Systèmes d'information centrés réseau

Agnes Lancini, Jean-Fabrice Lebraty

Systèmes d'information centrés réseau : Contributions à la gestion des situations de crise

Le cas d'une crise sanitaire chez Leclerc

Agnès LANCINI

Maître de conférences en Sciences de Gestion
Université Aix Marseille II
IUT Département GEA
Laboratoire CRET-LOG
(http://www.cret-log.com)
Avenue Gaston Berger
13625 Aix-en-Provence Cedex 1
Téléphone : (33) 4.42.93.90.28
Fax: (33) 4.42.93.90.22
E-mail : lanciniagnes@hotmail.com

Jean-Fabrice LEBRATY

Professeur des Universités en Sciences de Gestion
Université Nice-Sophia-Antipolis
Laboratoire GREDEG CNRS
Téléphone : (33) 6.03.13.70.88
E-mail : lebraty@unice.fr

Résumé :
La gestion des situations de crise constitue un thème de recherche particulièrement d'actualité en raison de la complexité de l'environnement dans lequel les entreprises évoluent. Cette communication a pour objectif d'apporter un éclairage original à la gestion de crise en entreprise, en s'appropriant les travaux menés et les concepts déployés dans le monde militaire. Après avoir montré en quoi les conditions organisationnelles pouvaient se rapprocher du contexte militaire, cet article décrit les concepts de « décision en situation », « conscience de la situation » et d' « information centrée réseau ». L'articulation du cadre conceptuel conduit à présenter une structure de Système d'Information Centré Réseau (Net Centric Information Structure – NCIS) permettant de faire face à une crise dans le domaine militaire. Afin d'illustrer l'intérêt d'un tel SI pour l'organisation faisant face à une crise, une relecture du cas de la crise sanitaire des steaks hachés contaminés, vécue par le groupe Leclerc en octobre 2005, est menée. Cette analyse a posteriori souligne toute la pertinence des architectures NCIS pour améliorer la gestion des crises organisationnelles et propose des pistes innovantes pour faire évoluer le SI organisationnel vers une architecture centrée réseau.

Systèmes d'information centrés réseau : Contributions à la gestion des situations de crise

Le cas d'une crise sanitaire chez Leclerc

Résumé :
La gestion des situations de crise constitue un thème de recherche particulièrement d'actualité en raison de la complexité de l'environnement dans lequel les entreprises évoluent. Cette communication a pour objectif d'apporter un éclairage original à la gestion de crise en entreprise, en s'appropriant les travaux menés et les concepts déployés dans le monde militaire. Après avoir montré en quoi les conditions organisationnelles pouvaient se rapprocher du contexte militaire, cet article décrit les concepts de « décision en situation », « conscience de la situation » et d' « information centrée réseau ». L'articulation du cadre conceptuel conduit à présenter une structure de Système d'Information Centré Réseau (Net Centric Information Structure – NCIS) permettant de faire face à une crise dans le domaine militaire. Afin d'illustrer l'intérêt d'un tel SI pour l'organisation faisant face à une crise, une relecture du cas de la crise sanitaire des steaks hachés contaminés, vécue par le groupe Leclerc en octobre 2005, est menée. Cette analyse a posteriori souligne toute la pertinence des architectures NCIS pour améliorer la gestion des crises organisationnelles et propose des pistes innovantes pour faire évoluer le SI organisationnel vers une architecture centrée réseau.

Le 22 novembre 2005[1], le groupe Nestlé retire du lait pour enfants en France, Italie, Espagne et au Portugal après avoir découvert les traces d'un produit chimique. Peu de temps après, la société d'emballage Tetra Pak est incriminée. Le 13 décembre 2005[2], Le *leader* mondial de l'emballage annonce qu'il était informé dès le mois de septembre d'une contamination inoffensive due à l'encre d'impression. Tetra Pak, principal accusé, semble alors tirer les premières conclusions d'une crise sanitaire qu'il pensait ne jamais voir éclater. Gérer une telle crise est une tâche délicate pour l'ensemble des parties prenantes. Dans ce cadre, disposer d'un système d'information adapté peut permettre de prendre des décisions dans l'urgence qui conduiront à résoudre efficacement la crise. Mais, que signifie un système d'information adapté ? Le thème général de cette communication porte sur la manière de concevoir un tel système d'information, il s'agira donc de proposer des pistes innovantes pour construire une architecture des Systèmes d'information adaptée à la gestion des situations de crise.

La question de la gestion des situations de crise a fait l'objet de nombreux travaux en Sciences de Gestion. Le management des crises liées aux évolutions de l'environnement externe (Ritchie, 2004), ou de l'organisation elle-même (Muller, 1985) ont ainsi été analysés. La communication de crise a aussi été abordée (Coombs, 2001), mais la recherche semble se centrer sur la mise en œuvre de stratégies pour prévenir (Kovoor-Misra et al., 2001), voire planifier les futures crises (Spillan et Hough , 2003).

Cependant, d'autres disciplines ou domaines d'activités ont aussi exploré ce domaine et notamment le monde militaire. En effet, le domaine de la stratégie militaire a du s'adapter aux évolutions du contexte géopolitique se traduisant par la disparition d'un monde bipolaire relativement prévisible pour un environnement complexe dans lequel de nombreux acteurs sont en interrelations[3].

Examinons les nouvelles conditions dans lesquelles opèrent les unités militaires occidentales, puis décrivons en quoi ces conditions peuvent être comparables à celles rencontrées par les entreprises. Les conditions particulières dans lesquelles opèrent actuellement les unités américaines (face à des organisations terroristes en réseau, une difficulté d'identification de l'ennemi, par exemple) ont conduit à renouveler un certain nombre de concepts fondant le socle du fonctionnement de la pensée militaire américaine. Parmi toutes les conditions évoquées (Francart , 1999 ; Bauer et Raufer, 2002), deux retiennent ici notre attention : l'asymétrie des moyens et des ressources, et la coopération d'organisations aux caractéristiques différentes.

La notion d'asymétrie est redevenue d'actualité en raison de la fin de l'affrontement Est-Ouest. Le mythologique combat de David contre Goliath peut être retrouvé dans des conflits à l'échelle mondiale entre des adversaires dont les tailles, les modes d'organisation, la culture et les moyens à disposition, notamment technologiques, sont disproportionnés. Le terme de guerres asymétriques est alors employé (Courmont et Ribnikar, 2002). La guerre du Kosovo opposant une coalition de pays occidentaux à un petit pays en transition, ou celle contre le terrorisme qui concerne aussi bien des Etats très structurés que de petites cellules prospérant dans des zones de non-droit, sont deux exemples d'affrontement entre des adversaires aux forces déséquilibrées. Ce déséquilibre ne signifie pas que l'ensemble des moyens est détenu par un seul des protagonistes, mais que chacun possède des avantages incomparables dans un domaine particulier. Par exemple, la domination

technologique des unités américaines sur les groupes terroristes sunnites est écrasante. Mais, les répercutions médiatiques de la perte de vies humaines sont nettement plus importantes du coté américain. Dans de tels affrontements, la disproportion entre moyens conduit, à complexifier l'environnement et à rendre imprévisibles les crises susceptibles de se dérouler. Cette difficulté de prévision alliée à une contrainte médiatique forte renforce l'importance d'une gestion efficace des situations de crise.

La seconde condition importante qui est apparue, réside dans la nécessité de faire coopérer dans un même but des éléments disparates. Ainsi, dans le cadre d'opérations menées par des alliances, vont coopérer différentes organisations (militaires, ONU, ONG), armées (terre, air, mer, gendarmerie, marines), armes (infanterie, génie, artillerie etc..) et différentes nationalités[4], le tout sur un théâtre extérieur. La coordination de telles opérations a un impact fort sur la réalisation des systèmes d'informations militaires.

Une réflexion sur des concepts de systèmes d'informations adaptés à ces nouvelles contraintes a donc été logiquement menée par le milieu militaire. La maîtrise du concept de réseau est apparue déterminante. Or la maitrise du réseau implique sa compréhension, la gestion de l'élément circulant sur le réseau : l'information et donc la constitution d'architectures permettant d'obtenir un avantage informationnel afin de répondre de manière plus efficace aux nombreuses situations de crise.

Mais qu'en est-il de l'activité économique et donc du monde des entreprises ? Voyons si les deux conditions contextuelles précédemment évoquées peuvent être transposées aux entreprises.

Premièrement, prenons le cas du marché de la numérisation des livres et de la recherche dans ces ouvrages. On observe actuellement, une lutte entre deux organisations nettement différenciées. D'un côté, l'entreprise Google qui est une ex-jeune start-up devenue aujourd'hui une entreprise dont la capitalisation est de 85 milliards de dollars. De l'autre côté, la Bibliothèque Nationale (BNF) et six pays européens se sont regroupés veulent mettre en œuvre un projet concurrent à celui de Google. L'asymétrie se trouve ici dans les propos d'un conseiller gouvernemental français qui estime que : « il ne faut pas laisser le patrimoine français esseulé, mais pas question pour autant de mettre des années à construire une usine à gaz publique face à Google, entreprise privée hyper-réactive » (5 mai 2005).

Deuxièmement, le cas de la coopération d'organisations très différentes est une problématique déjà ancienne en Sciences de Gestion et peut s'illustrer brièvement au travers des deux exemples suivants. Le cas de l'entreprise 9 Cegetel peut être évoqué car cette entreprise résulte d'un regroupement de neufs entreprises[5] de tailles fort diverses qui s'est réalisé en moins de cinq années. Le cas de la mise en place des pôles de compétitivité représente aussi un autre exemple de coopération entre entités différenciées. En effet, le Comité interministériel à l'aménagement et à la compétitivité des territoires[6] a labellisé 67 pôles mêlant autour de thématiques définies un grands nombre d'acteurs fort variés (Centre de R&D, groupes industriels, Universités etc.). Nous estimons que la gestion de l'entreprise 9 Cegetel ou d'un pôle de compétitivité possède des similitudes avec la conduite d'une opération militaire actuelle[7] du moins en terme de conception de systèmes d'information.

La recherche managériale et les entreprises ont pourtant conduit à développer de nombreuses solutions de système d'information pour, notamment, résister aux phénomènes de mondialisation et d'hyper concurrence. Ces avancées ont d'ailleurs été antérieures à celles du monde militaire qui s'est, un moment, lui-même inspiré de la recherche civile. Cependant, comme nous allons le décrire, les recherches militaires proposent des concepts innovants sur des segments bien spécifiques, comme ceux de la gestion des crises ou de la prise de décision en situation d'urgence. Il nous apparait alors pertinent de porter, à notre tour, un regard sur ces nouveaux concepts et leur opérationnalisation.

Enonçons, maintenant, les apports d'une recherche sur l'utilisation de concepts provenant du monde militaire. Cette recherche présente un double avantage.

Elle recouvre un intérêt théorique fort, dans la mesure où elle permet de proposer une définition précise et éclairée des concepts tels que : *Naturalistic Decision Making*, *Situation Awareness*, *Network Centric Information*. Elle présente aussi des intérêts managériaux importants puisqu'il s'agit de transposer des architectures ayant fait leurs preuves sur le terrain militaire à des situations organisationnelles de crise de plus en plus récurrentes[8].

Notre communication aura ainsi, comme objectif de porter un éclairage sur les concepts développés dans le milieu militaire et, plus particulièrement, dans l'armée

américaine afin de proposer des pistes innovantes pour les entreprises. Notre problématique s'exprime de la manière suivante :

Quels peuvent être les apports des concepts en systèmes d'information employés au niveau Etat-Major de l'armée américaine pour les managers en entreprise dans le cadre de la gestion des situations de crise ?

Afin de répondre à cette problématique, nous développerons le plan suivant : dans une première partie nous décrirons les concepts développés dans le cadre de l'armée américaine, ainsi qu'une architecture de système d'information adaptée à la gestion des situations de crise. Dans une seconde partie, nous analyserons une crise sanitaire en montrant comment l'architecture présentée aurait permis de mieux gérer cette crise.

I. Les nouveaux concepts et leur mise en œuvre

Dans cette partie, nous présenterons dans un premier temps trois approches peu encore mobilisées en Sciences de Gestion, mais déjà éprouvées dans le domaine militaire : la décision en situation, la conscience de la situation et l'information centrée réseau. Dans un second temps, nous présenterons une architecture de système d'information proposée par une équipe de chercheurs travaillant au profit du Département de la Défense américain.

I.1. Du contexte au réseau

Nous intitulons ce point du contexte au réseau car comme nous allons le voir, tout est parti d'une prise en compte du contexte dans lequel les décisions sont prises, pour aboutir à une conception centrée réseau des systèmes d'information.

Le schéma ci-dessous illustre les liens entre concepts que nous allons développer :

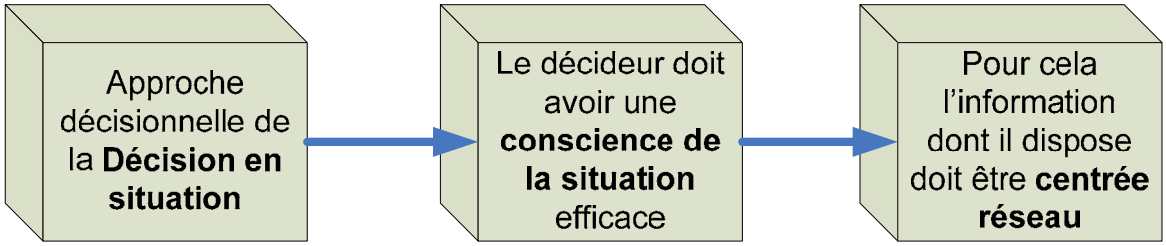

Figure 1 : Présentation et mise en relation des concepts étudiés

Décrivons les grands principes de l'approche de la décision en situation (Naturalistic Decision Making). Cette approche décisionnelle initiée par G. Klein (1993 ; 1998) se fonde sur l'observation en situation de décideurs expérimentés dans des situations décisionnelles urgentes et risquées. A partir de ces observations, G. Klein a proposé un modèle dit de « première reconnaissance ».

Cette approche constitue une troisième voie par rapport aux modèle classiques optimisateurs et aux modèles cognitifs de type satisfaisant (Lebraty et Pastorelli, 2004). La principale différence dans cette approche, réside dans le fait que la décision n'est plus un choix entre des options. En effet, la décision prise dépend principalement de la reconnaissance de la situation qu'a réalisée le décideur. Tout va dépendre de la manière avec laquelle le décideur perçoit et comprend la situation dans laquelle il se trouve. De l'importance de ce mécanisme de reconnaissance, découle la mise en avant du concept de « conscience de la situation ». M.R. Endsley (1995) a défini la « Situation Awareness » de la manière suivante : « la perception des éléments de l'environnement dans un volume de temps et d'espace, la compréhension de leur signification et la projection de leur état dans un futur proche. » Ainsi, M.R. Endsley détermine trois niveaux de conscience. Tout d'abord, la personne doit discerner les éléments pertinents de la situation dans l'information contextuelle qui lui parvient. Elle intègre ensuite cette information à l'aide de son expérience et de ses connaissances propres. Ainsi, elle va déterminer les relations existantes entre les éléments perçus. Enfin, elle imagine la dynamique du système ainsi repéré. Toute incohérence à l'un ou plusieurs de ces niveaux conduit à des décisions jugées « absurdes » (Morel, 2002).

Les conditions d'une conscience de la situation efficace dépendent donc de l'expérience de la personne, des caractéristiques (quantité, qualité, globalité, ergonomie) de l'information dont elle dispose et des contraintes exercées par le

contexte. Afin qu'un système d'information puisse prendre en compte ce système complexe homme-information-contexte, il a été mis en avant le concept d'information centré réseau.

Développé dans le domaine militaire, on trouve aussi le terme de « Combat en réseau info-centré[9] » (Net Centric Warfare). Afin de préciser ce concept d'information centrée réseau, nous nous fonderons sur des documents du « *Department of Defense Chief Information Officer* » et plus particulièrement sur celui intitulé « *Net-Centric Checklist - Version 2.1.3* » du 23 Mai 2004. L'idée fondatrice de la volonté de centrer le système d'information sur l'information peut apparaitre trivial. Cependant, dans les systèmes d'information militaires, les évolutions des différentes architectures technologiques ont conduit à la coexistence d'un grand nombre d'applications hétérogènes. Or dans le contexte que nous avons décrit, les impossibilités pour ces applications de communiquer entre elles ont été jugées comme une faiblesse stratégique. L'idée est donc de refondre les architectures pour replacer les données et informations au centre du SI[10]. Ceci entraine alors la nécessité de rendre interopérable ces données et informations et donc de créer des liaisons entre elles sur un mode de maillage réseau. C'est de cette manière que s'est élaboré ce concept d'information centrée réseau.

Répétons que même si cette ligne directrice semble évidente, elle demeure pertinente pour de nombreuses organisations. Il suffit, par exemple, d'observer le fonctionnement des différentes applications récemment mises en service dans nos universités et le manque de communication qu'il existe entre elles pour en conclure que le concept de Net Centric Information mérite d'être exploré. Cependant la mise en œuvre de ce concept est délicate notamment en raison :

- de l'architecture informatique existante ;
- des usages des utilisateurs ;
- de la nécessite de maitriser les outils et méthodes récentes ;
- du coût des investissements à réaliser.

Après avoir décrit trois nouveaux concepts initiés dans les Etats-Majors américains, voyons les moyens conduisant à rendre opérationnel ces concepts. Ainsi, dans le point suivant, nous allons présenter une architecture de système d'information adaptée à la gestion des crises.

I.2. Une structure de système d'information adapté au concept d'information centrée réseau : Le NCIS

Après avoir détaillé les approches conceptuelles favorisant la prise de décision en situation de crise, voyons un exemple d'architecture technologique permettant de rendre opérationnel ces concepts. Deux chercheurs et membres de l'entreprise norvégienne TELEPLAN, spécialisée dans le management des systèmes à risques et la gestion des réseaux, E. Aarholt et O. Berg (2002 ; 2004) proposent une solution pour ériger une structure d'information centrée réseau (**N**etwork **C**entric **I**nformation **S**tructure : **NCIS**). Il s'agit d'une architecture visant à créer une gestion centrée réseau de l'information nécessaire pour faire face à une crise. Trois principaux aspects paraissent pertinents dans cette structure de gestion de l'information de crise.

En premier lieu, les auteurs identifient quatre catégories génériques d'information nécessaires aux cadres dirigeants de l'entreprise :

- l'information générale qui concerne le métier et les activités de l'entreprise ;
- l'information sur les produits et les services ;
- l'information sur la sauvegarde et la sureté des actifs de l'entreprise[11] ;
- l'information sur les capacités en mesure d'être déployées rapidement pour faire face à une menace.

Lors d'une crise, toutes ces informations sont nécessaires, cependant, et surtout dès les premiers instants de la crise, un effort particulier doit être porté à la protection de l'entreprise et de ses parties prenantes. Aussi, nous nous focaliserons ici sur la troisième catégorie, à savoir sauvegarde et sureté. Rendre disponible ces éléments d'information pour l'équipe chargée de la gestion de la crise apparait déterminant.

En deuxième lieu, les auteurs proposent une solution possédant des caractéristiques techniques standards et fondée sur les outils existants. En effet, développer un NCIS suppose « simplement » de dédier une zone bien précise de l'intranet de l'entreprise à la gestion de crise et n'implique pas d'investissement supplémentaire en technologie. La zone permanente de l'intranet est alimentée par des liaisons dynamiques avec les données de l'entreprise de telle sorte qu'à chaque consultation, les données soient réactualisées. Il faut noter que dans bien des cas, il

s'agit tout simplement de réaliser des « Copier – Coller avec liaisons » entre des documents Excel ou Word.

En dernier lieu, et ce point parait déterminant, les auteurs proposent de classer l'information relative à la sauvegarde et la sûreté en six dimensions. Les quatre premières concernent l'intérieur de l'entreprise, tandis que les deux dernières ont trait à son environnement externe. Le tableau suivant indique et détaille ces six dimensions :

	Classes d'information	Description
Interne	Personnel	Ensemble de l'information disponible sur les personnes travaillant dans l'entreprise : • Nombre de personnes sur site • Localisation des acteurs • Système de suivi et de traçabilité du personnel • Membre du personnel ayant des besoins spécifiques (médical, autres, …)
	Infrastructure de l'entreprise	Cette information peut être présentée graphiquement et concerne • Local d'aide d'urgence, Sortie de secours, Equipements d'urgence • Plans des locaux, cablage électrique, portes, ventilation, etc.
	Ressources locales	Concerne aussi bien les ressources que les menaces potentielles • Ressources locales : personne détenant un brevet de secourisme, état du système électrique et téléphonique • Dangers associés à la crise : existence de produits chimiques, bactérie, virus, explosifs, etc.
	Plan de réaction en urgence face aux crises	Ensemble des plans déjà réalisés pour faire face à des crises. Généralement, il s'agit de dossiers décrivant les conduites à tenir. • Existence de plan d'urgence et d'exercices de simulation en grandeur réelle • Communication au sein de l'équipe d'urgence : lien entre les sauveteurs, avec la presse, l'administration, la défense civile et militaire,… • Etablissement de réseau de communication physique : téléphone, radio
Externe	Procédures d'alerte et de remontée d'information	Ensemble des points de contact et des personnes qu'il faut informer lors d'une crise (police, journaliste etc.), ainsi que les procédures pour les contacter. • Capacité à contacter et à informer la police, les pompiers, les médecins, … • Procédures pour mettre en œuvre ces contacts
	Accès géographique de l'entreprise ou de ses zones d'intérêt	Cette information eut aussi être présentée graphiquement et concerne la manière d'accéder à l'entreprise ou aux zones qui concerne la crise. • Adresse exacte du lieu, information GPS • Carte de l'endroit et de son environnement (ressource en eau, station de radio, …) • Information d'accès à la zone (rue en sens unique, rue bloquée, parking, aire d'atterrissage, …)

Tableau 1 : Classification de l'information nécessaire à la sauvegarde et la sureté de l'entreprise

Il s'agit ici de catégories génériques dont le contenu dépend fortement de l'état des données disponibles et de la volonté des dirigeants de tenir actualisées ces informations.

Afin de permettre une gestion normalisée de cette information, il convient de se fonder sur des modèles de données et des standards ISO qui n'existent pas toujours. Le tableau suivant reprend les différentes normes susceptibles d'être employées :

Classes d'information	Normes susceptibles d'être suivies
Personnel	ISO 16739 (partie de ISO TC 184/SC4)
Infrastructure de l'entreprise	ISO 10303-239 (partie de ISO TC 184/SC4)
Ressources locales	ISO 10303-239 (partie de ISO TC 184/SC4)
Plan de réaction face aux crises	Pas de norme
Alerter et informer	ISO 10303-239 (partie de ISO TC 184/SC4)
Accès de l'entreprise ou de ses zones d'intérêt	ISO TC 211

Tableau 2 : Catégories d'information et standards ISO

Une fois ces informations disponibles, il s'agit de permettre leur maillage, c'est-à-dire de permettre le « centrage réseau » de ces informations.

Pour ce faire, une solution déjà employée dans des systèmes militaires (Lebraty, 2005) réside dans l'utilisation de calques. Dans le cas du NCIS, il existe deux catégories d'information qui peuvent être présentée graphiquement (l'infrastructure de l'entreprise et les accès de l'entreprise ou de ses zones d'intérêt). Ces deux éléments doivent être considérés comme deux fonds de carte sur lesquels pourront être placées les quatre autres catégories d'information (Personnel, Ressources locales, Plan de réaction en urgence face aux crises et Procédures d'alerte et de remontée d'information). Chacune de ces quatre catégories pourra être manipulée sous la forme d'un calque que l'on placera sur l'une ou l'autre des cartes. L'emploi des calques est laissé à la charge du décideur qui ainsi peu à peu prendre conscience de la situation.

Dans ce second point, nous avons vu les bases d'un système de gestion des risques fondé sur l'information centrée réseau. Dans une deuxième partie, nous

allons voir comment un tel système aurait pu améliorer la gestion d'une crise sanitaire récente.

II. Application du NCIS à la gestion d'une crise sanitaire.

Le cas de la crise sanitaire des steaks hachés contaminés, vécue par le groupe Leclerc en octobre 2005, permet d'illustrer l'intérêt de la mise en œuvre d'une architecture centrée réseau pour améliorer la gestion des situations de crise.

II.1. Gestion de crise : Le cas de l'intoxication au steak haché

Afin d'illustrer la mise en œuvre d'un SI basé sur une architecture centrée réseau, le cas d'une crise sanitaire va être détaillé. Il s'agit du cas de l'intoxication au steak haché, qui va être analysé du point de vue du distributeur : la chaine de magasins Leclerc. Dans un premier temps, le cas et la justification de ce choix sont présentés. La méthodologie de recueil des données est précisée dans un deuxième temps. Enfin, dans un dernier temps, le cas est traité en soulignant successivement les éléments informationnels présents dans la gestion réelle de la crise et les apports qu'aurait pu avoir une architecture de type NCIS.

II.1.1. Contexte, présentation du cas et justification du choix

Depuis le 25 octobre, près de 20 cas de syndrome hémolytique et urémique ont été observés chez des enfants de plusieurs départements de la région Aquitaine et Midi-Pyrénées. Une bactérie, du genre Escherichia Coli, a été identifiée comme responsable de ces cas. L'enquête menée par l'Institut de veille sanitaire (INVS) a mis en évidence que tous ont consommé des steaks hachés de marque Repère Chantegrill® achetés dans une enseigne de la chaîne de magasins Leclerc entre la fin septembre et la mi-octobre 2005. Les lots 206, 231 et 234 sont incriminés. Ils ont été retirés du marché par les magasins Leclerc dès le 28 octobre 2005. Toutefois, pour ce grand distributeur, la gestion de crise ne fait que commencer. En effet, il est nécessaire de procéder au rappel des produits concernés déjà vendus (dont la date limite de consommation est en 2006). Cette procédure de rappel met en exergue les limites du système de traçabilité des ventes de Leclerc. En effet, c'est à partir des tickets de caisse que les responsables de magasins ont identifiés quels étaient les acheteurs du produit suspect. Soit le client a utilisé une carte de fidélité et le groupe possède alors ses coordonnées, soit il n'en détient pas et c'est grâce à la transaction

par chèque ou carte bleue que l'enseigne arrive à remonter jusqu'au client. L'analyse des transactions a été rendue possible grâce à la coopération des banques. En revanche, rien n'a pu être fait pour les clients ayant réglé leurs achats en liquide.

Au-delà de la procédure de rappel, le groupe Leclerc doit assurer une communication permanente et rassurante en direction de ses clients. Il doit également être informé au plus près des nouveaux cas de contamination, de l'évolution des rappels clients et de manière plus générale, de toute information susceptible de faire évoluer les paramètres de la crise. Le groupe Leclerc doit également prévoir de proposer rapidement un produit de substitution à ses clients.

Gérer une telle crise suppose la présence d'un système d'information le plus fiable possible et permettant d'avoir une vision globale de la situation.

Trois dimensions se dégagent du cas étudié et justifient l'intérêt que nous lui portons pour illustrer les apports que peut avoir une architecture de type NCIS.

Tout d'abord, il s'agit d'une crise grave menaçant la crédibilité du distributeur et la confiance que les clients peuvent accorder à cette enseigne. Ainsi, les pistes visant à épauler les décideurs en charge de la gestion de cette crise méritent d'être explorées.

Le cas choisi présente ensuite une dimension « réseau ». Effectivement, la crise qui frappe le distributeur Leclerc touche, tout d'abord, ses clients mais implique forcément ses acteurs internes, ses fournisseurs, ses services de distribution, et également, l'environnement au sens large, à savoir, les pouvoirs et services publics, la presse ou les hôpitaux. Cette dimension est importante dans la mesure où elle révèle tout l'intérêt d'un maillage de l'information au détriment d'une configuration centralisée de l'information qui serait, de toutes manières, délicate à mettre en œuvre et à maintenir.

Enfin, le cas de l'intoxication au steak haché du point de vue du distributeur met en évidence la prédominance de la dimension externe sur l'interne. La mise en danger de la vie d'autrui concerne ici exclusivement des personnes externes à l'enseigne, ce qui n'est pas forcément le cas, comme par exemple, lors de l'explosion de l'usine AZF de Toulouse, où des personnes internes et externes sont concernées. Le cas choisi suppose notamment une gestion efficace du rappel des produits et du contact avec les médias et les pouvoirs publics. Or, souvent la gestion de la dimension externe de la crise s'avère le point le plus délicat, notamment en raison de problèmes informationnels.

Aux vues de ces trois dimensions, une architecture NCIS parait pertinente dans la mesure où elle permet le maillage multidimensionnel des informations relatives au métier et activités, aux produits et service, à la sauvegarde et sécurité des actifs, et, aux capacités de réaction.

II.2. Méthodologie de recueil des données

La méthodologie mise en œuvre dans ce travail de recherche exploratoire est qualitative. Cette phase exploratoire a consisté en la collecte de documents et extraits de presse permettant de mieux cerner le déroulement de la gestion de crise du point de vue du distributeur. Ces sources d'information ont permis une meilleure connaissance de l'environnement de la crise et des spécificités du secteur de la grande distribution. La consultation de blogs et du site internet de Leclerc sont également une source d'information utilisée. Ce recueil de données a été enrichi et recoupé par des rencontres et discussions informelles avec certains membres du personnel du groupe Leclerc ainsi qu'un entretien téléphonique avec une attachée de presse du groupe E. Leclerc.

II.3. Présentation du NCIS

Il s'agit ici de s'intéresser, dans le cas des steaks contaminés, aux six dimensions informationnelles du NCIS identifiées pour la sauvegarde et la sureté des actifs de l'entreprise (voir tableau 1). Cette présentation formalise dans l'absolu les informations nécessaires à une architecture de type NCIS. Une fois ces dimensions informationnelles décrites, une discussion sera menée sur la gestion de la crise et les informations réelles détenues par le groupe Leclerc et celles dont il aurait pu bénéficier dans le cas du NCIS.

Information relative au personnel

Cette information concerne le recensement et le positionnement des salariés des magasins Leclerc concernés. Il s'agit notamment de savoir quel est le nombre de salariés ayant été en contact avec le produit : commandes, gestion des stocks, manutention, mise en rayon, vente. Mais aussi, qui était le responsable qualité au moment de la mise en rayon, afin de déterminer s'il y a eu rupture de la chaine du froid.

Information relative à l'infrastructure de l'entreprise

Au moins trois éléments composent cette dimension.

Premièrement, une orientation « représentation graphique » doit exister et permettre de constituer une cartographie de l'entreprise et de ses différents sites.

Deuxièmement, cette dimension doit amener à une compréhension de la contamination ex-ante. Dans le cas des steaks contaminés, l'information utile est ici de savoir quel a été le parcours du produit suspect dans l'entreprise. Cette information permet d'identifier les salles dans lesquelles il a transité afin, éventuellement, de mettre en évidence une rupture de la chaine du froid à l'origine de la contamination. Elle permet également de dire s'il y a eu une possibilité de contaminer la viande à partir du moment où le produit a été dans l'entreprise.

Troisièmement, cette dimension visera à une gestion des produits retirés ex-post. L'infrastructure de l'entreprise doit permettre aussi de prévoir la procédure de destruction du produit contaminé. Les informations utiles au chef de rayon des magasins concernés sont : quels sont les lots à retirer ? Que fait-on de ces lots ? Quelles sont les salles de transit permettant l'élimination et la destruction du produit ?

Information relative aux ressources locales

Cette information concerne, d'une part, les ressources locales existantes pour faciliter la gestion de crise. Cela peut concerner notamment l'existence de produits de substitution capable de remplacer le stock des produits incriminés ou la possibilité de passer un ordre de réapprovisionnement à un autre fournisseur.

Elle concerne, d'autre part, les menaces et dangers potentiels associés à la crise. Dans le cas étudié, il pourrait s'agir notamment de pouvoir apporter une réponse non équivoque à la question : le produit suspect peut-il potentiellement avoir contaminé d'autres produits dans l'entreprise ?

Information relative au plan de réaction d'urgence

Cette information s'intéresse à l'existence d'exercice de simulation en grandeur réelle de la gestion de crise. A l'issue de ces exercices, des plans d'urgence sont élaborés intégrant les ressources humaines, matérielles, informationnelles et géographiques à prendre en compte. Ces plans concernent l'identification et le retrait de la distribution des produits suspects.

Elle concerne aussi l'existence d'une cellule de crise et l'identification de ses composantes, généralement acteurs clés de la crise. De plus, les procédures de communication au sein de cette cellule de crise doivent être élaborées.

Procédures d'alerte et de remontée d'information

Cette information d'ordre externe joue, dans le cas de la crise des steaks, un rôle clé. Elle concerne, tout d'abord, la procédure de rappel des produits détenus par le client. Cette procédure suppose une connaissance fiable des achats clients afin de savoir qui est en possession du produit incriminé. Elle implique ensuite une bonne maintenance des coordonnées clients afin de pouvoir contacter l'ensemble des personnes concernées. L'alerte suppose, enfin, la capacité de mobiliser les acteurs du réseau et, plus particulièrement, les pouvoirs publics pour relayer le message et transmettre toutes les informations relatives au produit incriminé. Sur ce dernier aspect, la cellule de crise aura un rôle important à jouer comme fédérateur d'un réseau temporaire.

La remontée d'information implique un lien étroit avec les services sanitaires et pédiatres hospitaliers afin de suivre en temps réel les évolutions de la contamination. Elle suppose aussi un prolongement de la remontée d'information au-delà de l'entreprise vers les fournisseurs concernés par la fabrication des lots incriminés.

Information relative à l'accès géographique de l'entreprise ou de ses zones d'intérêt

Cette information concerne la capacité à identifier et cartographier les magasins distribuant ou ayant distribué le produit contaminé. Il s'agit aussi de représenter les éléments d'intérêt qui sont à proximité des magasins (hôpitaux et points d'information de consommateurs notamment).

Après avoir décrit de quoi se compose le NCIS selon la dimension « sauvegarde et sûreté », il convient de préciser comment le groupe Leclerc a géré cette crise et en quoi le NCIS aurait pu améliorer cette gestion.

II.4. Les apports potentiels du NCIS

Les différentes étapes de la gestion de crise chez Leclerc se sont déroulées comme suit :

- **La DGAL alerte le groupe Leclerc de la série d'intoxications (décelées du 5 au 26 octobre) (27/10)**

- **Constitution d'une cellule de crise (27/10)**

Cette cellule est composée de Michel-Edouard Leclerc (alors en déplacement en Italie), responsable qualité acheteur produits, chef de marché (relation avec les fournisseurs), docteur vétérinaire conseil, spécialiste logistique industrielle, communication interne et externe, tous en relation directe avec les administrations (Ministère de la Santé, Ministère de l'agriculture).

- **L'Institut de veille sanitaire (INVS) confirme la présomption du steak haché (18h - 28/10)**
- **Prise de décision de retirer les produits dans les magasins (19h - 28/10)** (selon le principe de précaution car aucune analyse ne valide le diagnostic)
- **Envoi d'un message de crise sur l'Intranet à l'attention des responsables qualité des magasins (après 19h - 28/10)**
- **Lien et contact avec les fournisseurs pour approfondir les tests (28/10)**

Les fournisseurs ont l'obligation de conserver des échantillons témoins qui ici vont permettre d'approfondir les tests.

- **Retrait concret du produit dans les magasins (29/10)**
- **Confirmation par l'INVS de 14 cas et 3 lots incriminés (17h- 29/10)**
- **Mise en place d'une cellule de rappel des clients (30/10)** (7500 personnes appelées ce jour)
- **Procédure de rappel des produits (30 et 31/10).** Cette procédure suppose :
  - → L'affichage en magasin des lots et du produit
  - → L'envoi du communiqué aux médias sur zone et à l'AFP
  - → La relecture fastidieuse des tickets de caisse pour identifier les clients concernés par l'achat de ces produits et les appeler

La direction du groupe Leclerc reste, à ce jour, vigilante même si au 02 novembre 2005, 95% des personnes ayant acheté ces lots étaient repérées et 13000 paquets restaient à récupérer.

L'examen de la chronologie de gestion de la crise révèle une approche centralisée de l'information au détriment d'une approche centrée réseau de type NCIS. Il convient de revenir sur les grandes étapes de la gestion de la crise afin de souligner comment une architecture centrée réseau fait évoluer la position du décideur et sa compréhension du problème. Une analyse des changements nécessaires, pour faire évoluer le SI classique de l'organisation vers un SI centré réseau, est menée. Trois phases peuvent être mises en évidence.

Phase 1 : la cartographie micro et macro :

La structure NCIS permet de cartographier dans un premier temps la vision micro-interne et macro-externe de la crise et d'offrir immédiatement une image de la situation aux décideurs.

En l'occurrence, dans le cas de Leclerc, il s'agit rapidement d'avoir des cartographies qui :

- d'une part, au niveau interne (micro), indique la procédure d'acheminement du produit depuis son arrivée dans l'entreprise jusqu'à sa mise en rayon, ce qui permet de souligner les pièces dans lesquelles le produit a transité et, le cas échéant, les produits qu'il a pu à son tour contaminer ;
- d'autre part, au niveau externe (macro), précise les magasins concernés ce qui permet de délimiter les régions et les zones françaises voire européennes touchées.

Concernant ces deux cartographies, il semble que le groupe Leclerc ne travaille pas à partir d'une visualisation cartographiée. Dans ce cas précis, ces cartes de fond auraient été utiles à une prise en compte de l'ampleur du problème et à une délimitation rapide de son périmètre. Cela aurait peut être favorisé une meilleure conscience de la situation et donc l'impact sur les premières décisions prises aurait été important.

Phase 2 : enrichissement de la cartographie interne

Comme nous l'avons précisé, le maillage de l'information consiste à enrichir les cartes servant de fond par des calques successifs apportant des éléments informationnels supplémentaires. Pour ce qui concerne la cartographie interne du processus d'acheminement du produit, elle peut notamment être enrichie en positionnant les différents salariés ayant interagit avec le produit (c'est-à-dire tous les salariés relatifs à la commande, la gestion des stocks, la manutention, la mise en

rayon, la vente). Etant donné l'absence de risques liés à la manipulation du produit, le groupe Leclerc s'est peu attaché à identifier ces salariés.

Cette carte peut également être enrichie par les ressources locales existantes. Leclerc a stoppé ses commandes auprès du fournisseur incriminé et n'a pas communiqué sur ses procédures de réapprovisionnement. Concernant les dangers potentiels associés à la crise, le produit contaminé ne peut à son tour, contaminer d'autres produits. Par contre, la recherche de la bactérie ne s'est pas limitée aux seuls lots suspectés mais à l'ensemble de la production du fournisseur. Le groupe Leclerc a bien géré la crise ici puisque aucune rupture de la chaîne du froid n'a pu être mise en évidence.

Les informations liées au plan de réaction en urgence sont susceptibles d'enrichir la cartographie interne. Le NCIS peut indiquer les plans de simulation déjà effectués et les procédures suivies. Concernant le grand distributeur, il semble que la mise en œuvre de simulation de crise en grandeur réelle n'ait jamais été réalisée. Pourtant les retours d'expérience survenus lors de ces simulations mettent en évidence les manques informationnels et organisationnels notamment. A l'instar de certaines entreprises procédant à des exercices d'évacuation, il serait intéressant pour un distributeur comme Leclerc de travailler sur la simulation grandeur nature du retrait d'un produit. Ces exercices permettent rapidement d'identifier où se trouvent les produits et quels magasins les ont en stock ou en rayon. Leclerc a mobilisé un espace de son Intranet pour indiquer aux responsables qualité sa décision de retirer les produits des rayons, comme le prône l'architecture NCIS. Par contre, la procédure de rappel des produits/clients, bien plus complexe, car elle suppose d'avoir un SI intégrant des données externes liées au client, a posé davantage de problèmes.

Phase 3 : enrichissement de la cartographie externe

Le NCIS revêt ici toute son importance en raison de la dimension externe que nous avons mentionnée plus haut. Il s'agit ici de relier toutes les informations liées au produit (marque, n° de lot, signe distinctif etc.) avec les informations externes essentielles à la gestion de la crise comme par exemple, les informations sur le client, sur les services sanitaires ou encore les médias.

Les liens entre les produits et les clients, par exemple, vont conditionner la procédure de rappel visant à rapatrier le plus rapidement possible les produits

suspects sachant que leur date limite de consommation est juin 2006 ce qui fait 8 mois de stockage possible. Dans ce cadre, l'enrichissement de la carte externe consiste à associer à chaque magasin les noms et coordonnées des clients concernés. Cette procédure de rappel aurait pu être facilitée si le système d'information du groupe Leclerc intégrait une partie de gestion des données clients (coordonnées) mais aussi une traçabilité des ventes, permettant de savoir qui achète quoi. Le recours de Leclerc à la relecture « manuelle » des copies de tickets de caisse s'est révélé particulièrement fastidieuse et parfois peu fiable. Pourtant certaines sources d'informations (les Blogs notamment) auraient pu être prises en compte et intégrée à la recherche des clients.

Les liens avec les autres organisations concernées par la crise sont aussi essentiels. En effet, si par malheur un décès s'était produit, il aurait fallu une réaction immédiate du groupe Leclerc. Cependant, il faut premièrement disposer de cette information au plus tôt ce qui implique un lien permanent avec les hôpitaux. Deuxièmement, une communication de crise doit être menée au niveau national, mais aussi local. Dans ce cadre, disposer immédiatement des informations relatives à la presse locale (noms des journaux et points de contact etc.). Sur ce point, le groupe Leclerc a mis en place une cellule de crise chargée d'assurer l'interface non seulement avec les hôpitaux mais aussi avec la presse régionale et nationale.

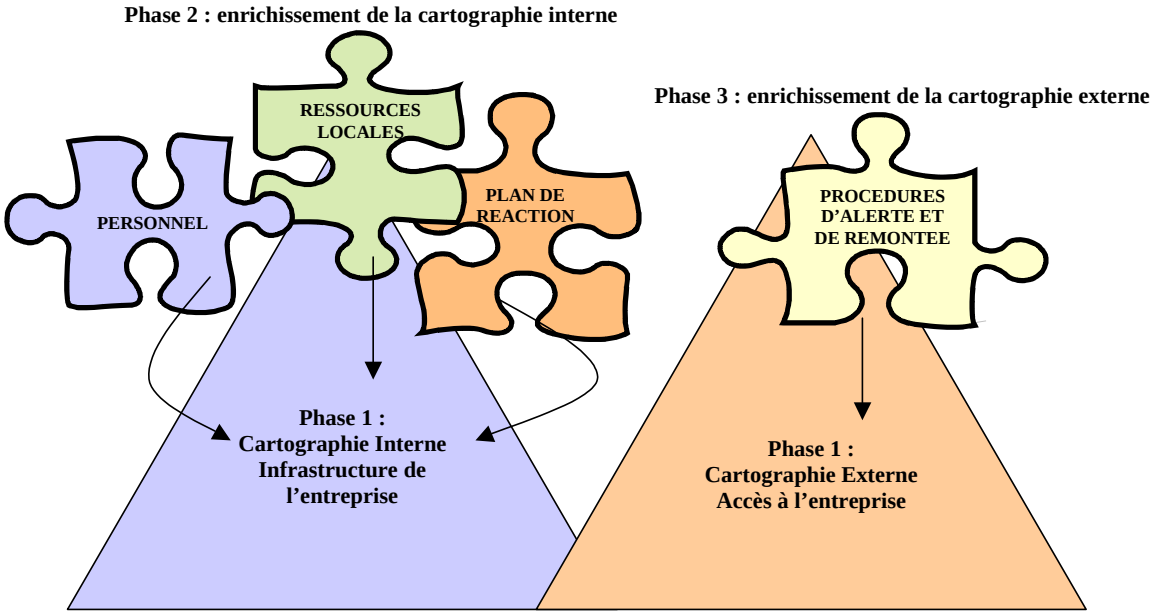

Figure 2 : Les trois phases informationnelles de gestion de la crise

Ainsi, au travers de ces trois phases informationnelles (figure 1), il se crée une image de la situation de crise qui permet une certaine conscience de la situation et de réagir le plus rapidement possible. De plus, et c'est peut être le principal apport lié à la mise en place d'une architecture de type NCIS, la conscience de la situation et les actions des décideurs vont suivre la même échelle de temps. Limiter les décalages entre la vitesse avec laquelle se développe la crise dans l'environnement et celle avec laquelle les décisions sont prises aurait permis au Groupe Leclerc d'être toujours le premier à répondre, laissant ainsi au devant de la scène les autres protagonistes, et notamment l'entreprise Chantegrill.

En conclusion de cette communication, nous rappelons l'intérêt de la mise en œuvre d'une architecture de gestion de crise centrée réseau. En effet, certes dans notre cas, le groupe Leclerc a géré efficacement la crise, notamment en raison des compétences des cadres concernés. Cependant, deux éléments conduisent à rendre les situations plus complexes et moins prévisibles, même à court terme :

- le développement des outils de communications (notamment les Blogs et les Podcasts) qui conduit à informer et désinformer les clients très rapidement ;
- le grand nombre de parties prenantes extérieures[12] qui sont toutes en relations de manière plus ou moins formelle.

Dans ce cadre, une conscience de la situation est essentielle pour les dirigeants. Or pour que les décideurs aient conscience de la situation, encore faut-il qu'ils puissent comprendre les évènements qui se déroulent. Les relations entre ces évènements doivent être intelligibles pour eux. Or, seule une information centrée réseau peut témoigner de ces liens entre acteurs de la crise. Mettre en œuvre de telles architectures nécessite de mener des projets ambitieux. Ainsi, bénéficier de la recherche et des réalisations du monde militaire peut être une piste visant à diminuer le montant de tels investissements.

Bibliographie

Aarholt, E. & Berg, O. (2002), « Information grid in support of crisis management », *Command and Control Research Technology Symposium*

Aarholt, E. & Berg, O. (2004), « Network Centric Information Structure - Crisis Information Management », *Command and Control Research Technology Symposium*, 083

Bauer, A. & Raufer, X. (2002) *La guerre ne fait que commencer* JC Lattès.

Coombs, W.T. (2001), « Teaching the crisis management/communication course », *Public Relations Review*, Vol. , no1, pp.89-101.

Courmont, B. & Ribnikar, D. (2002) *Les guerres asymétriques* PUF.

Endsley, M.R. & Garland, D.J. (2000) *Situation Awareness Analysis and*

Endsley, M.R. (1995), « Toward a theory of situation awareness », *Human Factor*, Vol. 37, no1, pp.32-64.

Francart, L & Patry, J.J. (1999) *Maîtriser la violence, une option stratégique* Economica.

Klein, G. (1998) *Sources of Power How People Make Decisions* MIT Press.

Klein, G.A. & Orasanu, J. & Calderwood, R. & Zsambok, C.E. (1993) *Decision Making in Action* Ablex Publishing Company.

Lebraty, J.F. & Pastorelli-Nègre, I. (2004), « Biais cognitifs : quel statut dans la prise de décision assitée ? », *Systèmes d'Information et Management*, vol. 9, no3, pp.87-116.

Lebraty, J.F. (2005), « Aide à la décision et compréhension de la situation : Analyse d'une « mauvaise » décision », *10ème colloque de l'AIM - Toulouse*, Actes, pp..

Measurement Lawrence Erlbaum Associates.

Morel, C. (2002) *Les décisions absurdes* Gallimard.

Müller, R. (1985), « Corporate crisis management », *Long Range Panning*, Vol. 18, no5, pp.38-48.

Ritchie, B.W. (2004), « Chaos, crises and disasters: a strategic approach to crisis management in the tourism industry », *Tourism Management*, Vol. 26, no6, pp.669-683.

Spillan, J. & Hough, M. (2003), « Crisis Planning in Small Businesses: Importance, Impetus and Indifference », *European Management Journal*, Vol. 21, no3, pp.398-407.

---

[1] AFP Infos Economiques du 22 novembre 2005 15h48.

[2] Le Figaro Économie, mardi 13 décembre 2005, p. 28

[3] La réflexion sur les évolutions à accomplir par le monde militaire a été si profonde qu'elle s'intitule « Revolution in Military Affairs » (RMA).

[4] La KFOR et la MINUK, par exemple, comprennent plus de 30 nationalités

[5] LDCom, Ventelo, Kaptech, Kertel, Belgacom France, Siris, Firstmark, Fortel et Cegetel

[6] http://www.competitivite.gouv.fr

[7] Nous convenons que ce point mériterait de plus amples développements.

[8] La gestion de crise peut concerner des crises aussi diverses que des crises environnementales (par exemple l'accident nucléaire de Tchernobyl en 1986, explosion AZF à Toulouse en 2001), des crises liées à la raréfaction de produits (crise pétrolière de 1973) mais également des crises sanitaires (vache folle, listériose, etc.)

[9] Traduction proposé par Sagem qui développe des architectures de ce type.

[10] « Data-Centric—focusing on the central design data repository as the foundation or starting point. In a data-centric system, the data is primary and services manipulate the data » Ibid

[11] Rappelons qu'il existe une différence entre sureté et sécurité : pour assurer la sureté, il convient de mettre en œuvre des mesures de sécurité.

[12] Dans notre cas, la crise était limitée à quelques régions françaises, une crise internationale est toujours possible.