conduite à faire une analyse plus détaillée du trafic sur le réseau de l'entreprise ainsi qu'un ensemble de vérifications dans le but de cerner le problème.

Le détail des analyses effectuées une heure après la détection du premier message a montré qu'effectivement une source essaye d'obtenir des informations sur les caractéristiques du réseau de l'ANACE en utilisant cinq classes de tentatives. Ces informations peuvent être utilisées pour :

- mener ultérieurement une attaque de type déni de service,
- rechercher des portes dérobées « *backdoors* »,
- tester la possibilité de mener une attaque en utilisant une connexion à distance,
- connaître le fonctionnement du serveur Web,
- spécifier le fonctionnement d'un service offert par l'ANACE.

L'amplification du premier signal détecté a amené l'ERI de l'ANACE de conclure que le hacker est en train de scanner le réseau de l'entreprise en vue d'obtenir différentes informations sur ce dernier susceptibles d'être utilisées ultérieurement pour mener des agressions numériques.

Pour cerner l'identité du hacker, l'ERI de l'ANACE a opéré à son tour un certain nombre de scanning et de tentatives d'accès et de collecte d'informations sur la source des messages dont l'adresse est devenue connue. L'accès à un certain nombre de registres a permis de localiser le serveur source de l'attaque. Un accès direct à l'entreprise détenant le serveur a permis l'arrêt du scanning sur demande de l'ANACE. La connaissance de l'identité du hacker

est, dans ce cadre, une tâche nécessaire dans la mesure où elle peut révéler le nom d'un concurrent, d'un fournisseur, d'un groupe de pression ou même d'un client.

L'ERI a enfin dressé un rapport d'analyse totale de l'action à la direction générale de l'entreprise afin de prendre les mesures possibles de prévention contre ce type d'agression.

La figure 10 montre les différentes étapes d'amplification, de recherche complémentaire d'informations et de raisonnement conduites par l'ERI de l'ANCE afin de construire le scénario de l'attaque. Les concepts et les relations colorés en rouge marquent, par exemple, un chemin de raisonnement construit à partir de la réalisation de ces trois étapes afin de cerner la nature de l'agression.

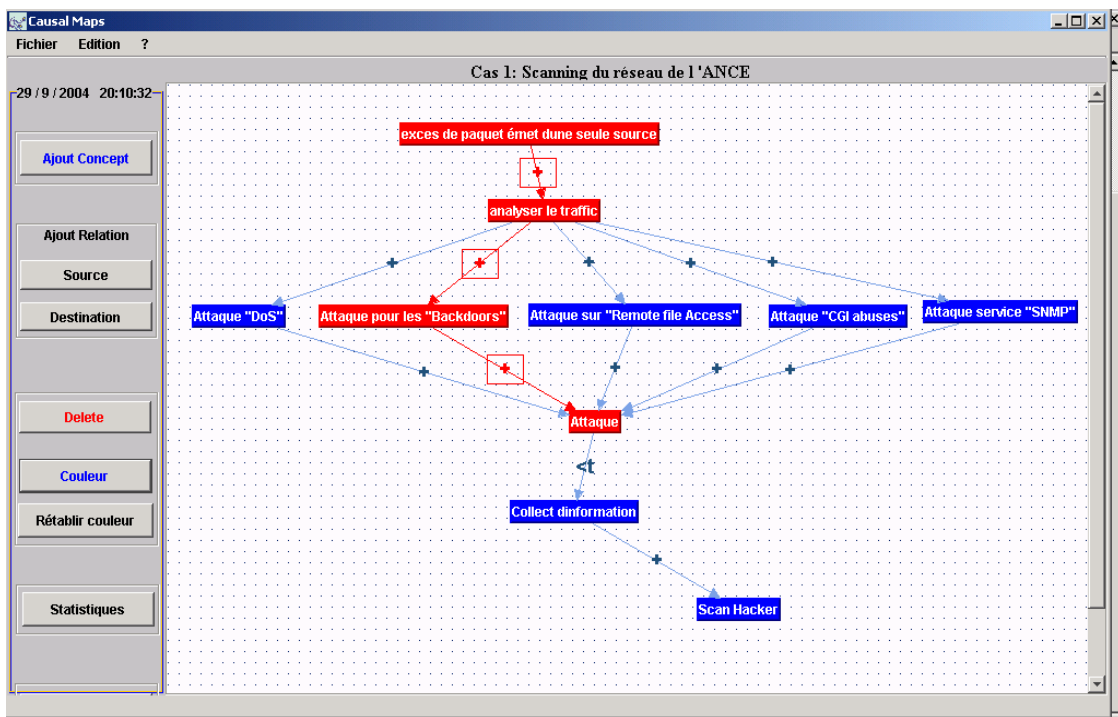


Figure 13: Représentation graphique du scénario de l'attaque à l'ANCE

5.1.2 Cas n°2 : “A Thousand Razors”

Ce cas représente le **challenge 15** qui est traité dans l’ouvrage de Schiffman (2001). Ce challenge décrit le cas d’une agression numérique de type déni de service contre le site Web d’une entreprise gouvernementale. Le déni de service est une agression visant à générer des arrêts de service à travers l’envoi à une machine cible, qui gère le service, de nombreux paquets IP de grosse taille. Celle-ci ne pourra pas répondre à toutes les requêtes finira par se déconnecter du réseau.

Cet exemple met en évidence l’importance du temps mis pour construire le scénario d’une attaque de ce type. Plus ce temps est réduit plus il serait possible de diminuer les dommages occasionnés par le déni de service.

En effet, et d’après les rapports publiés par le FBI/CSI depuis l’année 2000 jusqu’à l’année 2004 portant sur les pertes financières engendrées par les agressions numériques, le déni de service demeure l’agression la plus coûteuse pour les entreprises.

Dans cet exemple, un haut responsable de l’équipe de sécurité de l’entreprise en question a remarqué une baisse du niveau de performance du serveur Web. Un nombre important de clients ont appelé pour signaler un problème d’accès au site Web de l’entreprise.

Comme le problème d’accès peut avoir plusieurs causes, l’équipe de sécurité a commencé à faire des analyses des fichiers log du serveur Web, des fichiers log du *firewall* qui protège le serveur et des fichiers log du routeur. Ces analyses sont susceptibles d’amplifier progressivement le premier signal/signe détecté indiquant des difficultés lors de l’accès au site Web de l’entreprise en permettant de cerner l’origine du problème.

La première analyse des fichiers log du serveur Web n’a pas montré un trafic suspect. Quant à la visualisation des fichiers log du *firewal*, celle-ci a révélé, par contre, une adresse suspecte qui a essayé de se connecter plusieurs fois et à des moments successifs à un endroit précis du réseau de l’entreprise. Cette première constatation a conduit l’ERI de cette entreprise à orienter le raisonnement vers la possibilité d’occurrence d’une attaque de type déni de service.

Cependant, pour confirmer cette première constatation, il est nécessaire de continuer l’analyse des fichiers log du routeur afin de cerner la nature des connexions effectuées par

l'adresse suspecte. La comparaison des fichiers log du routeur par rapport à un niveau habituel d'activité, a montré un nombre très important de paquets de type « *UDP other* ».

La corrélation entre les deux types d'analyses effectuées sur les fichiers log du *firewall* et les fichiers log du routeur a amené l'ERI de l'entreprise en question à conclure avec une forte probabilité l'existence d'une agression de type déni de service.

La construction du scénario de cette agression a permis à l'ERI d'identifier la voie empruntée ou la méthode utilisée par le hacker pour mener cette attaque. Cette identification permet à son tour de prendre les mesures nécessaires compte tenu d'un certain nombre de contraintes techniques et opérationnelles afin de remédier aux problèmes occasionnés par cette agression. La décision prise dans ce cas, consistait à bloquer toutes les entrées par la porte "*UDP*" ce qui est de nature à générer une baisse du trafic à cause de la perte de certains clients qui choisissent cette porte d'accès au réseau de l'entreprise.

Ce qu'il faut noter dans cet exemple, c'est que l'amplification progressive du signal détecté a utilisé certaines fonctionnalités de la technologie Internet pour l'accès à distance, la visualisation et la comparaison des fichiers log.

La figure 11 montre les différentes étapes d'amplification, de recherche complémentaire d'informations et de raisonnement conduites par l'ERI de l'entreprise considérée dans ce cas afin de construire le scénario de l'attaque.

La figure montre également l'évolution du raisonnement à travers ces trois étapes au cours desquelles l'ERI de cette entreprise retient à chaque fois un concept (un nœud) amélioré et moins ambigu. L'affinement du raisonnement se traduit essentiellement par des relations probabilistes qui s'affirment de plus en plus au fur et à mesure de l'intégration des informations complémentaires collectées au moment de la construction du scénario de l'agression. Le chemin de raisonnement coloré en rouge représente le résultat de ce raisonnement itératif qui a conduit à reconnaître la nature de l'agression (déni de service) avec une forte probabilité.

Les mesures prises pour connaître puis bloquer la source de l'agression, sont aussi représentées dans cette figure.

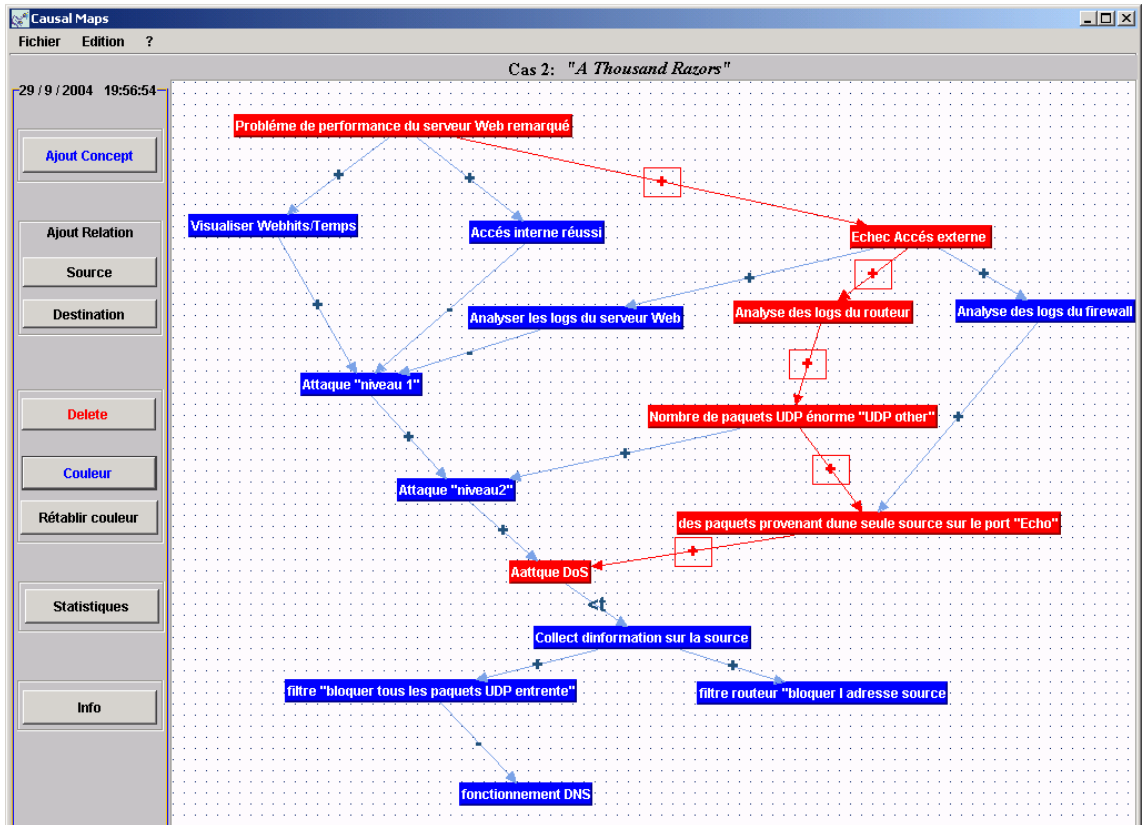


Figure 14: Représentation graphique de l'agression “A Thousand Razors”

5.1.3 Cas n°3 : “The Parking Lot”

Ce cas représente le **challenge 3** qui est traité également dans l’ouvrage de Schiffman (2001). Ce challenge décrit les conséquences de l’utilisation d’une nouvelle technologie à savoir le réseau sans fil « *wireless network* ». Ce type de réseau présente plusieurs avantages notamment en termes de facilité d’installation, le nomadisme de certains salariés, la mobilité à l’intérieur des bâtiments de l’entreprise et le faible coût apparent de la mise en œuvre (ces spécificités sont décrites dans le site Web du CLUSIF dont l'adresse est la suivante: www.clusif.asso.fr/fr/production/ouvrage).

Cependant, l'utilisation des réseaux sans fil présente certains risques comme le montre bien le présent exemple d'agression numérique.

La victime dans cet exemple est une entreprise de taille moyenne spécialisée dans la vente au détail et qui commercialise tous ses produits en ligne via son site Web. Le réseau de cette entreprise est composé en partie par une connexion sans fil utilisée pour des fins de gestion des stocks. L'agression a transité à travers cette partie du réseau et a provoqué l'accès d'un hacker (donc une personne non autorisée) à certaines données en exploitant une vulnérabilité liée à la norme en vigueur du réseau sans fil.

La première responsable de sécurité dans cette entreprise a été surprise un jour par un appel téléphonique de la part d'un responsable informatique d'une entreprise de consulting, qui travaille dans l'entourage de l'entreprise concernée, signalant une activité suspecte sur une partie du réseau de celle-ci.

L'analyse des fichiers log du *firewall* a indiqué effectivement un trafic inhabituel sauf que l'identification du programme utilisée par la source de ce trafic a été difficile à réaliser. En d'autres termes, l'amplification du premier signal détecté révèle, avec une forte probabilité, une attaque possible sans savoir exactement ni sa nature ni la technique utilisée pour la mener.

Suite à un ensemble d'opérations de vérification et d'exécution d'un certain nombre de commandes, et de recherches d'informations complémentaires internes et externes à l'entreprise, l'ERI a pu préciser le moyen employé par le hacker pour mettre en œuvre son attaque.

En effet, l'ERI de cette entreprise a effectivement identifié une porte dérobée « *backdoor* » dans le réseau de l'entreprise et qui a été utilisée par le hacker pour effectuer des opérations de scanning de type actif et passif.

Dans le domaine de la sécurité des réseaux, les scanners actifs visent à envoyer des requêtes d'identification ou de connexion au réseau de l'entreprise alors que les scanners passifs se limitent à des écoutes aux différents canaux de communication.

Le raisonnement à partir de cette identification de la porte dérobée a permis, ensuite, à l'ERI de l'entreprise agressée de déterminer le type de connexion ou le point d'accès utilisé par le hacker qui s'est avéré le réseau sans fil. Le hacker a exploité une vulnérabilité liée à la norme caractérisant le fonctionnement du réseau sans fil pour mettre en œuvre son attaque (il s'agit de la norme 802.11b, qui présente certaines faiblesses. Plusieurs informations

concernant cette vulnérabilité sont disponibles sur le site Web du CLUSIF dans l'adresse suivante www.clusif.asso.fr/fr/production/ouvrage/pdf/RSF.pdf)

La figure 12 représente les différentes étapes d'amplification, de recherche complémentaire d'informations et de raisonnement itératif conduites par l'ERI de l'entreprise considérée dans ce cas afin de construire le scénario de l'attaque. **Les labels utilisés permettent de voir que toutes les relations mentionnées au chapitre quatre sont utilisées.** Les concepts utilisés pour la représentation du scénario peuvent être classés en deux types:

- Des concepts d'ordre technique, qui analysent le résultat d'exécution de certaines commandes informatiques ou de télécommunications telles que "commande *ps*", "se connecter avec *telnet* et *netstat*" qui permettent d'indiquer l'état des connexions ouvertes et suspectes.
- Des concepts résultant du raisonnement itératif autour des informations détectées et collectées tel que l'existence d'une porte dérobée, et l'identification du type de connexion au réseau utilisée par le hacker pour mener son attaque.

Le chemin de raisonnement en rouge, dans la figure 12, désigne le résultat de l'amplification progressive du premier signal détecté et qui révèle, avec une forte probabilité, l'existence d'une porte dérobée dans le réseau. Ce résultat constitue en fait une amélioration de la situation initiale qui se caractérise par une ambiguïté autour de la nature de l'agression et de la technique utilisée pour la mener.

De même, le chemin de raisonnement en mauve indique le résultat de l'itération effectuée à partir de l'existence d'une porte dérobée pour déterminer le type de connexion ou le point d'accès utilisé par le hacker dans le but de mettre en œuvre son attaque.

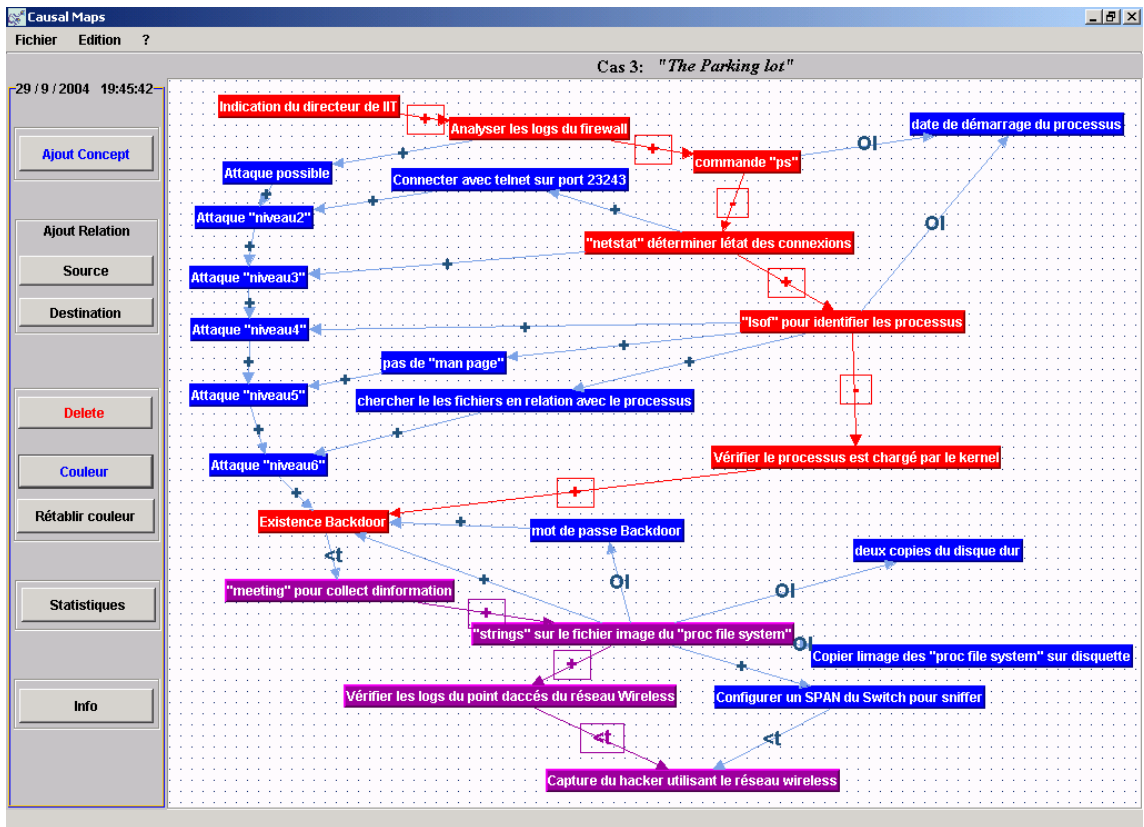


Figure 15: Représentation graphique de l'agression "The Parking Lot"

5.1.4 Cas n°4: "Injection Indigestion"

Ce cas est traité dans l'ouvrage de Schiffman *et al.*, (2003). Il s'agit du **challenge 18** et qui illustre également la pression du temps comme étant une contrainte majeure pour répondre à une agression en limitant ses dégâts matériels et immatériels. L'entreprise considérée dans cet exemple opère dans le domaine du commerce électronique et commercialise des jeux de puzzle à l'échelle internationale.

La responsable du département marketing de l'entreprise en question a reçu un mail de chantage de la part d'un inconnu. Cette personne demande une somme importante d'argent suite à la découverte d'une faille de sécurité dans le réseau de l'entreprise en proposant une solution à ce problème de sécurité. Pour appuyer ses propos, le hacker a donné des numéros de cartes de crédit de trois clients de l'entreprise.

L'équipe de sécurité, en consultant la base des données clients, a confirmé l'information donnée par le hacker concernant les numéros des cartes de crédit. La responsable marketing a refusé d'informer la police de cette tentative d'extorsion pour éviter une mauvaise publicité qui est de nature à nuire à l'image de l'entreprise.

Cette position est largement partagée par plusieurs entreprises puisque le rapport CSI/FBI pour l'année 2003 indique que 70% des entreprises interrogées ne reportent pas les incidents de sécurité aux autorités officielles pour éviter la publicité négative qui peut en résulter.

La situation paraissait très complexe pour l'équipe de sécurité de cette entreprise et la pression du temps pour agir se présente comme étant une contrainte majeure pour construire le scénario de cette agression. La vérification des fichiers log du *firewall* et du diagramme du réseau ne montre pas une tentative d'attaque ou une activité suspecte surtout que tous les correctifs "*patches*" nécessaires ont été accomplis.

Dans cette première étape d'amplification, l'ERI a éliminé la possibilité d'exploitation d'une vulnérabilité liée à la configuration du *firewall*. Ceci n'est pas toujours le cas et l'ERI ne devrait pas lors d'une phase d'investigation écarter cette possibilité.

Les doutes se sont donc orientés vers le serveur Web afin d'examiner les vulnérabilités à travers l'analyse des fichiers log pendant les deux semaines qui ont précédé l'agression.

L'ERI a détecté un trafic douteux au niveau des fichiers log du serveur SQL qui affiche des erreurs pour des requêtes erronées. Le hacker essaye de détecter les paramètres de fonctionnement du réseau pour pouvoir y accéder à travers une série de questions posées au serveur. A chaque réponse, même si celle-ci est négative, le hacker peut progressivement détecter les paramètres d'accès à la base de données clients ou à d'autres informations stockées dans le serveur Web. Le serveur ne vérifie, à chaque requête, que le nombre de caractères envoyés, avec 32 essais il est possible de compromettre n'importe quel compte.

La corrélation de cette information avec l'adresse source du mail du hacker a confirmé la méthode utilisée pour mener son attaque. En effet, le message envoyé par le hacker fournit deux **signes faibles** mais pertinents pour la construction du scénario de l'attaque. Il s'agit premièrement de l'adresse électronique du hacker qui a été utilisée pour envoyer le mail mais aussi pour mener l'attaque. Deuxièmement, le hacker a fourni des données concernant

des clients, ce qui est de nature à orienter les investigations vers les moyens utilisés pour accéder à la base de données clients.

Cette agression de type injection SQL exploite une vulnérabilité de sécurité dans le développement d'un site Web. Cette faille permet de pirater une requête envoyée par l'application Web à un système de back office (par exemple une base de données) en vue d'exécuter une commande non autorisée sur ce dernier.

L'injection SQL est dangereuse dans la mesure où elle permet de manipuler les bases de données des sites ce qui pourrait causer le détournement de certaines données confidentielles, l'affichage de mots de passe, l'authentification illégitime sur un service, etc.

L'ERI a ensuite pris un ensemble de décisions techniques pour pallier aux insuffisances du serveur SQL de façon à éviter dans l'avenir des agressions de cette catégorie.

La figure 13 montre les différentes étapes d'amplification, de recherche complémentaire d'informations et de raisonnement conduites par l'ERI de l'entreprise considérée dans ce cas afin de construire le scénario de l'attaque. Le chemin de raisonnement en rouge souligne le déroulement de ces étapes afin de reconnaître progressivement, et avec des probabilités de plus en plus importantes, la nature de l'agression numérique de type injection SQL.

Les mesures de réparation et de prévention contre ce type d'attaque sont également représentées dans cette figure.

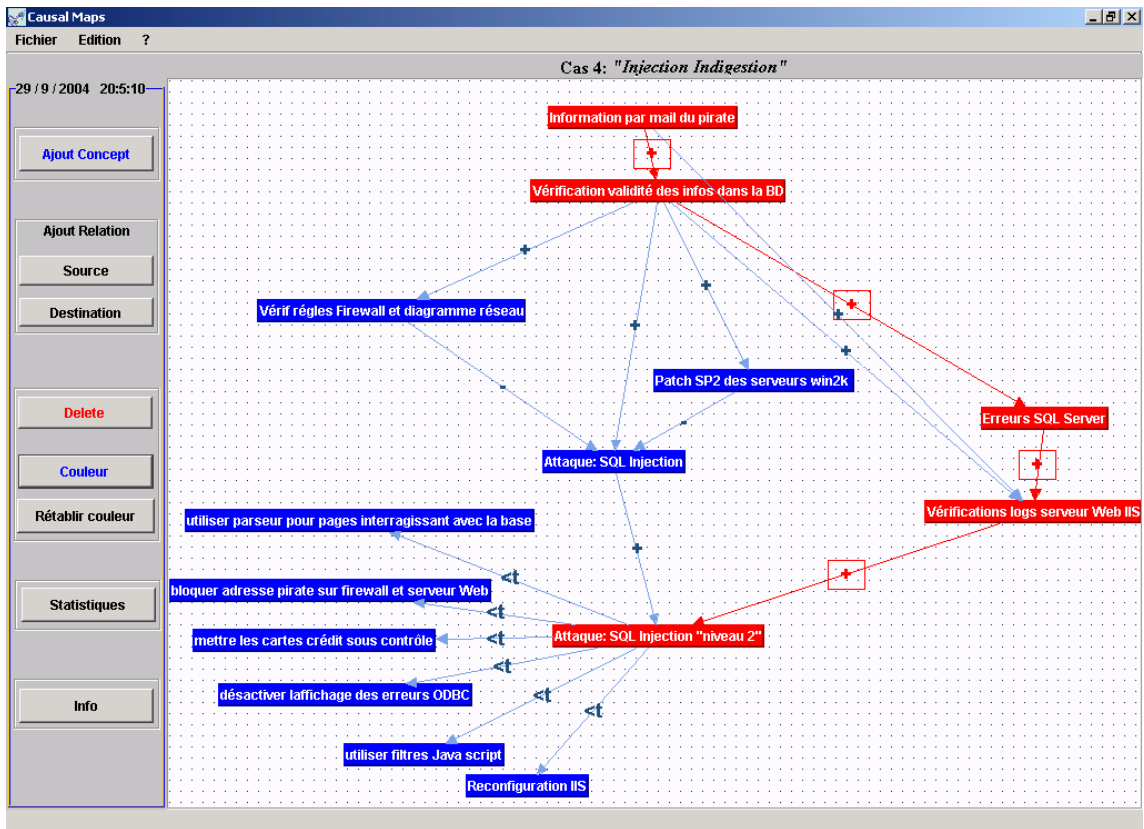


Figure 16: Représentation graphique de l'agression "Injection Indigestion"

5.2 Spécification des conditions d'expérimentation de la méthode

Nous présentons dans cette section une liste des conditions d'expérimentation de la méthode proposée liées au contexte des agressions numériques et aux cas traités, en vue de la réplique de celle-ci pour d'autres cas.

Bien évidemment cette liste n'est pas exhaustive, mais contient les conditions que nous jugeons minimales pour la réplique de notre méthode. L'expérimentation sur d'autres cas permettra de compléter et d'enrichir cette liste.

Cependant, l'utilité et l'efficacité de notre méthode supposent un niveau d'utilisation important des TIC dans les systèmes de production et de gestion de l'entreprise. Ceci suppose

un niveau de développement du réseau qui devrait être suffisamment étendu, ouvert et portant des fonctions importantes de l'entreprise.

5.2.1 Existence d'une politique de sécurité

L'établissement d'une politique de sécurité suite à une analyse du risque liée aux caractéristiques du réseau de l'entreprise est de nature à diminuer la complexité du raisonnement lors de la construction du scénario de l'agression numérique.

En effet, la politique de sécurité précise principalement les informations à protéger en fonction de leur importance, les personnes autorisées à effectuer des applications et des modifications sur les ressources informationnelles de l'entreprise ainsi que l'ensemble des règles formelles et des principes répondant aux besoins de sécurité de l'entreprise.

L'expérimentation de la méthode nécessite un niveau important de pratiques mécanisées de sécurité, de procédures à caractère opérationnel et technique, et d'expertise dans le cadre d'une politique générale de sécurité.

Comme nous l'avons déjà mentionné au deuxième chapitre de notre recherche, la mise en œuvre d'une politique de sécurité devrait permettre de :

- implémenter des mesures nécessaires et suffisamment décourageantes pour limiter l'exploitation des vulnérabilités liées aux caractéristiques du réseau et de son fonctionnement
- mettre en place un ensemble de procédures et de mécanismes pour détecter et identifier des problèmes potentiels de sécurité.

Ces actions de prévention et de détection sont susceptibles de limiter l'exposition de l'entreprise à un risque d'intrusion et les dommages possibles d'une telle agression ainsi que d'orienter et d'encadrer le raisonnement lors d'élaboration d'une réponse face à un problème de sécurité.

Ainsi, en absence d'une politique de sécurité qui détermine d'une façon claire et précise les règles, les actions à entreprendre et les autorisations assignées aux utilisateurs du système d'information, la détection et la réponse sont très difficiles à cause de l'**ambiguïté** et de l'**abondance** des informations générées par le réseau d'une entreprise.

5.2.2 Caractéristiques des informations utilisées

Dans la plupart des cas, la détection et l'anticipation des agressions numériques s'effectuent à travers la détection et l'interprétation des informations, de type signal et/ou signe faible, générées par le trafic sur le réseau de l'entreprise.

Les informations, de type signe/signal faible, sont des informations fragmentaires, incertaines, incomplètes, imprécises et ambiguës et dont les caractéristiques ont été explicitées dans les chapitres précédents.

Les agressions numériques sont incertaines dans la mesure où leur visibilité n'est clairement possible que lorsqu'elles sont terminées. De plus, une entreprise peut être attaquée sans en avoir conscience.

Ainsi, il est nécessaire de collecter des informations à **caractère anticipatif** relatives à des **alertes précoces** liées à des problèmes potentiels de sécurité et dont l'interprétation est susceptible de réduire et/ou d'anticiper le risque des agressions numériques.

La méthode propose trois étapes pour le traitement de ce type d'informations. La première étape réside dans l'amplification progressive de ces informations, sert à filtrer les signaux/signes captés qui peuvent représenter un important pourcentage de fausses alertes et cerner le problème rapidement.

La deuxième étape est une étape de recherche d'informations complémentaires disponibles dans des bases de données internes ou externes. L'efficacité de cette étape dépend de la disponibilité de ces informations et de la pertinence des moyens employés pour leur recherche.

La troisième étape est une étape d'interprétation par raisonnement itératif sur les liens créés entre l'ensemble des informations détectées et collectées. A la fin de cette étape, la construction du scénario de l'attaque devrait être achevée.

5.2.3 Possibilité de détection de signaux/signes faibles

L'entreprise devrait disposer de mécanismes de détection des signaux/signes faibles à travers des outils appropriés et nécessaires pour détecter des activités suspectes sur le trafic du réseau.

L'implémentation de ces mécanismes dépend des objectifs et des caractéristiques de la politique de sécurité adoptée par l'entreprise. Sans ces mécanismes de détection, la méthode ne peut fonctionner.

En effet, les mesures de prévention et de détection explicitées au sein de la politique de sécurité supposent l'implémentation des mécanismes appropriés d'exploitation et de supervision permanents des signes d'intrusions ou des tentatives d'intrusion contre les ressources informationnelles de l'entreprise. Ces actions devraient permettre de maintenir un niveau continu de vigilance, et de détecter des activités non autorisées, inattendues ou suspectes contre l'intégrité, la disponibilité ou la confidentialité des ressources informationnelles de l'entreprise.

De plus, il est indispensable de stocker les données relatives à ces actions anormales ou suspectes permettant de conserver la trace de l'historique de tous les flux entrant et sortant. Ceci est de nature à permettre la comparaison entre les états d'information attendus et opérationnels, comparaison susceptible de révéler une indication sur l'occurrence d'une agression et d'investiguer plus rapidement des nouvelles agressions numériques inconnues.

De ce fait, la mise en place d'un système de captage, de sélection et de remontée des signaux/signes faibles liés à la détection des intrusions ou à des tentatives d'intrusion constitue une **condition nécessaire** et préalable à l'expérimentation de la méthode qui se base sur ce type d'informations.

5.2.4 Examen de cas d'agressions numériques non répétitives à l'identique

La méthode est expérimentée sur des cas d'agressions non répétitives dans la mesure où les techniques utilisées ou les moyens employés pour mener ces attaques sont nouvelles ou inconnues par l'entreprise. Les conséquences de ces agressions sont également différentes d'un cas à un autre, et ce sur un plan technique et/ou de gestion.

La méthode, qui a pour objectif d'agir vite ou par anticipation afin de protéger les ressources informationnelles de l'entreprise, est expérimentée sur deux types d'agressions :

- des agressions numériques qui ont été préalablement répertoriées (et largement commentées dans des sites spécialisés et destinés à leur analyse)
- des agressions numériques non encore répertoriées à travers l'analyse de certains signaux et/ou signes faibles détectés par des systèmes de captage implémentés par l'entreprise

Sur le plan stratégique, les décisions relatives à la réponse à ces agressions numériques sont essentiellement de nature non répétitives, non programmables, dont l'enjeu peut être énorme pour l'entreprise et prises dans un contexte d'incertitude.

Cette condition d'expérimentation de notre méthode tient compte du caractère variable, complexe et imprévisible des menaces et des vulnérabilités liées aux réseaux des entreprises. Elle s'intègre bien dans une optique de mise en place des approches et des méthodes de sécurité dynamiques et adaptatives.

5.2.5 Face à face et possibilités d'interaction rapides à distance

Les étapes d'amplification progressive et d'interprétation des signaux/signes faibles nécessitent le face à face. Ce médium riche (Daft et Lengel, 1986 ; 1988) est approprié à la nature des informations interprétées dans le cadre de la **création collective de sens**. Cependant, la pression du temps exige des possibilités d'interaction rapides et à distance.

La méthode proposée fonctionne en face à face et/ou à distance. Dans ce dernier cas, il est intéressant de chercher du côté des technologies de l'information et de la communication pour assister et faciliter cette interaction à distance.

En effet, lors des phases d'amplification et de création collective des liens entre les informations relatives à une agression donnée, les membres d'une ERI ont besoin d'interagir en face à face mais aussi à distance pour construire le plus rapidement possible le scénario de l'agression et par conséquent formuler les réponses adéquates pour réduire le risque et anticiper l'occurrence d'agressions similaires.

L'outil informatique qui assiste la méthode et dont les caractéristiques seront explicitées dans la section suivante, tient compte de cette condition.

Ainsi, les possibilités d'interaction en face à face et/ou à distance constituent une condition d'expérimentation qui répond aux spécificités du contexte de détection et d'analyse des agressions numériques caractérisé particulièrement par une contrainte majeure liée à la pression du temps.

5.2.6 Possibilités d'accéder rapidement à des informations appropriées et disponibles dans des bases de données internes et/ou externes à l'entreprise

Lors de la phase d'amplification progressive des signaux/signes faibles ainsi que de raisonnement sur les liens entre celles-ci, il est important de pouvoir accéder à des informations complémentaires dans des bases de données internes et/ou externes à l'entreprise. L'efficacité et l'utilité de la recherche complémentaires d'informations sont largement dépendantes des moyens employés pour effectuer cette activité.

Dans ce cadre, nous mettons l'accent sur quatre fonctionnalités de la technologie Internet qui sont susceptibles d'offrir un support adéquat à l'expérimentation de notre méthode. Ces fonctionnalités sont les suivantes:

- L'emploi **des moteurs de recherche approchée** en utilisant des liens sémantiques, des liens de dépendance et hiérarchiques, ainsi que des liens avancés, comme les hyperliens, et les adresses URL. Ces moteurs de recherche se basent sur des relations diverses entre les éléments en mémoire incluant l'analogie, la similarité, et la proximité. Cette potentialité de la technologie Internet offre des possibilités étendues de recherche d'informations complémentaires ou de connaissances mémorisées afin de conduire et d'enrichir les phases d'amplification et de raisonnement collectif.
- L'emploi **des moteurs d'inférence** permettant de faire de la déduction automatique à partir d'hypothèses et de règles de déduction approchée en créant des liens sémantiques et/ou probabilistes. Cette fonctionnalité de l'Internet assiste la **manipulation des liens** lors de la phase de raisonnement collectif à travers la création de liens utiles pour structurer et organiser les informations collectées d'une manière intelligente et dynamique.
- L'emploi des mécanismes permettant de **contrôler l'accès** à une base de données et de **garder les traces** de toutes les opérations réalisées sur celles-ci. Cette fonctionnalité de l'Internet permet la capitalisation et le stockage des représentations formulées et

construites par les membres d'une ERI, ainsi que les validations éventuelles de celles-ci en cas de prise de décision. Elle représente également un support pour **manipuler plus commodément** les heuristiques résultant de l'apprentissage collectif au sein de l'ERI et de les capitaliser.

L'outil conçu et développé pour assister notre méthode et dont les caractéristiques seront présentées dans la section suivante, exploite ces quatre fonctionnalités de la technologie Internet.

5.2.7 Existence d'un animateur/médiateur

Le chapitre précédent a signalé le rôle important que peut jouer le médiateur pour intégrer les différents fragments d'information et des points de vue des participants, construire collectivement le scénario de l'agression, et trouver les mesures correctives.

Particulièrement, le médiateur valide les concepts qui sont représentés par les nœuds, manipule les liens qui sont représentés par les arcs et contrôle le processus d'affinement conduisant à une vision collective et intelligible.

De plus, le médiateur cerne les zones de conflit en vue de trouver des arrangements possibles à travers la négociation et la conciliation. Ces mécanismes permettent l'enrichissement et la modification des vues en conflit par affinement des nœuds et des liens représentés dans le graphe.

L'activité de médiation nécessite l'usage de certains outils pour réduire la complexité du raisonnement et faire converger les points éventuellement en conflit d'une façon aussi objective que possible.

Dans notre cas, le médiateur devrait savoir manipuler l'outil mis en œuvre pour assister la méthode proposée. Nous laissons ainsi entendre que le médiateur doit posséder certaines compétences de technicien dans l'utilisation de cet outil.

5.3 Conception et mise en œuvre d'un outil informatique pour assister la méthode d'aide à la création collective de sens

Dans cette section, nous décrivons les spécificités d'un outil informatique qui a été conçu et développé par un ingénieur en réseaux informatiques et de télécommunications pour assister la méthode proposée dans cette recherche. Cet outil est susceptible d'aider l'ERI lors du processus de création collective de sens pour les fins de réduction et d'anticipation du risque des agressions numériques.

Nous énonçons, d'abord, les caractéristiques et les objectifs de développement de cet outil. Ensuite, nous présentons les étapes réalisées dans le cadre de sa mise en œuvre.

5.3.1 Objectifs et caractéristiques de l'outil informatique

L'outil utilise certaines applications de la technologie Internet et présente des innovations sur les plans de conception et de mise en œuvre dans le domaine informatique.

Les objectifs de conception et de mise en œuvre de cet outil dans le but d'assister la méthode proposée, peuvent être résumés au niveau des quatre activités suivantes :

- La représentation graphique de l'ensemble des nœuds et des liens montrant les points de vue élaborés par les membres de l'ERI lors du processus de la création collective de sens. Les objets graphiques générés au cours de cette activité bénéficient d'une construction évolutive, flexible et structurelle (par exemple, un simple clic sur un nœud ou un arc peut faire accéder à une information riche).
- La construction de base de données et de connaissances afin d'assister le processus de la création collective de sens et de mémoriser des connaissances **acquises** lors des validations passées de scénarios ayant servi à l'ERI de résoudre des problèmes de sécurité dans le passé, ou **intégrées** dans le processus de raisonnement ou d'affinement et acquises suite à des recherches d'informations à l'interne ou à l'externe de l'entreprise (disponibles par exemple dans des sites Web spécialisés).
- L'intégration de moteurs de recherche de type « recherche exacte et/ou approchée » pour la collecte des informations complémentaires lors de la construction du scénario de l'agression. Les moteurs associent un certain nombre de techniques de recherche

pour tenir compte de la diversité des informations potentiellement utiles à la construction du scénario de l'attaque ainsi que des spécificités de l'entreprise.

- La mise en place d'une assistance au raisonnement collectif permettant la construction et l'analyse des scénarios d'attaque afin de réduire la complexité du raisonnement et faciliter la navigation sur les graphes représentant les points de vue des membres de l'ERI.

Pour atteindre ces objectifs, l'outil informatique comporte quatre principaux modules. Il s'agit de:

- Module de représentation des nœuds et des liens permettant d'intégrer progressivement les éléments de raisonnement lors de la construction du scénario de l'attaque
- Module de collecte et d'extraction des informations comportant des moteurs de recherche de type exacte/approchée et un gestionnaire de la base de données et de connaissances. Les moteurs de recherche permettent d'établir des liens sémantiques, des liens de dépendance et hiérarchiques, ainsi que des liens avancés lors des requêtes. Le gestionnaire de la base de données permet de contrôler l'accès à la base de données et de garder les traces de toutes les opérations réalisées sur celles-ci
- Module de manipulation dynamique des nœuds et des liens au sein d'un graphe permettant la mise en œuvre des opérations de réécriture et de remplacement des éléments de raisonnement lors de l'intégration des points vues partiels ou d'affinement du raisonnement.
- Module pour assister le raisonnement à travers l'emploi des moteurs d'inférence permettant de faire de la déduction automatique à partir d'hypothèses et de règles de déduction approchée. Ce module permet également de **manipuler plus facilement les heuristiques** résultant de l'apprentissage collectif

5.3.2 Réalisation de l'outil

La conception et la mise en œuvre d'une partie de l'outil informatique ont été réalisées dans le cadre des travaux d'encadrement de projets de fin d'études d'ingénieurs liés à des travaux d'innovation à l'ANCE. Ces travaux de recherche visent essentiellement à produire des outils

d'assistance au travail de l'ERI de cette entreprise. A la date de rédaction de ces pages, les **trois premiers** modules sont opérationnels. La base des données et des connaissances comporte huit scénarios d'attaque incluant les cas traités précédemment dans le cadre de l'expérimentation de notre méthode.

Le **principe de fonctionnement** de l'outil est le suivant :

L'outil permet dans une première étape de construire le graphe en ajoutant des concepts. Pour chaque concept, nous avons la possibilité de spécifier son nom, son type (pour le classifier, par la suite, dans la base de données) et les attributs associés servant de description et d'informations supplémentaires pour ce concept.

Une fois ajoutés, nous relient ces concepts entre eux en spécifiant le concept source, puis celui de destination. En conséquence, une fenêtre apparaît, permettant de spécifier le type et la probabilité assignée à cette relation.

Nous pouvons mettre ces concepts dans la position adéquate, qui permet d'avoir une vision claire de la totalité du graphe, ou encore les supprimer ou supprimer les liens qui les relient.

Un chemin de raisonnement donné, peut être coloré, en sélectionnant les concepts qui constituent ce chemin et en cliquant sur l'option « Couleur », une fenêtre apparaît permettant de choisir la couleur désirée.

Lorsque nous cliquons sur l'option « Statistiques », après avoir sélectionné quelques concepts, nous obtenons un histogramme traçant l'évolution de ces derniers.

Pour effectuer une recherche pour l'affinement d'un concept, il suffit de sélectionner ce dernier et de cliquer sur l'option « Info ». Le moteur de recherche associé (tel que www.google.com) utilisera les mots clés qui décrivent le concept pour rechercher les pages Web (information ou concept) liées à ces mots. Une recherche approchée peut être également effectuée à travers l'utilisation d'un module (développé sur la base de l'activité de l'entreprise) qui détermine les mots approchés ou les mots clés présélectionnés. La recherche à ce moment là permettra de retrouver les pages Web liées aux mots approchés.

Le graphe construit peut être enregistré dans la base des données sous sa nouvelle forme ou bien l'effacer complètement.

La figure 17 représente un schéma synoptique de l'outil déjà réalisé. Ce schéma montre les différents modules mentionnés précédemment ainsi que l'interopérabilité entre ces derniers.

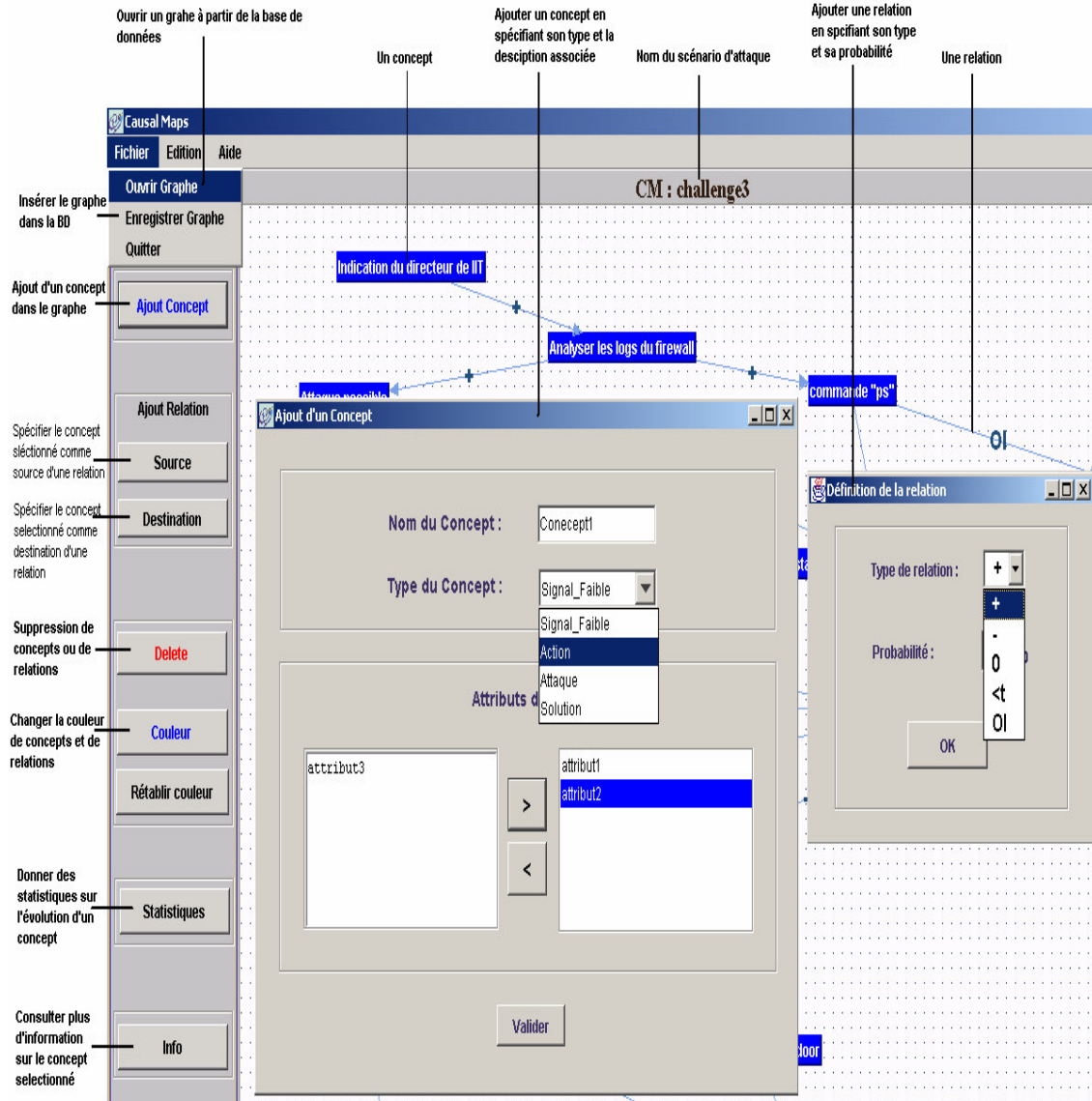


Figure 17: Description du logiciel

Conclusion Chapitre 5

Nous avons procédé dans ce chapitre à l'expérimentation de la MARRAN sur quatre cas réels d'agressions numériques tout en justifiant le choix de ces cas.

Il apparaît à travers ces expérimentations que la MARRAN est adaptée à l'activité de réponse aux agressions numériques et plus particulièrement au travail d'une ERI. Dans cette activité, les étapes d'amplification progressive des signaux/signes faibles, de recherche complémentaire d'informations et de raisonnement itératif sur les liens sont nécessaires pour construire le scénario d'attaque. La MARRAN offre une méthodologie de travail à cette activité en mettant l'accent sur le rôle central du médiateur ainsi que la nécessité de mémoriser les raisonnements afin de pouvoir les utiliser dans des constructions ultérieures de scénarios d'attaque.

Pour des fins de validité externe de la MARRAN dans le cadre de travail d'une ERI, nous avons présenté également dans ce chapitre une liste non exhaustive des conditions d'expérimentation en vue de sa réplication pour d'autres cas.

Sur le plan de l'instrumentation de la MARRAN, nous avons présenté un logiciel utilisant certaines applications de la technologie Internet et qui a été conçu et développé pour supporter la MARRAN. Ce logiciel permet la représentation graphique de l'ensemble des nœuds et des liens décrivant les points de vue élaborés par les membres de l'ERI lors de la construction du scénario d'attaque. Il permet également la construction des bases de données et de connaissances afin d'assister le processus de la création collective de sens et de mémoriser les connaissances **acquises**. Il permet enfin l'intégration de moteurs de recherche de type « recherche exacte et/ou approchée » pour la collecte des informations complémentaires.

Ces fonctionnalités sont nécessaires pour assister le travail d'une ERI afin de réduire la complexité du raisonnement, et aider à la prise de décision dans le domaine de réponse aux agressions numériques.

Évaluation de la méthode et analyse des résultats

Ce chapitre présente les résultats d'évaluation de la méthode MARRAN à travers le traitement des entretiens effectués auprès des experts en sécurité. Cette méthode de collecte des données auprès des experts a été choisie principalement à cause de l'impossibilité d'utiliser les critères de mesure spécifiques au contexte de notre recherche et qui ont été mentionnés au quatrième chapitre.

Par ailleurs, la réponse à la question de recherche devrait permettre de produire de nouvelles connaissances académiques particulièrement dans les domaines du management stratégique et des systèmes d'information.

Ainsi, la première section énonce la méthodologie de recherche poursuivie en justifiant le recours à la collecte des données à travers des entretiens semi directif auprès des experts en sécurité informatique. Nous présentons, en tenant compte de nos objectifs d'évaluation, les observations à collecter et la méthode d'analyse utilisée.

La deuxième section est consacrée à l'évaluation de la méthode à travers l'exploitation des informations recueillies lors des entretiens. Cette évaluation auprès des experts vise principalement à affirmer l'utilité perçue de la méthode et si elle aide efficacement les ERI. Nous cherchons également à évaluer un autre aspect lié à la praticité de la méthode et la facilité perçue d'utilisation de l'outil informatique qui la supporte en analysant les réponses concernant le fonctionnement de la méthode proprement dite.

La troisième section résume les contributions des résultats empiriques de notre recherche à la production des connaissances académiques nouvelles

6.1 Méthodologie de collecte de données

Dans cette section, nous précisons, d'abord les conditions de la présente recherche qui nous a amener à choisir les **entretiens auprès des experts** comme moyen pour collecter les données. Ensuite, nous décrivons les données à recueillir au regard des objectifs de l'évaluation de la méthode proposée. Puis, nous détaillons les étapes de déroulement des entretiens auprès des experts en sécurité. Nous présentons enfin la méthode d'analyse adoptée pour traiter les données collectées lors des entretiens.

6.1.1 Conditions de la recherche et choix d'une méthode de collecte des données

Comme nous l'avons signalé en introduction, la présente recherche s'apparente à l'étude d'un problème stratégique perçu complexe par les praticiens et lié au processus de réduction et d'anticipation du risque des agressions numériques sachant que peu de connaissances théoriques sont disponibles ou adaptées à cette problématique. Dans ce contexte, la présente recherche est de nature exploratoire et aura pour principal objectif de produire des connaissances actionnables au sens d'Argyris (1995) afin d'aider efficacement les ERI à réduire et anticiper le risque des agressions numériques.

Pour apporter des éléments de réponse à cette question, nous avons proposé une méthode d'interprétation d'informations de type signal/signe faible qui peuvent indiquer ou anticiper l'occurrence d'une agression numérique. Cette interprétation s'opère à travers un processus de création collective de sens. La conception et la construction de la méthode sont issues d'une série d'observations du terrain et d'une articulation et extension de certaines connaissances théoriques et actionnables disponibles.

Ce processus de recherche s'intègre bien dans le cadre d'une recherche ingénierique au cours de laquelle le chercheur "ingénieur" conçoit un outil, le construit et le met en œuvre sur le terrain dans le but d'induire des connaissances théoriques plus générales (Chanal *et al*, 1997).

Par ailleurs, la dimension temporelle a une importance capitale dans ce type de recherche puisque le chercheur doit mesurer le changement induit par l'implémentation de son outil dans le terrain afin de saisir son effet dans le temps. Ceci implique la définition d'un ensemble de

paramètres de mesure à différents moments de la mise en pratique de cet outil en entreprises et ce dans le cadre d'une étude longitudinale.

Ainsi, l'évaluation de cet outil à travers le choix d'une méthode de collecte de données en accord avec les choix méthodologiques liés à la recherche ingénierique, devrait s'appuyer sur les appréciations formulées par les praticiens ainsi que sur des indicateurs de mesure de l'effet du temps. La méthode de collecte des données devrait tenir compte de ces deux considérations afin de pouvoir saisir les apports de la méthode et les améliorations possibles de celle-ci suite à sa mise en application dans le terrain.

Dans le cas de notre recherche, nous avons choisi les entretiens semi directifs pour collecter les données susceptibles de nous permettre d'évaluer notre méthode. Quant à la dimension temporelle, nous avons défini un ensemble de critères mentionnés au niveau du quatrième chapitre permettant de mesurer le progrès perçu par l'ERI suite à l'implémentation de la méthode proposée.

Nous avons été amenés à choisir les entretiens semi directifs auprès des experts en sécurité pour l'évaluation de la MARRAN puisque la mesure des critères quantitatifs requiert une certaine période, au moins deux années d'expérimentation, ce qui est impossible à réaliser compte tenu du temps imparti à la thèse.

En effet, les entretiens face à face sont considérés comme principal mode de collecte de données primaires dans le cadre d'une recherche qualitative. Il représente "une technique destinée à collecter, dans la perspective de leur analyse, des données discursives reflétant notamment l'univers mental conscient ou inconscient des individus" (Baumard *et al.*, 1999). Les entretiens sont de nature à générer des données riches dont la validité est très importante (Allard-Poesi, *et al.*, 1999).

Nous avons choisi de réaliser des entretiens semi-directifs individuels et collectifs. L'utilisation comme canevas pour ces entretiens d'une grille de questions nous permet de remédier partiellement au caractère non structuré des entretiens, comme elle peut servir à débiter et encadrer les discussions. La grille des ces questions utilisée comme canevas aux entretiens est détaillée en annexe. De même des questions d'investigation et d'implication (Rubin et Rubin,

1995) ont été également posées au fur et à mesure de l'entretien afin de clarifier une réponse incomplète ou de préciser une idée avancée par un expert.

6.1.2 Canevas des entretiens et description des informations à recueillir

Rappelons que le but de la collecte des données est de tester l'hypothèse centrale de cette recherche concernant la mesure de l'efficacité de la méthode en terme d'utilité perçue et de praticabilité/facilité perçue d'utilisation. Le canevas d'entretien se présente sous la forme d'une grille de questions devant nous permettre d'évaluer, d'abord, ces deux aspects de la méthode. Ensuite, nous avons préparé des questions qui concernent l'état des pratiques en matière de réduction et d'anticipation du risque des agressions numériques afin de savoir si notre proposition apporte une amélioration par rapport à l'état des ces pratiques. Enfin, une série de questions concerne l'évaluation des critères de mesure au cours du temps lors la mise en pratique de la méthode en entreprises.

Ainsi, le canevas comporte quatre groupes de questions. Le premier groupe comportant une série de cinq questions ayant pour objectif d'évaluer l'utilité perçue de la méthode. A cet effet, nous avons cherché à mesurer l'utilité des différentes étapes de la méthode pour réduire et anticiper le risque des agressions numériques. Particulièrement, nous avons cherché à connaître les appréciations des experts concernant l'utilité de :

- l'étape d'amplification progressive des signaux/signes faibles
- l'étape de la recherche complémentaire des informations
- l'étape du raisonnement itératif sur les liens créés entre les informations collectées.

En outre nous avons cherché à vérifier si :

- les étapes de la méthode permettent la construction significative des scénarios d'attaques.
- les experts sont intéressés par l'intégration de la méthode proposée dans leur travail de réponse aux agressions numériques.

Par rapport à l'étape du raisonnement itératif sur les liens, nous avons cherché à savoir :

- si les liens proposés sont suffisants et adaptés au contexte des agressions numériques,

- si d'autres liens peuvent être ajoutés pour couvrir le raisonnement dans ce contexte,
- si l'activité de médiation, dans le travail d'une ERI pour conduire le raisonnement lors de la construction du scénario de l'attaque, est utile.

La deuxième partie du canevas d'entretien comprend une série de questions ayant pour objectif de mesurer la facilité perçue d'utilisation de la méthode. A cet égard, nous avons cherché à mesurer :

- si l'utilisation de chaque étape de la méthode est perçue comme étant facile,
- si l'activité de médiation est facile d'utilisation,
- si l'outil informatique qui assiste la méthode est facile d'utilisation et s'il est susceptible d'apporter une aide au travail de l'ERI lors de sa mise en œuvre,
- si les experts proposent certaines conditions dans lesquelles ils pensent pouvoir utiliser la méthode.

S'agissant de la troisième partie du canevas d'entretien, nous avons collecté des informations qui concernent l'état des pratiques dans le domaine de détection, de réponse et d'anticipation des agressions numériques. Nous avons cherché à connaître :

1. l'élément déclencheur habituel d'une réunion de réponse à une agression numérique annoncée,
2. la fréquence et la périodicité des réunions,
3. la nature des informations qui annoncent l'agression, ou qui déclenchent la réunion,
4. la forme sous laquelle ces informations se présentent,
5. la manière dont elles sont obtenues ou captées,
6. la durabilité de mémorisation des informations,
7. la méthode d'analyse des informations détectées (individuelle ou collective, en face à face ou bien à distance),
8. la démarche d'interprétation (tacite ou formalisée, mémorisée ou non),
9. les outils Internet utilisés dans le traitement,
10. les actions qui découlent de l'interprétation des informations.

Dans la dernière partie du guide de l'entretien, nous avons exploré la pertinence des indicateurs de mesure, dans le temps, au cours du déroulement de la méthode et que nous

avons déjà présentés dans le quatrième chapitre. L'objectif de cette exploration est, d'une part, de valider les indicateurs de mesure déjà construits et adaptés aux spécificités du contexte des agressions numériques, d'autre part, de chercher d'autres indicateurs jugés pertinents par les experts.

6.1.3 Dispositif de recherche

Nous avons contacté neuf experts en sécurité informatique se présentant comme suit :

- Trois membres de l'ERI de l'ANCE
- Trois experts de l'ANCE
- Trois experts en sécurité de trois entreprises qui sont des fournisseurs des services Internet et pour lesquelles le risque des agressions numériques est d'une ampleur considérable compte tenu de la nature de leurs activités.

Description des experts (profil, expérience) :

Les trois membres de l'ERI de l'ANCE ont une expérience de quatre ans dans le domaine de la sécurité informatique. Ils sont chargés de surveiller d'une façon permanente/quotidienne le trafic sur le réseau de l'entreprise et de répondre en cas d'urgence à des problèmes de sécurité.

Les trois experts de l'ANCE sont impliqués dans la prise de décision concernant la réponse aux agressions numériques que l'entreprise peut rencontrer. Ils sont également impliqués dans le développement et la mise à jour de la politique de sécurité de l'ANCE. Deux des experts ont une expérience de quatre ans. Le troisième expert, outre son expérience de cinq ans, est également reconnu sur le plan international pour ses travaux de recherche dans le domaine de la sécurité des réseaux d'entreprise.

Les trois autres experts sont impliqués directement dans la gestion des agressions numériques au sein de leurs entreprises qui sont classées comme étant des entreprises fortement utilisatrices des TIC. Ces experts sont confrontés quotidiennement à des problèmes de sécurité et ils ont déjà pilotés des projets importants dans ce domaine. L'expérience de ces experts est de dix ans.

L'organisation des entretiens auprès des experts a été effectuée à travers des prises de rendez-vous par téléphone ou suite à des déplacements effectués pour accéder aux entreprises considérées. Les experts contactés ont fait preuve de beaucoup de collaboration afin de nous aider à mener à bien notre recherche.

Déroulement des entretiens: La durée moyenne des entretiens est de deux heures. Ce qu'il faut préciser c'est que les entretiens qui ont été effectués auprès des membres de l'ERI de l'ANCE sont collectifs. Tandis que les autres entretiens sont individuels.

Au début de l'entretien, nous avons présenté l'objet de nos travaux de recherche ainsi que les différentes étapes et l'objectif de la méthode. Pour concrétiser la méthode, nous avons également présenté deux cas de construction d'un scénario d'attaque à l'aide de l'outil informatique en explicitant son mode opératoire. Suite à la démonstration informatique, nous avons posé aux experts les questions préparées à l'avance pour connaître leurs réactions et leurs critiques.

Lors des entretiens, nous avons utilisé un magnétophone pour recueillir et enregistrer fidèlement les propos, les remarques et les commentaires des experts.

6.1.4 Méthode d'analyse des données collectées lors des entretiens

La méthode d'analyse des données collectées lors des entretiens est inspirée de celle adoptée par Valette (1993) dans son travail de recherche.

Le canevas d'entretien comporte des questions ouvertes réparties selon quatre thèmes. Nous avons essayé à l'issue de chaque entretien, de reprendre l'ensemble des réponses des experts interrogés par thème à l'aide d'un tableau en trois colonnes :

- La première colonne comporte les questions qui décrivent les informations à recueillir par thème,
- La seconde colonne est réservée aux réponses, et commentaires des experts interrogés,
- La troisième colonne indique le nom de l'expert et le nom de son entreprise.

Cette méthode nous permet d'analyser les propos des experts interrogés point par point par rapport aux données que nous entendons recueillir, tout en ayant la possibilité de comparer les réponses les unes par rapport aux autres.

6.2 Exploitation des données recueillies lors des entretiens auprès des experts

Cette section est consacrée à l'analyse des données collectées au cours des entretiens auprès des experts en sécurité. Cette analyse est divisée sur quatre parties. La première partie concerne l'évaluation de l'utilité perçue de la méthode proposée pour réduire le risque des agressions numériques afin d'agir vite ou par anticipation. La deuxième partie s'intéresse à l'évaluation de la facilité perçue d'utilisation de la méthode proposée. La troisième partie de l'analyse concerne l'état des pratiques des experts interviewés en matière de gestion du risque des agressions numériques afin de positionner l'apport ou les améliorations possibles de la méthode proposée par rapport à ces pratiques. La quatrième partie est réservée à l'exploitation des données relatives à l'évaluation de la méthode dans la durée et sur la base de critères de mesure quantitatifs.

6.2.1 Analyse des résultats concernant l'utilité perçue de la méthode

L'analyse des résultats empiriques liés à l'utilité perçue de la méthode concerne le traitement des informations de type signal/signe faible, l'activité de médiation et la phase de mémorisation des raisonnements lors des constructions des scénarios d'attaques.

6.2.1.1 Enseignements tirés concernant le traitement des signaux/signes faibles

Les étapes d'amplification progressive des signaux/signes faibles, de recherche complémentaire d'informations et du raisonnement itératif sont reconnues à l'unanimité des experts comme étant des étapes utiles dans le cadre du travail d'une ERI pour répondre aux agressions numériques, et particulièrement dans le cas des agressions numériques inconnues par l'entreprise. De ce fait, ils pensent que les trois étapes de la méthode permettent une construction significative des scénarios d'attaques.

De même, les experts sont tous d'accord sur le fait que le processus de création de sens devrait être collectif vu la nature des informations de type signal/signe faible. Cependant,

l'output de ce processus dépend également de la méthode de travail utilisée et des compétences et des expertises des membres de l'ERI.

La typologie des liens proposés est considérée par la plupart des experts comme suffisante pour l'instant pour la représentation des points de vue. Trois des experts contactés suggèrent d'étendre les liens de raisonnement afin de couvrir la complexité des raisonnements lors de construction de scénarios d'attaques inconnues.

6.2.1.2 Enseignements tirés concernant le rôle du médiateur

S'agissant de l'activité de médiation, celle-ci est perçue comme étant une activité nécessaire pour le travail d'une ERI. De plus, elle est susceptible d'améliorer les temps de réponse particulièrement en présence de méthodes de travail et des outils appropriés.

Pour le rôle du médiateur, il consiste à valider les concepts représentés par des nœuds au sein du graphe, concilier en cas de points de vue divergents, à incuber des liens et des concepts utiles à la création collective de sens, et à faire converger le raisonnement vers une représentation significative du scénario d'attaque. Les experts contactés sont tous d'accord sur le fait que ce rôle est important et même déterminant pour l'efficacité du travail de l'ERI. Il est également essentiel pour détecter de nouvelles attaques.

Certains experts sont concernés par l'activité de médiation et découvrent lors des entretiens qu'ils pratiquent la médiation, « sans le savoir » c'est-à-dire sans une démarche explicite et une formation appropriée.

Toutefois, l'utilité du médiateur peut être faible dans le cas des agressions traditionnelles ou connues lorsque le raisonnement est simple à réaliser. L'utilité est importante lorsque l'agression est nouvelle à l'entreprise. Ces constats sont signalés par l'ERI de l'ANCE ainsi que par un expert d'une entreprise fournisseur de services Internet.

Par ailleurs, la taille et la nature d'activité de l'entreprise sont des variables importantes à considérer pour l'activité de médiation.

Les experts contactés sont tous favorables à l'intégration de la méthode proposée dans leur travail de réponse aux agressions numériques. Mais, ils exigent une formation préalable pour l'apprentissage de la méthode et l'adaptation de l'outil au contexte de l'entreprise par

l'intégration à la base de données d'un ensemble d'informations et de liens relatifs à la nature d'activité de celle-ci. Certains experts contactés pensent que la méthode proposée constitue un excellent outil pédagogique pour former les membres d'une ERI dans le domaine de réponse aux agressions numériques. L'intérêt d'adopter la méthode réside également dans le fait qu'elle peut être intégrée dans une démarche prospective des cas d'agressions numériques inconnues.

6.2.1.3 Enseignements tirés concernant la mémorisation des raisonnements

Lors des entretiens, les experts ont été particulièrement intéressés par les possibilités offertes par la méthode proposée de garder des traces des raisonnements effectués lors des constructions des scénarios d'attaques. La mémorisation de ces raisonnements est nécessaire à cause de la grande mobilité des ingénieurs et le coût élevé de leur formation dans les tâches d'investigation électronique (enquête numérique à la détection d'un signal faible) et de réponse aux incidents de sécurité.

Les bases de données et de connaissances sont considérées par l'ensemble des experts comme étant déterminantes et indispensables dans le processus d'itération et d'affinement des raisonnements. Dans ce cadre, la nécessité de démarrer avec une base de connaissances acquise est une condition qui paraît très importante, selon les experts rencontrés, pour l'utilisation de la méthode. Certains experts considèrent même qu'il s'agit d'une condition sine qua non pour l'efficacité de la méthode.

Certains experts (de l'ANCE notamment), considèrent que la mémorisation constitue un moyen susceptible d'aider à répondre à des attaques nouvelles. De ce fait, la méthode permet de prospecter et de réagir à des attaques nouvellement créées.

A travers la mémorisation, l'activité de réponse aux agressions numériques permet la capitalisation des connaissances dans l'entreprise. Ainsi, les connaissances acquises et mémorisées, émergeant de l'activité de réponse aux agressions numériques, constitue une ressource de valeur pour l'entreprise, et même un produit susceptible d'être vendu, puisque sa réplique sur d'autres entreprises est possible.

6.2.2 Analyse des résultats concernant la facilité perçue d'utilisation de la méthode

Les experts mentionnent la difficulté de réaliser (facilité d'utilisation) les trois étapes de la méthode à cause de la complexité du raisonnement surtout dans le cas des agressions inconnues par l'entreprise, et l'abondance des informations liée à l'étendue du champ d'investigation.

De même, le rôle du médiateur est perçu difficile et intimement dépendant des compétences et de la formation du médiateur. Certains experts soulignent même que la facilité d'utilisation de la méthode proposée est principalement liée à l'expertise du médiateur.

Par ailleurs, les experts sont d'accord dans l'ensemble sur le fait que l'outil informatique supportant la méthode est convivial, facile à manipuler et présente l'avantage d'être graphique (mais ces experts sont bien familiers de l'informatique). La notion de concept représenté par un nœud dans le graphe est acceptée par l'ensemble des experts interviewés.

Les experts sont tous d'accord sur l'aide que peut fournir l'outil informatique afin d'assister le travail de l'ERI.

Cependant, la facilité perçue d'utilisation de la méthode reste très dépendante de la réalisation de la base des données et des connaissances ainsi que de l'expertise des membres de l'ERI et du médiateur.

6.2.3 Analyse des résultats par rapport à l'état des pratiques des experts rencontrés

Ce qui diffère dans l'état des pratiques des entreprises contactées c'est l'étape d'initiation du traitement du signal/signe faible détecté et la convocation de l'ERI pour effectuer l'opération d'interprétation. La gestion de l'intervention de l'ERI et le rôle du médiateur sont également différents d'une entreprise à l'autre. Ceci est dû principalement à des différences au niveau de la structure et du fonctionnement de l'ERI.

6.2.3.1 Enseignements tirés concernant la structure de l'ERI

La réponse aux agressions numériques à travers le travail de l'ERI est une activité qui a été jugée comme étant fondamentale, par les experts rencontrés. Ils soulignent que sans ressources allouées à cette activité, ni outils adéquats ils sont en difficulté pour remplir leur

rôle. Nous avons constaté l'existence très fréquente d'une structure minimale ne dépassant pas trois personnes, chargée de la tâche de réponse aux problèmes de sécurité. Il n'y a pas d'existence réelle d'une ERI mais plutôt d'une cellule qui s'occupe du travail d'une ERI. L'organisation du travail d'une ERI, en termes de répartition des tâches et d'élaboration des mécanismes de coordination, est insuffisante aux yeux des experts rencontrés.

Généralement, l'équipe ERI n'est pas pluridisciplinaire : c'est l'équipe qui s'occupe de la gestion du réseau d'entreprise dans la plupart des cas. Seule, parmi les entreprises rencontrées, l'ANACE a mis en place une ERI composée de 7 personnes pluridisciplinaire faisant intervenir des experts dans d'autres départements. Cependant, même ici, nous avons noté l'absence de gestionnaires dans l'équipe.

Les ERI dans les entreprises contactées ne disposent pas de procédures formalisées ni d'outils appropriés pour assister la démarche d'interprétation des signaux/signes faibles détectés.

6.2.3.3 Enseignements tirés concernant le fonctionnement de l'ERI

Tous les experts interviewés sont d'accord sur le fait que les informations de type signal/signe faible caractérisent bien les alertes et les anomalies détectées par les équipements ou les personnes et qui constituent le point de départ de travail d'une ERI.

Le travail de l'ERI requiert effectivement, selon eux, la création collective de sens à partir des signaux/signes faibles. Ils soulignent que la médiation, qu'ils découvrent parfois à l'occasion de l'entretien, joue un rôle important dans ce processus même si elle n'est pas visible.

La démarche d'interprétation n'est pas généralement formalisée dans les entreprises contactées, à l'exception de l'ANACE qui a procédé à l'établissement d'une politique de sécurité qui est absente dans les autres entreprises.

La définition des tâches et des responsabilités liées à la démarche d'interprétation des signaux/signes faibles n'est pas suffisamment visible comme fonction dans la structure de l'entreprise.

La collecte d'informations est une étape jugée nécessaire dans la démarche d'interprétation des signaux/signes faibles détectés et qui devrait être assistée par des techniques de recherche de type approchée.

6.2.3.4 Enseignements tirés concernant les outils de collecte des signaux faibles

La plupart des experts reconnaissent la nécessité des équipements de détection des signaux/signes faibles, ce qui n'exclut nullement les interventions humaines jugées inévitables.

Les outils de détection utilisés sont primitifs pour la plupart des entreprises consultées : appels téléphoniques, détection accidentelle d'une anomalie, constat d'un dommage.

Pour l'ANCE, l'ERI dispose d'un réseau de capteurs avec la mise en place d'un ensemble de métriques pour filtrer une partie des signaux/signes faibles détectés mais non significatifs et une mise à jour afin d'analyser les événements avant de déclarer une alerte qui constitue le signal faible de départ.

Les alertes sont stockées à l'ANCE, mais ne sont pas stockées dans les autres entreprises contactées.

6.2.4 Analyse des résultats concernant les indicateurs de mesure (dans la durée) que nous avons proposé pour l'évaluation de la méthode

Les experts contactés sont tous d'accord sur le fait que l'évaluation qualitative de la méthode à travers les interviews doit être suivie par une évaluation quantitative qui requiert une période assez longue et variable d'une entreprise à l'autre. La période de l'apprentissage dépend aussi de l'état des pratiques dans le domaine de réponse aux agressions numériques.

Les critères proposés pour mesurer l'efficacité de la méthode sont jugés pertinents par l'ensemble des experts.

Les experts ont proposé deux autres critères de mesure. Un des experts propose de mesurer l'impact de l'implémentation de la méthode sur l'activité de l'entreprise en termes de gain sur

le coût de sécurité, la gestion de la clientèle, performance des services offerts...etc. le deuxième critère propose de mesurer la réactivité de l'ERI par rapport à des agressions nouvelles ou inconnues par l'entreprise. Ceci permet de voir dans quelle mesure la méthode proposée permet la gestion du flou voire de l'inconnu.

6.3 Contributions théoriques et pratiques de la recherche

Dans cette section, nous exposons les apports théoriques et pratiques de notre recherche. Ces apports sont issus de l'exploitation des données recueillies lors des entretiens auprès des experts en sécurité informatique et ce dans le cadre d'une recherche exploratoire. La réponse à la question de recherche, relative à un problème d'origine terrain, vise la production de connaissances actionnables dans le domaine de la sécurité informationnelle, utiles aux praticiens, à travers la proposition d'une méthode pour aider une ERI à réduire voire anticiper le risque des agressions numériques.

6.3.1 Apports théoriques de la recherche par rapport aux connaissances académiques

Les apports théoriques de la présente recherche peuvent être situés sur quatre plans.

6.3.1.1 Risque en général versus risque des agressions numériques

Ce travail de recherche a mis l'accent sur un **nouveau risque**, rencontré par les entreprises, suite à l'accroissement de leur connectivité à travers l'utilisation des réseaux comme moyen de travail et de communication. Ce nouveau type de dépendance des entreprises vis-à-vis des réseaux pose le problème de la **sécurité des ressources informationnelles** à l'égard du **risque des agressions numériques**.

La présente recherche a montré qu'à l'ère numérique, le risque des agressions numériques est planétaire, instantané et dont l'ampleur économique semble d'ores et déjà considérable pour l'entreprise.

De plus, cette recherche a permis de mettre en relief les problèmes de gestion liés au risque des agressions numériques qui ne devrait plus être considéré uniquement comme un risque technique mais également de management.

A notre connaissance, très peu de travaux théoriques en **sciences de gestion** se sont intéressés à cette problématique, ont traité ce nouveau type de risque ou proposé des connaissances actionnables devant permettre aux managers réduire le risque des agressions numériques.

6.3.1.2 Nouveau type d'acteurs de l'environnement de l'entreprise : les « hackers »

Dans le contexte de la présente recherche, notre intérêt a porté sur une nouvelle catégorie d'acteurs pertinents de l'environnement de l'entreprise. Il s'agit des hackers qui, par leurs actions, peuvent compromettre la sécurité informationnelle de l'entreprise.

Comme les acteurs classiques, ces nouveaux acteurs peuvent être actuels ou potentiels, agissent d'une façon directe ou indirecte sur la survie et la croissance de l'entreprise, et devraient être pris en compte dans l'élaboration de sa stratégie.

6.3.1.3 Transposition et adaptation de la phase de création collective de sens de la méthode L.E.SCAnning®

La présente recherche a contribué à des enrichissements de la phase de création collective de sens de la méthode L.E.SCAnning® dans un domaine nouveau à savoir la sécurité informationnelle à l'égard des agressions numériques. Cette phase a été transposée et adaptée à ce nouveau domaine d'étude comme étant des connaissances actionnables à intégrer dans la conception et la construction de la méthode proposée dans ce travail.

Par rapport à la phase de création collective de sens, nous avons proposé un enrichissement de la typologie des liens en intégrant la **probabilité et l'approximation** pour assister la création de relations entre les informations de type signal/signe faible dans un contexte d'incertitude. Les liens probabilistes et dynamiques utilisés dans cette recherche permettent de réduire la complexité du raisonnement liée à la réponse aux agressions numériques ainsi que d'aider à la prise de décision dans ce domaine particulier.

6.3.1.4 Proposition de nouveaux indicateurs de mesure

A l'issue des entretiens réalisés auprès des experts, nous avons validé six critères quantitatifs de mesure qui pourront servir à d'autres recherches dans le domaine des agressions numériques sur réseau d'entreprise.

Ces critères sont les suivants :

- le temps de traitement de chaque signal faible,
- le ratio des fausses décisions sur le nombre total des décisions prises,
- le ratio des décisions incomplètes sur le nombre des agressions qui se répètent,
- le temps de réaction globale qui mesure le temps de détection, de traitement et de réponse à une agression numérique,
- l'impact de l'implémentation de la méthode sur l'activité de l'entreprise en termes de gain sur le coût de sécurité, la gestion de la clientèle, la performance des services offerts...etc.
- le nombre des agressions nouvelles ou inconnues détectées par l'entreprise.

6.3.2 Apports pratiques de la recherche

L'exploitation des données collectées lors des entretiens auprès des experts nous a permis de mettre en relief les contributions pratiques de la présente recherche. Ces contributions touchent particulièrement les aspects de gestion liés au fonctionnement d'une l'ERI.

6.3.2.1 L'organisation du travail de l'ERI

Par organisation nous voulons désigner : une structure appropriée, une définition claire et précise des tâches, des responsabilités explicitées, et des moyens de coordination. Sans quoi le temps de réponse à une agression augmente ce qui est de nature à aggraver les dommages et à alourdir les coûts de réparation.

Dans le domaine de la sécurité des réseaux d'entreprise, la capacité de détecter et de répondre à une agression numérique le plus rapidement possible est nécessaire. Le travail de l'ERI, assistée par une logistique associée (en termes d'outils de collecte d'informations, des

procédures et des méthodologies de travail), répond à la nécessité de réduire le temps de réponse à une agression numérique et de minimiser les dégâts occasionnés par celle-ci.

6.3.2.2 La gestion des ressources humaines liée à l'ERI

La réponse aux agressions numériques à travers la détection des signaux/signes faibles, l'amplification de ceux-ci, et la mise en œuvre de mesures correctives et préventives, est une activité pour laquelle l'entreprise devrait avoir une stratégie de GRH appropriée.

L'ERI est constituée d'experts, donc de compétences techniques à caractère fortement transverse, et, par définition, des compétences rares et «volatiles», dans la mesure où, plus les membres de l'ERI possèdent un haut potentiel, plus ils sont sollicités par le marché externe. Les questions qui se posent donc sont d'une part, comment **recruter, motiver** ces ressources pour les **impliquer**, les **retenir** et **pallier à la fuite des savoirs et des compétences**, et d'autre part, comment favoriser le **travail d'équipe**.

La réponse à l'ensemble de ces questions se situe sur le plan de la gestion des ressources humaines (rétribution, reconnaissance, équité...) et sur celui, plus large, du management des connaissances (transfert des savoirs tacites et explicites, Nonaka & Takeuchi (1995)). Or, jusqu'à présent, le **knowledge management** reste l'apanage des spécialistes des systèmes d'information, les **compétences** celui des DRH, et les **compétences clés** (Prahalad et Hamel, 1990) celui des stratèges.

En effet, si la gestion des compétences a occupé l'esprit des responsables des ressources humaines depuis plusieurs années, celle des connaissances, favorisée par l'arrivée des Technologies de l'Information et de la Communication (TIC) est plus récente. Cependant, l'enjeu étant devenu de pouvoir capitaliser les savoirs des acteurs et les mettre en commun, la Gestion des Ressources Humaines voit de ce fait, ses contributions à la gestion des connaissances se multiplier et se renforcer pendant que la stratégie s'appuie de plus en plus sur les capacités cognitives, développant ses fonctions de veille à tous les niveaux.

Dans le cas des ERI, la question est plus complexe dans la mesure où il ne s'agit pas seulement de gérer les connaissances de l'équipe mais, celle-ci devant anticiper chaque scénario d'attaque, il s'agit de la construction des savoirs à partir d'informations incomplètes,

fragmentaires et incertaines, de la création de nouveaux savoirs : ce qu'on gère n'est donc plus ce qu'on sait mais ce qu'on ne sait pas et, de plus, dans un contexte d'urgence.

Or, la plupart des travaux sur le *knowledge management* ont débattu largement de la nature du savoir, de son appropriation et de sa diffusion mais développent peu son apport à l'action. Que dire alors lorsqu'il s'agit d'un savoir, à la fois, à construire et à traduire en action ?

Ceci pose de bonnes perspectives de recherche mais ne constitue pas notre propos, nous dirons simplement que plus que des cellules de veille, des structures de management des connaissances et de ressources humaines sont donc à mettre **conjointement** en place pour favoriser la gestion des savoirs et compétences stratégiques dans les ERI, pour mobiliser les compétences individuelles et collectives en favorisant la capitalisation des compétences et des connaissances.

Cette question de la capitalisation des connaissances renvoie ainsi à deux niveaux de préoccupation :

- le niveau du **management stratégique des connaissances** ou "comment capitaliser les connaissances afin d'enrichir l'entreprise de l'expérience des anticipations réussies aux agressions ?".
- le niveau du **management stratégique des ressources humaines** ou "comment penser une capitalisation des connaissances qui ait toutes les chances d'être appropriée positivement par les acteurs concernés et qui donne lieu à des modes de participation effectifs? ".

Il semble donc essentiel d'intégrer la capitalisation des connaissances à la politique de GRH existante tout en ne perdant pas de vue les enjeux de pouvoir pouvant être soulevés par cette capitalisation. Ceci nous amène à la notion de **fit**, d'alignement cohérent des deux démarches. Par ailleurs, une organisation du travail plus transversale avec un système d'information performant favoriserait la **collaboration**, la **coopération**, la **confiance** qui permettent à une équipe de travail d'échanger, partager, accroître et construire de nouvelles connaissances et compétences.

A ce niveau, apparaissent la centralité de la fonction Ressources humaines et la nécessité d'introduire de nouvelles pratiques d'attraction, de fidélisation et de développement des ressources clés.

La stratégie de GRH devrait tenir compte la pluridisciplinarité de l'activité d'une ERI qui implique des compétences spécifiques et des prérequis à prendre en considération lors de la définition des critères de recrutement et/ou des programmes de **formation**.

Dans ce cadre, les membres de l'ERI devraient savoir faire preuve de vigilance, d'ingéniosité, posséder une grande intelligence des situations mais aussi avoir les savoirs suivants :

- la **gestion du temps**, le sien, celui du collectif,
- la gestion de l'**urgence**, (juste à temps, ruptures...)
- la gestion des connaissances
- le travail en équipe, en réseau, avec les TIC....

6.3.2.3 La génération des connaissances à partir des constructions des scénarios d'attaques

L'activité de réponse aux agressions numériques est génératrice de connaissances au sein de l'entreprise. Ces connaissances émergent des constructions des scénarios d'attaques et sont susceptibles de réduire la complexité du raisonnement, assister la médiation et aider à la convergence des points de vue formulés par les membres de l'ERI. Les connaissances mémorisées peuvent également être utiles lors de constructions ultérieures de scénarios d'attaques.

Pour l'implémentation de la méthode, les experts interviewés ont signalé la nécessité de démarrer avec une **base de connaissances initiale** pour leur fournir une assistance dans leur travail. Cette demande est une condition nécessaire à la réplique sur d'autres cas d'agressions numériques et dans d'autres entreprises. Elle peut être ajoutée à la liste des conditions de réplique de la méthode que nous avons déjà proposée au niveau du cinquième chapitre.

Nous croyons pouvoir dire que, dans le domaine de la lutte contre les agressions numériques, une base de connaissances déjà constituée dans une organisation, est relativement facilement transportable/applicable dans une autre organisation (qui serait également concernée par le risque numérique). Cette relative facilité de transfert ouvre des portes d'espérance pour la diffusion de la méthode **MARRAN** que nous proposons.

6.3.2.4 La formation des médiateurs

Les résultats empiriques de la recherche ont montré que le rôle du médiateur est essentiel, même sans méthodologie appropriée de travail. L'efficacité de son rôle nécessite l'usage de méthodes (heuristiques) et d'outils appropriés ainsi qu'une compétence et une expertise spécifiques. La compétence du médiateur devrait présenter **plusieurs facettes** jugées indispensables par les experts interviewés : facette technique, mais aussi pédagogique, relationnelle, de gestion. Ceci pose le problème de la formation appropriée à donner au médiateur pour qu'il remplisse son rôle convenablement afin de réduire le temps de réponse face aux agressions numériques et par conséquent limiter les pertes occasionnées par celles-ci.

De plus, le caractère variable et « inventif » des agressions numériques impose une mise à jour ou une réadaptation des programmes de formation et des connaissances susceptibles d'être enseignées à de futurs médiateurs novices. Une telle formation reste totalement à imaginer ou concevoir.

6.3.2.5 Apports pratiques de l'usage de la technologie Internet

La mise en application de la méthode à travers l'assistance active qu'a pu fournir l'utilisation de certaines potentialités techniques de l'Internet, avec un prolongement jusqu'au stade de prototype en vue de validation sur le terrain, a répondu selon les experts interviewés à deux principales contraintes relatives au contexte de réponse aux agressions numériques.

a) La première contrainte est liée à la nécessité de garder des traces des raisonnements effectués lors des constructions de scénarios d'attaques. La mémorisation des raisonnements est jugée nécessaire par les experts afin d'assister le processus de création collective de sens mais aussi pour limiter l'impact de la mobilité importante des ingénieurs dans le domaine des réseaux de télécommunication. Ceci pourrait justifier la construction d'une base de connaissances qui ont émergé d'une démarche heuristiques.

Dans ce cadre, l'outil informatique réalisé se base sur des mécanismes de structuration des mémoires en base de données et base de connaissances ainsi que sur des mécanismes de

gestion des mémoires pour enregistrer les enrichissements et réaliser des recherches de type exact et/ou approché en fonction des besoins des utilisateurs.

b) La deuxième contrainte signalée par les experts contactés est relative à la pression du temps qui est une variable considérable dans le domaine de réponse aux agressions numériques de telle sorte qu'un médium qui avantage la rapidité de communication pourra être le plus préféré et le plus approprié. Dans le domaine de la réponse aux agressions numériques, ceci peut nuancer la théorie de la richesse des médias « *media richness* » (Daft et Lengel, 1986 ; 1988) qui privilégie le face à face pour échanger ou traiter des informations riches en contexte.

L'outil informatique qui assiste la méthode MARRAN proposée offre des possibilités d'interactions à distance entre les membres de l'ERI afin de pallier à la contrainte liée à la pression du temps. Le médiateur peut dialoguer à **distance** avec les membres de l'ERI et intégrer des informations ou des éléments de raisonnement formulés par ceux-ci.

Conclusion Chapitre 6

Nous avons présenté dans ce chapitre les résultats de la recherche suite au traitement des données recueillies lors des entretiens semi directifs auprès des experts en sécurité informatique tout en justifiant le choix de cette méthode de collecte des données.

Les données recueillies ont concerné l'utilité perçue de la MARRAN, sa facilité perçue d'utilisation, les améliorations possibles apportées par celle-ci par rapport à l'état des pratiques dans le domaine de réponse aux agressions numériques, ainsi que la pertinence des critères de mesure quantitatifs nécessitant un historique suffisamment long après implémentation de la MARRAN.

Les résultats empiriques ont montré que les différentes étapes de la MARRAN sont perçues utiles permettant la construction significative des scénarios d'attaques en assistant le raisonnement. La médiation est considérée comme étant une activité nécessaire pour assister le travail d'une ERI mais qui requiert une formation appropriée. La constitution des bases de données et de connaissances est considérée par l'ensemble des experts comme étant nécessaire pour assister le processus d'itération et d'affinement et pour mémoriser les raisonnements lors des constructions des scénarios d'attaques.

Cependant, la complexité du raisonnement surtout dans le cas des agressions inconnues, et l'abondance des informations liée à l'étendue du champ d'investigation rendent difficiles l'utilisation de ces étapes ainsi que l'activité de médiation. Dans ce cadre, le logiciel qui supporte la MARRAN est apprécié par l'ensemble des experts interviewés en signalant l'aide qu'il peut fournir afin d'assister le travail d'une ERI.

Par rapport à l'état des pratiques, les résultats empiriques ont indiqué que la MARRAN est adaptée aux activités et au fonctionnement d'une ERI et permet de les organiser pour plus d'efficacité et de considération comme étant une fonction nécessaire dans la structure de l'entreprise. La MARRAN est considérée, dans le domaine de réponse aux agressions numériques, comme un outil approprié pour formaliser et assister la démarche d'interprétation des signaux/signes faibles détectés.

Nous avons terminés ce chapitre par la récapitulation des contributions théoriques et pratiques de la recherche suite à l'analyse des résultats empiriques.

Conclusion de la deuxième partie

Dans la deuxième partie de ce travail, et en répondant à nos objectifs de recherche, nous avons conçu, expérimenté et évalué la MARRAN.

La conception et la construction de la MARRAN ont pris appui sur certains éléments de la méthode L.E.SCAning® ainsi que sur l'extension des liens de causalité afin d'assister le raisonnement créatif à partir d'informations de type signal et/ou signe faible. Les liens de raisonnement qui soutiennent le modèle conceptuel de la MARRAN sont probabilistes, variables en fonction du temps et incluent l'approximation dans la création de relations entre les informations et/ou les concepts manipulés. Dans le domaine de réponse aux agressions numériques, ce modèle conceptuel trouve une application appropriée à travers le travail d'une ERI et assiste l'activité de médiation dans le but de conduire, de converger et d'affiner le raisonnement collectif.

Dans le chapitre cinq, l'expérimentation de la MARRAN sur quatre cas réels d'agression numérique a montré l'adaptation de celle-ci au travail d'une ERI et plus spécifiquement au travail du médiateur. Sur le plan de l'instrumentation de la MARRAN, nous avons présenté un logiciel se basant sur certaines potentialités de la technologie Internet.

Dans le chapitre six, les données recueillies lors des entretiens semi directifs auprès des experts en sécurité informatique concernant l'utilité perçue et la facilité perçue d'utilisation de la MARRAN soulignent des réactions plutôt positives. De même, l'implémentation de la MARRAN est susceptible d'apporter des améliorations par rapport à l'état des pratiques dans le domaine de réponse aux agressions numériques en termes d'amélioration de la gestion et de l'organisation du travail de l'ERI. Le chapitre six a tracé également les contributions théoriques de la présente recherche qui se positionnent principalement au niveau de la prise en considération des problèmes induits par l'apparition de nouveaux acteurs de l'environnement de l'entreprise et d'un nouveau type de risque suite à l'accroissement de la connectivité de celle-ci. S'agissant des contributions pratiques de la recherche, celles-ci se situent particulièrement au niveau de l'organisation du travail de l'ERI et la gestion des connaissances qui émergent de la construction des scénarios d'attaques.

Rappel de l'objet et des objectifs de la recherche

Le présent travail s'inscrit dans le cadre des travaux de recherche orientés vers la veille anticipative stratégique et plus particulièrement vers le développement d'un processus d'intelligence collective au sein de l'entreprise. Il vise à répondre à une « **problématique d'origine terrain** ».

La présente recherche s'est intéressée à la sécurité informationnelle de l'entreprise à l'égard du risque des agressions numériques. Notre intérêt a porté sur le travail de l'ERI (Equipe de Réponse aux Incidents, *Incident Response Team*) qui exige des outils et des méthodes de travail appropriés répondant à la nécessité de réduire le temps de réponse à une agression numérique et ce, dans le but, de minimiser les dégâts matériels et immatériels occasionnés par celle-ci.

Pour répondre à cette problématique de terrain, nous avons conçu la méthode MARRAN, assistée par une utilisation innovante de la technologie Internet, afin de pouvoir agir vite voire par anticipation face au risque des agressions numériques. Cette réponse s'inscrit dans le cadre d'une recherche exploratoire.

Nous avons visé la proposition de **connaissances actionnables** (au sens de Argyris) devant être utiles aux praticiens dans le domaine de réponse aux agressions numériques. Nous avons, ensuite, **validé** le fonctionnement de la MARRAN sur des cas réels d'agressions numériques. Ceci nous a amené à proposer une liste, non exhaustive, des conditions de réplication de la MARRAN sur d'autres cas d'agressions numériques et dans d'autres entreprises. Le mode d'évaluation de la MARRAN, choisi dans cette recherche, est qualitatif effectué à travers la réalisation d'entretiens semi directifs auprès des experts en sécurité informatique. Ce choix découle du positionnement épistémologique et des conditions spécifiques de cette recherche.

Les résultats de la recherche

À l'issue de notre travail, les résultats de recherche s'articulent autour des cinq points suivants :

1. la méthode proposée est assistée par l'outil informatique et est adaptée à l'activité de réponse aux agressions numériques ainsi qu'au fonctionnement de l'ERI. Cette activité est appréhendée selon un processus d'intelligence collective. Ce processus est nécessaire pour assister l'amplification progressive des informations détectées de type signal/signe faible ainsi que le raisonnement itératif à partir de ces informations.
2. la méthode proposée et assistée par l'outil informatique devrait permettre : a) l'organisation efficace de l'activité d'une ERI et b) une nette visibilité de l'activité de l'ERI dans l'entreprise. Ceci est de nature à permettre la réduction du temps de réponse face aux agressions numériques.
3. L'utilité perçue, par les experts contactés, de la **méthode** proposée et assistée par l'outil informatique, réside essentiellement : a) dans la possibilité de formaliser une partie de la démarche d'interprétation des signaux/signes faibles détectés, b) ainsi que par l'assistance qu'elle est susceptible de fournir au raisonnement collectif et itératif dans des situations d'incertitude et de complexité.
4. L'utilité perçue de l'**outil informatique** qui assiste la méthode proposée, réside dans les possibilités de garder une trace des raisonnements et de pouvoir les utiliser dans des raisonnements ultérieurs lors de construction des scénarios d'attaque. Ceci est de nature à permettre la capitalisation des connaissances spécifiques à la réponse aux agressions numériques au sein de l'entreprise.
5. l'intérêt de l'**outil informatique** qui supporte la méthode MARRAN est de faciliter, d'abord, la constitution des graphes ainsi que la manipulation des nœuds et des liens au sein des graphes représentant les points de vue des membres d'une ERI. Ensuite, il offre des possibilités importantes pour effectuer des **recherches d'informations** de type « exactes ou approchées » afin d'assister l'**amplification** progressive des signaux/signes faibles détectés et le raisonnement itératif. Enfin, il permet mémoriser

les scénarios d'attaques construits. Ces considérations sont jugées nécessaires par les experts interviewés pour assister le travail d'une ERI.

Les limites « scientifiques » et pratiques des résultats de recherche

La présente recherche est de nature **exploratoire**. L'expérimentation de la méthode MARRAN n'a concerné que quatre cas réels d'agressions numériques. Nous ne pouvons pas généraliser notre réponse à la question de recherche, en revanche nous fournissons les conditions de réplication de la MARRAN sur d'autres cas d'agressions et dans d'autres entreprises. Ainsi pouvons-nous espérer d'accroître progressivement la portée de nos résultats, conformément à la **démarche inductive** que nous avons choisi pour notre recherche.

En cas de réplication, nous ne pouvons pas affirmer que si nous refaisons la même expérimentation, dans les mêmes conditions, nous obtiendrions le même résultat car nous n'avons pas pu, à ce jour, refaire suffisamment d'expérimentations, dans les mêmes conditions. Mais, rien ne permet non plus d'affirmer le contraire ce qui demande à être testée par des recherches ultérieures.

Ce qu'il faut signaler, c'est que le résultat de l'expérimentation de la MARRAN, refaite dans les mêmes conditions est intimement lié :

- au niveau du savoir et d'expertise des membres de l'ERI,
- à l'existence et au contenu des bases de données et de connaissances locales,
- au niveau d'évolution de la complexité des attaques et des techniques de réponse,
- au savoir faire du médiateur,
- à la nature aléatoire du processus d'intelligence collective.

Pour toutes ces raisons il ne semble pas concevable de vouloir généraliser immédiatement les résultats empiriques de notre recherche.

Par ailleurs, le sujet de recherche (veille anticipative stratégique pour réduire le risque lié aux agressions numériques) a des **limites floues**, difficiles à fixer une fois pour toutes.

Ainsi nous avons trouvé des difficultés à recenser les publications académiques pertinentes, compte tenu du fait que peu d'auteurs traitant notre sujet ont été identifiés. Le recensement a été également difficile à réaliser à cause de la dispersion des articles dans des revues mal connues ou inconnues de nous relevant parfois de domaines étrangers au champ disciplinaire d'un doctorant en sciences de gestion.

Les perspectives de recherche

Les perspectives de recherche peuvent être situées sur un double plan : technique et de management. Nous sommes en sciences de gestion et la technique n'est pas l'essentiel. Cependant, dans le cas considéré, sans le passage par la technique, le sujet n'aurait pas pu être étudié, ni donner lieu à validation. C'est précisément pour cette justification que nous nous sommes placé dans le mode « **recherche ingénierique de gestion** ».

Sur le plan technique, la représentation et la manipulation des graphes sont des tâches nouvelles et complexes pour les ERI. De plus, le contexte de réponse aux agressions numériques est caractérisé par la complexité du raisonnement ainsi que par la complexité de la convergence des points de vue des membres de l'ERI. Ces considérations rendent nécessaire la gestion des sémantiques qui prennent leur signification dans l'activité et le contexte de l'entreprise et utiliser des heuristiques pour la convergence du raisonnement.

Ainsi, il serait opportun d'intégrer dans les étapes d'élaboration du logiciel qui assiste la MARRAN :

- Le développement d'une structure adaptée et d'une gestion efficace des bases de données et de connaissances parce que les concepts et les liens utilisés pour la création collective de sens sont complexes, intègrent des objets à sémantique variable, et évoluent avec le raisonnement. Il serait utile de structurer et de gérer le **contenu des concepts** d'une manière hiérarchique où le raisonnement s'opère par niveau ainsi que d'uniformiser le langage employé pour la description des concepts et des liens. Cette uniformisation devrait permettre la réplique de la méthode sur d'autres cas d'agression et dans d'autres entreprises dans le domaine de la réponse aux agressions numériques. Il serait également nécessaire de définir et d'utiliser des requêtes

appropriées pour la recherche et l'extraction de l'information contenue dans les bases de données et de connaissances.

- Le développement d'une base de données et de connaissances, orientée **heuristiques**, capable d'être intégrée dans le travail d'une ERI comme étant une base de connaissances initiales. Cette base devrait être accompagnée, également, d'un langage uniforme de description des concepts et des liens.
- Le développement d'un module ou d'un programme de **formation**, des membres de l'ERI, incluant l'apprentissage de l'outil, de la méthode et la formation aux techniques de construction des points de vue, de conciliation et d'aide à la décision à travers des études de cas.
- La mise en place d'un module de **suit** des critères d'évaluation quantitative et **dans le temps**. Ce module devrait permettre l'historisation et la gestion des critères de mesure en utilisant des interfaces graphiques et un dialogue avec l'outil informatique développé pour supporter la méthode.

Sur le plan de management, il serait intéressant de regarder du côté des **heuristiques spécifiques à la réponse aux agressions numériques** permettant la convergence des raisonnements, la construction des vues alternatives et l'assistance de l'activité du médiateur.

Par ailleurs, il serait intéressant d'élaborer un modèle pour l'**étude d'impact**, des activités de réponse aux agressions numériques à travers le travail d'une ERI, sur le recrutement et la formation des personnes appelées à faire partie de l'ERI, y compris le médiateur.

BIBLIOGRAPHIE

- Aaker, D. (1983), "Organizing a strategic information scanning system", *California Management Review*, Vol. XXV, n° 2, January, pp.76-83.
- Ab Hamid N-R et Kassim N. (2004): "Internet Technology as a tool in Customer Relationship Management", *Journal of American Academy of Business*, March, Vol. 4, pp.103-108.
- Aguilar, F. J. (1967), *Scanning the business environment*, New York, Macmillan, 239p.
- Ahituv, N. ; Zif, J. et Machlin, I. (1998), "Eenvironmental scanning and information systems in relation to success in introducing new products ", *Information and Management*, Vol. 33 (4), pp.201-211.
- Alberts C., Dorofee A. (2003), *Managing Information Security Risks: the OCTAVESM Approach*, CMU/SEI, 471 p.
- Allard-Poesi F., Drucker-Godard C. et Ehlinger S. (1999). - Analyses de représentations et de discours. -In : *Méthodes de recherche en management*. - Sous le Direction de Thiétart, R-A. – Dunod. - p. 449-475.
- Ansoff, I. (1975), "Managing strategic surprise by response to weak signals" *California Management Review*, Vol.18 (2) p.21-33.
- Argyris C. (1996) – Actionable knowledge: Intent versus actuality. *The Journal of Applied Behavioral Science*, Vol.32, Iss.4, p. 441.
- Argyris C. (1976), "Single-loop and double-loop models in research on decision making", *Administrative Science Quarterly*, Vol. 21 (3), pp.363-375.
- Arnet, D.B. ; Menon, A. et Wilcox, J.B. (2000), " Using competitive intelligence: antecedents and consequences ", *Competitive Intelligence Review*, Vol. 11(3), 16-27.
- Ashmos D.P. et Nathan M.L. (2002), "Team sense-making: a mental model for navigating uncharted territories", *Journal of Managerial Issues*, Vol. XIV, n° 2, Summer, pp.198-217.
- Atamer, T. et Calori, R. (2003), *Diagnostic et décisions stratégiques*, Dunod, 2^{ème} édition, 509p.
- Bartoli J. A. et Le Moigne J. L. (1996), *Organisation intelligente et système d'information stratégique*, Paris, Ed. Economica, 281 p.
- Baumard, P. (1991), *Stratégie et surveillance des environnements concurrentiels*, Paris, Masson, 181p.

- Baumard P, Donada C., Ibert J. et Xuereb J-M (1999). -La collecte des données et la gestion de leurs sources. -In : *Méthodes de recherche en management*. - Sous le Direction de Thiétart, R-A. – Dunod. - p. 224-256.
- Bitouzet, Ch. (1999), *Le commerce électronique : création de valeur pour l'entreprise*, Hermès, 185p.
- Blanco S., Caron M.L. et Lesca H., (2003) “ Developing capabilities to create collective intelligence within organizations”, *Journal of Competitive Intelligence and Management*, Volume 1, Number 1, Spring, pp.80-92.
- Bort J. et Cummings J., (2003) "Incident response teams gain allure", *Network World*, Oct., Vol. 20 (42), pp.8-10.
- Bourgeois, L.J. (1985), “Strategic goals, perceived environmental uncertainty, and economic performance in volatile environments”, *Academy of Management Journal*, Vol. 28 (3), pp.548-573.
- Bourgeois L. J. et Eisenhardt K. M. (1988), “Strategic decision processes in high velocity environments: four cases in the microcomputer industry”, *Management Science*, Vol. 34 (7), pp.816-835.
- Boyd, B.K. et Fulk, J. (1996), “Executive scanning and perceived uncertainty: a multidimensional model”, *Journal of Management*, Vol. 22 (1), pp1-22.
- Boyd, B; Dess, G. et Rasheed, A. (1993), “Divergence between archival and perceptual measures of the environment: causes and consequences” *Academy of Management Review*, Vol. 18, n° 2, pp.204-226.
- Boyle B. A. (2001), “The Internet in industrial channels: the use in (and effects on) exchange relationships”, *Journal of Business & Industrial Marketing*, Vol. 16, pp.452-469.
- Bradshaw D. et Brash C. (2001), “Managing customer relationships in the e-business world: how to personalize computer relationships for increased profitability”, *International Journal of Retail and Distribution Management*, Vol. 29, pp.520-529.
- Brenton C. et Hunt C. (2003): *Network Security*, SYBEX, 490p.
- Buchko, A.A. (1994), “Conceptualization and measurement of environmental uncertainty: an assessment of the Miles and Snow perceived environmental uncertainty scale”, *Academy of Management Journal*, Vol. 37 (2), pp.410-425.
- Burns, T. et Stalker, G. M. (1961), *The management of innovation*, London: Tavistock Publications.
- Canavan J. E. (2001): *Fundamentals of Network Security*, Artech House, 307p.

- Caron-Fasan M.L., *Veille stratégique : Créaion de sens à partir de signaux faibles*, Thèse de Doctorat soutenue le 11 septembre 1997, École Supérieure des Affaires, Grenoble, 428 p.
- Chaib-draa, B. (2002), "Causal maps: Theory, Implementation, and Practical Applications in Multiagent Environments", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 14, N°. 6, November/December, pp. 1-17.
- Chanal, V. ; Lesca, H. et Martinet, A-C. (1997), " Vers une ingénierie de la recherche en sciences de gestion ", *Revue Française de Gestion*, Novembre- Décembre, pp.41-53.
- Chattopadhyay P., Glick W. H. et Huber G. P. (2001), "Organizational actions in response to threats and opportunities", *Academy of Management Journal*, Vol. 44 (5), p.937-955.
- Chen H., Chau M. et Zeng D. (2002), "CI Spider: a tool for competitive intelligence on the Web", *Decision Support systems*, vol. 34, pp.1-17.
- Child, J. (1972), "Organizational structure, environment and performance- the role of strategic choice", *Sociology*, Vol. 6, pp. 1-22.
- Choo, Ch. W. (2001), The knowing organization as learning organization, *Education & Training*, Volume 43, number 4/5, pp. 197-205.
- Choo, Ch. W. (2002), *Information Management for The Intelligent Organization : the art of scanning environment*, Information Today, Inc. Medford, NJ
- Choo, Ch. W., Deltor B. et Turnbull D. (2000), *Web Work: information seeking and knowledge work on the World Wide Web*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 236 p.
- Culnan, M. J. (1983), "The effects of task complexity and source accessibility on information gathering behavior", *Decision Sciences*, Vol. 14, pp.194-206.
- Cyert, R. et March, J. (1963), *A behavioral theory of firm*, Englewood Cliffs, NJ: Prentice-Hall.
- Daft, R.L. ; Sormunen, J. et Parks, D. (1988), " Chief executive scanning, environmental characteristics, and company performance : an empirical study ", *Strategic Management Journal*, Vol. 9, pp.123-139.
- Daft, R.L. et Huber G., (1987) "How Organizations Learn: a communication framework", *research in the Sociology of Organizations*, Vol. 5, p. 1-36.
- Daft, R.L. et Lengel, R. (1986), "Organization information requirements, media richness and structural design", *Management Science*, Vol. 52, N°.5, p. 554-571.
- Daft, R.L. et Weick K.E. (1984) "Toward a model of Organizations as Interpretation systems", *The Academy of Management Review*, Vol. 9, n° 2 p. 284-295.

- Daft R.L. et Macintosh N. B. (1981), A tentative exploration into the amount and equivocality of information processing in organizational work units, *Administrative Science Quarterly*, Vol. 26 (2), pp.207-224.
- Davis F. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information technology", *MIS Quarterly*, Minneapolis, September, Vol. 13 (3), pp. 319-340.
- DeLone W. H. et McLean E. R. (1992), "Information System Success: The Quest for the Dependat Variable", *Information Systems Research*, Vol. 3, March, pp.60-95.
- Doll W. et Torkzadeh G. (1988), "The measurement of end-user Computing satisfaction", *MIS Quarterly*, Minneapolis, Vol. 12 (2), June, pp. 259-274.
- Doty D. H., Glick W. H. et Huber G. P. (1993), "Fit, equifinality, and organizational effectiveness: A test of two configurational theories", *Academy of Management Journal*, Vol. 36, pp.1196-1251.
- Dowling G. R. et Staelin R. (1994), "A Model of Perceived Risk and Intended Risk-Handling Activity", *Journal of consumer Research*, vol. 21, 119-134.
- Downey, H. K. ; Hellriegel, D. et Slocum, JR. (1975), "Environmental uncertainty: the construct and its applications, *Administrative Science Quarterly*, Vol. 20 (4), p.613.
- Drazin R., Glynn M.A. et Kazanjian R.K. (1999), "Multilevel theorizing about creativity in organizations: a sensemaking perspective", *Academy of Management Review*, Vol. 24, n° 2, pp.286-307.
- Duncan, R. B. (1972), "Characteristics of organizational environments and perceived environmental uncertainty", *Administrative Science Quarterly*, Vol. 17, pp.313-327.
- Ebrahimi B. P. (2000), "Perceived Strategic Uncertainty and Environmental Scanning Behavior of Hong Kong Chinese Executives", *Journal of Business Research* 49, pp. 67-77.
- El Sawy, O. A. (1985), "Personal information systems for strategic scanning in turbulent environments: can the CEO go on-line?" *MIS Quarterly*, vol.9, n° 1, pp.53-60.
- El Sawy O. A. et Pauchant T. C. (1988), "Triggers, templates and twitches inn tracking of emerging strategic issues", *Strategic Management Journal*, Vol.9, pp. 455-473.
- Elenkov, D. (1997), "Strategic uncertainty and environmental scanning: the case for institutional influences on scanning behavior", *Strategic Management Journal*, Vol. 18 (4), pp.287-302.
- EMERY, F. TRIST, E.L. (1965) – The causal texture of organisational environments. *Human Relations*, n°18, pp.21-32.
- Feldman, M.S. et March, J. G. (1981), " Information in organizations as signal and symbol ", *Administrative Science Quarterly*, vol. 26 (2), pp.171-186.

- Fiol C.M. et Huff A. S. (1992), "Maps for managers: where are we? Where do we go from here?", *Journal of Management studies*, Vol. 29 (3), May, pp.267-285.
- Fisher, C. (1996), "The impact of perceived environmental uncertainty and individual differences on management information requirements: a research note", *Accounting, Organizations and Society*, Vol. 21, n°4.
- Fontenot N.A. (1993), "Effects of training in creativity and creative problem finding upon business people", *Journal of Psychology*, vol.133, p.11.
- Ford J. et Baucus D. (1987), "Organizational adaptation to performance downturns: An interpretation-based perspective", *Academy of Management Review*, Vol. 12, pp.366-380.
- Frishammer J. (2002), "Characteristics in information processing approaches", *International Journal of Information Management*, Vol. 22, p.143-156.
- Galaskiewicz J. et Bielefeld W. (1998), *Nonprofit organizations in an age of uncertainty: A study of organizational change*, Hawthorne, NY: Aldine de Gruyter.
- Ganesh U., Miree C.E. et Prescott J. (2003), "Competitive intelligence field research: moving the field forward by setting a research agenda", *Journal of Competitive Intelligence and Management*, Vol. 1, n° 1, Spring, pp.1-12.
- Gavetti G. et Levinthal D. (2000), "Looking forward and looking backward: cognitive and experiential search", *Administrative Science Quarterly*, vol. 45, pp. 113-137.
- Ghoshal, S. et Westney, D. E. (1991), "Organizing competitor analysis systems", *Strategic Management Journal*, Vol. 12 (1), pp.17-31.
- Gibbons, P. T. et Prescott, J. E. (1996), "Parallel competitive intelligence processes in organizations ", *Int. J. Technology Management*, Vol. 11, pp.162-178.
- Gifford W. E., Bobbitt H. R. et Slocum J. W. (1979), "Message Characteristics and Perceptions of Uncertainty by Organizational Decision Makers", *Academy of Management Journal*, Vol. 22 (3), pp.458-481.
- Gilad B. (1996), *Business blindspots* (2nd ed.), Calne: Infotronics Ltd.
- Gilad T. et Gilad B. (1986), "Business intelligence: the quiet revolution", *Sloan Management Review*, Vol. 27, n° 4, pp. 53-61.
- Ginzberg M. J. (1980), "An organizational contingencies view of accounting and information systems implementation", *Accounting, Organizations and Society*, Vol. 5 (4), p.369-382.
- Ginzberg A. (1988), "Measuring and modelling changes in strategy: Theoretical foundations and empirical directions", *Strategic Management Journal*, Vol. 9, pp.559-576.

- Gorry A. et Scott-Morton M. S. (1971), "A framework for management information systems", *Sloan Management Review*, Vol. 13, n° 1, pp. 55-70.
- Grandon E. et Pearson J. (2003) : "Strategic Value and Adoption of Electronic Commerce : An empirical Study of Chilean Small and Medium Business", *Journal of Global Information Technology Management*, Vol. 6 (3), pp.22-43.
- Greenberg, J. (2003), "The semantic Web: more than a vision", *Bulletin of the American Society for Information Science and Technology*, May/April, Vol. 29 (4), pp. 6-7.
- Grewal D., Gotlieb J. et Marmonstein H. (1994), "The Moderating Effects of Message Framing and Source Credibility on the Price-Perceived Risk Relationship", *Journal of Consumer Research*, vol. 21, 145-153.
- Hambrick, D. (1981), Specialization of environmental scanning activities among upper level executives, *Journal of Management Studies*, Vol. 18, pp.299-320.
- Hambrick D. et Mason P.A. (1984), Upper echelons : The organization as a reflection of its top managers, *Academy of Management Review*, Vol. 9, pp. 193-206.
- Hamdi M., Boudriga N. et Krichène J. (2003), "Netram: A Novel Method for Network Security Risk Management", Nordic Workshop on Security IT Systems, 11p.
- Hassler V. (2001): Security fundamentals for e-commerce, Artech House, 409p.
- Hervier G. (2001) : *Le commerce électronique*, Editions d'Organisations, 276p.
- Hofbauer T. H., Woo C. C. et Martens C. D. (1994), "Decision support through facilitating the exchange of experiences in a distributed environment", *International Journal of Intelligent and Cooperative Information Systems*, Vol. 3 (3), pp.255-278.
- Huber, G. P. (1990), "A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making", *Academy of Management Review*, Vol. 15 (1), pp.47-71.
- Huber G. P. et Daft R. L. (1987), *The information environments of organizations*, Handbook of organizational communication: an interdisciplinary perspective, publié sous la direction de F.M. Jablin, L.L. Putnam, K.H. Roberts, et L.W. Porter, Sage Publications, Beverly Hills, pp.130-164.
- Huff S.A. (1990), *Mapping strategic thought*, Ed. John Wiley and Sons, 426p.
- Jacoby et al., (1994), "Tracing the impact of Item-by-item Information Assessing on Uncertainty Reduction", *Journal of Consumer Research*, vol. 21, pp.291-303.
- Jain, S. C. (1984), "Environmental scanning in U.S. corporations ", *Long Range Planning*, Vol. 17 (2), pp.117-128.

- Jauch, L. R. et Kraft, K. L. (1986), “ Strategic management of uncertainty ”, *Academy of Management Review*, Vol. 11 (4), pp.777-790.
- Jennings, D. F. et Lumpkin, J. R. (1992), “Insights between environmental scanning activities and Porter’generic strategies : an empirical analysis ”, *Journal of Management*, Vol. 18 (4), pp.791-803.
- Joffre P. et Koenig G. (1985), *Stratégie d’entreprise : antimanuel*, Ed. Economica, 247 p.
- Kefalas A. G. (1980), “Defining the external business environment”, *Human Systems Management*, Vol. 1, pp.253-260.
- Killcrece G., Kossakowski K-P., Ruefle R. et Zajicek M. (2003), *State of the Practice of Computer Security Incidents Response Teams (CSIRTs)*, Carnegie Mellon, 153p.
- Koenig, G. (1990), *Management stratégique : vision, manœuvres et tactiques*, Paris, Nathan, 399p.
- Koenig, G. (1996), *Management stratégique, paradoxes, interactions et apprentissages*, Ed. Nathan, 544 p.
- Kohberg C. (1987), “Resource scarcity, environmental uncertainty and adaptive organizational behaviour”, *Academy of Management Journal*, Vol. 30 (4), pp.798-807.
- Lackman, C. L. ; Saban, K. et Lanasa, J. M. (2000), “ Organizing the competitive intelligence function : a benchmarking study ”, *Competitive Intelligence Review*, Vol. 11 (1), pp.17-27.
- Lawrence, D. et Lorsch, J. (1967), *Organization and environment*, Harvard University Press, Boston, MA, 279p.
- Le Moigne J. L. (1979), « Informer la décision ou décider de l’information », *Economie et Société*, Cahiers de l’ISMEA, Série SG, n° 1, pp. 889-918.
- Lesca H. et Blanco S. (2002), Contribution à la capacité d’anticipation des entreprises par la sensibilisation aux signaux faibles, Actes du VIème congrès international francophone sur la PME, 30 octobre – 1^{er} novembre, Montréal, 19p.
- Lesca, H. (1986), *Système d’information pour le management stratégique de l’entreprise*, McGraw-Hill, 146p.
- Lesca, H. (1989), *Information et adaptation de l’entreprise*, Masson, Institut de l’Entreprise, 223 p.
- Lesca, H. et Caron, M-L. (1995), “ Veille stratégique : créer une intelligence collective au sein de l’entreprise ”, *Revue Française de Gestion*, Sep-Oct, pp.58-68.
- Lesca, H. et Schuler, M. (1998), “Veille stratégique : Comment ne pas être noyé sous les informations”, *Economies et Sociétés*, Série Sciences de Gestion, n°2, pp. 159-177.

- Lesca, H. (1994), “ Veille stratégique pour le management stratégique, état de la question et axes de recherche ”, *Economies et Sociétés*, Série Sciences de Gestion, n°20, Vol. 5, pp 31-50.
- Lesca, H. (2001), “Veille stratégique orientée signaux faibles : concept et méthode d’identification, retours d’expérience”, *Actes du Colloque VSST’2001*, octobre, Barcelone, 20p.
- Lesca H. (2003) – Veille stratégique La méthode L.E.SCAning. Ed. ems Management et société, 190 p.
- Lesca N. (2002), Construction du sens à priori, construction du sens à posteriori : pourquoi ne peut-on pas savoir que les avions arrivent tant que les tours ne se sont effondrées ?, *Actes de la XIème conférence de l’AIMS*, 5-8 juin, Paris, 25p.
- Lesca N. (2002), « Construction du sens : le cas de la veille stratégique et l’exploitation des signes d’alerte précoce », Thèse de doctorat, ESA, Grenoble, 492p.
- Llorens C. et Levier L. (2003) : Tableaux de bord de la sécurité réseau, Eyrolles, 340p.
- Lozada H. R. et Calantone R. J. (1996), “Scanning behaviour and environmental variation in the formulation of strategic responses to change”, *The Journal of Business & Industrial Marketing*, Vol. 11 (1), pp.17-41.
- March G. J. et Feldman M. (1981), “Information in organizations as signal and symbol”, *Administrative Science Quarterly*, Vol. 26, p. 171-186.
- Marmuse C. (1992), *Politique Générale : langages, intelligence, méthode et choix stratégiques*, Ed. Economica, 592 p.
- Martinet A. C. et Petit G. (1982), *L’entreprise dans un monde en changement*, Seuil, 150 p.
- Martinet A. C. (1983), *Stratégie*, Ed. Vuibert Gestion, 322 p.
- Masseti, B. (1996), “An empirical examination of the value of creativity systems on idea generation”, *MIS Quarterly*, Vol. 20 (1), March, pp. 83-97.
- Matthews, C.H. et Scott, S. (1995), “Uncertainty and planning in small and entrepreneurial firms: an empirical assessment”, *Journal of Small Business Management*, octobre, pp 31-52.
- May, R. C.; Stewart, JR. et Sweo, R. (2000), “Environmental scanning behavior in a transitional economy : evidence from Russia”, *Academy of Management Journal*, Vol. 43 (3), pp.403-427.
- McLain D. L. et Hackman K., (1999) “Trust, risk and decision-making in organizational change”, *Public Administration Quarterly*, Summer, Vol. 23 (2), pp.152-176.
- Miles, R. E. et Snow, C. C. (1978), *Organizational strategy, structure, and processes*, McGraw-Hill.

- Miles, R.E.; Snow, CH. et Pfeffer, J. (1974), "Organization-environment: concepts and issues", *Industrial Relations*, Vol.13, pp. 244-264.
- Miller, D. (1988), "Relating Porter's business strategies to environment and structure: analysis and performance implications", *Academy of Management Journal*, Vol. 31, n° 2, pp 280-308.
- Miller, K. (1993), "Industry and country effects on managers' perceptions of environmental uncertainties" *Journal of International Business Studies*, Fourth Quarter, pp 693-714.
- Milliken, F. J. (1987), "Three types of perceived uncertainty about the environment : state, effect, and response uncertainty ", *Academy of Management Review*, vol. 12 (1), pp.133-143.
- Milliken, F.J. (1990), "Perceiving and interpreting environmental change: an examination of college administrators' interpretation of changing demographics", *Academy of Management Journal*, Vol. 33 (1), pp.42-63.
- Montagnon J-A. (2001) : Les réseaux d'entreprise aujourd'hui, Dunod, Paris, 360 p.
- Moore A. P., Ellison R. J. et Linger R. C. (2001), *Attack Modeling for Information Security and Survivability*, Technical Note CMU/SEI, 33p.
- Narchal, R.M. ; Kittappa, K. et Bhattacharya, P. (1987), "An environmental scanning system for business planning ", *Long Range Planning*, Vol. 20 (6), p. 96-105.
- Nonaka, I. (1994), "A dynamic theory of organizational knowledge creation", *Organization Science*, Vol. 5 (1), pp. 14-37.
- Nonaka I. et Takeuchi H. (1995), *The Knowledge Creating Company*, Oxford University Press, New-York.
- O'Reilly, C. A. (1982), "Variations in decision makers' use of information sources : the impact of quality and accessibility of information ", *Academy of Management Journal*, Vol. 25 (4), pp.756-771.
- Palmer T. B. et Wiseman R. M., (1999) "Decoupling risk taking from income stream uncertainty: a holistic model of risk", *strategic Management Journal*, Vol. 20 (11), pp.1037-1062.
- Pawar, B. S. et Sharda, R. (1997), "Obtaining business intelligence on the Internet ", *Long Range Planning*, Vol. 30 (1), pp.110-121.
- Perrouty J-P et D'Hauteville F. (2000), « A la recherche d'un lien entre risque, incertitude et qualité perçus dans les choix alimentaires : pour une approche conventionnaliste », *Iers Ateliers de Recherche sur le Risque en Marketing*, 10-26.
- Petit B., (2002) : Architecture des réseaux, Ellipses Édition, 211p.

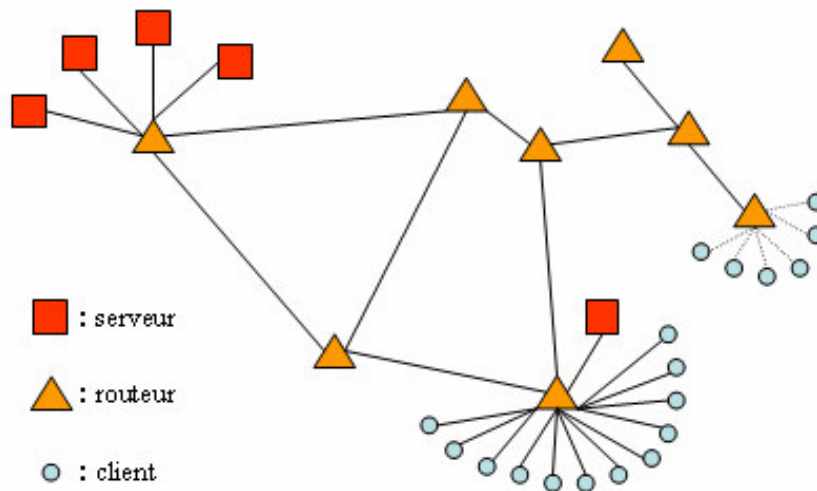
- Pole, J.G.; Madsen, E. et Dishman, P. (2000), “ Competitive intelligence as a construct for organizational change ”, *Competitive Intelligence Review*, vol. 11(4), pp. 25-31.
- Porter, M. (1982), *Choix stratégiques et concurrence*, Economica, Paris, 426p.
- Porter, M. (1986), *L'avantage concurrentiel*, InterEditions, Paris, 647p.
- Prahalad C.K. et Hamel G. (1990), “The core competence of the corporation”, *Harvard Business Review*, May-June, Vol. 68 (3), p. 79-92.
- Prax, J.Y. (1997), *Manager la connaissance dans l'entreprise*, INSEP éditions, 270 p.
- Priem R. L., Rasheed A. M. & Kotulic A. G., (1995), “Rationality in strategic decision processes, environmental dynamism and performance”, *Journal of Management*, vol.21, pp.913-929.
- Reix, R. (1999), “ Les technologies de l'information, facteur de flexibilité ?”, *Revue Française de Gestion*, Mars-Avril-Mai, pp.111-119.
- Revelli, C. (1998), *Intelligence stratégique sur Internet*, Dunod, 212 p.
- Rouibah K. (1998)- Veille stratégique : vers un outil d'aide au traitement des informations fragmentaires et incertaines. Université Pierre Mondès France, Grenoble 2, CERAG, ESA.,
- Rubin H. J. et Rubin I. S. (1995), *Qualitative Interviewing, The Art of Hearing Data*, Thousand Oaks, CA, Sage.
- Sadok M. Benabdallah S. et Lesca H. (2003), « Apports Différentiels de l'Internet pour la Veille Anticipative : Application au cas de réponse aux Atteintes à la Sécurité des Réseaux d'entreprise », *Actes du 8^{ième} Colloque de l'AIM*, MAI, Grenoble, 8 p.
- Sawyer O. O., Ebrahimi B. P. & Thibodeaux M. S. (2000), “Executive Environmental Scanning, Information Source Utilisation, and Firm Performance: the case of Nigeria”, *Journal of Applied Management Studies*, Vol. 9, N°. 1, pp. 95-115.
- Seddon P. et Kiew M. (1994), “A partial test and development of the DeLone and McLean model of success”, *Proceedings of the 15th International Conference of Information Systems*, December, 14-17, Vancouver, Canada, pp. 99-110.
- Simon, H. A. (1991), “Bounded rationality and organizational learning”, *Organization science*, Vol. 2, n° 1, pp. 125-134.
- Sitkin S. B. et Weingart L. R. (1995), “Determinants of Risky Decision-Making Behavior: a Test of the Mediating Role of Risk Perceptions and Propensity”, *Academy of Management Journal*, Vol. 36(6), 1573-1592.
- Smith A. D. et Rupp W. T. (2002) “Issues in cybersecurity: understanding the potential risks associated with hackers/crackers”, *Information Management & Computer Security*, Vol. 10 (4), pp.178-183.

- Stallings W. (2000), *Network Security Essentials: Applications and Standards*, Prentice Hall, 366 p.
- Stoffels J. D. (1982), "Environmental scanning for future success", *managerial planning*, Vol. 3 (3), pp.4-12.
- Subramanian, R.; Fernandes, N. et Harper, E. (1993), "An empirical examination of the relationship between strategy and scanning", *The Mid-Atlantic Journal of Business*, Vol. 29 (3), December, pp. 315-330.
- Subramanian, R.; Fernandes, N. et Harper, E. (1993), "Environmental scanning in U.S. companies: their nature and their relationship to performance", *Management International Review*, vol. 33 (3), pp. 271-286.
- Teo, T.S.H. (2000), "Using the Internet for competitive intelligence in Singapore", *Competitive Intelligence Review*, Vol. 11(2), p. 61-70.
- Teo, T.S.H. et Choo, W. Y. (2001), "Assessing the impact of using Internet for competitive intelligence", *Information Management*, Vol. 39, p. 67-83.
- Thiéart, R-A. (1991), *La stratégie d'entreprise*, McGraw-Hill, 247p.
- Thiéart, R-A. (1984), *La stratégie d'entreprise*, McGraw-Hill, 185p.
- Thomas, J.B.; Clark, S.M. et Gioia, D.A. (1993), "Strategic sensemaking and organizational performance linkages among scanning, interpretation, action, and outcomes", *Academy of Management Journal*, Vol. 36, n° 2, pp. 239-270.
- Thompson, J. D. (1967), *Organizations in action: social science bases of administrative theory*, McGraw-Hill.
- Tosi, H. ; Aldag, R. et Storey, R. G. (1973), "On the measurement of the environment: an assessment of the Lawrence et Lorsch environmental uncertainty scale", *Administrative Science Quarterly*, Vol. 18, pp. 27-36.
- Tung, R. L. (1979), "Dimensions of organizational environments: an exploratory study of their impact on organization structure", *Academy of Management Journal*, Vol. 22, pp. 672-693.
- Valette F. (1993), "Le concept de puzzle: Coeur du processus d'écoute prospective de l'environnement de l'entreprise", Thèse en Sciences de Gestion, Grenoble II: ESA, 378 p.
- Vermeulen C. et Solms R. V., (2002), "The information security management toolbox-taking the pain out of security management", *Information Management & Computer Security*, Vol. 10 (3), pp.119-125.

- Volle P. (1995), « Le concept de risque perçu en psychologie du consommateur : antécédents et statut théorique », *Recherche et Applications Marketing*, Vol. 10(1), 39-56.
- Weber C.E. (1984), Strategic Thinking-Dealing with Uncertainty, *Long Range Planning*, Vol. 17 (5), pp.60-70.
- Weick, K.E. (1995), *Sensemaking in Organizations*, London: Sage Publications, 231p.
- West-Brown M. J., Stikvoort D., Kossakowski K-P, Killcrece G., Ruefle R. et Zajicek M. (2003), *Handbook for Computer Security Response Teams (CSIRTs)*, Carnegie Mellon, 200p.
- White D., (1995), “Application of systems thinking to risk management: a review of the literature”, *Management Decision*, Vol. 33(10), 35-45.
- Wierenga B. et Bruggen G. H. (1998), “The dependent variable in research into the effects of creativity support systems: quality and quantity of ideas”, *MIS Quarterly*, March, pp.81-87.
- Williamson, O.E. (1991), Comparative Economic Organization : The Analysis of Discrete Structural Alternatives, *Administrative Science Quarterly* 36 : 269-296.
- Wholey D. R. et Brittain J. (1989), “Characterizing environmental variation”, *Academy of Management Journal*, Vol. 22 (4), pp. 867-882.
- Wood C. M. et Sheer L. K. (1996), “Incorporating perceived risk into models of consumer deal assessment and purchase intent”, *Advances in Consumer Research*, vol. 23, 399-404.
- Woodcock J. (1999) : Les réseaux Notions de base, Microsoft Press, 345p.
- Yasai-Ardekani, M. et Nystrom, P. C. (1996), “Designs for environmental scanning systems : tests of a contingency theory ”, *Management Science*, Vol. 42 (2), p. 187-204.

GLOSSAIRE

Réseau client/serveur : groupe d'ordinateurs et autres périphériques, tels que des imprimantes et des scanners, connectés entre eux par une liaison de communication permettant à tous les périphériques d'interagir entre eux. Les réseaux peuvent être de grande ou de petite taille, connectés durablement par des câbles, ou temporairement par des lignes téléphoniques ou des transmissions sans fils. Le plus grand réseau est l'Internet, qui est un groupement de réseaux du monde entier.



Représentation schématique d'un réseau client/serveur

Réseau local (LAN, Local Area Network) : réseau de communication permettant de connecter des ordinateurs, des imprimantes et d'autres périphériques situés dans une zone limitée (par exemple, dans un immeuble). N'importe quel périphérique connecté peut communiquer avec tous les autres périphériques du réseau local.

Réseau étendu (WAN, Wide Area Network) : réseau de communication permettant de relier des ordinateurs, imprimantes ou autres périphériques éloignés géographiquement. N'importe quel périphérique connecté peut communiquer avec tous les autres périphériques du réseau étendu.

Intranet : réseau d'entreprise qui utilise des protocoles et des technologies Internet, mais qui est accessible uniquement à certaines personnes, par exemple aux employés d'une société. Un intranet est également appelé réseau privé.

Extranet : réseau informatique à caractère commercial, constitué des intranets de plusieurs entreprises qui communiquent entre elles, à travers le réseau Internet, au moyen d'un serveur Web sécurisé. Par extension, désigne plus généralement les sites à accès sécurisé permettant à une entreprise de n'autoriser sa consultation qu'à certaines catégories d'intervenants externes, ses clients ou ses fournisseurs en général.

Réseau VPN (*Virtual Private Network*) : réseau étendu privé établi en créant des liaisons spécialisées entre réseaux d'entreprises à travers des réseaux publics afin de répondre aux besoins en partage des ressources de ses utilisateurs.

Réseau Wi-Fi (*Wireless Fidelity*) : réseau local de type Ethernet (protocole de communication sur réseau local) à accès sans fil permettant d'obtenir des débits pouvant atteindre 2 mégabits par seconde. Le logo Wi-Fi, défini par WECA (Wireless Ethernet Compatibility Association), indique que le matériel sur lequel il est apposé respecte la norme 802.11b de l'IEEE (Association d'ingénieurs américains) pour la communication sans fil et dans le but d'unifier toutes les technologies existantes.

Serveur : Un ordinateur qui fournit des ressources partagées aux utilisateurs réseau.

Serveur Web : Ordinateur géré par un administrateur système ou un fournisseur de services Internet et qui répond aux requêtes du navigateur d'un utilisateur.

SQL (*Structured Query Language*) : langage d'interrogation et de manipulation de bases de données relationnelles. Il permet de décrire le schéma conceptuel de la base, de construire des requêtes ou questions concernant le contenu de la base et de gérer la structure et le contenu grâce à des demandes de création, de mise à jour, de suppression.

Routeur : matériel qui participe à l'interopérabilité et à la connectivité des réseaux locaux et des réseaux étendus. Les routeurs font correspondre les en-têtes de paquets à un segment du réseau local et choisissent le meilleur chemin à emprunter pour le paquet, ce qui optimise les performances du réseau.

Client : ordinateur ou programme qui se connecte à un autre ordinateur ou programme, ou qui sollicite des services de celui-ci. Le client peut aussi être le logiciel qui permet à l'ordinateur ou au programme d'établir la connexion.

Modem (Modulateur/Démodulateur) : périphérique qui permet de transmettre des informations d'un ordinateur à l'autre via une ligne téléphonique. Le modem émetteur transforme les données informatiques numériques en signaux analogiques pouvant être acheminés par une ligne téléphonique. Le modem récepteur transforme les signaux analogiques en signaux numériques.

Commutateur (Switch): C'est un élément actif du réseau permettant d'analyser les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguillées sur les ports adéquats.

TCP/IP (Transmission Control Protocol/Internet Protocol) : ensemble de protocoles réseau largement utilisés sur Internet qui assurent les communications entre des réseaux interconnectés d'ordinateurs possédant des architectures matérielles et des systèmes d'exploitation différents. TCP/IP comprend des normes qui régissent la manière dont les ordinateurs communiquent ainsi que des conventions relatives à la connexion des réseaux et au routage du trafic.

Pare-feu (Firewall) : dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public.

Cryptage/Chiffrement : opération par laquelle un message en clair est transformé en un message codé inintelligible pour tout intercepteur qui ne dispose pas du code. Appelée également chiffrement, cette technique s'appuie sur un jeu de clés pour permettre cryptage et

décryptage d'informations. Sur le Net, elle est notamment utilisée pour protéger les *e-mails*, les données relatives aux transactions bancaires et les informations d'entreprise.

Détecteur d'intrusions (IDS, Intrusion Detection System) : système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne ou sur un seul ordinateur hôte, de neutraliser ces attaques réseaux ou systèmes et d'assurer ainsi la sécurité du réseau. Deux méthodes sont principalement utilisées par les systèmes de détection d'intrusions : la reconnaissance de signatures et la détection d'anomalies. La reconnaissance de signatures est une approche consistant à rechercher dans l'activité de l'élément surveillé les signatures d'attaques connues. Le SDI fait appel à une bibliothèque de signatures (bases de données) et ne peut alors détecter que les attaques dont il possède la signature. La détection d'anomalies utilise l'analyse de statistiques du système et le SDI signalera les divergences par rapport au fonctionnement normal (ou de référence) des éléments surveillés.

Ver : type de virus particulier. Le ver est un programme qui peut se répliquer à travers les terminaux connectés à un réseau, et d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation. Actuellement, les vers se développent surtout à travers la messagerie en repérant l'ensemble des contacts d'un utilisateur et en s'envoyant à ceux-ci sous forme d'une pièce jointe.

Porte dérobée (*Backdoor*) : point d'accès confidentiel à un système d'exploitation, à un programme ou à un service en ligne. Ces passages secrets sont ménagés par les concepteurs des logiciels pour fournir des accès privilégiés pour les tests ou la maintenance. Mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.

Fichier log : fichier dans lequel sont stockés les messages générés par une application, un service ou le système d'exploitation. Ces messages permettent de suivre l'exécution des opérations. Les serveurs Web, par exemple, gèrent des fichiers journaux qui répertorient toutes les requêtes adressées au serveur. Les fichiers journaux sont généralement des fichiers en texte clair qui possèdent souvent l'extension .log.

Commande "ps" : permet de visualiser tous les processus ou toutes les tâches (Applications ou commandes) qui tournent sur une machine ainsi que d'afficher leurs états.

Telnet : les commandes Telnet permettent de communiquer avec un ordinateur distant qui utilise le protocole Telnet via une fenêtre de terminal. Le serveur Telnet fonctionne comme une passerelle par laquelle les clients Telnet communiquent entre eux.

Netstat : une commande qui affiche les connexions TCP actives, les ports sur lesquels l'ordinateur procède à l'écoute, la table de routage IP ainsi que des statistiques de divers protocoles de connexions.

```
C:\Documents and Settings\moufida>netstat -a
Connexions actives

Proto  Adresse locale          Adresse distante        Etat
TCP    isetcom:epmap           0.0.0.0:0               LISTENING
TCP    isetcom:microsoft-ds   0.0.0.0:0               LISTENING
TCP    isetcom:1025            0.0.0.0:0               LISTENING
TCP    isetcom:5000            0.0.0.0:0               LISTENING
TCP    isetcom:1027            0.0.0.0:0               LISTENING
UDP    isetcom:epmap           *:*
UDP    isetcom:microsoft-ds   *:*
UDP    isetcom:isakmp          *:*
UDP    isetcom:1026            *:*
UDP    isetcom:1028            *:*
UDP    isetcom:ntp             *:*
UDP    isetcom:1900            *:*
UDP    isetcom:60571           *:*
```

Exécution d'une commande Netstat

ANNEXE

Canevas d'entretien

Ce canevas comporte quatre parties de questions.

1^{ère} Partie :

Cette partie comporte une série de questions ayant pour objectif de mesurer l'utilité perçue de la méthode proposée.

1. est ce que l'étape de l'amplification progressive des signaux/signes faibles est utile ?
2. est ce que l'étape de la recherche complémentaire des informations est utile ?
3. est ce que l'étape du raisonnement itératif sur les liens créés entre les informations collectées est utile ?
4. est ce que les liens proposés sont suffisants et adaptés au contexte des agressions numériques ?
5. est ce que vous proposez d'autres liens afin de couvrir le raisonnement dans le contexte des agressions numériques ?
6. est ce que l'activité de médiation, dans le travail d'une ERI pour conduire le raisonnement lors de la construction du scénario de l'attaque, est utile ?
7. est ce que les étapes de la méthode permettent-elles la construction significative des scénarios d'attaques ?
8. est ce que vous êtes intéressé par l'intégration de la méthode proposée dans votre travail de réponse aux agressions numériques ?

2^{ème} Partie :

Cette partie comporte une série de questions ayant pour objectif de mesurer la facilité perçue d'utilisation de la méthode proposée.

1. est ce que l'étape de l'amplification progressive des signaux/signes faibles est facile d'utilisation ?
2. est ce que l'étape de la recherche complémentaire des informations est facile d'utilisation ?
3. est ce que l'étape du raisonnement itératif sur les liens créés entre les informations collectées est facile d'utilisation ?
4. est ce que l'activité de médiation est facile d'utilisation ?
5. est ce que l'outil informatique qui assiste la méthode est facile d'utilisation ?
6. est ce que l'outil informatique qui assiste la méthode est susceptible d'apporter une aide au travail de l'ERI ?
7. est ce que vous proposez certaines conditions pour faciliter l'utilisation de la méthode ?

3^{ème} Partie :

Cette partie comporte une série de questions ayant pour objectif de collecter des informations qui concernent l'état des pratiques dans le domaine de détection, de réponse et d'anticipation des agressions numériques.

11. qu'est ce qui déclenche, d'habitude, une réunion de réponse à une agression numérique annoncée ?
12. les réunions se font-elles au coup par coup ou selon un calendrier bureaucratique ?
13. Quelle est la nature des informations qui annoncent l'agression (qui déclenchent la réunion) ?
14. sous quelle forme ces informations se présentent ?
15. comment elles sont obtenues ou captées ?
16. les informations sont elles mémorisées, si oui durablement ou non ?
17. est-il procédé à une analyse individuelle ou collective des informations détectées ?
18. si elle est collective, l'analyse se fait en face à face ou bien à distance ?
19. quelle démarche d'interprétation : tacite ou formalisée ?
20. quels sont les outils Internet utilisés dans le traitement ?
21. la démarche est-elle mémorisée ou non ?
22. quelles actions peuvent découler de l'interprétation des informations ?

4^{ième} Partie :

Cette partie comporte deux questions ayant pour objectif d'explorer la pertinence des indicateurs de mesure, dans le temps, au cours du déroulement de la méthode et que nous avons déjà présentés dans le quatrième chapitre.

1. est ce que vous pensez que chacun des critères quantitatifs suivants sont pertinents :
 - le temps de traitement de chaque signal faible ;
 - le ratio des fausses décisions sur le nombre total des décisions prises (indicateur de qualité)
 - le ratio des décisions incomplètes sur le nombre des attaques qui se répètent (indicateur qui concerne la capacité d'anticipation, et la qualité de l'information anticipative)
 - le temps de réactivité globale qui mesure le temps de détection, d'analyse et de réponse à une agression numérique.
2. est ce que vous proposez d'autres critères de mesure ?