UNIVERSITÉ DE MONTRÉAL

PORTRAIT DE LA VULNÉRABILITE D'UNE ORGANISATION FACE AUX UTILISATIONS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

ARTHUR BENON

DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAITRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INDUSTRIEL)

DÉCEMBRE 2017

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

PORTRAIT DE LA VULNÉRABILITÉ D'UNE ORGANISATION FACE AUX UTILISATIONS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

présenté par : BENON Arthur

en vue de l'obtention du diplôme de : Maîtrise és sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. AGARD Bruno, Doctorat, président

M. ROBERT Benoît, Ph. D, membre et directeur de recherche

M. GAGNON Benoit, M. A., membre

DÉDICACE

Avoir le sentiment de tourner en rond n'est que l'assimilation des nouvelles perspectives d'un problème - Anonyme

À ma famille qui m'a soutenu durant ces deux longues années loin de chez moi par de nombreuses visites et petites attentions

À mes colocataires durant ces deux années qui ont tous su à tour de rôle me motiver ou me faire décompresser

À cette personne si particulière qui a pu occuper mon esprit tant et si bien que j'ai presque oublié la véritable raison de ma présence dans ce pays

Merci au Canada et particulièrement au Québec de m'avoir accueilli et offert deux si belles années qui resteront sans doute gravées parmi les plus mémorables de ma vie

REMERCIEMENTS

Mes premiers remerciements vont évidemment à mon directeur de recherche Benoît Robert qui a su prendre de longues réunions de discussions pour débattre sur ce projet qui aura connu de nombreux revirements. Mais son influence ne s'arrête pas au simple cadre académique, j'aimerais surtout me souvenir du party d'été qui m'a offert de superbes souvenirs et permis de faire des rencontres vraiment sympathiques !

Mes remerciements vont également à Yannick Hémond qui a toujours su trouver les points qui aurait pu me faire défaut, qui a su me montrer tout ce qui relevait du perfectible dans mes réflexions. Sa justesse d'analyse sur certains point et ses questionnements ont su me faire progresser dans mon projet, mais aussi sur ma façon d'être.

Grâce à Benoît et Yannick je suis en mesure aujourd'hui de dire que ma façon de réfléchir et d'approcher certaines problématiques a évoluée vers quelque chose de plus cadré et rigoureux (« oublies tes tableaux », « arrête avec tes élans de style »...).

Un remerciement spécial à Luciano Morabito, dont le départ du CRP nous a privés d'un voisin de bureau absolument génial par sa gentillesse et sa courtoisie.

Je voudrais remercier dans un second temps tous mes collègues de bureau ! Ils sont nombreux, mais méritent chacun un petit mot :

Les deux joyeux lurons du C314.3, Amine et Thierry que j'ai le plaisir d'appeler mes amis plus que mes collègues. Ils ont constitué pour moi les éléments qui ont rendus les longues journées de bureau un peu plus supportables par leur bonne humeur et leurs talents cachés (jonglage, histoires sentimentales et/ou de soirée rocambolesques, parachute et j'en passe...).

Delphine, la « maman » des élèves du CRP, toujours de bon conseil et souriante qui a su m'expliquer beaucoup sur le fonctionnement du centre et sur la vie en recherche.

Marieme et Luisa les petites nouvelles qui auront, je l'espère, des projets prometteurs et passionnants.

RÉSUMÉ

Parmi les différentes technologies disponibles pour faciliter le quotidien des organisations, les technologies de l'information et de la communication s'imposent comme l'une des révolutions à laquelle font face les organisations dans ces dernières années, et ce notamment avec l'avènement des technologies liées au nuage (cloud-computing).

En posant l'utilisation réelle comme la base de réalisation d'un portrait de vulnérabilité, ce projet vise dans son ensemble à sensibiliser les gestionnaires des PME à un nouveau type d'approche des risques développé par le Centre risque & performance de Polytechnique Montréal : l'approche par conséquences. Cette approche s'oppose à la vision classique du risque qui place l'aléa et sa probabilité d'occurrence au centre de la plupart des analyses des risques.

Ce mémoire de maîtrise présente dans un premier temps une revue de littérature portant sur la vision de la vulnérabilité technologique classique, puis expose des concepts permettant de proposer aux gestionnaires des petites et moyennes entreprises une analyse approchant cette vulnérabilité technologique sous un nouvel angle : celui des utilisations réelles faites des différentes technologies. Par la suite, une étude de cas est présentée. Elle incorpore les retours obtenus en procédant à des réunions avec les gestionnaires des PME partenaires et amène finalement à une nouvelle définition de la vulnérabilité face aux utilisations des TIC. Enfin, le dernier chapitre propose une discussion et ouvre la voie vers de potentiels travaux dans cette direction.

ABSTRACT

Among all the technologies that are available for businesses in order to improve their daily activities, the information and communication technology are today seen as one of the most challenging changes in their business model especially with the cloud-computing based technologies soaring.

Considering the actual real usage of ICT in business as a basis for a vulnerability analysis, the project tries to make business owners aware of the existence of a new way to approach risk analysis: “l’approche par conséquences” which you can translate by consequences’ approach. This approach is an alternative to the traditional way most risk management methods adopt which consist in establishing the probability of an unwanted event to happen.

This master report presents in its first part a literature review about the general view of classic technological vulnerability, then highlights the concepts that are used to propose to small and medium business owners an analysis based upon the actual real usage of their technologies in their business. Therefore, a case study is presented, including the feedback received during the meetings with the project partner SMBs and leads to a new definition of technological vulnerability. The last chapter is a discussion about the results of the tests that were made and opens on future potential projects.

TABLE DES MATIÈRES

DÉDICACE III

REMERCIEMENTS IV

RÉSUMÉ V

ABSTRACT VI

TABLE DES MATIÈRES VII

LISTE DES TABLEAUX X

LISTE DES FIGURES XI

LISTE DES SIGLES ET ABRÉVIATIONS XII

LISTE DES ANNEXES XIII

CHAPITRE 1 INTRODUCTION 1

CHAPITRE 2 REVUE DE LITTÉRATURE 2

2.1 Les petites et moyennes entreprises 2

2.1.1 En Europe 2

2.1.2 Au Canada 3

2.1.3 Autres caractéristiques 3

2.2 Technologie d'information et de communication 5

2.2.1 Les TIC : une nécessité pour se développer 5

2.2.2 Caractérisation des TIC et données 6

2.3 L'utilisation effective des TIC dans les PME 11

2.3.1 Utilisation selon un aspect technique 11

2.3.2 Utilisation selon un découpage par activités ou secteurs 12

2.3.3 Utilisation par processus globaux 14

2.4 Risque et vulnérabilité 17

2.4.1 Définition du risque dans le domaine industriel....17
2.4.2 La vulnérabilité comme composante du risque....18
2.4.3 L'approche par conséquences des risques et de la vulnérabilité....21
2.5 Méthodes de gestion pour les PME....22
2.5.1 Mehari Pro....24
2.5.2 Octave-S....27
2.5.3 L'analyse de la vulnérabilité....30
2.6 Synthèse de la revue de littérature....32
CHAPITRE 3 QUESTION DE RECHERCHE....33
3.1 Définition du problème et contexte de recherche....33
3.2 Objectif de recherche....34
3.3 Méthodologie de recherche....34
CHAPITRE 4 VERS UNE VULNÉRABILITÉ LIÉE À L'UTILISATION....36
4.1 Définition du système à l'étude : l'organisation....36
4.2 Utilisation et contraintes....37
4.2.1 Catégories....37
4.2.2 Critère qualitatif de criticité....39
4.2.3 Notion temporelle....40
4.3 Les technologies de l'information et de la communication....41
4.3.1 Caractérisation des technologies de l'information....42
4.3.2 Caractérisation des technologies de la communication....42
4.3.3 Caractérisation des données / informations....43
4.4 Caractérisation de la défaillance....43
4.4.1 Défaillance de l'organisation....44

4.4.2 Défaillance d'un système lié aux TIC 44
4.4.3 Catégorie d'impact pour l'organisation 46
4.5 Synthèse du chapitre 48
CHAPITRE 5 PORTRAIT DE VULNÉRABILITÉ 50
5.1 Inventaire de contraintes 50
5.1.1 Identification des contraintes 50
5.1.2 Caractérisation des contraintes 52
5.1.3 L'utilisation des TIC pour satisfaire des contraintes 54
5.2 Caractérisation de la défaillance 56
5.2.1 Conséquences 56
5.2.2 Marge de manœuvre 57
5.2.3 La détectabilité 58
5.3 Analyse organisationnelle et technique 58
5.3.1 Analyse organisationnelle 59
5.3.2 Analyse technique 62
5.3.3 Mise en regard des analyses 63
5.3.4 Une définition de la vulnérabilité spécifique aux TIC 67
5.4 Synthèse de l'étude de cas présentée 68
CHAPITRE 6 RÉSULTATS, PERSPECTIVES ET CONCLUSION 70
6.1 Résultats 70
6.2 Perspectives de recherche 71
6.3 Conclusion 72
BIBLIOGRAPHIE 73
ANNEXES 80

LISTE DES TABLEAUX

Tableau 2.1 : Caractéristiques des PME en Europe (Commission européenne, 2013) 2

Tableau 2.2 : Données, information et connaissance selon différents auteurs (interprété et traduit de Stenmark, 2002) 7

Tableau 2.3 : Les différentes méthodes adaptées aux PME selon l'ENISA (2006, adapté et traduit) 23

Tableau 5.1 : Exemple de l'identification des contraintes d'une PME partenaire 51

Tableau 5.2 : Caractérisation des contraintes 53

Tableau 5.3 : Utilisation des TIC pour la satisfaction des contraintes identifiées et des critères impactants 55

Tableau 5.4 : Analyse organisationnelle 60

Tableau 5.5 : Analyse technique 62

Tableau 5.6 : Mise en regard des analyses organisationnelle et technique 65

LISTE DES FIGURES

Figure 2.1 : Découpage des utilisations selon le principe de chaîne de valeur avec ajout de la notion de spatialisation de l'activité (amont/cœur/aval) 14

Figure 2.2 : Triptyque du risque du CRP (adapté de Petit, 2009) 18

Figure 2.3 : Représentation du risque naturel (Petit, 2009, adapté de MEEDA, 2008b) 20

Figure 5.1 : Cas idéal : adéquation 64

Figure 5.2 : Temps de reprise sous-estimé du point de vue organisationnel : exemple de la facturation (échelle temporelle non uniforme) 66

LISTE DES SIGLES ET ABRÉVIATIONS

La liste des sigles et abréviations présente, dans l'ordre alphabétique, les sigles et abréviations utilisés dans le mémoire ou la thèse ainsi que leur signification. En voici quelques exemples :

PME	Petites et moyennes entreprises
TIC	Technologies de l'information et de la communication
TI	Technologies de l'information
TC	Technologies de la communication
PCO	Plan de Continuité des Opérations
ERP	Entreprise Ressource Planner (Progiciel de Gestion Unifié)
CRM	Client Relation Manager (Progiciel de gestion de la relation client)
B2B	Business to Business
AFNOR	Association Française de Normalisation
CRP	Centre risque & performance
ENISA	Europea Union Agency for Network and Information Security (Agence européenne chargée de la sécurité des réseaux et de l'information)
Mehari	Méthode Harmonisée d'Analyse des Risques
Octave	Operationnal Critical Threat, Asset, and Vulnerability Evaluation

LISTE DES ANNEXES

ANNEXE A – FICHE PRE-RENCONTRE 80

CHAPITRE 1 INTRODUCTION

Les enjeux soulevés par la gestion de la technologie en général dans les entreprises sont aujourd'hui la source de nombreux questionnement du point de vue de la recherche. Face à l'augmentation importante de son implication dans le monde industriel depuis les années 1980, la technologie fait l'objet d'études et de tentative de classification de son utilisation. Les premières études sur l'utilisation des technologies portent sur la capacité de celles-ci à fournir aux entreprises un avantage concurrentiel (Porter, 1985) ou à changer leur manière de voir la compétition avec leur environnement (McFarlan, 1984). Ces premières approches ont également souligné que la technologie, et plus particulièrement celle liée à la communication ou l'obtention d'information, constituait une opportunité pour les entreprises de se démarquer et de profiter d'une croissance supérieure à celle pronostiquée (Benjamin, 1983). Les premières intégrations de la technologie d'information en tant que partie intégrante des processus d'administration et de production des entreprises remontent à la fin des années 80 lorsque l'ordinateur personnel et l'accès à internet deviennent disponibles pour un public moins restreint que l'armée ou les centres de recherche. Cette intégration amène vers une nouvelle conception de l'ingénierie industrielle qui lie les technologies de l'information avec la transformation et la refonte des processus de développement de l'industrie (Davenport & Short, 1990).

Aussi, la technologie est devenue une composante essentielle du monde industriel et confère aux entreprises des moyens de contrôle et d'action plus rapides et efficaces. Cependant, cette augmentation du niveau technologique (compris comme étant le rapport du nombre d'activités effectuées à l'aide de la technologie par rapport au nombre total d'activité de l'entreprise) introduit de nouveaux risques liés aux différentes technologies pour les entreprises (Rainer et al, 1991). Cette exposition à de nouvelles menaces nécessite une prise en compte de la part des gestionnaires des entreprises dans leur processus de gestion.

Avec l'aide de PME de la région montréalaise, le Centre risque & performance de Polytechnique Montréal s'est proposé pour développer une méthodologie adoptant une vision novatrice concernant l'analyse de vulnérabilité technologique : celle de l'utilisation réelle faite des technologies dans les organisations. Ce mémoire en présente le développement et les principaux résultats.

CHAPITRE 2 REVUE DE LITTÉRATURE

Ce chapitre présente dans un premier temps les grandes définitions des concepts clés de cette étude à savoir : les petites et moyennes entreprises qui constituent l'objet d'analyse de cette étude et les technologies de l'information et de la communication qui constituent le sujet d'analyse. La notion de vulnérabilité sera abordée et décrite et une emphase sera portée sur la vision développée au Centre risque & performance de Polytechnique Montréal. Par la suite sera exposée la littérature qui traite de l'utilisation des technologies de l'information et de la communication par les petites et moyennes entreprises. Une dernière partie exposera, enfin, les méthodes aujourd'hui utilisées par les PME dans le cadre de leur processus de gestion des risques liés aux TIC.

2.1 Les petites et moyennes entreprises

Le tissu économique mondial est partagé entre deux types d'entreprises : celles considérées comme de grandes entreprises et celles considérées comme des petites et moyennes entreprises (auxquelles on référera à partir de maintenant par l'acronyme PME).

Storey (1994), déclare qu'il n'existe pas de définition simple et généralisable pour tous des PME du fait que la définition même varie selon la plupart des pays, des auteurs ou des organismes d'étude qui définissent les PME. Depuis, un certain formalisme a été adopté dans le cadre de l'étude des PME et des caractéristiques précises ainsi que des seuils ont été déterminés afin d'encadrer leur étude.

2.1.1 En Europe

La Commission européenne emploie depuis plusieurs années, dans ses différents rapports concernant les PME, une classification des PME qui se subdivise elle-même en 3 sous catégories : micro, petite et moyenne.

Tableau 2.1 : Caractéristiques des PME en Europe (Commission européenne, 2013)

Company category	Employees	Turnover	or	Balance sheet total
Micro	<10	< € 2 million		< €2 million
Small	<50	< €10 million		< € 10 million
Medium	<250	< €50 million		< €43million

Cette classification est donc basée sur 3 critères :

- Le nombre d'employés, dont le nombre pour appartenir à la catégorie des PME ne doit pas excéder 250 personnes
- Le chiffre d'affaires, qui ne doit pas dépasser les 50 millions d'euros

  OU

- Les bénéfices, qui ne doivent pas excéder les 43 millions d'euros

Les PME représentent ainsi en 2013 près de 66,8% de la masse salariale européenne et participent à hauteur de 57,9% de la valeur ajoutée totale générée par le secteur non financier (Commission européenne, 2013). Ces chiffres tendent à prouver l'importance de cette catégorie d'organisation pour le continent européen.

2.1.2 Au Canada

Au Canada, l'appartenance d'une organisation à la catégorie des PME est souvent basée uniquement sur son nombre d'employés. Le Ministère de l'Économie, de la Science et de l'Innovation du Québec partage avec l'Europe la limite haute de 250 employés. Industrie Canada fixe de son côté la limite d'appartenance à la catégorie des PME à 500 employés.

En 2014, les PME ont en moyenne participé à hauteur de 30% du produit intérieur brut du Canada. Elles y emploient durant l'année 2015 plus de 8,2 millions de personnes soit près de 70,5% de l'ensemble de la main-d'œuvre du secteur privé (Industrie Canada, 2016). On peut également ainsi juger de l'importance dans le tissu économique canadien des PME.

2.1.3 Autres caractéristiques

Outre les caractéristiques exposées précédemment pour juger de l'appartenance d'une organisation à la catégorie des PME, une dernière caractéristique existe et permet de bien cerner les spécificités des PME notamment en termes de gestion. Il s'agit du principe de proximité (Torrès, 1997) qui se comprend comme étant la conséquence de la taille réduite des PME sur leur organisation et leur méthode de gestion. On assiste alors à deux phénomènes propres aux PME (les éléments suivants sont une adaptation des propos de Torrès) :

- La centralisation de la gestion

Le mode de gestion de la PME est bien souvent centralisé. On assiste parfois même à une incarnation de la gestion en la personne du dirigeant-propriétaire ou gestionnaire. Aussi: « an essential characteristic of a small firm is that is managed by its owners or part owners in a personalised way, and not through the medium of a formalized management structure » (Bolton,1971). S'il faut souligner une chose sur la centralisation des PME, c'est que celle-ci est accentuée par la proximité entre le dirigeant et les employés. Cette proximité amplifie la centralisation et élimine le besoin de passer par des intermédiaires contrairement à un grand groupe dans lequel des mécanismes de transmissions sont nécessairement utilisés afin de canaliser le flux de sources potentielles d'informations. Cette centralisation permet de mettre en valeur une caractéristique essentielle des PME : le gestionnaire possède une vision d'ensemble et est à l'origine de la prise de décision.

- Une spécialisation moindre

Pour ce qui traite des PME : « Au plan fonctionnel, on observe le plus souvent une difficulté à différencier les tâches, différenciation qui ne va s'affirmer qu'avec l'accroissement de la taille » (Marchesnay, 1990). La différenciation dans la division horizontale est floue pour une PME. Tant dans l'administration que dans la production, la notion de fonctions multiples est courante pour les employés. Il peut ainsi être commun que le gestionnaire de la PME soit à l'origine un spécialiste du domaine d'activité de l'organisation. Il sert donc à la fois dans l'administration en tant que preneur de décision, mais aussi en tant que spécialiste de son domaine et est alors amené à passer du côté opérationnel (Marchenay, 1990). Il obtient de cette façon également une meilleure visibilité des activités de son organisation.

Synthèse sur les PME

Les PME constituent un ensemble non négligeable du tissu économique d'Amérique du Nord et d'Europe. Elles sont caractérisées par leur nombre d'employés, leur taille réduite et par la proximité organisationnelle que celle-ci impose. Le principe de proximité de Torrès souligne enfin que le gestionnaire possède une vision d'ensemble de la PME et qu'il constitue un élément capital dans le processus de prise de décision.

2.2 Technologie d'information et de communication

La problématique des technologies de l'information et de la communication est depuis une vingtaine d'années en plein essor du fait de la croissance rapide des technologies associées comme les téléphones intelligents ou encore la technologie du nuage (cloud). Près de 70% des PME interrogées à propos des TIC voient dans ces technologies un véritable tremplin pour leur activité et prévoient d'investir des ressources financières dans l'acquisition et le développement de solutions allant dans ce sens, particulièrement dans tout ce qui touche au nuage (cloud) (Deloitte, 2014).

2.2.1 Les TIC : une nécessité pour se développer

La mise en place de nouvelles technologies afin de libérer des ressources et/ou adopter de nouveaux plans d'activités pour pouvoir rester compétitifs est depuis longtemps vue comme une nécessité à laquelle aucune PME ne peut échapper. (Julien & Jacob, 1993)

C'est pourquoi s'intéresser aux TIC est devenu un incontournable de la gestion organisationnelle. La problématique des TIC est transversale à l'ensemble du fonctionnement des organisations, dans la mesure où aujourd'hui l'ensemble des processus et activités sont monitorées, productrices d'informations diverses qu'il convient de traiter, d'analyser ou encore d'archiver ou au contraire nécessitent certaines informations pour être complétés (Chaffey & White, 2010). L'intervention de la technologie permet aux organisations d'effectuer ces activités avec plus de facilité, moins de ressources et tend ainsi à les rendre plus performantes. Les TIC répondent ainsi à plusieurs besoins des organisations : augmenter leur efficacité opérationnelle, améliorer la communication avec les fournisseurs, améliorer leurs relations client, conserver un avantage sur leurs concurrents, améliorer la collaboration avec leurs partenaires, améliorer la satisfaction des employés, répondre à une attente des clients qui s'attendent à un prestataire à jour avec les avancées technologiques (Harindranah et al, 2008).

Attention cependant, si la mise en place bien planifiée des TIC dans une PME permet l'avènement d'un réel avantage concurrentiel, l'intégration sans plan clair peut vite devenir problématique. Le coût financier de mise en place de manière non réfléchie ainsi que le maintien des différentes solutions peuvent devenir un véritable gouffre financier qui représente un risque non négligeable pour les PME par l'augmentation des risques associés.

2.2.2 Caractérisation des TIC et données

La première définition à donner lorsque l'on parle de technologies de l'information (TI) ou de technologies de communication (TC), est la notion de donnée.

2.2.2.1 Les données

Les données constituent l'élément le plus simple dans un processus de sauvegarde. Une donnée ayant subi un traitement, c'est-à-dire qui a été soit analysée soit mise en regard d'autres données constitue ce qu'on appelle alors une information. Un ensemble d'information, agrémenté d'une notion de jugement et de perception humaine, forme quant à lui ce que certains appellent la connaissance (Stenmark, 2002). Ces trois concepts ont été maintes fois étudiés dans la littérature et le tableau 2.2 regroupe une partie des résultats existants concernant la définition de chaque concept :

Tableau 2.2 : Données, information et connaissance selon différents auteurs (interprété et traduit de Stenmark, 2002)

Auteurs	Données	Information	Connaissance
Wiig	-	Faits organisés afin de décrire une situation ou une condition	Vérité et croyance, perspectives et concepts, jugements et attentes, méthodologies et savoir-faire
Nonaka et Takeuchi	-	Un flux de messages doté de sens	Engagement et croyance créés par ces messages
Spek et Spijkervet	Des faits encore non interprétés	Donnée dotée de sens	La capacité d'associer ce sens à d'autres faits
Davenport	Observations simples	Donnée avec un intérêt et un but	Information qui a un intérêt pour l'utilisateur
Davenport et Prusak	Un ensemble de faits distincts	Un message qui vise à changer la perception du récepteur	Expériences, valeurs, vision et information contextualisée
Quigley et Debons	Un texte qui ne répond à aucune question particulière	Texte qui répond aux questions : qui, quand, quoi, où	Texte qui répond aux questions pourquoi et comment
Choo et al.	Des faits et des messages	Des données assemblées et faisant sens	Des croyances justifiées

Un tiret signifie que le(s) auteur(s) n'a pas donné de définition de cet objet.

Les données possèdent une caractéristique reconnue et commune pour tous les auteurs : il s'agit d'un ensemble d'éléments dénué de sens a priori. Tout ce qui est stocké peut-être appelé donnée. Ce n'est que lorsque organisé et présenté de façon sensée que cela peut devenir une information (Kedar, 2009).

Dans le cadre des TIC, les deux éléments existent et cohabitent. Certaines données sont conservées à l'état brut en attendant d'être exploitées tandis que d'autres sont agrégées et sauvegardées sous la forme de rapport ou présentées directement dans des indicateurs de gestion. Le domaine de l'analytique de données massives (big data), qui représente un acteur majeur de l'utilisation des TIC, est d'ailleurs la science qui vise aujourd'hui à permettre une collecte, un raffinage, un stockage et enfin une utilisation profitable de la multitude de données présente sur les différents réseaux le tout dans des proportions toujours plus vastes.

2.2.2.2 Les technologies de la communication

Une définition de la communication en général permet de faire apparaître 3 types de communication différente (Rogers, 1986) :

- La communication d'humain à humain (« interpersonnel channels ») ou face à face.
- Une communication de masse, d'un émetteur unique vers des récepteurs multiples aidé par le relais de la technologie (les médias télévisés en sont un bon exemple).
- La communication interpersonnelle assistée par ordinateur, constitue un hybride des deux premières catégories. Possédant des caractéristiques des deux catégories précédentes, elle ne s'inscrit ni dans la catégorie face à face ni dans la catégorie un à plusieurs. Prenons comme exemple le téléphone, la visioconférence, les systèmes de courriel, etc.

Les technologies de la communication (TC) s'inscrivent dans cette dernière catégorie. Ils sont à la croisée de l'acquisition de données de multiples origines pour une redistribution à de multiples récepteurs.

Les TC sont donc à l'origine l'ensemble des outils qui permettent de faire transiter des données d'un ensemble d'émetteurs vers un ensemble de récepteurs. Les TC sont également majoritairement utilisés dans le cadre de la récolte de données et de la transmission d'informations une fois un processus de traitement effectué. Donner une définition technique de ce que représentent les TC n'est pas un point abordé souvent dans les publications scientifiques, qui préfèrent aborder le problème directement dans le cadre de leur champ de recherche en passant par des définitions basées sur le rôle rempli par les TC.

2.2.2.3 Les technologies de l'information

L'expression technologie de l'information a été utilisée pour la première fois par la Harvard Business Review pour faire la distinction entre les machines fabriquées afin de remplir un nombre de tâches spécifiques limitées et les machines de calcul pouvant être paramétrées pour de nombreuses tâches variables (Leavitt & Whisler, 1958).

L'expression TI est communément synonyme d'ordinateurs et de réseau d'ordinateurs, mais peut être utilisée pour désigner plus largement toute technologie qui est utilisée pour générer, sauvegarder et manipuler de l'information de manière électronique (Chandler & Munday, 2012).

Les TI s'inscrivent donc dans la catégorie des machines capables d'exécuter un nombre de tâches différentes élevé à condition de les programmer de la bonne manière. C'est particulièrement vrai pour ce qui touche au traitement des données, tâche de plus en plus importante et consommatrice de temps et de ressource avec l'augmentation du volume de données généré par l'activité des organisations (Isaac, Campoy & Kalika, 2007), qualifié par certains comme un « tsunami de données » (CGI, 2013).

La fin de la partie 2.2.1.1 montre que les données n'acquièrent un sens pour l'humain que lorsqu'elles sont correctement traitées et ordonnées en groupe afin de former des ensembles cohérents et dotés de sens. C'est à ce niveau qu'interviennent donc les TI. Aussi, dans sa définition la plus simple, la technologie de l'information fait référence aux équipements et logiciels qui permettent de manipuler et de traiter les données. Les TI incluent un nombre élevé de couches d'équipement physique (hardware) par exemple un serveur ou bien l'ordinateur portable personnel d'un employé. L'ensemble des équipements périphériques comme les tablettes, les stockages externes, les appareils d'enregistrements et même les téléphones intelligents peuvent être intégrés dans la notion de TI. La notion de TI intègre on l'a dit également l'ensemble des logiciels, des outils de virtualisation, de management ou d'automatisation qui pourrait se trouver dans l'environnement de l'organisation. On parle plus généralement d'applications qui peuvent alors prendre un nombre de formes presque illimitées : base de données, système de transaction, outil de commande en temps réel, serveur de courriel, serveur de soutien de site web, système de gestion des ressources (ERP) et système de gestion des relations clients (CRM), etc. (TechTarget, 2015).

Aujourd'hui, la notion de TI va même au-delà de l'environnement de l'organisation en incluant des notions comme celle de l'externalisation des structures informatiques : on parle du nuage (cloud-computing).

2.2.2.4 Le nuage (Cloud)

Avec l'avènement des réseaux de fibre optique offrant des débits de connexion de l'ordre du gigabit par seconde, les technologies infonuagiques (cloud-computing) représentent l'avenir des TIC pour les PME (Deloitte, 2014). En effet, la technologie infonuagique présente un avantage important pour les PME : elle ne nécessite a priori pas d'investissement en terme matériel. Offert comme un service d'entreprise à entreprise (business to business ou B2B), le cloud permet aujourd'hui aux organisations de faire héberger l'ensemble de leurs applications et données sur des serveurs

administrés et maintenus par des prestataires externes. Cette technologie permet donc de faire des économies en termes de matériel, mais permet également de s'affranchir des contraintes liées à la maintenance et la sécurité dont la responsabilité est transférée au prestataire (Marston et al., 2011).

Il n'est plus possible de douter que le nuage représente un bond en avant pour les TIC. En plus de proposer des solutions permettant des économies certaines (achat et maintenance), ce type d'architecture informatique permet l'unification des notions de TI et de TC en englobant l'ensemble des deux notions dans une seule solution. Cette solution présente d'autres nombreux avantages que les PME ne peuvent pas ignorer comme l'interopérabilité, une connectivité globale, une redondance des systèmes de sauvegarde et de sécurité, etc. (Avram, 2014).

L'expression « bond en avant » est à nuancer dans la mesure où le passage à la technologie de l'infonuagique ne vient pas sans une véritable période d'adaptation dont la durée peut varier d'une entreprise à une autre. Il est donc important de réaliser que l'avantage apporté par ce type de technologie peut ne pas apparaitre instantanément et peut nécessiter certains efforts organisationnels supplémentaires dans les entreprises.

2.2.2.5 La convergence des technologies

La convergence de l'informatique et de la télécommunication, mise en évidence notamment avec l'apparition du nuage, a donné naissance à ce que l'on appelle aujourd'hui les technologies de l'information et de la communication (Bouwman et al, 2005) ou TIC.

Ainsi on peut définir les TIC comme étant :

> L'ensemble des matériels, logiciels et services utilisés pour la collecte, le traitement et la transmission de l'information. Dans l'usage, on trouve le pluriel comme le singulier, tant en anglais qu'en français. L'emploi du pluriel est cependant plus logique, étant donné qu'il s'agit ici de plusieurs ensembles de techniques (sens moderne de technologie), dont chacun correspond à une technologie différente. Bien que le terme technologies de l'information ait toujours englobé les technologies de l'électronique, de l'informatique et des télécommunications, certains semblent sentir le besoin, aujourd'hui, de marquer le tournant dans l'évolution des TIC que représentent les développements du multimédia et des télécommunications, notamment les réseaux et Internet. C'est la raison pour laquelle on rencontre maintenant les expressions nouvelles technologies de l'information et de la

> communication ou technologies de l'information et de la communication, ainsi que leur forme abrégée (NTIC, TIC) et leurs nombreuses variantes. (Gouvernement du Québec, 2007)

Aujourd'hui, la convergence des technologies est, pour le monde de la recherche, un fait. La preuve la plus évidente de ce changement de vision est la quasi-inexistence des publications scientifiques récentes qui ne comportent que l'un des deux termes sans inclure le second (technologie de l'information et technologie de la communication). L'avènement d'internet et des systèmes de réseau élargis a définitivement scellé les deux notions au sein de la notion plus large de TIC.

2.3 L'utilisation effective des TIC dans les PME

Selon Devaraj & Kohli (2003), l'utilisation réelle des TIC par les organisations constituait le champ d'étude manquant dans le cadre d'une étude plus large portant sur la relation entre les organisations et les TIC. Aussi, afin de comprendre le rôle des TIC dans les organisations et plus particulièrement les PME, il est important de se pencher sur l'usage réel de ces organisations des différentes technologies présentées précédemment. Dans la littérature scientifique, la notion d'utilisation des TIC par les PME est un sujet abordé depuis moins d'une vingtaine d'années et qui expose différents angles d'approche. Plusieurs de ces angles vont être exposés dans la suite de cette partie sous la forme d'une liste de découpage provenant d'études de type empirique. Certaines présentations ont été approfondies plus en détail, car elles allaient de concert avec l'approche privilégiée dans cette étude.

2.3.1 Utilisation selon un aspect technique

Une classification possible des utilisations des TIC est celle qui se concentre essentiellement sur les fonctions techniques remplies par les différentes TIC. Cette classification répond à la question naturelle : « Que fait à proprement parler chaque technologie ? ». Ce type de classification ne considère que l'aspect technique, c'est-à-dire que les utilisations des TIC ne sont vues que par rapport à la fonction spécifique associée à chaque outil. Dans cet esprit, une analyse portant sur les PME de la région d'Oman a établi une analyse fine au niveau de l'infrastructure des TIC utilisées en entreprise et sur les fonctions primaires que ceux-ci sont supposés remplir par leur utilisation (Ashrafi & Murtaza, 2008). L'étude établit une classification des utilisations en rapport avec la

place dans l'infrastructure technologique que représente chaque élément affilié aux TIC. Les catégories retenues pour cette classification sont :

1. Les utilisations liées à la sécurité réseau
2. Les utilisations liées au stockage de données
3. Les utilisations liées à des progiciels
4. Les utilisations liées à des logiciels de productivité
5. Les utilisations permettant l'établissement d'un réseau sans fil (outils matériel et logiciel)
6. Les utilisations permettant l'établissement d'un réseau filaire (outils matériel et logiciel)
7. Les utilisations liées à l'interface homme/réseau (ordinateur de bureau, ordinateur portable ou encore tablette, etc.)

Cette classification des utilisations des TIC pourrait tout à fait être adaptée à une analyse de la vulnérabilité d'un point de vue technique. Une personne travaillant dans le domaine particulier de la gestion informatique verra un avantage certain à décomposer un processus en différentes actions techniques uniques permettant de cerner et d'adapter les procédures de reprise en cas de problème. En revanche, en se plaçant du point de vue du gestionnaire de l'organisation, cette classification arrive rapidement à ses limites par manque de connaissance du point de vue technique sur le sujet (Ashrafi & Mutaza, 2008).

2.3.2 Utilisation selon un découpage par activités ou secteurs

Pour catégoriser l'utilisation des TIC dans une organisation d'un point de vue moins technique, l'une des méthodes qui apparait comme envisageable est le découpage de l'organisation en secteurs ou type d'activités suivi d'un inventaire des différents systèmes utilisés dans les secteurs identifiés. Cette méthode a été appliquée par de nombreuses études dont certaines vont être exposées ici.

L'étude effectuée et publiée par Harindranath, Dyerson et Barnes (2008) adopte une méthodologie de découpage par activités et retient plusieurs catégories concernant les utilisations des TIC dans les PME anglaises. Ces catégories, au nombre de huit, apparaissent dans leur sondage au moment où les répondants sont interrogés sur les niveaux d'adoption technologique dans leurs différentes activités. Les catégories d'utilisation retenues sont :

1. Contrôle des stocks
2. Vente et marketing
3. Design
4. Recherche de marché
5. Gestion documentaire
6. Gestion de production et systèmes de contrôle
7. Gestion des ressources humaines
8. Gestion de l'ERP (entreprise ressource planner, ou en français progiciel de gestion intégré).

Schubert et Leimstoll (2007) prennent quant à eux le parti de mener une analyse sur l'importance de l'utilisation réelle faite des TIC dans les organisations et en se concentrant sur les secteurs spécifiques de l'organisation dans lesquels ils interviennent. Ils décident d'ajouter une couche supplémentaire dans le découpage en procédant à un regroupement lié à la position dans le processus global en discernant, l'amont qui traite des activités liées à tout ce qui est préalable à l'activité principale de l'organisation (fournir un produit ou un service), le cœur qui s'attache à ce qui se déroule dans le périmètre direct de l'organisation et qui vise à réaliser les activités principales de l'organisation et enfin l'aval qui regroupe les processus liés à la mise à disposition du fruit de l'activité principale pour les clients de l'organisation. Cependant ce regroupement n'est utilisé que pour la présentation des statistiques, l'étude ayant été réalisée à partir du découpage fin. Leur découpage peut-être résumé comme présenté à la figure 2.1. Leur découpage se rapproche de celui par chaîne de valeur (Porter, 1985) qui faisait déjà une différenciation entre activités primaires (de base) et activités secondaire (de soutien).

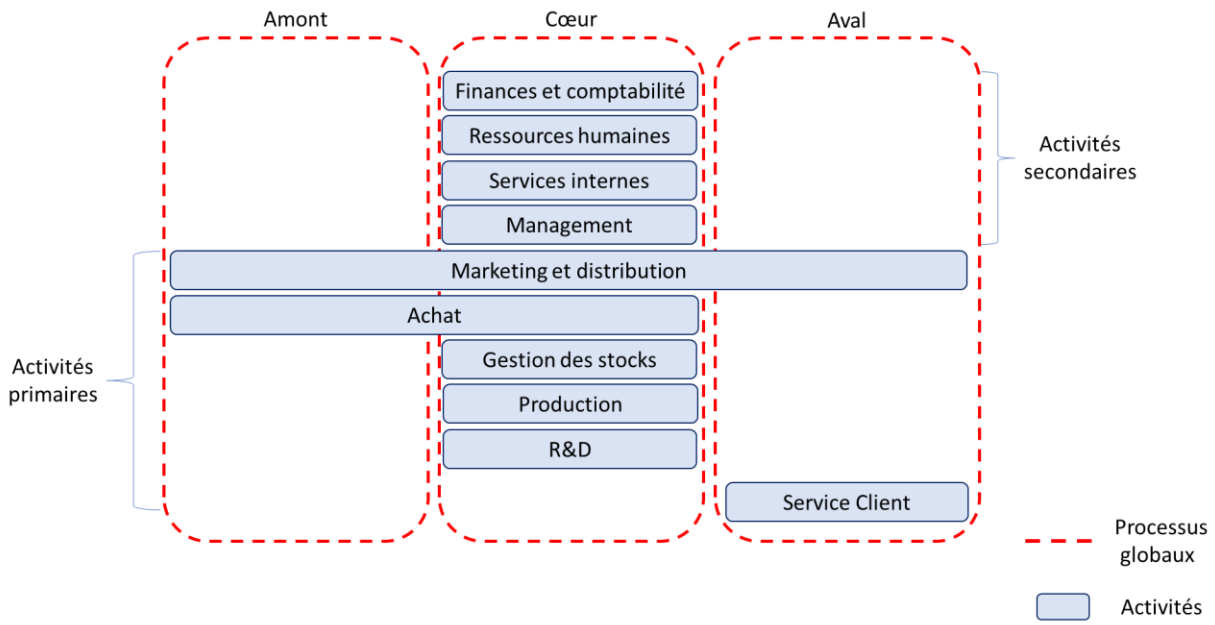

Figure 2.1 : Découpage des utilisations selon le principe de chaîne de valeur avec ajout de la notion de spatialisation de l'activité (amont/cœur/aval)

Aussi à la fin de leur découpage, Schubert et Leimstoll (2007) peuvent proposer deux interprétations : une interprétation par activités d'utilisation et une interprétation par ce qu'on pourrait appeler processus globaux. Cette dernière interprétation n'est cependant pour Schubert et Leimstoll qu'une manière de résumer leur étude. Certains auteurs ont décidé au contraire d'en faire le cœur de leur étude en proposant des découpages plus vastes comme présentés dans la section suivante.

2.3.3 Utilisation par processus globaux

Une autre catégorisation récurrente quand il est question de l'utilisation des TIC se base sur un découpage de l'organisation en termes de processus ayant une portée vaste. Le but de ce type de découpage est de réussir en général à faire un bilan complet des activités liées aux TIC dans l'organisation en faisant apparaître moins de 5 catégories différentes. Ceci permet aux auteurs d'élargir le questionnement sur d'autres critères, comme le niveau d'incorporation des TIC dans les processus (Caldeira & Ward, 2002) ou encore sur les facteurs d'acceptabilités des TIC dans chaque processus (WestFocus, 2007).

L'étude proposée par Caldera & Ward en 2002, développe un modèle d'utilisation basé sur quatre grandes catégories d'utilisations liées à différents grands processus des organisations. Selon eux, l'utilisation des TIC peut être classée dans une des catégories suivantes :

1. Les systèmes liés à la gestion administrative, qui regroupent l'ensemble des équipements ou applications liées à la prise de décision et la gestion de l'organisation. Cet ensemble est considéré par les auteurs de l'étude comme celui dans lequel les TIC se sont le mieux incorporées, car il s'agit de celui dans lequel le nombre de données à traiter était le plus important.
2. Les systèmes liés à la composante de production l'organisation, qui représente pour les auteurs l'ensemble des processus liés à l'activité principale de l'organisation (l'étude portant majoritairement sur des PME manufacturières).
3. Les systèmes liés au contrôle et au suivi intégré à la fois au niveau de la production et au niveau de l'administration. Ces systèmes permettent notamment la génération et la mise à jour de tableau de bord et d'indicateurs qui permettent une meilleure gestion globale de l'organisation.
4. Les systèmes permettant l'interaction avec l'environnement de l'organisation. Les auteurs catégorisent ici les systèmes qui permettent d'avoir des contacts avec l'extérieur, qu'il s'agisse des clients, des fournisseurs ou toute autre entité hors du périmètre de l'organisation (les entités gouvernementales pas exemple).

Ce type de découpage ne cible pas un processus ou un département particulier de l'organisation, mais plutôt un objectif global imposé par le fonctionnement même de celle-ci.

Le projet Abandoned Heroes, conduit par l'équipe de travail WestFocus, composée de membres de sept universités londoniennes, dont Royal Holloway, Brunel et Kingston, vise par une analyse des utilisations des TIC dans les PME anglaises à étudier les « bonnes pratiques » et facteurs qui favorisent l'acceptabilité des diverses technologies reliées aux TIC. Pour ce faire, le découpage adopté par le consortium diffère de celui proposé par Caldeira et Ward. Plutôt que de voir les utilisations associées à des processus gravitant autour des différents processus de l'organisation, WestFocus présente un modèle d'utilisation qui gravite autour de l'organisation elle-même. Ainsi le nombre de catégories distinctes est réduit à seulement trois (WestFocus, 2007) :

1. Les utilisations liées à la promotion de l'organisation et ses produits. Très centrée autour de la notion de technologies de la communication, cette catégorie vise à regrouper l'ensemble des fonctions liées purement aux clients (actuels et potentiels) de l'organisation.
2. Les utilisations liées aux opérations de l'organisation. Cette catégorie englobe l'ensemble des TIC impliquées dans les activités interne à la structure organisationnelle. On y retrouve les outils administratifs, mais aussi ceux alloués à la gestion de production ou encore au contrôle.
3. Les utilisations liées à la collaboration. Cette dernière catégorie d'utilisation regroupe l'ensemble des TIC qui permettent à l'organisation d'échanger données et informations avec ses partenaires d'affaires (fournisseurs, sous-traitants, etc.).

Cette classification pourrait s'apparenter au découpage global proposé par Schubert et Leimstoll (2007) avec le trio amont/cœur/aval, mais diffère dans la mesure où les catégories ne possèdent pas de découpage plus fin.

Synthèse sur l'utilisation des TIC dans les PME

L'utilisation des TIC dans les PME a fait l'objet de nombreuses études empiriques qui ont chacune adopté des modèles de classification de ces utilisations différents. Cependant, 3 grands types se dégagent : l'approche technique, l'approche par secteur et l'approche par processus globaux. Les deux derniers modèles proposent des découpages adaptés à une analyse basée sur la connaissance des gestionnaires en s'éloignant du point de vue purement technique pour embrasser un point de vue adapté à la gestion. Aussi il semblerait plus pertinent dans le cadre d'une analyse de vulnérabilité visant à être effectuée par un gestionnaire de s'orienter vers un découpage d'utilisations de cet acabit.

Cette partie démontre également que les TIC sont utilisées dans l'ensemble des activités des PME. Cette omniprésence dans l'ensemble des processus pourrait donc en cas de défaillance avoir des conséquences sur de nombreux processus ou activités de l'organisation. Aussi il semblerait pertinent de s'intéresser maintenant à la notion de vulnérabilité, induite par l'utilisation des TIC dans les PME.

2.4 Risque et vulnérabilité

« Chaque nouvelle technologie semble amener son lot de nouvelles vulnérabilités pour l'utilisateur, une vulnérabilité à l'accident, à la maladie, à la dégradation environnementale ou encore à la dégradation sociétale » (traduction libre de Martin, 1996). Les TIC ne sont pas une exception à ce constat réalisé à la fin des années 90, évoluant sans cesse et autorisant les utilisateurs d'avoir de plus en plus de fonctions automatisées ou grandement simplifiées. Cet ajout de fonctionnalités entraîne le passage d'une activité humaine vers une activité technologisée (Powell & Dent-Micallef, 1997) et engendre ainsi l'apparition de nouveaux risques et vulnérabilités associés qu'il convient de prendre en compte et d'intégrer dans la politique de gestion de l'organisation.

Aussi afin de cerner le concept de vulnérabilité et particulièrement celui en rapport avec les TIC, il est nécessaire de passer en revue les différentes définitions et modèles d'approche de la vulnérabilité ainsi que les critères qui servent à la mesurer dans la littérature. Pour ce faire, il faudra au préalable présenter une définition du risque de manière générale afin de situer les deux notions l'une par rapport à l'autre.

2.4.1 Définition du risque dans le domaine industriel

Du point de vue le plus proche de notre étude, celui adoptant la vision industrielle, le risque est un concept qui regroupe trois notions bien connues des gestionnaires de risques (ISO, 2009)

- Un objet de risque ou système analysé
- Des causes ou aléas caractérisés par une probabilité d'occurrence qui entraînent la perte partielle ou totale d'une ressource pour l'organisation
- Des conséquences qui caractérisent les impacts potentiels sur la structure de l'organisation en termes d'objectifs et de missions

On remarque qu'avec cette dernière définition, dans le cadre de la gestion des risques, la vulnérabilité en tant que telle n'apparaît pas. Cependant, elle peut être comprise comme une composante du risque en raffinant les notions exposées ci-dessus (Robert, 2007 et Petit, 2009). Ce raffinage proposé dans le cadre des travaux du CRP de Polytechnique Montréal peut se représenter par le triptyque du risque.

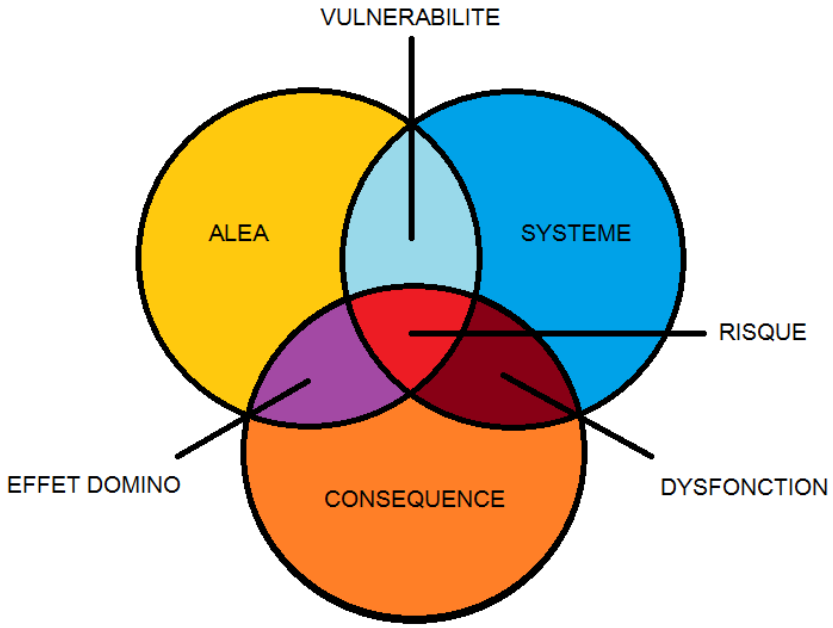

Figure 2.2 : Triptyque du risque du CRP (adapté de Petit, 2009)

Cette figure reprend les 3 caractéristiques du risque exposées par exemple dans la définition selon l'AFNOR et ajoute une analyse plus fine des interactions entre ces différentes composantes, faisant apparaître de nouvelles caractéristiques du risque.

La vulnérabilité est l'interaction des aléas et du système à l'étude. La notion sera approfondie par la suite.

Les effets domino qui lient aléa et conséquences caractérisent la capacité des conséquences d'un aléa à engendrer un nouvel aléa ayant lui-même de nouvelles conséquences sur le système (Robert & Morabito, 2009).

Enfin la dysfonction représente l'effet des conséquences sur le système analysé en termes de fonctionnement (Petit, 2009).

2.4.2 La vulnérabilité comme composante du risque

La vulnérabilité apparaît donc comme une composante du risque qui se trouve être à la croisée des aléas et du système étudié. La notion possède de nombreuses définitions qu'il est important de passer en revue afin de cerner au mieux une approche valide.

Un grand nombre d'auteurs ont utilisé à tort le terme vulnérabilité afin de référer au risque lui-même particulièrement dans le domaine des sciences sociales (Cardona, 2003). La notion de vulnérabilité doit plutôt être vue comme un facteur de risque interne au sujet ou système qui est exposé à un aléa et correspond à sa prédisposition intrinsèque à être affecté ou à subir des dommages. (Cardona, 2003).

Une vision simple propose de voir le risque comme le croisement de l'aléa (un évènement probable) et la vulnérabilité à cet aléa. C'est le cas notamment en ce qui concerne le risque naturel qui est la plupart du temps vu comme le rapport entre la nature, qui se caractérise par l'apparition d'évènements aléatoires (aléas) et la société, qui présente de par son organisation et sa composition des prédispositions à subir des dommages de la part de ces aléas (la vulnérabilité) (Peinturier, 2015).

La Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) établit quant à elle le risque comme étant un triplet : une méthode d'attaque, un élément menaçant et une vulnérabilité (DCSSI, 2006). Ici la vulnérabilité prend la définition d'une faille qui peut être exploité par des personnes ou programmes afin de s'introduire dans un système auquel ils ne devraient pas avoir accès et en prendre le contrôle.

Robert (communication personnelle, 2016), opte aussi pour une vision de la vulnérabilité comme l'une des trois composantes du risque. Selon lui, « le risque correspond à l'évaluation de la vulnérabilité d'un système face à des aléas susceptibles d'engendrer des conséquences ». La vulnérabilité est ici alors la caractérisation de la sensibilité d'un système susceptible de subir des défaillances en fonction de son état. L'aléa est un évènement naturel ou anthropique (interne ou externe) susceptible de survenir (Robert et al., 2004). Les conséquences sont quant à elles la caractérisation d'une défaillance en termes d'effets sur un environnement (humain, technologique, socio-économique, biophysique, etc.).

Les travaux de Petit (2009) décrivent également la vulnérabilité comme une composante du risque, mais cette fois-ci dans le cadre spécifique de la cybernétique. Pour lui, le concept de vulnérabilité doit alors intégrer dans la notion de risque la caractérisation temporelle du milieu et la sensibilité de celui-ci face à un aléa. Le risque est ici la combinaison de trois composantes, l'aléa, le système et les conséquences. Le propos est illustré par Petit à l'aide de la métaphore du glissement de terrain : l'aléa matérialisant le potentiel de glissement de terrain, le système matérialisé par le village à proximité et les conséquences correspondant à l'affectation du village en cas d'éboulement.

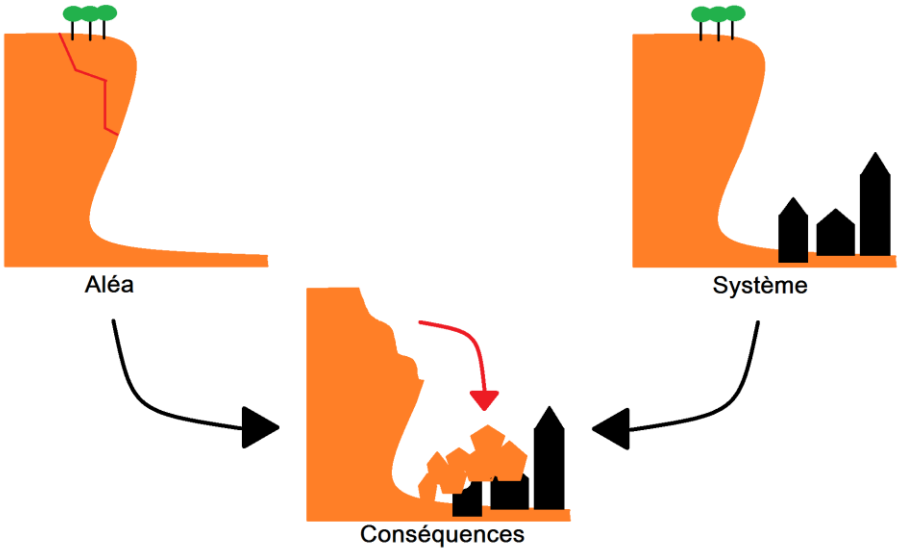

Figure 2.3 : Représentation du risque naturel (Petit, 2009, adapté de MEEDA, 2008b)

La notion temporelle que Petit désire intégrer s'explique avec l'image du village qui, vu comme un système, est amené à évoluer sur une période de temps donnée. La population peut varier, la disposition des bâtiments et leur capacité de résistance aux dommages potentiels d'un éboulement peuvent être amenées à varier, les périodes de l'année peuvent influer sur la population totale mise en danger, etc. Ce changement dans le temps est selon lui une caractéristique peu prise en considération et qu'il a tenté d'implémenter dans sa thèse. Cette image de la variation temporelle peut s'appliquer aux autres systèmes étudiés, qu'ils s'agissent d'organisations ou d'administrations (Petit, 2009). La notion de vulnérabilité est donc obtenue à la croisée de plusieurs critères distincts et Petit ajoute à la définition de vulnérabilité de Robert, la notion de variabilité temporelle du système jusqu'alors absente.

2.4.3 L'approche par conséquences des risques et de la vulnérabilité

Le CRP, mené par Benoît Robert, entreprend depuis plusieurs années de mettre en lumière un nouveau type d'approche en ce qui concerne le risque en général. Cette approche favorise la centralisation de la problématique du risque autour des conséquences que celui-ci a sur les différents systèmes analysés. Contrairement à l'approche classique probabiliste qui s'intéresse aux probabilités d'avènement des aléas, l'approche par conséquence a pour but de s'assurer que la notion de risques soit circonscrite à ce qui est vraiment important pour les organisations : assurer la continuité des opérations et augmenter leur résilience aux conséquences des aléas (Robert & Morabito, 2009). L'approche par conséquences présente un avantage par rapport à la vision probabiliste : elle permet d'établir en premier lieu un portrait des conséquences inacceptables sur l'organisation plutôt que de faire d'abord un portrait des aléas susceptibles d'avoir des conséquences critiques selon leur probabilité d'occurrence. Par conséquent, cette approche permet de ne pas laisser de côté des risques dont la probabilité d'occurrence serait trop faible pour être prise en compte. Elle met l'accent sur la préparation des organisations face aux conséquences des aléas et non les aléas eux-mêmes.

Aussi la notion de vulnérabilité devrait aller dans ce sens selon le CRP. La notion même de vulnérabilité devrait pouvoir se définir comme étant une composante qui fait intervenir des paramètres non reliés au probabilités pour se concentrer sur la notion de conséquence pour les organisations analysées.

Synthèse sur le risque et la vulnérabilité

La vulnérabilité est une notion qui possède de nombreuses définitions en fonction du milieu d'étude. La vision classique de la gestion des risques, caractérise les notions de risque et de vulnérabilité en se basant en général sur une approche probabiliste liée à l'occurrence des aléas. La vision développée par le CRP se détache en amenant la notion d'approche par conséquence qui relègue l'intervention des probabilités d'occurrence des aléas au second plan par rapport aux conséquences réelles sur les organisations analysées. La notion de vulnérabilité temporelle est également soulevée par l'ajout de cette composante par Petit dans les travaux du CRP.

2.5 Méthodes de gestion pour les PME

La partie portant sur l'utilisation effective des TIC dans les PME (section 2.3) a permis de mettre en évidence que les TIC d'une organisation font aujourd'hui partie des ressources importantes de son activité économique, qu'il s'agisse d'outils servant au pilotage de l'activité, à la gestion de l'administration ou encore à la réalisation des activités d'affaire. Or ces technologies amènent leur lot de vulnérabilités (cf. introduction 2.4) dans les organisations qui les adoptent. La gestion des TIC d'une organisation est donc un requis important pour la poursuite de ces activités. Une gestion des risques peu effective peut entraîner de nombreuses conséquences non négligeables pour la viabilité de l'organisation.

Organiser cette sécurité n'est pas chose facile, c'est pourquoi il existe des méthodes reconnues pour aider les responsables informatiques à mettre en place une bonne politique de gestion et de sécurité et à procéder aux audits permettant d'en vérifier l'efficacité. Le groupe de travail mis en place par l'ENISA (European Union Agency for Network and Information Security) a publié en 2006 une liste présentant les méthodes de gestion des risques technologiques les mieux adaptées aux PME. Le tableau ci-après présente les différentes méthodes retenues et certaines de leurs caractéristiques :

Tableau 2.3 : Les différentes méthodes adaptées aux PME selon l'ENISA (2006, adapté et traduit)

	Austrian security handbook	Dutch A&K analysis	Ebios	IT-Grund-schutz	Mehari	Octave
Méthode d'identification (MI) et/ou méthode de gestion (MG)	MI / MG	MI	MI / MG	MI / MG	MI	MI / MG
Gratuité	Oui	Oui	Oui	Oui	Non	Oui
Portée d'utilisation	Autriche	Pays-Bas	France, Espagne, Italy, Belgique, Amérique du Sud	Allemagne, Autriche,Suisse, Estonie	France et pays francophones	États-Unis
Information adaptée aux PME	Oui	Oui	NA	Oui	Oui	Oui
Outils associés disponibles	Prototype gratuit	Oui Certains sont gratuits	Oui Logiciels open source	Oui Payant	Oui Payant	Oui Payant
Applicable sans consultant	Oui	Oui	Non	Oui	Oui	Oui

Ce tableau met donc en lumière 5 méthodes a priori adéquates pour mener à bien un processus d'analyse et de gestion des risques technologiques dans les PME. La méthode Ebios ne présente pas de documentation spécifique pour les PME et est par conséquent jugée inapplicable dans ce cadre. De plus, compte tenu de la portée de ce travail de recherche (le Canada et plus particulièrement le Québec), le choix a été fait de porter une attention particulière à la méthode francophone : Mehari par intérêt culturel, ainsi qu'à la méthode privilégiée aux États-Unis : Octave par intérêt géographique. Ces deux méthodes possèdent des versions simplifiées et adaptées à la structure des PME : Mehari Pro et Octave-S. Ces deux variantes seront donc présentées afin de mettre en lumière leurs cheminements et caractéristiques.

2.5.1 Mehari Pro

2.5.1.1 Présentation

La Mehari (MEthode Harmonisée d'Analyse de RIsques) a été développée par le Clusif (CLUb de la Sécurité de l'Information Français) en 1996. Depuis lors, elle a été mise à jour de nombreuses fois et a fait l'objet d'un transfert vers le CLUSIQ (CLUb de la Sécurité de l'Information Québécois) qui la distribue aujourd'hui. Elle est dérivée des méthodes Melisa et Marion, deux méthodes d'analyse aujourd'hui délaissées (Meharipédia, 2015). Cette méthode est aujourd'hui utilisée dans le secteur public ainsi que dans les grandes organisations. Une variante de Mehari, Mehari Pro est une démarche ciblée pour les PME qui suit le même processus d'analyse et d'évaluation des risques. Elle utilise la même base de connaissance adaptée à la structure analysée (CLUSIF, 2013).

Outre la documentation disponible gratuitement en ligne, il existe de nombreux outils informatiques affiliés à Mehari afin de proposer une analyse des risques pour les organisations. Le plus communément utilisé aujourd'hui, car sponsorisé par le CLUSIF est le logiciel RISICARE distribué par la société BUC S.A. en France. Cet outil de gestion intègre tous les principaux outils d'analyse développés dans Mehari et fournit une synthèse des risques potentiels que l'organisation devrait considérer dans sa stratégie de protection (CLUSIF, 2010).

2.5.1.2 Objectifs

Mehari Pro vise principalement à faciliter l'adoption par les PME d'une méthode d'analyse et de gestion des risques. Le domaine d'analyse est centré autour de la sécurité de l'information en accord avec la norme ISO/IEC 27005 :2011. Les objectifs qu'elle poursuit sont les suivants :

- Identification exhaustive et précise des différentes situations de risques qui peuvent affecter l'organisation.
- Permettre une analyse directe et personnalisée des situations de risques explicitées par des scénarios de risques prédéfinis.
- Proposer la mise en place de mesure de sécurité ayant pour but de réduire les risques jugés inacceptables et permettre d'évaluer par la suite le niveau de risque résiduel dans l'organisation.

2.5.1.3 Étapes

1. Mehari Pro reprend la méthodologie générale de Mehari. Celle-ci se divise en 9 étapes distinctes.
2. Identification des situations de risques

Il existe deux façons de procéder :

- L'approche directe qui utilise un système d'échelle de dysfonctionnement. Le but étant d'identifier les dysfonctionnements ou les aléas qui pourraient influer sur les activités de l'organisation. On obtient alors : une description des différents types de dysfonctionnement possibles ; une définition des paramètres qui caractérisent l'ampleur de chaque dysfonctionnement ; la définition des seuils de criticité qui permettent de quantifier l'importance de chaque dysfonctionnement.
- Une approche systématique utilisant des scénarios préétablis et fournis par Mehari. Méhari propose à la fois une base de données pour les scénarios, mais aussi des modèles d'audit appropriés à l'évaluation des risques.

3. Évaluation de l'exposition

L'exposition provient de l'interaction entre le système organisationnel et son environnement. Mehari préconise l'utilisation d'une échelle à 4 niveaux afin de caractériser l'exposition à un aléa. Cette échelle va de « très peu probable » : chance d'occurrence extrêmement faible même sans aucunes mesures d'évitement ou de mitigation en place, à « haute exposition » : aléa qui dans le contexte actuel deviendra inévitable à court terme sans actions d'évitement majeures mises en place.

4. Évaluation des facteurs dissuasifs et préventifs

Un audit des facteurs d'évitement et des mesures préventives en place dans l'organisation

5. Évaluation des facteurs de protections, de palliation et de récupération

Un audit des moyens de protection, des méthodes palliatives et des mesures de récupération en place dans l'organisation

6. Évaluation de la probabilité d'occurrence

Cette étape vise à évaluer la potentialité d'occurrence d'un aléa. La question posée est : « Quelle est la probabilité que l'aléa analysé se produise effectivement ? ».

7. Évaluation de l'impact intrinsèque

À cette étape on évalue l'impact des aléas considérés précédemment indépendamment des mesures de sécurité mises en place dans la structure de l'organisation. Mehari fournit dans le cadre de son analyse une grille à remplir afin d'évaluer cet impact intrinsèque. Cette grille peut être utilisée dans le processus d'évaluation des risques.

8. Évaluation de l'impact et de la réduction d'impact

À partir de l'évaluation de l'impact intrinsèque, Mehari propose une évaluation automatique de l'impact après réduction en considérant les niveaux des mesures renseignées à l'étape 4. Cette évaluation se fait en deux étapes : évaluation d'un indicateur de réduction d'impact suivi d'une évaluation de l'impact réduit. L'indicateur permet de jauger le niveau de réduction induit par les différentes mesures en place dans l'organisation évaluées précédemment.

9. Évaluation globale du risque

Une fois l'ensemble des scénarios analysés, Mehari présente les principaux risques auxquels doit faire face l'organisation.

10. Décision concernant l'acceptabilité du risque

Étape finale qui a pour but de définir si un risque est acceptable ou non pour l'organisation. Dans le cas d'un risque non acceptable, il doit être mis en place un processus de création d'un mécanisme de contrôle afin de protéger l'organisation du dit risque.

2.5.1.4 Résultats et prise de décision

Mehari Pro apporte une première réponse complète aux nécessités de gestion des risques des PME. Les audits proposés par la suite amènent vers la génération de plan d'actions concrets. Cette méthode vise la prise de décisions en termes de changement au niveau de la politique de sécurité afin que les vulnérabilités constatées lors des audits atteignent un niveau de sécurisation / protection satisfaisant du point de vue de l'administration de la PME. La prise de décision porte aussi sur les notions d'acceptabilité du risque. L'organisation doit se poser la question de la pertinence de la couverture de certains risques par rapport à d'autres.

Mehari dans sa version générale est une méthode qui s'avère très populaire auprès des organisations de taille conséquente. Bien que la méthode fournisse de nombreuses bases de données afin de simplifier les audits et les caractérisations, elle reste une méthode lourde à mettre en place qui requiert des ressources conséquentes. Mehari Pro se présente ici comme une variante allégée, mais cependant complète destinée aux PME. En proposant de mettre la méthodologie générique de Mehari à disposition des PME, le Clusiq a assuré la couverture de l'ensemble du panel des organisations présentes sur le marché et répond à un besoin grandissant mis en évidence par la partie traitant des PME et les vulnérabilités amenées par les TIC et leurs utilisations.

2.5.2 Octave-S

2.5.2.1 Présentation

La méthode Octave-S (Operationnally Critical Threat, Asset, and Vulnerability Evaluation – Small) est une méthode dérivée de la méthode pour les grandes organisations OCTAVE développée par l'université Carnegie Mellon. Les deux méthodes ont vu le jour en 2003. La méthode Octave-S est encore aujourd'hui en version bêta et propose aux utilisateurs une expérience de gestion adaptée à la petite structure comprenant entre 20 et 80 salariés. Octave-S a été élaborée afin de permettre à une équipe de 3 à 5 personnes de mener à bien une analyse complète de l'organisation dans laquelle elle est déployée. Pour cela, l'accent a été porté sur deux points : la limitation du rassemblement d'informations nécessaire et l'allègement du nombre d'actifs analysés (Caralli, Stevens, Young & Wilson, 2007). Cette méthode sera présentée ci-après.

2.5.2.2 Objectifs

Les méthodes OCTAVE (normale et S), partagent les mêmes objectifs. Ils sont au nombre de 5 et sont sujets à modification en fonction des besoins de l'organisation analysée.

- Identification des systèmes contenant de l'information et ayant une importance pour l'organisation.
- Prioriser l'analyse de risques sur ces systèmes.
- Considérer les relations entre la criticité de ces systèmes, les menaces qui pèsent sur ces systèmes et les vulnérabilités (à la fois organisationnelles et technologiques) qui pourraient affecter ces systèmes.

- Évaluer les risques dans un contexte opérationnel. Leur utilité dans le processus général de l'organisation et leur vulnérabilité aux failles de sécurité.
- Créer une stratégie de protection basée sur des formations afin d'atteindre une amélioration organisationnelle et produire des plans de gestion des risques.

2.5.2.3 Étapes

La méthode Octave-S possède 3 phases subdivisées en processus (notés S).

- Phase 1 : Construire des profils de menace des actifs. Durant cette phase, l'organisation identifie et définit des profils de menace (c'est-à-dire les menaces potentielles ainsi que leur probabilité d'occurrence) pour 3 à 5 actifs liés à l'information.
    - Processus S1 : Identification des informations organisationnelles. L'équipe d'analyse identifie quelles sont les informations importantes pour l'organisation, définit des critères d'impact sur l'organisation et établit le niveau actuel des pratiques de sécurité de l'organisation.
    - Processus S2 : Créer des profils de menace. L'équipe d'analyse sélectionne 3 à 5 actifs d'information et définit les requis de sécurité associés ainsi que les profils de menace pour ces actifs.
- Phase 2 : Identifier les vulnérabilités de l'infrastructure. Cette étape nécessite la conduite par l'équipe d'analyse d'un diagnostic approfondi de l'infrastructure technologique ainsi que des pratiques utilisées afin de raffiner les profils de menace.
    - Processus S3 : Examen de l'infrastructure informatique en lien avec les actifs critiques. L'équipe analyse les moyens d'accès aux différents systèmes et sous-systèmes qui supportent les actifs critiques et détermine dans quelle mesure leur processus technologique protège ces actifs.
- Phase 3 : Développer la stratégie de sécurité et les plans associés. Durant cette phase, les risques concernant les actifs critiques sont évalués et des mesures de protection et d'atténuation sont définies à un niveau stratégique.

- Processus S4 : Identification et analyse de risques. L'équipe d'analyse évalue l'ensemble des risques sur les actifs par rapport à leur impact et optionnellement en termes de probabilité.
- Processus S5 : Développement de plans de protection et d'atténuation. L'équipe d'analyse développe des plans de protection et d'atténuation basés sur des formations de sécurité à l'échelle de l'organisation dans son ensemble.

2.5.2.4 Résultats et prise de décision

Octave-S est une méthode qui pousse les organisations vers la réalisation de plans de protection et d'atténuation au niveau stratégique. La prise de décision concerne surtout la mise en place de nouvelles formations afin de préparer au mieux les employés concernés aux différents scénarios possibles envisagés pour les actifs liés aux informations dans l'organisation.

Largement utilisée aux États-Unis, cette méthode présente un double avantage pour les PME. Le premier concerne la quantité de ressources nécessaires à sa mise en place. L'allègement des phases d'analyse par la réduction du nombre d'objets analysés (3 à 5 actifs) permet aux organisations de réaliser des économies en termes de ressources. Le second avantage est lié au type de mesures qu'Octave-S propose de mettre en place. Contrairement à d'autres méthodes qui proposent la mise en place de mesures techniques supplémentaires (nécessitant a priori un investissement pour l'achat des équipements nécessaires), Octave-S se focalise sur la mise en place de formations et sur la préparation de l'organisation dans son ensemble à faire face à des défaillances du point de vue des TIC (Caralli et al., 2007).

Un point est cependant soulevé par les concepteurs de la méthode elle-même : Octave-S par sa construction et son modèle d'application est une méthode qui s'avère peu flexible aux exigences de l'organisation qui l'applique. En effet les différentes fiches qui permettent de conduire les différentes analyses sont très dirigées et ne permettent que peu d'écart au cheminement d'analyse prévu par les concepteurs (Caralli et al., 2007). C'est le prix à payer entre le méthode générique Octave et son homologue destinée aux PME.

Après ces deux présentations de méthodes adaptées aux PME, il semble nécessaire de revenir sur le point important pour le projet : l'analyse de vulnérabilité proposée par chaque méthode.

2.5.3 L'analyse de la vulnérabilité

Ainsi, dans l'optique de se diriger vers la proposition d'une nouvelle approche de la vulnérabilité, il convient de faire une synthèse sur la façon dont est abordée la vulnérabilité dans les méthodes présentées précédemment. Pour cela on propose de classer les méthodes en fonction des critères pris en compte lors de l'étape d'évaluation des vulnérabilités.

2.5.3.1 L'analyse de vulnérabilité par l'aléa et sa probabilité d'occurrence

Comme exposé dans la partie 2.4 une façon d'analyser la vulnérabilité d'un système est de chercher à déterminer la probabilité que celui-ci défaille ou qu'un aléa entraînant sa défaillance advienne, et ce quelle que soit la cause ou l'utilisation qu'il soit effectivement faite du système dans l'organisation. Dans cette mesure, les méthodes qui utilisent cette vision de la vulnérabilité accordent une grande importance aux lois statistiques qui déterminent ces probabilités d'occurrence et peu d'importance à la notion d'utilisation réelle des TIC. Cette façon de procéder est une des raisons qui rend les méthodes de gestion des risques, utilisant ce principe, lourdes à mettre en place : l'étape d'analyse requiert de se concentrer sur un grand nombre de systèmes qui ne sont pas nécessairement utilisés par les activités importantes de l'organisation. En effet la probabilité nulle n'existant pas, l'ensemble des aléas possibles doit être considéré et analysé. La méthode Mehari (et par conséquent Mehari Pro) par exemple se base essentiellement sur le doublet exposition et probabilité afin de déterminer la vulnérabilité des différents actifs informationnels d'une organisation. En passant par un ensemble de scénarios, l'approche probabiliste est nécessaire. De trop nombreux scénarios entraîneraient une lourdeur d'analyse que les concepteurs de Mehari ont voulu éviter. Aussi l'analyse du contexte de l'organisation constitue une part non négligeable de l'analyse de vulnérabilité en vue d'étudier la probabilité des différents scénarios proposés par la base de connaissance de la méthode.

2.5.3.2 L'analyse de la vulnérabilité basée sur l'importance des données et critères associés

La méthode Octave-S fait apparaître la notion de vulnérabilité lors de sa seconde phase (Phase 2, Processus S3). Celle-ci préconise l'analyse de vulnérabilité basée sur le lien entre les outils technologiques critiques mis en évidence en phase 1 avec leur intervention dans le processus technologique global de l'organisation. Cette vision de la vulnérabilité rejoint celle que le CRP souhaite introduire dans l'analyse de vulnérabilité. En effet, Octave-S fait bel et bien appel à la

notion d'utilisation dans le processus d'analyse de vulnérabilité de sa méthode de gestion de risques. Cependant Octave-S présente deux particularités : la première est de se concentrer exclusivement sur les données et leurs contenants. Cependant l'activité d'une organisation et sa vulnérabilité concernant l'utilisation des TIC ne peut se réduire à la catégorie qui concerne le stockage des données et les données en elles même. La seconde particularité d'Octave-S est de partir d'un inventaire exhaustif des actifs informationnels pour aller vers leurs utilisations dans l'organisation Un portrait complet de vulnérabilité devrait selon le CRP faire intervenir la notion d'utilisation plus tôt et être le centre d'intérêt dans le cadre d'une analyse de vulnérabilité.

Synthèse

L'analyse de la vulnérabilité des organisations face aux TIC apparaît sous deux formes différentes dans les méthodes présentées plus tôt. Mehari propose une vision probabiliste et basée sur des scénarios afin d'estimer cette vulnérabilité. Octave-S propose une approche axée vers l'utilisation des outils, mais n'en fait qu'un point d'étape et laisse de côté une grande partie des outils technologiques contenus dans les TIC en se concentrant sur les données et leurs contenants. Or les TIC, comme présentées en introduction, avant d'être un moyen de manipulation de données, représentent un ensemble bien plus vaste orienté vers une mission : faciliter les activités des utilisateurs humains et leur permettre de libérer des ressources afin de pouvoir investir ces dernières dans d'autres tâches. Le point qui semble manquer dans les différentes approches est l'inclusion de l'utilisation des TIC comme point de départ d'une analyse de vulnérabilité.

Fort de ces différents constats il semble intéressant pour les PME d'avoir à leur disposition une méthodologie d'analyse de vulnérabilité qui prendrait en compte l'utilisation réelle faite de l'ensemble des technologies liées à l'information et la communication et en ferait la base de cette analyse. Si l'on parvenait à inclure cette notion dans une méthodologie d'analyse, de nombreux progrès pourraient en découler concernant l'approche de la vulnérabilité en termes d'utilisations et pourraient être intégrés dans les méthodes précédentes afin de mieux appréhender la notion de vulnérabilité des organisations face à l'utilisation des TIC.

2.6 Synthèse de la revue de littérature

Cette revue de littérature a permis de souligner qu'aujourd'hui la problématique des TIC et en particulier leur utilisation réelle dans les organisations de type PME est un point sur lequel la recherche se penche et pour lequel elle a développé différents modèles de découpage associés. Si l'étude de la vulnérabilité et du risque associés à l'incorporation des TIC dans les différents pans de l'activité des PME ont fait l'objet de nombreuses recherches et ont été abordés par un certain nombre de méthodes de gestion des risques, il convient de souligner qu'un point important semble avoir été négligé ou ne pas encore avoir fait l'objet d'une contextualisation ni d'une conceptualisation : l'utilisation des TIC comme centre de l'analyse de la vulnérabilité d'une organisation. Ce manque de documentation ainsi que la volonté d'apporter l'esquisse d'une solution, on conduit le CRP à proposer un projet de recherche exploratoire en partenariat avec des PME québécoises.

Cette étude vise à proposer une variante de l'analyse de vulnérabilité des organisations en proposant d'inclure l'utilisation des TIC par les PME comme un point de départ pour une analyse de vulnérabilité. Cette analyse se veut orientée vers les utilisateurs et plus particulièrement le gestionnaire de la PME par rapport à la vision d'ensemble que lui confère la structure spécifique des PME.

CHAPITRE 3 QUESTION DE RECHERCHE

3.1 Définition du problème et contexte de recherche

Le CRP est actuellement au centre d'un projet global sur la résilience des PME. Le projet de recherche général est réalisé en collaboration avec des organisations classifiées comme des petites et moyennes entreprises de la région québécoise. Ces PME partenaires ont initié le projet en acceptant de faire l'objet d'analyses afin de développer des méthodes visant à leur donner une meilleure vision de leur capacité de résilience dans différents domaines (changement climatique, interdépendances internes et TIC). Dans ce cadre, des analyses préliminaires sur le niveau de résilience des partenaires du CRP ont démontré l'existence possible de vulnérabilités au niveau de l'utilisation des TIC.

Les différents points soulevés dans ce projet ont été les suivants :

- État des connaissances en matière de vulnérabilité technologique des organisations
- L'utilisation effective des TIC dans les PME
- La proposition d'un nouveau modèle de vulnérabilité lié aux utilisations

Le projet constitue une introduction à un problème plus global qu'est la résilience des petites et moyennes structures face aux TIC et leurs utilisations. Ce projet particulier a pour objectif de proposer une nouvelle approche de la vulnérabilité, de proposer une méthodologie afin d'établir un portrait de vulnérabilité en rapport avec l'utilisation des technologies d'information et de communication et enfin de valider cette méthode chez les différents partenaires. Ce projet s'inscrit donc bien dans l'ensemble de projets plus large qui vise à rendre les PME plus résilientes face aux technologies et aux vulnérabilités qui les accompagnent.

Après avoir exposé les différentes composantes du contexte qui entourent les PME et les technologies d'information et de communication, mais surtout la notion d'utilisation qui les accompagne, il vient naturellement à se poser la question de recherche :

Comment peut-on permettre à des gestionnaires de petites et moyennes entreprises de caractériser la vulnérabilité de leur organisation face aux technologies de l'information et de la communication et plus particulièrement par rapport à l'utilisation qui en est faite au sein de l'organisation ?

3.2 Objectif de recherche

Afin d'apporter une réponse à la question posée, le projet s'est défini comme suit :

1. Définir et vulgariser les notions de technologies de l'information et de la communication.
2. Caractériser les grandes catégories d'utilisations des TIC.
3. Définir la notion de vulnérabilité dans le contexte des TIC, proposer une caractérisation de cette vulnérabilité et valider une méthodologie adaptée aux structures de petite ampleur afin de pouvoir réaliser le portrait de vulnérabilité.

Afin de parvenir à réaliser les différents objectifs, plusieurs sous étapes ont été nécessaires :

- Réaliser une revue des différents systèmes technologiques existants au sein des organisations ainsi qu'une caractérisation de leur utilisation.
- Définir la vulnérabilité spécifique par rapport à l'utilisation des TIC.
- Proposer l'approche par utilisations et non par scénario ou par probabilité.
- Réaliser une première version des outils d'analyse.
- Effectuer la première itération de validation avec les partenaires.

3.3 Méthodologie de recherche

Le CRP inscrit sa méthodologie de recherche dans le cadre de la recherche-action soit « un processus collectif mettant en relation des chercheurs et des praticiens visant à résoudre un savoir en prise directe sur les pratiques des acteurs sociaux » (Merini & Ponté, 2008). La recherche-action vise à traduire un problème initial en une problématique théorique basée sur des hypothèses qui seront testées sur le terrain (Argyris, Putnam & MacClain Smith, 1985) et cette construction se réalise en collaboration avec les acteurs de terrain (Thietart, 2007). Le projet est effectué en partenariat avec des PME québécoises qui se sont portées volontaires pour développer les différents outils. Ici le problème initial se construisait autour de l'utilisation des TIC dans les organisations qui est trop souvent laissée pour compte dans les analyses de vulnérabilité.

Ce projet particulier constitue donc une première étape du processus global de recherche-action. Il s'agit du développement théorique qui sera proposé aux partenaires et qui nécessitera un retour de ces derniers afin d'évoluer dans des instances futures de développement.

Il existe deux intérêts simultanés à ce type de recherche. Il permet une avancée scientifique en testant son applicabilité et permet de résoudre un problème de l'organisation (O'Brien, 1998).

Synthèse

L'objectif du projet de recherche est de développer une méthodologie simple et peu exigeante en termes de ressources qui puisse être utilisée par les gestionnaires et qui permette d'établir le portrait de vulnérabilité spécifique aux TIC de leur organisation. L'un des objectifs principaux est d'inclure la notion d'utilisation et d'utilisateur dans l'analyse de vulnérabilité. Le projet s'achèvera sur la rencontre avec les partenaires du projet afin de juger la pertinence et la viabilité des questionnements et analyses proposés dans les outils. Les PME partenaires ayant elles-mêmes pris la décision de se préparer à faire face aux risques engendrés par les technologies d'information et de communication, les objectifs du projet de recherche et des PME se rejoignent. La validation des outils sera possible grâce à la méthodologie de recherche-action utilisée.

CHAPITRE 4 VERS UNE VULNÉRABILITÉ LIÉE À L'UTILISATION

Le projet de cette étude est donc de proposer une nouvelle approche du portrait de vulnérabilité liée à l'utilisation des TIC dans une organisation. Pour ce faire, la réflexion s'est basée sur une définition plus générale de la vulnérabilité utilisée au sein du CRP. Par la suite les concepts amenés par cette définition ont été déconstruits et rétablis afin de proposer un modèle de vulnérabilité adapté aux TIC et leurs utilisations.

La définition de vulnérabilité utilisée au sein du CRP est celle proposée par Benoît Robert, directeur du centre. Comme exposé dans la revue de littérature, « la vulnérabilité constitue la caractérisation dans le temps de la sensibilité d'un système susceptible de subir des défaillances en fonction de son état ». Cette définition s'applique dans le champ de l'analyse de vulnérabilité globale. L'étude suivante vise, entre autres, à adapter cette définition dans le cadre de la vulnérabilité des organisations liées à l'utilisation réelle des TIC.

Dans ce chapitre seront exposés les différents concepts et critères retenus en vue de proposer un portrait de vulnérabilité basé sur les utilisations des TIC dans les PME. La première partie concernera la définition du système analysé et de l'ensemble des paramètres influant dans la caractérisation de celui-ci. La seconde partie mettra en évidence un modèle simplifié sur la façon de considérer les TIC afin de les distinguer entre eux. La fin de ce chapitre fera enfin le lien entre la défaillance des TIC (qui sera caractérisée également) et la défaillance de l'organisation analysée.

4.1 Définition du système à l'étude : l'organisation

Le système à l'étude ici est une organisation de type PME dans son ensemble. La définition conservée sera celle ne faisant intervenir que le nombre d'employés avec une limite haute établie à 250. Ceci permet de se placer en accord avec le MESI au Québec et avec la Commission européenne. Celle-ci est caractérisée par un ou des objectifs principaux qui peuvent prendre plusieurs formes : produire un bien, délivrer un service, etc.

L'idée amenée par le principe de proximité des PME est que le gestionnaire se trouve au centre de l'activité et possède une vision d'ensemble qui devrait être utilisé afin d'obtenir un portrait à la fois global et précis des activités de l'organisation. C'est dans cette optique que les critères qui ont été retenus portent plus sur la dimension organisationnelle que sur la dimension technique. L'approche

proposée aura ainsi de meilleures chances d'être utilisable et d'être pertinente pour les gestionnaires voulant l'appliquer.

4.2 Utilisation et contraintes

Un point important du projet est de parvenir à introduire l'utilisation des TIC dans l'analyse comme point de réflexion central pour les gestionnaires des organisations. Pour cela les premières idées ont été de se tourner vers la proposition d'un découpage d'utilisation semblable à ceux vus dans la revue de littérature et particulièrement ceux basés sur le découpage par processus globaux. Cependant les interactions avec les organisations partenaires et particulièrement leurs dirigeants ont permis de mettre en lumière que ce type de découpage n'est pas assez porteur de sens pour les gestionnaires.

Les éléments qui, en revanche, prennent une dimension intéressante du point de vue des gestionnaires et qu'ils sont capables de lier avec les utilisations réelles des TIC sont ce que nous avons identifié comme les contraintes qui s'appliquent à l'organisation. En effet, outre les éléments constitutifs cités précédemment, l'organisation est soumise en permanence à des contraintes diverses. Ces contraintes doivent être gérées par l'organisation afin d'être respectées, car de celle-ci dépend l'activité de l'organisation. Or aujourd'hui l'utilisation importante des TIC dans les organisations entraîne que la plupart de ces contraintes font appel à ces mêmes TIC afin d'être satisfaites.

Afin de pouvoir discuter de manière plus spécifique des différentes contraintes identifiables dans l'organisation, une caractérisation s'est avérée nécessaire. Il est possible de discerner plusieurs catégories de contraintes que nous avons identifiées et classées :

4.2.1 Catégories

Le premier point important dans l'identification des différentes contraintes a été de définir des catégories générales. Six catégories prédéfinies de contraintes ont été mises en évidence et une septième propose un degré de liberté supplémentaire en proposant l'ajout d'une catégorie spécifique à l'organisation analysée.

- Contractuelles

Les contraintes contractuelles proviennent d'un engagement passé entre l'organisation et un acteur extérieur via un contrat reconnu et accepté par les deux parties.

Exemple : L'organisation doit livrer une quantité prédéfinie de produits finis à un client.

- Légales

Les contraintes légales font écho à tous les requis légaux que l'organisation se doit de respecter de par la nature de ses activités.

Exemple : La loi requiert que l'organisation remplisse une déclaration d'impôts une fois par an avant une certaine date.

- Organisationnelles

L'organisation s'impose un certain nombre de contraintes issues de sa règle ou politique de gestion interne. Bien souvent ces contraintes ont été développées et imposées par la volonté des dirigeants de l'organisation, y voyant un avantage concurrentiel à mettre en place ce type de contrainte dans leur organisation

Exemple : L'administration de l'organisation exige que les inventaires des stocks de matière première soient réalisés deux fois par mois.

- Techniques

Les contraintes techniques relèvent du domaine technique lié aux activités de l'organisation. Elles peuvent porter sur les équipements de l'organisation ou sur certaines étapes clés de la réalisation du processus industriel, etc.

Exemples : Certains tests sur les équipements de production ne peuvent pas être réalisés durant l'hiver en raison de la température.

L'obtention d'un type de matière première n'est possible que durant une période particulière.

- Économiques :

Les contraintes économiques portent sur l'ensemble des requis économiques que l'organisation doit respecter afin d'assurer sa pérennité financière.

Exemple : Les clients doivent payer sous 3 mois maximum, faute de quoi les payes ne pourront être assurées.

- Sécuritaires :

Les contraintes sécuritaires portent sur les conditions pour maintenir un environnement de travail sécuritaire pour le personnel, mais aussi pour la protection des biens et des actifs.

Exemple : Certaines zones doivent être dotées d'un accès restreint grâce à une carte d'accès magnétique

- Autre catégorie

D'autres types de contraintes peuvent être définis au besoin des organisations. Le but de cette catégorisation est d'offrir aux organisations un cadre leur permettant de ne pas omettre de contraintes afin d'avoir un portrait le plus complet possible.

La caractérisation d'une contrainte porte donc en partie sur sa nature. Cependant d'autres notions doivent être étudiées afin de pouvoir faire un portrait complet des différentes contraintes qui s'appliquent à une organisation. Aussi il est nécessaire d'introduire deux types distincts de contraintes : celles que l'on caractérisera d'obligatoires pour le bon fonctionnement de l'organisation et celles qu'on identifiera plutôt comme souhaitables pour l'organisation.

4.2.2 Critère qualitatif de criticité

Afin de classifier en termes de criticité, il semble important d'inclure dans la caractérisation de la vulnérabilité un critère portant sur le degré de nécessité pour l'organisation de satisfaire une contrainte. Plutôt que de baser ce critère sur une échelle quantitative (faible, moyen, haute par exemple avec des seuils à définir), le choix s'est porté sur un critère qualitatif qui fait la différence entre une contrainte non remplie ayant des effets inacceptables sur l'organisation et une contrainte que l'organisation peut se permettre de ne pas remplir.

Contraintes obligatoires

Les contraintes obligatoires sont celles dont le non-respect entraîne des conséquences considérées comme inacceptables par l'organisation. Les conséquences sur l'organisation peuvent être multiples : perte financière, dégradation de l'image, mise en danger du personnel, etc. La notion de non-acceptabilité des conséquences doit être établie par le gestionnaire de l'organisation. Certaines contraintes sont indiscutablement obligatoires comme par exemple l'obligation de fournir aux autorités compétentes une déclaration complète d'un point de vue fiscal.

Contraintes souhaitables

Les contraintes souhaitables sont celles qui ont été déterminées par l'administration de l'organisation comme aidant à l'atteinte des objectifs ou comme favorisant le fonctionnement global de l'organisation sans pour autant que leur non-respect n'entraîne des conséquences suffisantes sur l'organisation pour être considérées comme critique. Ces contraintes sont bien souvent le fruit d'une réflexion de l'administration basée sur l'expérience de leur activité. On retiendra particulièrement tout ce qui touche à la culture organisationnelle : périodicité des inventaires, roulement des effectifs, etc.

4.2.3 Notion temporelle

On a vu dans la revue de littérature que le problème de l'utilisation est bien souvent dissocié de la notion temporelle. L'analyse de vulnérabilité vue par le CRP devrait faire intervenir la notion temporelle dans la mesure où l'activité économique et industrielle d'une PME n'est pas un processus fixe dans le temps de même alors que les contraintes qui s'appliquent à elle. La définition du système à fait apparaître la notion de contrainte qui s'applique sur l'organisation. Aussi, afin de caractériser les différentes contraintes, il est nécessaire d'amener la notion de temporalité introduite par Petit (2009) et Robert (2007) dans la vision de la vulnérabilité et du risque. La notion de temporalité introduite dans celle des contraintes permet a priori de distinguer deux types de contraintes : les contraintes dites continues, qui s'appliquent en tout temps (les contraintes de sécurité par exemple) et les contraintes que l'on appellera les contraintes calendaires, qui possèdent des paramètres temporels différents.

4.2.3.1 Contraintes continues et calendaires

La caractéristique de continuité traduit pour une contrainte donnée le fait que celle-ci doive être respectée en tout temps par l'organisation. Ce type de contrainte est notamment présent dans le cadre de la sécurité des personnes, ou encore dans le cadre du respect de la loi. L'intérêt d'introduire les contraintes de type continu repose sur le fait que le caractère ininterruptible nécessite une attention constante de la part des entreprises afin d'éviter toute conséquence liée. Les mesures en place et la politique de gestion devraient être en accord avec ce caractère continu.

Cependant de nombreuses contraintes n'appartiennent pas à cette catégorie et sont définies par des dates d'échéance et des périodicités. C'est notamment le cas de la plupart des contrats qui en règle

générale stipulent la livraison d'un bien ou d'un service à une date donnée avec une certaine périodicité (du contrat unique au contrat s'étendant sur plusieurs années avec des livraisons périodiques). On réfère à ces contraintes par le qualificatif calendaire. Ces contraintes possèdent, deux paramètres que nous avons retenus afin de les caractériser.

4.2.3.2 Date d'échéance

Comme précisé dans le paragraphe précédent, une organisation subit de nombreuses contraintes provenant notamment de ses clients via les différents contrats dans lesquels elle est engagée. Ces contrats stipulent alors des dates auxquelles l'organisation devra avoir effectué la livraison du produit ou du service désiré par le client sous peine de sanctions financières (on parle de pénalités de retard) ou d'image (perte de la confiance de la clientèle) ayant alors des conséquences sur le futur de l'organisation plus ou moins importantes. La date d'échéance ne se limite bien évidemment pas à la seule catégorie des contraintes contractuelles. On peut penser à la date limite pour le dépôt des bilans fiscaux ou encore à certaines échéances imposées par la saisonnalité (comme c'est le cas par exemple pour les organisations agricoles).

Aussi lors de l'analyse de vulnérabilité il est important de s'intéresser aux différentes contraintes non seulement par rapport à ce qu'elles nécessitent de la part de l'organisation, mais aussi dans quels délais cela est requis.

4.2.3.3 Périodicité

Outre la notion de date de délivrance, les contraintes calendaires peuvent faire apparaître une seconde caractéristique qui fait référence à la périodicité de l'application de la contrainte à l'organisation. La caractérisation de cette périodicité peut, entre autres, permettre d'affiner la mise en perspective des différentes contraintes les unes par rapport aux autres (comparer deux contraintes ayant la même date d'échéance, mais donc la périodicité diffère). Elle peut également permettre de juger de la cohérence de la politique de gestion en place pour gérer une contrainte par rapport à la périodicité de la contrainte.

4.3 Les technologies de l'information et de la communication

Comme explicité dans la revue de littérature, les TIC sont décomposables en trois entités distinctes : les TC, les TI et les données ou informations.

4.3.1 Caractérisation des technologies de l'information

Par rapport à ce qui a été explicité dans la revue de littérature, il est possible de proposer une classification des TI en trois grands sous-ensembles que nous utiliserons pour aiguiller les gestionnaires lors de l'identification des outils technologiques utilisés dans leur organisation.

L'équipement technologique physique d'interface (hardware) qui comprend notamment les ordinateurs, les smartphones, les tablettes numériques, les imprimantes, les scanners et l'ensemble des autres périphériques qui permettent aux utilisateurs d'interagir avec le système technologique global de l'organisation.

Les logiciels utilisés par l'organisation. On y retrouve les outils tels que les logiciels de traitement de texte, de comptabilité, de pilotage machine etc. Les logiciels peuvent être installés localement sur des équipements ou bien être en accès depuis le réseau étendu de l'organisation.

Les systèmes de gestion et de sauvegarde de données qui regroupent les bases de données, les serveurs et les moyens de sauvegarde en ligne (nuage). Ces systèmes peuvent être couplés à des équipements dit de restauration qui permettent une reprise des activités rapide en cas d'échec de l'équipement ou des logiciels.

Les TI permettent donc à une organisation de gérer, de stocker et d'utiliser des données afin d'en fabriquer d'autres, plus utiles, ou bien afin de participer à la production d'un bien ou service grâce aux différentes données utilisées. Les TI remplissent également une fonction d'interface, permettant à l'utilisateur d'accéder à des fonctions de pilotage, de contrôle ou de suivi d'activité.

4.3.2 Caractérisation des technologies de la communication

La terminologie « technologies de la communication » fait référence à l'ensemble des équipements qui permettent la mise en place d'un système d'échange de données au sein d'une organisation. Pour utiliser une image, on peut voir les TC dans une certaine mesure comme le système routier qui lie plusieurs villes entre elles. Les villes faisant ici référence aux éléments de TI cités plus haut. La caractéristique première des TC est donc d'établir un lien entre des éléments appartenant au domaine des TI. Ce lien permet l'échange de données entre plusieurs éléments et rend l'information disponible en temps réel et ce peu importe de la localisation géographique des utilisateurs. Il est possible de citer certains éléments associés à cette catégorie particulière comme les routeurs, les commutateurs réseau, les commutateurs téléphoniques, fibre optique, etc.

Comme vu dans la revue de littérature, la dualité complémentaire TI / TC et l'évolution des systèmes de communication vers la technologie du tout numérique ont conduit à l'adoption de l'expression Technologie de l'Information et de la Communication (TIC) et à considérer les deux catégories comme un seul ensemble aujourd'hui difficiles à scinder. Cependant nous avons décidé de conserver les TC comme un ensemble indépendant dont la fonction est la transmission de données d'un émetteur vers un récepteur. Aussi, la catégorie TC fera surtout référence aux outils de transmission tels qu'internet, le réseau téléphonique ou encore les réseaux sans fil internes à l'organisation.

4.3.3 Caractérisation des données / informations

La littérature et les deux définitions adoptées précédemment ont fait apparaître la notion de données, qui caractérise les éléments qui sont échangés entre les éléments de TI via les éléments de TC. Ces données sont des ensembles de faits, de nombres ou une fois traités, des informations que l'organisation récolte et/ou produit afin d'atteindre ses objectifs tout en tâchant de satisfaire les contraintes qui s'appliquent sur elle. Les données peuvent être stockées sous la forme de fichiers informatiques dans différents types de plateformes de stockage comme des disques durs locaux, des serveurs dans l'organisation ou encore des serveurs externalisés. Une information sera donc définie comme l'assemblage ordonné de données qui s'échangent entre différents éléments de TI et qui participent à l'avancement des missions de l'organisation. Elles permettent soit la production d'un bien ou d'un service, soit la conservation d'éléments nécessaires à la satisfaction des contraintes qui affectent l'organisation par exemple les données comptables ou celles servant au suivi d'une garantie sur des contrats.

4.4 Caractérisation de la défaillance

Il existe deux notions différentes de défaillance dans le cadre de cette étude. En effet, on a fait la différence entre le système étudié qu'est l'organisation et les systèmes technologiques qui en font partie. L'altération d'un système technologique à des répercussions sur les capacités de l'organisation à effectuer certaines tâches et a donc un impact sur sa capacité à satisfaire les différentes contraintes qui s'appliquent à elle. Autrement dit, la défaillance d'un système lié aux TIC peut être à l'origine de la défaillance de l'organisation.

4.4.1 Défaillance de l'organisation

La première définition est celle que nous tentons de caractériser dans l'ensemble de ce portrait de vulnérabilité. Elle porte sur l'incapacité pour l'organisation de respecter certaines de ses contraintes. On appellera objectif un ensemble de contraintes que l'organisation se doit de respecter dans une optique de viabilité.

La défaillance d'une organisation traduit donc l'incapacité de celle-ci à respecter un certain nombre de contraintes par rapport à des critères quantitatifs, qualitatifs ou calendaires. Cette incapacité menace donc la pérennité de l'organisation.

4.4.2 Défaillance d'un système lié aux TIC

La défaillance des systèmes technologiques porte sur la capacité d'un outil ou équipement à remplir sa fonction. Dans le cadre de cette étude plus particulière des TIC, le choix a été fait de considérer que la défaillance d'un élément technologique peut être mesurée par rapport à trois critères qui constituent les principaux piliers d'analyse en sécurité de l'information :

4.4.2.1 Disponibilité

Soit le fait qu'une donnée ou un système soit effectivement utilisable à un moment donné. La disponibilité s'applique aux trois catégories concernées par l'analyse : les TI, les TC et les données.

La non-disponibilité soit l'impossibilité d'utiliser un système dans un délai acceptable définit la première catégorie de défaillance qu'une organisation peut rencontrer lorsqu'on parle de TIC. Elle peut avoir des causes multiples (arrêt momentané d'une machine, perte d'une ressource essentielle comme l'électricité, etc.) et engendre bien souvent des conséquences quasi immédiates sur l'organisation et ses différents éléments fonctionnels.

4.4.2.2 Intégrité

La caractéristique d'intégrité traduit au sens large la persistance d'un élément dans l'état dans lequel il a été laissé.

Pour les données, elle caractérise le fait que celles-ci sont conservées dans l'état dans lequel elles ont été introduites et ne subissent pas d'altération accidentelle ou non permises dans le temps.

Les TI sont concernées, car cette catégorie contient les logiciels. Ceux-ci peuvent par une manipulation involontaire ou simplement par une mauvaise paramétrisation devenir dysfonctionnels : ils remplissent leur tâche en partie seulement ou en introduisant des erreurs décelables et peuvent même devenir non fonctionnels : ils ne peuvent plus remplir leur tâche (équivalent à non disponible).

Les données sont évidemment sensibles du point de vue de l'intégrité. Même stockées sous forme digitale, les données peuvent subir des altérations d'origine accidentelles ou malveillantes (les accidents peuvent aller de la simple maladresse d'un employé durant la manipulation des données à l'accident d'ampleur affectant l'organisation dans son ensemble comme un départ de feu dans ses locaux).

L'intégrité en règle générale présente une dimension liée à sa détectabilité. En effet l'introduction de données non intègres dans un système de sauvegarde n'est pas quelque chose qu'il est toujours aisé de repérer et ceci constitue aujourd'hui un des enjeux importants de la notion de reprise d'activité.

Lorsqu'on repère une donnée ou un logiciel qui ne satisfait pas le critère d'intégrité (donnée corrompue ou logiciel mal paramétré par exemple) il est nécessaire de s'assurer d'un point important : l'organisation possède-t-elle les capacités et informations nécessaires afin de rétablir un état intègre de l'élément identifié comme défaillant ?

4.4.2.3 Confidentialité

La confidentialité est une caractéristique qui est souvent abordée dans la problématique de la gestion des privilèges dans les organisations. Il s'agit de la propriété qui à attrait aux autorisations d'accès aux TIC en termes d'utilisation : la consultation, l'édition ou encore le transfert.

Les TI et plus particulièrement les logiciels, pouvant avoir un impact sur les activités de l'organisation, font souvent l'objet d'une sécurisation quant à leur accès. Toutes les personnes au sein d'une organisation n'ont ainsi pas accès à certains logiciels afin de prévenir toute manipulation accidentelle ou malveillante qui pourrait compromettre certains éléments et donc entraîner une défaillance quelconque par la suite.

Une défaillance en termes de confidentialité signifie donc que la sécurité d'accès à un élément de TIC a été compromise. Cela peut vouloir dire qu'un utilisateur non autorisé à eu accès par exemple

à un logiciel normalement restreint, ou bien qu'il a pu avoir accès à des données supposément confidentielles pour diverses raisons (données bancaires, données sensibles sur les clients, etc.).

Synthèse sur la défaillance

Pour résumé on prendra pour référence que les éléments de TIC peuvent défaillir par rapport à trois critères. Un outil peut donc être indisponible, peut être non intègre (caractérisé alors à la fois en termes de détectabilité et de rétablissement) ou enfin peut faire défaut en termes de confidentialité (devenir accessible pour des personnes ou systèmes non autorisés).

Ce faisant, cette défaillance se répercute sur l'organisation via les contraintes identifiées précédemment et peut dans le cas d'une contrainte obligatoire, se transformer en une défaillance de l'organisation.

4.4.3 Catégorie d'impact pour l'organisation

Lorsqu'un outil TIC présente une défaillance sur l'un des trois critères précédents, les conséquences pour l'organisation peuvent se traduire sur différentes activités (elles-mêmes liées à la contrainte identifiée au début de l'analyse). Afin de faciliter la caractérisation de ces conséquences, ces trois catégories d'impact ont été explicitées afin de permettre d'orienter le gestionnaire dans la réalisation du portrait de vulnérabilité.

4.4.3.1 Gestion administrative

Il s'agit de l'ensemble des activités et utilisations liées à la gestion de l'organisation. On retrouve dans cette catégorie d'impact :

- Les activités liées à l'infrastructure de l'organisation
  Exemple : Accès restreint à certaines zones, autorisation de déplacement d'outil, gestion du personnel durant l'exercice des fonctions.
- Les activités liées à la gestion des ressources humaines.
  Exemple : Maintien du suivi de profil des employés, tri des informations liées à l'embauche, obtention des documents administratifs relatifs aux ressources humaines (VISA, NAS, etc.)
- Les activités liées à la recherche et au développement

Exemple : Conception, consultation de brevets, recherche d'opportunités et de marchés.

- Les activités liées aux achats
  Exemple : Passage de commande, négociation de contrats.

- Les activités liées au marketing et à la vente
  Exemple : Management de l'image de marque, réalisation de support de communication (publicité).

- Les activités liées aux différents services
  Service juridique, service comptable, service financier, etc.

4.4.3.2 Production

Il s'agit de l'ensemble des activités liées à la fabrication du produit (ou service) de l'organisation. On retrouve dans cette catégorie :

- Les activités liées à la fabrication
  Exemple : Pilotage de machine, logistique interne (mouvement de matière et de produits), inventaire et stock, suivi de production.

- Les activités liées à la logistique d'approvisionnement
  Exemple : Gestion des livraisons avec les fournisseurs, gestion du trafic des convoyeurs entrants.

- Les activités liées à la logistique de commercialisation
  Exemple : Gestion des exportations, gestion des plannings d'enlèvement.

4.4.3.3 Contrôle des processus et procédés

Ensemble des activités qui veillent au bon déroulement (selon les normes, selon les directives de l'administration, selon les règles de sécurité, etc.) des activités de l'ensemble des éléments de l'organisation. Cette catégorie est importante dans le cadre de l'étude des TIC du fait que l'une de leurs gammes d'utilisation principale est le contrôle et la surveillance des activités en tout temps dans l'organisation.

Cette catégorie d'impact fait appel aux activités de surveillance et de veille qui sont intégrées dans l'environnement industriel. Aujourd'hui un grand nombre de capteurs divers sont utilisés dans les espaces de travail afin de monitorer de nombreuses variables qui influent sur la capacité de

production et sur les conditions de travail. Les variables environnementales sont étudiées (température, humidité, etc.). Les variables spatiales qui concernent les accès et les mouvements de matière peuvent être suivis à l'aide de différents capteurs. On trouve également de nombreux systèmes de contrôle de la qualité automatisés (notamment dans les organisations ou le risque chimique existe).

Synthèse concernant les catégories d'impact

Les trois catégories d'impact explicitées précédemment permettent de couvrir a priori l'ensemble des impacts possibles lors de la défaillance d'un outil lié aux TIC. Ces catégories seront utilisées par la suite afin de caractériser plus en détail les conséquences des différentes défaillances possibles du point de vue de l'organisation.

4.5 Synthèse du chapitre

Le chapitre 4 de ce mémoire avait pour but de faire une synthèse des différents concepts qui ont servi pour le développement de la méthodologie du portrait de vulnérabilité proposé. De nombreux concepts ont été empruntés à des méthodes ou des normes comme les critères de sécurité servant à caractériser la défaillance des outils TIC. Le point novateur amené par la réflexion sur les utilisations est la notion de contrainte en tant que composante d'un objectif plus global. La notion de contrainte n'a en effet a priori pas été proposée comme la base d'une méthodologie d'analyse de vulnérabilité et permet de proposer une focalisation sur les utilisations effectives dans l'organisation des TIC. Cette approche se distingue des deux approches classiques que sont l'approche probabiliste et l'approche par criticité évaluée des différents outils. Il est certain que l'approche proposée présente des similitudes avec l'approche par criticité évaluée dans la mesure où l'évaluation de la criticité passe nécessairement par une caractérisation par rapport à leur utilité dans le processus industriel. Notre méthodologie diffère par son cheminement logique : on part des contraintes de l'organisation pour aboutir à la caractérisation d'un outil technologique par rapport à cette utilisation précise plutôt que de partir d'un outil technologique et évaluer sa criticité en fonction de toutes les activités auxquelles il prend part. Ce renversement du paradigme de l'analyse devrait selon nous permettre d'alléger le processus d'analyse dans le cadre des PME, car celui-ci portera l'attention du gestionnaire sur des notions qu'il connaît et maîtrise, car liées au cadre organisationnel plutôt qu'au cadre technique.

Le chapitre suivant aura donc pour objectif de décrire le cheminement d'analyse proposé pour permettre au gestionnaire de l'organisation d'établir un portrait de vulnérabilité par rapport à l'utilisation des TIC.

CHAPITRE 5 PORTRAIT DE VULNÉRABILITÉ

Dans ce chapitre, une étude de cas issue de rencontres avec les différents partenaires du projet sera présentée. Les cas présentés sont apparus durant les discussions ayant eu lieu lors de réunion avec les gestionnaires des différentes PME. Chaque rencontre était précédée de communication avec les gestionnaires des entreprises qui avaient alors reçu une fiche pré-rencontre disponible en annexe (annexe A). Par souci d'anonymat, aucun nom ne sera donné et les exemples resteront assez globaux pour ne pas nécessiter d'entrer dans les détails de fonctionnement de chaque organisation. Le cheminement d'analyse permettant de réaliser un portrait de vulnérabilité par rapport à l'utilisation des TIC dans les organisations de type PME se base sur les critères présentés dans le chapitre 4. Cette étude de cas se compose de deux grandes étapes, la première permet de réaliser un inventaire et une caractérisation des différentes contraintes qui s'appliquent à l'organisation et la seconde explicite les points d'analyses importants à effectuer afin de caractériser au mieux cette vulnérabilité afin d'obtenir un portrait probant.

5.1 Inventaire de contraintes

Cette analyse a pour vocation d'aider les gestionnaires d'organisation de type PME à identifier et caractériser les vulnérabilités à la fois organisationnelles et techniques introduites par l'utilisation des outils TIC dans leur activité industrielle. On prend comme hypothèse principale que les gestionnaires de ces différentes organisations partagent les traits des gestionnaires de PME décrits dans la revue de littérature : proximité avec les employés et avec le domaine d'exercice de l'organisation ainsi que centralisation de la gestion, en somme il suit le modèle du principe de proximité de Torres.

5.1.1 Identification des contraintes

La première étape est l'identification des contraintes qui s'appliquent à l'organisation. Pour se faire, on propose au gestionnaire d'identifier dans un premier temps l'ensemble des contraintes par type (organisationnelles, techniques, légales, etc.). Lorsque l'identification arrive à son terme, c'est-à-dire que l'ensemble des types a été abordé, mais pas nécessairement rempli (le type autre notamment), il faut alors s'assurer que l'ensemble de contraintes retenu couvre l'ensemble du

spectre d'activités de l'organisation. Cette première étape de l'analyse devrait donc mener à l'établissement de l'ensemble des contraintes associées à l'activité de l'organisation.

Dans le cadre de notre étude de cas, les exemples qui viendront remplir les différents tableaux corroboreront des situations que nous avons rencontrées lors des réunions de travail avec les partenaires du projet. Par souci de commodité, des résultats provenant de différentes organisations ont été incorporés dans les mêmes tableaux. L'idée de l'étude de cas est de présenter des résultats succincts ayant été obtenus grâce à l'approche proposée.

Tableau 5.1 : Exemple de l'identification des contraintes d'une PME partenaire

Contraintes	Contractuelles : - Quantité de produits à produire - Conserver les documents relatifs au suivi de garantie
	Légales : - Émission d'un rapport annuel pour le gouvernement
	Organisationnelles : - Approbation du design produit préalable - Réduire les stocks au minimum
	Techniques : - Assurer la réception de la matière première - Assurer la livraison du produit fini sur place
	Économiques : - Effectuer la facturation
	Sécuritaires : - Assurer un environnement de travail sécuritaire
	Autres : - Assurer aux clients la possibilité de créer des modèles de produits en ligne

Le tableau 5.1 présente un ensemble de contraintes ayant pu être identifiées lors des réunions avec les gestionnaires des PME partenaires. Par souci de commodité la suite de l'étude de cas portera sur deux contraintes en particulier : la contrainte économique liée à la facturation et la contrainte légale liée à l'émission d'un rapport pour le gouvernement. Ces deux contraintes ont été choisies, car ce sont celles qui ont suscité le plus de discussion, car l'utilisation des TIC contribuait grandement à leur satisfaction.

5.1.2 Caractérisation des contraintes

La seconde étape, une fois l'inventaire réalisé, est d'arriver à caractériser les différentes contraintes. Cette caractérisation devrait permettre de répondre aux questions suivantes :

- Quel est l'objet de la contrainte ?
- Quel est le degré de criticité organisationnelle de cette contrainte ?
- Quels sont les paramètres temporels associés ?

L'objet de la contrainte, ou requis, représente le produit ou le service ou toute autre production émanant de l'organisation qui doit être fourni afin de satisfaire ladite contrainte. C'est bien souvent par le requis qu'une contrainte est identifiée au premier abord dans la mesure où il s'agit de l'objet pour lequel les activités de l'organisation travaillent. La caractérisation doit si c'est nécessaire faire apparaître des notions quantitatives ou qualitatives. Cette étape fait donc intervenir les notions présentées en 4.2.1.

Le degré de criticité organisationnelle peut être soit « obligatoire » soit « souhaitable » et est présenté en partie 4.2.2 du chapitre précédent. Il doit être jugé par rapport à deux points.

- L'origine de la contrainte associée et la capacité pour l'organisation d'en négocier les termes.
- Les conséquences du non-respect de la date d'échéance en cas de négociation impossible. Ces conséquences peuvent alors être financières, en rapport avec la crédibilité envers les clients, l'image de marque de l'organisation, etc.

Les paramètres temporels (introduit en 4.2.3) concernent l'ensemble des dates et durées qui définissent les bornes temporelles de la contrainte. La notion de périodicité d'une contrainte doit également être évaluée dans la mesure du possible. Ces paramètres doivent être caractérisés sans prendre en compte les mesures de « sécurité temporelle » qui pourraient avoir été prises via des mesures organisationnelles précédentes à l'analyse. Si par exemple la facturation doit être effectuée à une certaine date, mais que l'organisation prévoit dans sa politique comptable de régler avec 15 jours d'avance sur l'échéance, cette durée ne doit pas être pris en compte dans la contrainte sur la facturation, mais faire l'objet d'une contrainte à part entière avec le statut de « souhaitable », tandis

que la facturation fera l'objet d'une autre contrainte avec le statut « obligatoire ». On observe ce cas dans l'exemple présenté dans le tableau 5.2.

Tableau 5.2 : Caractérisation des contraintes

Contrainte	Criticité organisationnelle	Temporalité
	Obligatoire / Souhaitable	Continue / Date échéance / Périodicité
Émission rapport gouvernement	Obligatoire	Date butoir, chaque année
Facturation	Obligatoire	Spécifique au contrat
Facturation en avance	Souhaitable	Deux jours après la livraison au client
…	…	…

L'émission du rapport pour le gouvernement est une contrainte forte pour l'organisation qui en a fait état pour la simple raison que ce rapport est l'objet du service pour lesquels ses clients payent. La production d'un rapport pour chacun de ses clients constitue le cœur d'activité de cette organisation. Dans un souci de praticité, l'organisation effectue la transmission des rapports durant le cours de l'année au fur et à mesure de leur complétion. Cependant la date d'échéance imposée par le gouvernement dont les clients sont conscients, entraîne une hausse du nombre de dossiers à l'approche de celle-ci. Le mois avant la date butoir constitue donc une période particulièrement critique pour l'organisation qui se repose sur un logiciel spécifique afin de procéder au dépôt des dossiers sur les serveurs du gouvernement. Le gestionnaire nous confiera même que des incidents eurent lieu il y a quelques années et ont entrainés la mise en place de routines de vérification à l'approche de la période critique.

On remarque que la facturation possède deux contraintes associées. La première correspond à l'obligation pour l'organisation d'effectuer cette facturation. La date d'échéance dépend alors évidemment du contrat passé avec les clients ou fournisseurs de l'organisation. La seconde contrainte par contre provient d'un besoin exprimé par l'organisation lors de la rencontre : celle-ci a besoin d'effectuer la facturation le plus tôt possible (dans les jours qui suivent la

production/livraison), car le fonds de roulement permettant l'achat de la matière première pour les commandes suivantes en dépend. Cette contrainte présente donc un degré de criticité caractérisé comme souhaitable (pas de requis légal ou contractuel associé), mais présente en cas de rupture des conséquences fortes sur l'organisation pouvant impacter sa viabilité économique.

5.1.3 L'utilisation des TIC pour satisfaire des contraintes

Lorsque l'organisation estime avoir réalisé un inventaire de contraintes complet, c'est-à-dire qu'elles forment un ensemble d'objectifs n'ayant laissé pour compte aucun pan de l'organisation, il est possible de passer à la seconde étape de l'analyse. Cette seconde étape vise à faire le lien entre les contraintes identifiées précédemment et l'utilisation des TIC faite dans l'organisation afin de satisfaire celles-ci. Pour cela, il peut être nécessaire pour le gestionnaire de requérir l'avis de personnes travaillant dans les différents services et possédant une vision différente de la sienne sur le déroulement des activités. Cependant le principe de proximité évoqué dans la revue de littérature et confirmé lors des différentes entrevues avec les partenaires permet d'envisager que le lien peut être fait par le gestionnaire seul, fort de sa vision globale de l'organisation et ses processus.

Afin de permettre une analyse fine, le gestionnaire devrait réaliser cet inventaire d'outils en procédant séparément pour chaque catégorie d'outil retenue : TI, TC et données. La séparation des TI en suivant les trois sous-ensembles évoqués précédemment est possible si le niveau d'analyse s'avérait ne pas être assez fin pour le gestionnaire. Pour chaque TIC identifiées comme partie prenante d'une activité, il est nécessaire d'expliciter par rapport à quel critère (disponibilité, intégrité, confidentialité) la défaillance pourrait empêcher l'organisation de satisfaire la contrainte. Cette précision permettra plus tard d'orienter la prise de décision lors de la mise en place de mesures correctives.

Tableau 5.3 : Utilisation des TIC pour la satisfaction des contraintes identifiées et des critères impactants

Contrainte	Données			TI			TC		
	D	I	C	D	I	C	D	I	C
Émission rapport gouvernement	X		X			X	X	X	X
Facturation				X	X		X	X	
Facturation en avance				X	X		X	X	
…									

Dans le tableau 5.3, ci-dessus, les lettres D, I, C signifient respectivement Disponibilité, Intégrité et Confidentialité.

L'exemple ci-dessus permet de préciser certaines choses concernant l'utilisation des TIC pour satisfaire les contraintes. Ainsi pour chaque contrainte identifiée le gestionnaire doit établir si des données, des TI ou des TC qui viendraient à défaillir selon leur disponibilité, leur intégrité ou leur confidentialité, porteraient atteinte à la satisfaction de ladite contrainte. À chaque fois que c'est le cas, une croix est portée dans la case correspondante. Chaque croix peut alors faire l'objet d'un paragraphe explicatif par exemple :

> Émission du rapport gouvernemental / TC / Confidentialité :
>
> **L'émission du rapport et surtout sa remise sur les serveurs du gouvernement** (l'objet de la contrainte) passent par un **canal sécurisé via un réseau privé** (l'élément de TC concerné) conçu par le gouvernement et mis à disposition de l'organisation. Du fait du caractère privé des informations transmises (informations par rapport à la profitabilité des clients), une défaillance concernant l'accès et **la confidentialité** de ce réseau (le critère de défaillance) entraînerait une violation de l'objectif de l'organisation dont un des requis est d'assurer le respect de la confidentialité des données transmises sur leurs clients.

Ou encore :

> Facturation en avance / TI / Disponibilité :
>
> Le caractère pressé de **la facturation** contraint l'organisation à avoir un **logiciel spécialisé dédié à cette activité** disponible et opérationnelle en tout temps. Une **indisponibilité** entraînerait alors un retard d'approvisionnement qui aurait alors des conséquences importantes quant aux capacités d'achat et impacterait donc de façon non négligeable la capacité de l'organisation à satisfaire les commandes suivantes.

Ces paragraphes visent à s'assurer que la raison pour laquelle un élément des TIC intervient dans la satisfaction de la contrainte est la même pour toutes les parties prenantes du processus, car rappelons que l'analyse est supposément réalisée par le gestionnaire.

En répétant ce processus pour chaque élément identifié, il est aisé d'obtenir pour l'organisation un document qui recense les potentielles défaillances impactantes des TIC sur leur activité. Une fois ceci réalisé pour l'ensemble des contraintes identifiées, il est possible de passer à l'étape suivante du processus d'identification des vulnérabilités.

5.2 Caractérisation de la défaillance

Dans l'optique d'établir un portrait de vulnérabilité, il est important pour l'organisation de pouvoir établir une caractérisation de la défaillance et des conséquences induites par celle-ci.

5.2.1 Conséquences

Les défaillances de l'organisation peuvent être nombreuses et possèdent chacune des conséquences qui peuvent être caractérisées selon une échelle de trois paliers :

- Les conséquences de faible ampleur. Elles affectent l'organisation seulement très peu et sont facilement compensables, que ce soit par un léger effort de la part d'un des services de l'organisation ou simplement grâce à la gestion courante en place dans l'organisation. L'organisation ou sa composante perdure dans un état de fonctionnement quasi nominal.
- Les conséquences d'ampleur moyenne. L'avènement de ce type de conséquence introduit ce que l'on appelle le mode de fonctionnement dégradé de l'organisation ou de l'une de ces composantes. Le mode de fonctionnement dégradé est caractérisé par une difficulté pour

un ensemble à remplir sa fonction par rapport au fonctionnement normal. La difficulté peut alors se traduire de plusieurs manières : ralentissement, coût supplémentaire, perte de qualité, etc. Les mesures qui entrent en action dans ce mode de fonctionnement sont celles reliées à la gestion adaptative et planifiée des perturbations.

- Les conséquences de grande ampleur. Les conséquences de grande ampleur entraînent le passage de l'organisation ou d'une de ses composantes en mode de fonctionnement défaillant. Ce mode de fonctionnement est caractérisé par une incapacité de l'ensemble concerné à remplir sa fonction. Cette incapacité perdure dans le temps jusqu'à ce que des mesures importantes soient prises afin de rétablir le niveau de fonctionnement soit au niveau dégradé soit au niveau normal. Dans le cadre particulier des TIC, il est intéressant de noter que le retour à un fonctionnement nominal est bien souvent effectué directement, sans passage par un état intermédiaire / dégradé (dans le cas d'un plan de relève, la plupart des fonctions sont rétablies dans leur fonctionnement normal lorsque les mesures de relève sont activées.)

L'évaluation des conséquences d'une défaillance est l'un des points qu'il est difficile de quantifier de façon purement conceptuelle. Chaque organisation devrait établir des seuils afin de séparer les différents états. Cette notion de seuil permet au gestionnaire de pouvoir plus efficacement caractériser les défaillances potentielles et permettra entre autres de hiérarchiser les différentes actions à mener en priorité dans l'organisation à la fin du processus d'évaluation.

5.2.2 Marge de manœuvre

En parallèle de l'établissement du niveau de conséquence d'une défaillance sur l'organisation, il est nécessaire de procéder à une évaluation des marges de manœuvre à la fois opérationnelles et stratégiques au sein de l'organisation. Ces marges doivent prendre en compte l'utilisation faite par l'organisation des TIC impliquées dans la défaillance et être capables d'estimer les durées disponibles entre la détection de la défaillance et l'application des conséquences estimées. Ce laps de temps permet de juger qu'elles devraient être les éléments TI/TC/données à devoir être prioritairement relevées en cas de défaillance. Ce critère particulier développé au sein du CRP est selon nous une composante essentielle de la vulnérabilité des organisations dans la mesure où il s'agit de la capacité temporelle réelle pour réagir et s'adapter aux conséquences des différentes défaillances et notamment ici celles liées à l'utilisation des TIC.

La marge de manœuvre représente le laps de temps disponible entre la prise de conscience d'une défaillance (qui implique ici donc la notion de détectabilité de la défaillance) et le moment où les conséquences de la défaillance s'appliquent à l'organisation. Cette durée est celle qui permet à l'organisation de prendre des mesures en adéquation avec la défaillance rencontrée. Ces mesures peuvent relever de la gestion courante ou de la gestion des urgences en fonction de la valeur de la marge de manœuvre. Cette caractéristique doit être évaluée par le gestionnaire de l'organisation à l'aide de sa connaissance de l'organisation et de sa politique de gestion.

5.2.3 La détectabilité

La notion de détectabilité vient d'être soulevée et représente une des problématiques majeures de la surveillance technologique. En effet si la disponibilité d'un outil est relativement facile à étudier (un outil non disponible est repéré dès qu'il est nécessaire de l'utiliser), les deux autres critères, intégrité et confidentialité, sont bien plus complexes à évaluer. L'intégrité d'une donnée peut passer inaperçue pendant une période de temps conséquente et n'être mise en évidence que tardivement. La confidentialité est encore plus problématique du point de vue de la détectabilité. C'est d'ailleurs bien souvent parce qu'une brèche à l'origine de la fuite d'informations n'est pas identifiée tout de suite que les conséquences sur l'organisation s'avèrent être importantes.

Aussi les organisations devraient-elles posséder des mesures permettant de s'assurer de la détectabilité des différents types de défaillances. Ces mesures peuvent être techniques et reposer sur la mise en place de protocoles de vérification et d'analyse d'intégrité. Les mesures peuvent également provenir de mesures organisationnelles visant à rendre le personnel compétent dans l'identification de défaillances de ce type.

5.3 Analyse organisationnelle et technique

Lorsque, l'ensemble des contraintes subies par l'organisation ont été inventoriées et caractérisées, l'organisation peut alors procéder à l'analyse de vulnérabilité qui se compose de deux étapes. Ces deux étapes se déroulent en parallèle, l'une devant être réalisée par le gestionnaire de l'organisation qui constituera l'analyse organisationnelle, l'autre, l'analyse technique, réalisée par le responsable des technologies informatiques de l'organisation (auquel on référera maintenant par responsable TI). Il se peut que l'organisation ne possède pas de référent du point de vue technologique et fasse appel à un prestataire externe. Cette étape est alors d'autant plus importante que la communication

entre les deux parties n'est pas aussi aisée pour la mise en place de mesures liées à la gestion courante, car il est plus simple de discuter avec un employé sur place qu'avec une personne extérieure au périmètre de l'organisation. De plus, le recours à un prestataire externe réduit le principe de proximité qui permet au gestionnaire d'avoir une vision globale de l'activité de son organisation. Il est donc important pour le gestionnaire de s'assurer des différents points liés à l'analyse technique avec le prestataire.

5.3.1 Analyse organisationnelle

Cette première analyse a pour objectif de caractériser l'influence d'une contrainte sur l'organisation en cas de défaillance et de définir s'il existe des mesures spécifiques au niveau organisationnel adaptées aux différentes utilisations des TIC mises en évidence lors de la caractérisation des contraintes. Il est possible pour le gestionnaire de l'organisation d'inclure pour cette analyse la personne en charge des différents plans de continuité des opérations (PCO) si ceux-ci existent ou toute autre personne en charge de la gestion des risques au sein de l'organisation. Leur connaissance des mesures en place est une partie décisive de cette étape.

À cette étape, plusieurs points devront être clarifiés pour chaque contrainte :

- Quelle conséquence organisationnelle aurait la défaillance d'un des outils TIC identifiées par rapport aux contraintes ? À quelle(s) catégorie(s) d'impact appartient-elle ?
- Ce type de défaillance fait-il l'objet de mesures organisationnelles ? en est-il fait mention dans le PCO ?
- L'organisation possède-t-elle une marge de manœuvre concernant ce type de défaillance ? Des ressources annexes peuvent-elles venir pallier la défaillance et si oui pendant combien de temps ?

L'ensemble des réponses à ces questions peut être reporté dans un tableau qui permet d'établir une synthèse préliminaire des résultats obtenus.

Tableau 5.4 : Analyse organisationnelle

Contrainte identifiée : Facturation			
Point de vue organisationnel			
TIC - Critère de défaillance	Conséquence organisationnelle	Adressé en PCO ?	Marge de manœuvre
TI : logiciel spécialisé dans l'édition et l'envoi de factures - Disponibilité	Conséquence de moyenne ampleur avec impact sur la production : Manque de trésorerie, retard d'approvisionnement, retard de fabrication	Possibilité de discuter les termes de facturation avec les fournisseurs moyennant pénalités financières. La reprise devrait s'effectuer rapidement, l'entreprise emploie un spécialiste TI.	2 jours

Le tableau précédent peut posséder autant de lignes qu'il y a d'éléments TIC impliqués dans la satisfaction de la contrainte. Ces lignes devraient exister à chaque fois qu'une croix a été portée dans le tableau 4.3.

La première colonne du tableau 5.4 devrait faire apparaître l'élément technologique dont la défaillance est identifiée comme impactante sur la contrainte analysée. Le critère par rapport auquel la défaillance est identifiée doit également apparaître. Dans l'exemple pris ici avec la contrainte de facturation, l'élément TI identifié comme pouvant défaillir est le logiciel spécifique utilisé par le service de facturation. Le critère de défaillance retenu est celui de disponibilité. Il est à noter que si par exemple le logiciel pouvait défaillir par rapport à un autre critère, il faudrait alors créer une seconde ligne à ce tableau pour y faire figurer les informations relatives à ce second critère pour chaque colonne décrite par la suite.

La seconde colonne doit établir la conséquence organisationnelle qui adviendrait sur l'organisation dans le cas de défaillance identifiée.

Les conséquences doivent être dans un premier temps localisées c'est-à-dire qu'elles doivent être associées à une catégorie d'impact comme explicité section 4.4.3. Ici les conséquences de la défaillance s'appliqueraient dans leur finalité à la production qui se trouverait ralentie par le manque d'approvisionnement en matière première. Il est possible que les conséquences aient plusieurs catégories d'impact par exemple un impact sur la production, mais aussi sur la gestion des processus. Il est alors recommandé de séparer la case pour faire apparaître chaque cas différent.

Les conséquences doivent également être mesurées par rapport aux trois seuils établis (section 5.2.1) par le gestionnaire. Dans le cas présenté, les conséquences ont été estimées d'ampleur moyenne, demandant à l'organisation de recourir à des mesures adaptatives et planifiées de gestion des perturbations. Il est possible que l'ampleur d'une conséquence ayant différentes catégories d'impact varie selon ces catégories.

La troisième colonne remplit deux fonctions. Elle s'intéresse dans un premier temps à savoir si ce type de situation (la défaillance de l'élément de TIC analysé) fait partie des situations prises en compte dans le PCO de l'organisation. Si c'est le cas, la seconde fonction de cette colonne est de recenser les mesures figurant dans le PCO afin de traiter la situation. Dans notre exemple, la situation avait déjà été identifiée comme à risque par le gestionnaire de l'organisation, car il est conscient que son fonds de roulement fonctionne en flux tendu. Les mesures en place sont des accords tacites avec ses différents fournisseurs prêt à discuter des avances de matière contre un payement plus tardif à intérêt. Le gestionnaire stipule cependant qu'il estime une reprise rapide du système de facturation, car il emploie un responsable TI sur son site d'exploitation.

La quatrième colonne permet de faire apparaître le dernier critère retenu du côté organisationnel : la marge de manœuvre. Le gestionnaire doit à l'aide de sa connaissance de l'organisation et des pratiques en place être en mesure de donner une estimation du temps disponible entre l'apparition d'une défaillance TIC (indisponibilité du logiciel de facturation dans notre cas) et l'avènement des conséquences caractérisé dans la seconde colonne. Pour notre exemple, le fonctionnement du flux de trésorerie particulier de cette organisation exerce un fort stress sur la rentrée d'argent et n'autorise pour fonctionner qu'un retard maximal de deux jours sur la facturation.

5.3.2 Analyse technique

L'analyse technique relève de la compétence du gestionnaire TI de l'organisation. Celle-ci vise à mettre en évidence les différents points relatifs à la gestion technique des TIC et notamment les mesures en place en cas de défaillance.

Tableau 5.5 : Analyse technique

Contrainte identifiée : Facturation			
Point de vue technique			
TIC - Critère de défaillance	Détectabilité	Mesures en place	Durée de reprise estimée
TI : logiciel spécialisé dans l'édition et l'envoi de factures - Disponibilité	À l'utilisation	Appel au support technique nécessaire.	3 jours ouvrables minimum

La première colonne du tableau 5.5 est identique à la première colonne de l'analyse organisationnelle. Elle vise à remettre en contexte quel outil TIC est caractérisé et par rapport à quel critère de défaillance il est analysé. Ici nous avons suivi le même exemple en considérant la défaillance en disponibilité du logiciel de facturation.

La seconde colonne s'intéresse ici à la capacité de la branche technique de l'organisation à se rendre compte que la défaillance a eu lieu. En effet comme explicité dans le paragraphe portant sur la détectabilité, certaines défaillances, notamment celles relatives à l'intégrité des éléments de TIC, peuvent s'avérer difficiles à repérer. Dans cette colonne il est donc demandé au gestionnaire de TI de faire figurer les méthodes ou mesures en place afin de repérer la défaillance analysée. L'exemple d'une indisponibilité du logiciel de facturation n'est ici décelable que lorsque l'usager

cherche à s'en servir et se rend compte que le logiciel n'est pas utilisable. Il n'existe a priori pas de mesure technique qui vérifie automatiquement la disponibilité de ce logiciel dans l'organisation.

La troisième colonne s'intéresse aux mesures en place du point de vue technique afin de traiter la défaillance analysée. Les mesures qui nous intéressent ici sont celles qui servent à assurer la continuité ou la reprise des activités, car dans le cadre de l'approche par conséquences, la cause de la défaillance n'est pas considérée. Le gestionnaire TI doit donc faire apparaître ici les mesures de mitigation des conséquences et de relève en place d'un point de vue technique. Dans l'exemple pris ici, le gestionnaire des TI n'a tout simplement pas de solution technique en place, car ce logiciel ne fait pas partie des éléments avec lequel il est habilité à travailler. La solution en cas d'indisponibilité de ce logiciel est alors de faire appel à la compagnie du logiciel pour obtenir l'aide d'un technicien, qui doit dans les cas les plus graves être dépêché sur place.

La quatrième colonne fait apparaître la durée de reprise estimée. Cette durée est liée aux mesures techniques en place et caractérise la durée nécessaire entre la détection de la perturbation et le retour vers un fonctionnement normal de l'outil TIC. Dans notre cas il s'agit du temps nécessaire afin de rendre le logiciel de facturation à nouveau disponible pour l'organisation. Ici cette durée est relative au temps séparant le contact de l'entreprise du logiciel et l'arrivée du technicien sur place. Cette durée a été estimée à 3 jours ouvrables par l'entreprise prestataire.

Il est important de noter que tout comme le tableau 5.4 de l'analyse organisationnelle, on peut ajouter autant de ligne qu'il existe d'éléments TIC pouvant affecter la contrainte par rapport à laquelle est faite l'analyse (autant qu'il y a de croix dans le tableau 5.3).

Lorsque les deux analyses ont été complétées, l'étape finale de l'établissement du portrait de vulnérabilité de l'organisation est la mise en regard des deux analyses précédentes.

5.3.3 Mise en regard des analyses

Dans le cas idéal, ces analyses devraient rassurer le gestionnaire en mettant en évidence que l'organisation est prête à faire face à la plupart des défaillances technologiques mises en évidence et se retrouver dans la situation présentée à la figure 5.1.

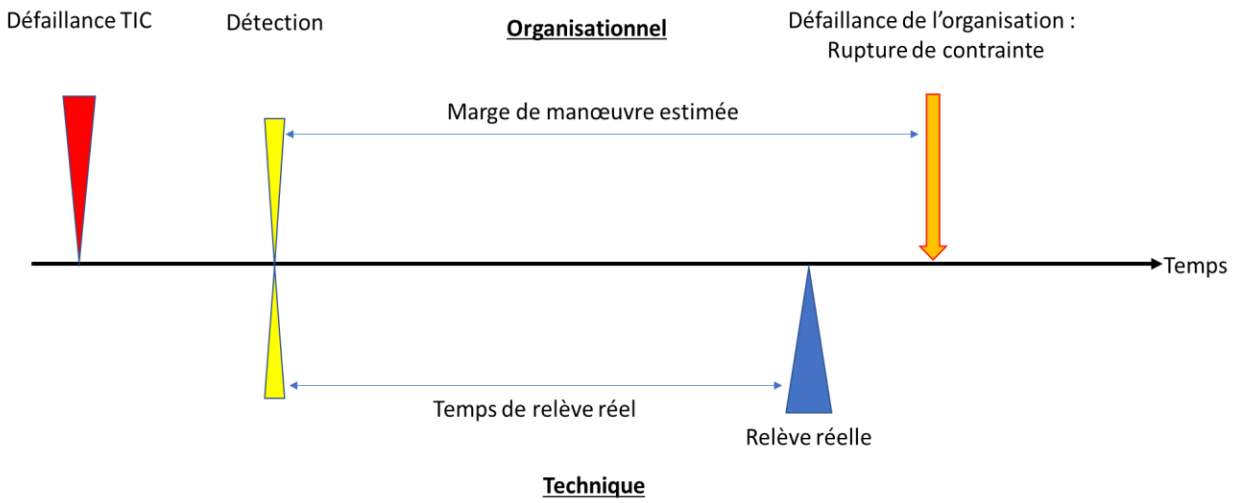

Figure 5.1 : Cas idéal : adéquation

Dans la figure 5.1 ci-dessus, on remarque que la reprise des activités assurée par la branche technique se trouve être inférieure à la marge de manœuvre estimée par la branche organisationnelle. Ce cas garantit a priori qu'une défaillance dans cette configuration n'aura que très peu de conséquences sur l'organisation et que les mesures en places semblent connues et suffisantes pour assurer la continuité des activités de l'organisation.

Cependant il est également probable que les deux analyses soient en désaccord voire même en contradiction. Par exemple le PCO peut, dans les faits, compter sur une mesure TI alors que celle-ci n'est pas implémentée ou bien n'a pas les mêmes effets qu'escomptés. C'est ce cas qui s'est illustré dans l'exemple de la facturation. Le gestionnaire pense que son responsable TI est à même de solutionner le problème de la disponibilité du logiciel de facturation en une durée inférieure à la marge de manœuvre qu'il prévoit par rapport à cette défaillance. Le responsable TI quant à lui prévoit l'intervention d'un technicien pour ce problème spécifique et le temps d'intervention dépasse la marge de manœuvre organisationnelle.

Le but du tableau 5.6 est de faire apparaître ces incohérences.

Tableau 5.6 : Mise en regard des analyses organisationnelle et technique

<table>
<tr><td colspan="4">Contrainte identifiée : Facturation</td></tr>
<tr><td colspan="4">Point de vue organisationnel</td></tr>
<tr><td rowspan="4">TI : logiciel spécialisé dans l’édition et l’envoi de factures
Disponibilité</td><td>Conséquence organisationnelle</td><td>Adressé en PCO ?</td><td>Marge de manœuvre estimée</td></tr>
<tr><td>Conséquence de moyenne ampleur avec impact sur la production :
Manque de trésorerie, retard d’approvisionnement, retard de fabrication</td><td>Possibilité de discuter les termes de facturation avec les fournisseurs moyennant pénalités financières.
La reprise devrait s’effectuer rapidement, l’entreprise emploie un spécialiste TI.</td><td>2 jours</td></tr>
<tr><td>À l’utilisation</td><td>Appel au support technique nécessaire.</td><td>3 jours ouvrables minimum</td></tr>
<tr><td>Détectabilité</td><td>Mesures en place</td><td>Temps de relève estimé</td></tr>
<tr><td colspan="4">Point de vue technique</td></tr>
</table>

Dans l’exemple, on peut remarquer que la marge de manœuvre associée au processus de facturation est estimée à 2 jours alors que la durée avant l’intervention d’un technicien est estimée à 3 jours ouvrables dans le meilleur des cas. Nous nous retrouvons alors dans la situation exposée en figure 5.2 où la reprise réelle arrive après l’avènement des conséquences non négligeable sur

l'organisation (on peut aussi parler alors de rupture de la contrainte associée à la facturation), mais surtout n'est pas en accord avec ce que la partie organisationnelle pense.

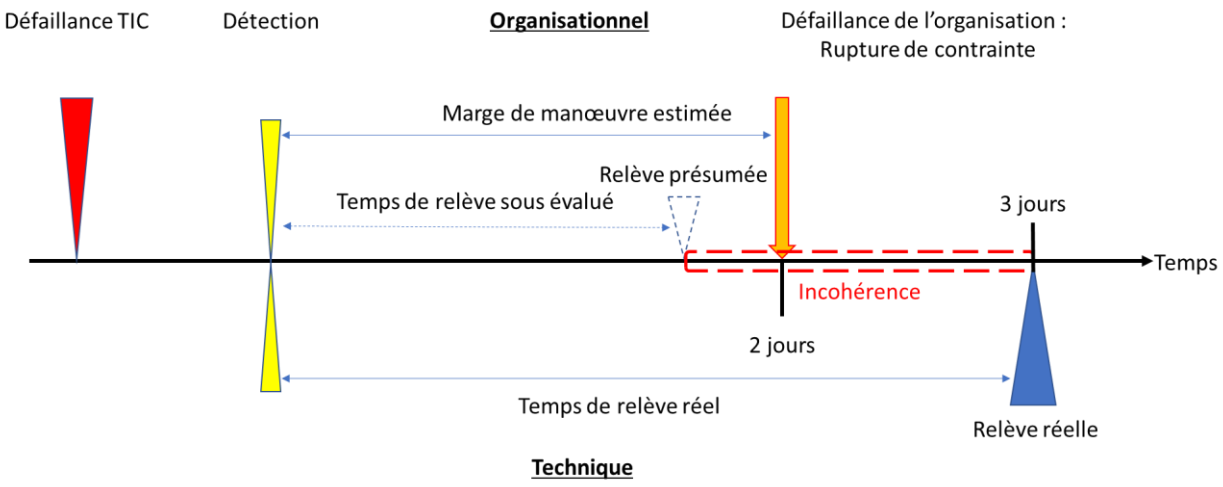

Figure 5.2 : Temps de reprise sous-estimé du point de vue organisationnel : exemple de la facturation (échelle temporelle non uniforme)

La mise en lumière de cette incohérence entre les deux visions est importante dans la mesure ou sans cette comparaison, l'incohérence pourrait rester inconnue, au risque de ne jamais voir de mesure prise pour y remédier jusqu'à l'avènement d'une défaillance ayant des conséquences sur l'organisation.

Les éléments qui apparaissent en faute dans ce cas semblent être, premièrement, un manque de communication entre les deux parties puisque le gestionnaire semble penser que le gestionnaire TI est capable de s'occuper de ce type de problème alors que ce n'est pas le cas. Deuxièmement le temps nécessaire pour l'intervention du technicien est supérieur à la marge de manœuvre associée à une défaillance du logiciel de facturation.

Il faut faire attention à bien prendre en compte qu'incohérence et rupture potentielle de contrainte ne sont pas forcément liées. En effet il aurait été possible que la relève réelle advienne avant la rupture, mais à une date cependant postérieure à celle estimée par le gestionnaire. L'incohérence existe alors toujours et nécessite d'être mise en lumière pour les deux parties afin d'être prise en compte dans la mise en place de futures mesures ou dans l'établissement d'un consensus de connaissance.

5.3.4 Une définition de la vulnérabilité spécifique aux TIC

La mise en regard des caractérisations organisationnelle et technique peut donc faire apparaître des contradictions entre deux points de vue distincts présents dans l'organisation. Cette contradiction traduit que les deux visions des TIC : leurs utilisations d'un point de vue organisationnel et leur gestion d'un point de vue technique ne sont pas en accord. La différence des points de vue crée alors des zones floues, des « failles » que des perturbations pourraient être à même d'exploiter, ouvrant alors la voie à de nombreuses conséquences de niveaux divers. Pour reprendre la formulation adoptée au sein du CRP, une définition équivalente de la vulnérabilité par rapport à l'utilisation des TIC est alors :

> **La caractérisation dans le temps de la susceptibilité d'une PME à subir des défaillances par rapport à l'utilisation des TIC et à la cohérence entre les visions organisationnelle et technique de ces utilisations.**

Aussi le but final de la démarche est de faire apparaître le maximum de ces désaccords ou contradiction entre ces deux visions afin de générer une prise de conscience à la fois chez le gestionnaire et chez le responsable des TIC dans l'organisation (que celui-ci soit interne ou externe à l'organisation).

On parle de vulnérabilité face à l'utilisation des TIC, car, on le précise à nouveau, le point important de l'analyse est la mise en regard de l'utilisation réelle des TIC dans l'organisation via les contraintes face à celle perçue d'un point de vue purement technique. Les méthodes de gestion explicitées dans la revue de littérature souffraient selon nous de l'absence d'une mise en parallèle des deux approches en se focalisant sur des approches basées généralement sur un seul des deux points. Ainsi, Mehari Pro porte l'accent sur le point de vue administratif en tâchant de proposer des scénarios que les gestionnaires doivent évaluer par rapport aux mesures organisationnelles en place dans leur organisation. Octave-S quant à elle se focalise grandement sur le point de vue technique en abordant la problématique technologique via les actifs informationnels et leurs contenants technologiques.

En renversant le paradigme de l'analyse classique pour produire une analyse centrée sur les utilisations, le CRP espère que les gestionnaires prendront conscience de l'importance de la considération des utilisations réelles des différentes technologies de l'information et de la

communication à la fois comme base d'analyse des risques, mais aussi comme un pont entre les points de vue organisationnel et technique.

En cas de désaccord entre les deux analyses, il est préconisé que le gestionnaire prenne les devants et demande une réunion des parties prenantes afin de pouvoir discuter vers un consensus. Ce consensus peut être atteint de plusieurs façons : l'organisation peut décider d'accepter la situation et le fait qu'elle soit vulnérable à ce type de défaillance ou bien elle peut décider de la mise en place de nouvelles mesures organisationnelles ou techniques afin de répondre à la vulnérabilité mise en lumière si cela est possible des points de vue organisationnel et financier.

Pour ce qui est de l'exemple de la facturation pris au long de cette étude de cas, puisque l'existence d'une incohérence a été établie, plusieurs possibilités de prise de décision s'offrent au gestionnaire. Le premier type de décision viserait à réduire le temps nécessaire à l'intervention du technicien, par exemple en signant un accord avec le prestataire qui lui assurerait alors une intervention plus rapide. Il serait également possible d'offrir au gestionnaire TI une formation afin de le préparer à ce genre de défaillance et lui permettre d'intervenir lui-même sur le logiciel en faute. Une autre solution possible, mais d'ampleur plus large serait d'envisager un transfert vers une solution externalisée avec les solutions de cloud-computing disponibles aujourd'hui (bénéficiant alors de l'expertise des responsables de la plateforme d'hébergement). Enfin la prise de décision pourrait simplement être l'acceptation de cette vulnérabilité pour l'organisation. L'étude de la prise de décision et des mesures n'a pas été plus approfondie, car le projet visait essentiellement à proposer une définition de la vulnérabilité et non pas le traitement de celle-ci.

5.4 Synthèse de l'étude de cas présentée

L'étude de cas qui vient d'être présentée a permis de donner des exemples des contraintes que nous avons pu mettre en évidence lors de nos rencontres avec les partenaires du projet. Elle a également permis de mieux présenter la structure que les outils d'analyse devraient adopter. Ces travaux proposent donc une alternative quant à la caractérisation de la vulnérabilité et plus particulièrement la vulnérabilité par rapport à l'utilisation des outils liés aux technologies de l'information et de la communication. Celle-ci pourrait par exemple servir d'approche alternative dans un processus d'identification et de gestion plus abouti comme Octave-S en s'insérant en parallèle de la phase 2 de celle-ci afin de proposer une approche mettant en regard la vision administrative et la vision

technique plutôt que se focalisant exclusivement sur la vulnérabilité liée à l'architecture technologique. Il faut bien comprendre que le but n'est pas de remplacer l'approche d'Octave-S, mais de la compléter par une prise en compte de la double vision qui existe au sein des PME.

CHAPITRE 6 RÉSULTATS, PERSPECTIVES ET CONCLUSION

Durant ce projet, des réunions avec certaines organisations partenaires ont permis d'orienter les choix faits parmi les différents critères et découpages qui étaient possibles afin d'essayer de caractériser la vulnérabilité des PME par rapport à l'utilisation des TIC. Si l'idée d'un découpage sectoriel a été celle qui nous a inspirés au début, les échanges avec certains gestionnaires ont permis d'entrevoir que la solution pour introduire les utilisations réelles des TIC résidait dans ce qu'ils maîtrisent mieux : les contraintes que l'organisation doit satisfaire afin de remplir ses objectifs. En effet il est vraisemblable qu'une personne dont le rôle est de s'assurer que l'ensemble des éléments fonctionnels d'une organisation travaillent de concert soit à l'aise avec la notion de contraintes qui représentent finalement la raison même de l'existence de ces éléments fonctionnels (le service de facturation cherche à satisfaire l'ensemble des contraintes liées à la facturation, et ce pour un ensemble d'objectifs différents).

6.1 Résultats

Les dernières réunions où le concept d'approche par contraintes a été présenté ont permis de mettre en lumière plusieurs points qui répondent à certaines interrogations que nous avions et qui ouvrent la voie vers des raffinements qui pourraient avoir lieu sur ce concept :

Le concept d'approche par contraintes est parlant pour les gestionnaires, ainsi lors de réunions d'une durée approximative de 2h nous avions pu mettre en évidence un nombre satisfaisant de contraintes et avions même pu démarrer la caractérisation en termes de temporalité de celles-ci ainsi que l'identification des TIC impliquées.

Un point noir peut être relevé par rapport à ce projet. Les PME dans lesquelles nous avons procédé à l'analyse préliminaire sont des organisations « matures » qui présentent un ensemble de mesures et de routines de gestion qui ont d'ores et déjà fait leurs preuves (par l'expérience d'incidents et de défaillances passées). Aussi notre méthode n'a souvent fait que remettre en lumière des vulnérabilités dont les gestionnaires étaient conscients. Il serait pertinent pour une évaluation future de pouvoir tester cette approche sur des PME jeunes dont la gestion des risques technologiques débute ou sur des PME qui décident d'adhérer à une nouvelle technologie globale par exemple une PME qui déciderait de faire passer l'intégralité de son architecture informatique interne vers une architecture externalisée de type cloud. Ce dernier cas pourrait être d'autant plus intéressant que la

transition vers une architecture externalisée change en général les manières de procéder dans les processus affectés par ce changement, mais aussi transfère une part de la responsabilité (et non pas du risque). Il serait alors intéressant de procéder à une analyse avant et une analyse après la transition afin d'observer les changements dans les utilisations des TIC apportés.

Pour conclure, on retiendra que ces travaux ont donc permis d'ouvrir la voie prometteuse à une approche de la vulnérabilité technologique basée sur l'utilisation des technologies de l'information et de la communication au sein des petites et moyennes entreprises. Fort de la méthodologie de recherche-action, ce projet marque la première étape de ce processus et ouvre potentiellement la voie à une étude plus profonde de la vulnérabilité et dans une mesure plus grande du risque technologique dans les organisations en se basant sur l'utilisation réelle faite des TIC au sein de ce type d'organisation. On peut enfin souligner que la notion de « conscience de la vulnérabilité » à été mise en lumière et jette les bases pour de nouveaux axes de recherche future. Cette dernière idée pose la question de savoir pourquoi dans les différentes organisation certaines vulnérabilités ne sont pas corrigées alors même qu'elles sont connues (problème « d'opposition au changement », faible capacité d'adaptation etc…).

6.2 Perspectives de recherche

Les résultats obtenus permettent d'ouvrir la voie à d'autres potentiels sujets de recherche qui pourraient le cas échéant être intégrés dans le processus de recherche-action entamé dans ce projet. Les différents points qui mériteraient ainsi une attention particulière sont les suivants :

Il sera vraisemblablement nécessaire de raffiner également les notions de temporalité amenée par la définition des contraintes définies comme calendaires. En effet la caractérisation de la marge de manœuvre est, comme on l'a explicité, partiellement liée à la distance à la date d'échéance. Il est apparu comme évident que plus on approche des dates butoirs, plus les marges de manœuvre se réduisent et appliquent donc un stress sur le respect des contraintes pour l'organisation. Les tableaux d'analyse proposés pourraient donc être remaniés pour faire apparaître cette notion. La notion de marge de manœuvre pourrait aussi être adaptée en proposant un version « dynamique » intégrant la prise en compte des dates d'échéance et de la périodicité des contraintes.

La notion de contrainte cependant mériterait d'être revue pour y intégrer directement le critère portant sur ce que nous avons appelé la catégorie d'impact pour l'organisation. En effet pour les

gestionnaires une contrainte s'identifie de façon rapide par l'impact que cette celle-ci aurait sur l'organisation en cas de non-satisfaction.

Un raffinage du processus d'identification des contraintes est également envisageable dans la mesure où l'un des partenaires cherchait à établir seulement les contraintes qui faisaient intervenir des outils TIC et revenait donc à faire un inventaire de l'ensemble des technologies afin de discuter de l'usage qu'il en était fait. Il est nécessaire de bien insister sur le fait que c'est par les contraintes que nous souhaitons aborder les technologies et non le contraire.

Enfin, de futurs travaux pourraient également envisager l'inclusion de ce type d'analyse dans une méthode de gestion des risques plus globale tels que Mehari ou Octave. Cet ajout pourrait être bénéfique dans la mesure où le cheminement d'analyse proposé dans ce mémoire adopte un point de vue différent et pourrait donc offrir un œil complémentaire sur la caractérisation de la vulnérabilité technologique.

6.3 Conclusion

Le cheminement d'analyse et ainsi la définition de vulnérabilité que nous avons établie se placent comme une alternative à la vision traditionnelle de la vulnérabilité qu'on retrouve dans les méthodes de gestion des risques classiques. En proposant une approche basée sur l'utilisation effective des outils dans l'organisation plutôt que sur la criticité estimée des intrants informationnels et leur contenant (Octave-S) ou que sur la probabilité d'occurrence d'un aléa (Mehari Pro), cette méthodologie se veut novatrice et abordable par un comité réduit de gestion centralisé autour du gestionnaire de la PME. Cette nouvelle vision conduit surtout à repenser la façon dont l'utilisation des TIC peut être perçue dans les organisations. Loin d'être un simple critère de criticité, cette notion devrait constituer un point de départ pour une analyse spécifique de la vulnérabilité des organisations par rapport aux TIC.

BIBLIOGRAPHIE

Adger, W. N. (2006). Vulnerability. *Global Environmental Change*, *16*(3), 268‑281. doi:10.1016/j.gloenvcha.2006.02.006

Alwang, J., Siegel, P. B., & Jorgensen, S. L. (2001). *Vulnerability: a view from different disciplines*. Social protection discussion paper series.

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*(Supplement C), 529‑534. doi:10.1016/j.protcy.2013.12.525

Benjamin, R. I. (1983). *Information Technology: A Strategic Opportunity*. Cambridge, Massachussets: Center for Information System Research.

Blili, S., & Raymond, L. (1993). Information technology: Threats and opportunities for small and medium-sized enterprises. *International Journal of Information Management*, *13*(6), 439‑448. doi:10.1016/0268-4012(93)90060-H

Bouwman, H., Van der Hoof, B., Van de Wijngaert, L. (2005). *Information and Communication Technology in Organisations: Adoption, Use and Effects*. Thousand Oaks, California: SAGE Publications.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* (CMU/SEI-2007-TR-012). Tiré de http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

CGI Business Consulting (2013). *Alerte au tsunami des données*. Tiré de https://www.cgi.fr/sites/default/files/files_fr/brochures/cbc_-_magazine_ap_si_-_1_-_alerte_au_tsunami_des_donnees_-_vf.pdf

Chaffey, D., White, G., Chaffey, D., & White, G. (2010). *Business information management: Improving performance using information systems*. UK: Pearson Education.

Chandler, D., & Munday, R. (2016). *Dictionary of Media and Communication*. Oxford University Press. Tiré de http://www.oxfordreference.com/view/10.1093/acref/9780191800986.001.0001/acref-9780191800986

Chong, S., & Pervan, G. (2007). Factors influencing the extent of deployment of electronic commerce for small- and medium-sized enterprises. *Journal of Electronic Commerce in Organizations*, 5(1), 1‑29.

Choo, C. W., Detlor, B., & Turnbull, D. (2000). *Web work: Information seeking and knowledge work on the World Wide Web* (Vol. 1). Springer Science & Business Media.

CLUSIF. (2010). Mehari 2010 : Overview. Tiré de https://clusif.fr/publications/mehari-2010-overview-2/

CLUSIF. (2013). Mehari Pro : Manuel de référence de la base de connaissance. Tiré de http://meharipédia.org

Cragg, P. B., & King, M. (1993). Small-firm Computing: Motivators and Inhibitors. *MIS Q.*, *17*(1), 47–60. doi:10.2307/249509

Davenport, T. H. (1997). *Information Ecology: Mastering the Information and Knowledge Environment*. Oxford, New York: Oxford University Press.

Deloitte. (2014). *Small Business, big technology. How the cloud enables rapid growth in SMBs*. Tiré de https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-small-business-big-technology.pdf

Dercon, S. (2005). *Vulnerability: a micro perspective* (QEH Working Papers No. qehwps149). Queen Elizabeth House, University of Oxford.

European Network and Information Security Agency (ENISA). (2006). *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises*. Tiré de https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes

Gouvernement du Québec. (2007). *Thésaurus de l'activité gouvernementale du Québec*. Tiré de http://www.thesaurus.gouv.qc.ca/tag/terme.do?id=12320

Harindranath, G., Dyerson, R., & Barnes, D. (2008). ICT adoption and use in UK SMEs: a failure of initiatives? *The Electronics Journal Information Systems Evaluation*. 11(2), 91-96.

Hashmi, M. S. J., & Cuddy, J. (1990). Strategic Initiatives for Introducing CIM Technologies in Irish SME's. Dans *Computer Integrated Manufacturing* (p. 93‑104). Springer, London. doi:10.1007/978-1-4471-1786-5_8

Kedar, S. (2009). *Database Management System*. Pune, Inde : Technical Publications.

Leavitt, H. J., & Whisler, T. L. (1958). *Management in the 1980's*. tiré de https://hbr.org/1958/11/management-in-the-1980s

Levy, M., & Powell, P. (2000). Information systems strategy for small and medium sized enterprises: an organisational perspective. *The Journal of Strategic Information Systems*, *9*(1), 63‑84. doi:10.1016/S0963-8687(00)00028-7

Marchesnay, M. (1991). La PME : une gestion spécifique. *Économie rurale*, *206*(1), 11‑17. doi:10.3406/ecoru.1991.4231

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud Computing — The Business Perspective. *Decision Support Systems*, *51*(1), 176‑189. doi:10.1016/j.dss.2010.12.006

Martin, B. (1996). Technological vulnerability. *Technology in Society*, *18*(4), 511‑523. doi:10.1016/S0160-791X(96)00029-2

Marty, M. (2014). *Analyses-diagnostics du potentiel de résilience d'une organisation*. (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

McFarlan, F. W. (1984). Information Systems Changes the Way You Compete. *Harvard Business Review*. Tiré de https://hbr.org/1984/05/information-technology-changes-the-way-you-compete

Micouleau, D. (2016). *Potentiel De Résilience D'une Organisation – Application À Des Services Municipaux.* (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Mills, D. E., & Schumann, L. (1985). Industry Structure with Fluctuating Demand. *The American Economic Review*, *75*(4), 758‑767.

Neo, B. S. (1991). Information technology and global competition: A framework for analysis. *Information & Management*, *20*(3), 151‑160. doi:10.1016/0378-7206(91)90052-4

Nonaka, I., & Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press.

Paradas, A., & Torrès, O. (1996). Les politiques de formation de PME françaises de classe mondiale. *Revue internationale P.M.E. : Économie et gestion de la petite et moyenne entreprise*, *9*(2), 7‑35. doi:10.7202/1008260ar

Porter, M. E., & Millar, V. E. (1985). *How information gives you competitive advantage*. Harvard Business Review, Reprint Service Watertown, Massachusetts, USA.

Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: The role of human, business, and technology resources. *Strategic management journal*, 375–405.

Quigley, E. J., & Debons, A. (1999). Interrogative Theory of Information and Knowledge. In *Proceedings of the 1999 ACM SIGCPR Conference on Computer Personnel Research* (p. 4–10). New York, NY, USA: ACM. doi:10.1145/299513.299602

Rainer Jr, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129–147.

Robert, J.M. (2009). Analyse de risque – Méthodologie Octave [Présentation PowerPoint]. Tiré de https://cours.etsmtl.ca/gti719/documents/cours/Cours-02-Analyse_Risque_Octave.pdf

Robert, B., Morabito, L. (2009). Réduire la vulnérabilité des infrastructures essentielles – Guide méthodologique. Paris, France : Editions TEC&DOC

Robert, B., Morabito, L., Quenneville, O. (2007). The preventive approach to risks related to interdependent structures. *International journal of emergency management*, *4(2)* , 166-182

Robert, B., Petit, F., Rouselle, J. (2004) Une nouvelle approche pour la caractérisation des aléas et l'évaluation des vulnérabilités des réseaux de support à la vie. Tiré de http://www.nrcresearchpress.com/doi/pdf/10.1139/l04-008

Smit, B., & Wandel, J. (2006). Adaptation, adaptive capacity and vulnerability. *Global environmental change*, *16*(3), 282–292.

Stockdale, R., & Standing, C. (2004). Benefits and barriers of electronic marketplace participation: an SME perspective. *Journal of Enterprise Information Management*, *17*(4), 301–311.

Storey, D. J. (1994). *Understanding the Small Business Sector*. Abington-on-Thames, Londres : Routledge.

TechTarget. (2015) Information Technology (IT) . Tiré de http://searchdatacenter.techtarget.com/definition/IT

Torres, O. (2000). Du rôle et de l'importance de la proximité dans la spécificité de gestion des PME. *5ème Congrès International sur la PME*, 25–27.

Turner, B. L., Kasperson, R. E., Matson, P. A., McCarthy, J. J., Corell, R. W., Christensen, L., Martello, M. L. (2003). A framework for vulnerability analysis in sustainability science. *Proceedings of the national academy of sciences*, *100*(14), 8074–8079.

Van der Spek, R., & Spijkervet, A. (1997). Knowledge management: dealing intelligently with knowledge. Dans Liebowitz, J., Wilcox, L.C. (édit.), *Knowledge management and its integrative elements* (p. 31–59). Boca Raton, Floride : CRC Press.

Rae, A. (2006). Abandoned Heroes – ICT Adoption and Use in SMEs. West Focus ICT Project. Tiré de http://kurir.kingston.ac.uk/AbandonedHeroes.pdf

Wiig, K. M. (1994). *Knowledge Management Foundations: Thinking about Thinking-how People and Organizations Represent, Create, and Use Knowledge*. Arlington, TX : Schema Press, Limited.

ANNEXE A – FICHE PRÉ-RENCONTRE

Objectif pré-rencontre : Caractériser les contraintes de l'organisation et commencer à réfléchir aux différents outils technologiques liés aux technologies d'information et de communication (TIC) utilisées afin de satisfaire ces contraintes.

Objet de la réunion : À partir des contraintes de l'organisation, faire le lien avec l'utilisation de TIC et caractériser la vulnérabilité associée à ces systèmes.

Identification des contraintes

Qu'est-ce qu'une contrainte : Il s'agit d'une condition à satisfaire afin d'atteindre les objectifs de l'organisation.

Nous avons identifié six types de contraintes :

1. Contractuelles : proviennent d'un engagement passé entre l'organisation et un acteur extérieur via un contrat reconnu et accepté par les deux parties.
2. Légales : requis légaux que l'organisation doit respecter de par la nature de ces activités.
3. Organisationnelles : issues de règles ou politiques de gestion internes.
4. Techniques : relèvent du domaine technique des activités de l'organisation. Elles peuvent porter sur les équipements de l'organisation ou sur certaines étapes clés du processus industriels, etc.
5. Économiques : requis économiques afin d'assurer la pérennité financière de l'organisation.
6. Sécuritaires : conditions pour maintenir un environnement de travail sécuritaire pour le personnel, mais aussi pour la protection des biens et des actifs.
7. Toutes autres contraintes

Avant la rencontre, il faut identifier diverses contraintes et lors de la rencontre, nous ferons avec vous le lien entre ces contraintes et :

- L'identification des conséquences pouvant en résulter
- L'utilisation des TIC qui en découle.