Equipe de recherche Sécurité de l'Information et Intelligence Economique
Université Montpellier I – Groupe Sup de Co Montpellier

Cahiers francophones de la recherche en sécurité de l'information

Numéro II

1er trimestre 2003

Faculté d`administration et Gestion
Espace Richter – Avenue de la Mer
BP 9640
34054 MONTPELLIER Cedex 1

Groupe Sup de Co Montpellier
2300, Avenue des Moulins
34185 Montpellier Cedex 4

Présentation du département

Sécurité de l'Information et Intelligence Economique S2IE

Le CRIC

Le Centre de Recherche en Information et Communication est une équipe de Recherche universitaire « labellisée » appartenant à l'Université de Montpellier I, autrement dit « équipe d'accueil ». Elle assure en son sein l'encadrement des thèses de doctorat et s'appuie sur un Diplôme d'Etudes Approfondies (DEA) qui prépare les étudiants souhaitant se tourner vers la recherche dans le domaine de « l'Info-Com », en particulier sur les Nouvelles Technologies de l'Information et de la Communication (NTIC).

Il comprend quatre départements : Médiation des savoirs, Communication d'Entreprise, Journalisme et Sécurité de l'Information, regroupant près de 50 chercheurs de tous niveaux.

Le département Sécurité de l'Information et Intelligence Economique

est une des nombreuses traductions du partenariat entre l'Université de Montpellier I et le groupe Sup de Co Montpellier. Il compte 12 chercheurs dont 7 doctorants et travaille dans diverses directions de recherche :

- Sécurité et Qualité
- Sécurité de l'Information et Management
- Sécurité de l'Information Médicale
- Sécurité sur le WEB
- Intelligence Economique et Sécurité de l'Information
- Communication institutionnelle et Sécurité de l'Information
- Epistémologie de la sécurité de l'Information.

Il est membre du CLUSIF, Club de la Sécurité des Systèmes d'Information Français.

L'équipe est susceptible de signer et de gérer des conventions de recherche avec différents partenaires (administrations, institutions diverses et entreprises) qui utilisent ses services dans le développement de moyens techniques, organisationnels et de formation en vue de faire monter les niveaux de sécurité de leurs systèmes d'information. En proposant ses compétences de haut niveau, l'équipe mobilise des moyens qui justifient une rémunération, modeste en regard des services offerts, et conduit des travaux de terrain pour l'avancement des connaissances dans son domaine

Elle gère une publication de recherche (Les Cahiers Francophones de la Recherche en Sécurité de l'Information). Elle participe à diverses manifestations organisées par d'autres organismes ou par elle même (salon INFOSEC fin Mai au CNIT de la Défense, colloque de recherche à Montpellier en novembre).

L'Equipe Sécurité de l'Information et Intelligence Economique du CRIC

Barlette Yves	Doctorant en sciences de gestion, Responsable du département systèmes d'information du Groupe Sup de Co Montpellier
Boursinou Eléni	Doctorante en information et communication, Université Montpellier I
Bruté de Rémur Damien	Maître de conférences, Directeur de recherches, Directeur du Département Sécurité de l'Information du CRIC, Université de Montpellier I
Chometon Pierre	Doctorant en sciences de gestion, université de Montpellier I Consultant, Professeur associé Groupe Sup de Co Montpellier
Dermigny Philippe	Consultant en Intelligence Economique
Drillon Dominique	Professeur du Groupe Sup de Co Montpellier Docteur en psychologie
Ferrand Christian	Président du CLUSIR LR, Membre du bureau du CLUSIF
Garcia Francis	professeur ENSAM en informatique à l'IUT, Université de Montpellier II
Gros Gilles	Doctorant en Intelligence économique, université de Montpellier I
Kaiel Abdelmalik	Doctorant en sciences de gestion, Université de Montpellier I
Touron Xavier	Doctorant , sciences de l'information et de la communication, Université de Montpellier I
Zalonis Dimitri	sciences de l'information et de la communication, Université de Montpellier I

Adresse du site CRIC : www.cric-france.com

Centre de Recherche en Information et Communication Faculté d'Administration et Gestion, UM1 Espace Richter, Avenue de la Mer, BP 9640 34054 Montpellier Cedex 1	Département Sécurité de l'Information et Intelligence Economique Groupe Sup de Co 2300, Avenue des Moulins 34185 Montpellier Cedex 4

SOMMAIRE

Titre	Auteur	Page
Editorial	Damien Bruté de Rémur	6
La sécurité de l'information : les enjeux	Damien Bruté de Rémur	7
Réflexions sur la communication publique entre PME et Commission Européenne en matière de sécurité de l'information	Eleni Boursinou	22
ORBAC : un modèle de contrôle d'accès basé sur les organisations	Yves Deswarte	30
Etude sur la sécurité du système d'information dans le milieu médical en Languedoc Roussillon	Francis Garcia	44
Partenariat interfirmes et securité des systèmes d'informations	Abdelmalik Kaiel	57
La prise en compte des émotions peut trouver une place dans la planification stratégique de la sécurité d'un système d'information ?	Dimitri Zalonis	65
Quelques ouvrages récents consacrés à la sécurité de l'information		72

EDITORIAL

Le premier succès d'une revue, aussi modeste soit elle (à l'image des cahiers francophones de la recherche en Sécurité de l'Information), est de présenter son numéro 2 !

Notre équipe est donc très heureuse de vous présenter ce deuxième numéro. Il faut dire aussi que les 200 exemplaires du N° 1 ont été très rapidement diffusés et que nous prenons la précaution de mettre celui-ci en ligne sur le site www.cric-france.com . Ainsi tout le monde y aura accès au-delà du traditionnel tirage papier qui restera de diffusion restreinte.

La caractéristique de ce numéro 2 est d'avoir recueilli des contributions spécifiques et de ne pas se contenter de constituer les actes d'un colloque.

Vous remarquerez les travaux des jeunes doctorants qui se lancent dès la première année dans le challenge de la confrontation publique.

Je tiens aussi à souligner particulièrement les contributions sur la sécurité de l'Information médicale en remerciant le LAAS de Toulouse de sa collaboration et en rappelant l'appui de l'Union Professionnelle des Médecins Libéraux du Languedoc-Roussillon qui fait confiance depuis plus d'un an à notre équipe et grâce à qui nous avons réalisé une enquête qui porte un riche potentiel pour des travaux de recherche futurs. Ce domaine, qui est ciblé prioritairement par toutes les grandes nations développées et donne lieu en Europe à des programmes de recherche extrêmement complets, est aujourd'hui probablement un des domaines les plus riches pour la discipline.

Bonne lecture,

Damien Bruté de Rémur

La sécurité de l'information : les enjeux

Damien Bruté de Rémur
Maître de Conférences HDR en Sciences de Gestion
Directeur du Département « Sécurité de l'Information et Intelligence Economique »
Centre de Recherche en Information et Communication
Université de Montpellier I

Résumé

Il s'agit de repérer quelques caractéristiques du sujet qui permettent de mesurer l'enjeu des travaux actuellement menés dans les différentes institutions qui s'intéressent à la question et de repérer des champs et des pistes prometteurs.

Le premier point est celui de la place grandissante prise par l'information dans les différents secteurs de la vie économique et sociale. Il faut ensuite souligner la montée en puissance du facteur sécurité comme objectif sociétal.

Les conséquences directes sont repérables sinon mesurables et permettent une relative quantification des enjeux, en tout cas de souligner l'intérêt fort, pour tous les acteurs, de prendre en compte le phénomène. Les moyens développés récemment sont enfin là pour indiquer d'une part la prise en compte de ces enjeux, et d'autre part les voies déjà explorées de travail pour la lutte contre l'insécurité.

SECURITE DE L'INFORMATION
LES ENJEUX

Une des questions que doit se poser le chercheur est celle des enjeux engagés dans sa recherche. L'intérêt scientifique est une chose, l'intérêt économique et social en est une autre.
La seconde motivation n'est pas moins importante quoique placée dans un plan différent.
Notre objectif ici est de tenter de donner une appréciation des enjeux réels mis en cause par « l'insécurité de l'information ». La recherche doit trouver ici une motivation supplémentaire, et les partenaires économiques et sociaux directement concernés porter un intérêt spécial à ces travaux.
Au moment où le système d'information médical est sérieusement mis en cause dans la garantie de sécurité qu'il peut offrir aux usagers, il est clairement d'actualité de repérer et évaluer les enjeux de la discipline.
Les développements qui vont suivre reprennent partiellement un article à paraître dans « Les Cahiers de la Sécurité Intérieure »[1].

Nous exposerons les points saillants de la question sous quatre aspects :
Tout d'abord ce que l'information est devenue dans le monde économique et social d'aujourd'hui. Il s'agit de montrer que nombre de mécanismes, d'institutions ou de performances économiques et sociales sont appuyés de plus en plus sur l'information considérée comme élément central et outil majeur.
Dans la deuxième partie nous examinerons les fragilités engendrées par les évolutions technologiques et sociales en exposant ce qui constitue de nouveaux risques ou de nouvelles vulnérabilités.
Un minimum de mesure est également nécessaire pour parler des enjeux, et ce sera notre troisième point.
Enfin, et nous ferons avec cela l'économie d'une longue conclusion, on peut recenser les évolutions actuelles dans le domaine des mesures de lutte contre l'insécurité.

[1] L'INFORMATION : UN ENJEU DE SECURITE GLOBALE par Alain AUMONIER et Damien Bruté de Rémur.

PARTIE I
L'INFORMATION NOUVELLE

Il y a du nouveau en effet, dans l'information. Il ne s'agit pas ici d'examiner la chose sous l'angle de l'Info-Com mais sous les angles plus pragmatiques, plus tournés vers la recherche de la performance, des disciplines juridiques, économiques et de gestion.
Le rôle croissant des actifs incorporels dans les échanges et la constitution des valeurs place le concept d'information au devant de la scène dans ces matières : c'est la naissance du « bien informationnel »[2]
Il y a des travaux urgents à mener dans cette voie : « Le capital immatériel reste un concept encore trop peu exploré »[3].
La conception pyramidale des besoins humains chère à MASLOW[4] s'actualise 50 ans après. Le positionnement du besoin de sécurité apparaît en effet comme moins pertinent aujourd'hui, et l'actualité nous fournit de nombreux exemples du retour en force de ce besoin, au delà des besoins psychologiques supérieurs.

I. Le bien informationnel

Etre une valeur en soi pour une information, cette hypothèse était réservée à quelques cas particuliers pour lesquels un droit de la propriété industrielle a été largement développé.
Le point nouveau aujourd'hui est que la notion de valeur de l'information s'élargit considérablement.
Il n'est pas question ici d'être exhaustif sur le sujet, beaucoup trop vaste et source d'un nombre incalculable de pistes de recherche dans les diverses disciplines déjà évoquées.
Nous choisissons de repérer les enjeux sur ce point à travers deux éléments caractéristiques du phénomène : le développement des systèmes d'information comme une clef de la performance, d'une part, et l'émergence de l'Intelligence Economique comme une stratégie concurrentielle pour l'acquisition d'avantages compétitifs décisifs, d'autre part.

A. Le développement des Systèmes d'Information

L'expression Systèmes d'Information et d'Aide à la Décision (SIAD) introduit clairement les enjeux qui sont en cause.
Le processus informationnel s'est développé à l'instar d'autres processus et devient pour l'entreprise un outil fondamental. Les NTIC ont donné à cela une

[2] Voir les travaux du Professeur Michel VIVANT, Faculté de Droit de Montpellier, UM I.
[3] Jean Philippe LACOUR, La tribune, 18 juillet 2000
[4] « Motivation and personality » Harper, N.Y. 1954

dimension nouvelle, rendant incontournable le recours aux outils du Web et de l'informatique.
Ce sont d'abord les méthodes de travail qui intègrent ces outils en développant les occasions de circulation et de traitement des informations.
Ce sont ensuite les systèmes de décisions eux mêmes qui se nourrissent des informations ainsi saisies, recueillies, traitées et stockées en vue de leur utilisation.

Les méthodes de travail
Le développement des outils de « Groupware » de plus en plus intimement mêlés aux outils de « Workflow » pour le traitement en temps réel, ce qui donne l'ensemble des outils de travail collaboratif[5] (CSCW), constitue sans doute une des principales caractéristiques de l'évolution récente dans ce domaine.
Il n'est donc pas possible de travailler sans échanger des informations. Cela nous le savions depuis longtemps. Ce qui est nouveau c'est la vulnérabilité des informations ainsi échangées. La circulation et le traitement des informations suppose en effet l'utilisation de technologies qui, même si elles intègrent le plus souvent la dimension sécuritaire, créent des vulnérabilités nouvelles.
La plupart du temps, dans ces données échangées apparaissent des informations stratégiques et/ou confidentielles.
Les risques tiennent à la destruction ou au vol de ces informations. Nous développerons en deuxième partie les risques en question. Qu'il nous suffise ici de souligner que ces outils, qui mettent à la disposition des entreprises et de l'ensemble des agents économiques et sociaux des moyens très performants de collaboration qui font tous les jours leurs preuves, peuvent être aussi des points de faiblesse.
Fabrice LEBRATY[6] met aussi l'accent sur les informations qui se stockent toutes seules dans les différents circuits de circulation et peuvent constituer des informations intéressantes pour autrui. L'abondance et la facilité avec lesquelles ces manipulations sont exécutées ne rendent pas souvent compte des vulnérabilités créées. On a bien développé les destructeurs de documents, pas encore les méthodes de vérification des données « égarées » dans les outils bureautiques.

Les Bases de données
Une fois les informations stockées selon des critères préalablement définis, elles constituent des cibles relativement vulnérables. Or les prises de décisions stratégiques vont largement dépendre des informations en question. C'est même probablement là que se situe une des questions fondamentales du sujet : dans un contexte de mondialisation et de concurrence exacerbée, la confidentialité des données stratégiques et des plans construits par les entreprises en vue de leur survie ou de leur développement est une exigence de plus en plus forte. « Si l'on nous prend notre plan d'affaires nous sommes morts » disait Philippe BALLADUR, responsable sécurité du groupe CEGETEL. On comprend mieux cela encore en soulignant que « voler » une information peut se faire sans aucune trace… ! La lecture d'un plan stratégique est d'autant plus dangereuse qu'elle se fait, ou peut se faire, à l'insu de l'entreprise.
Apparaissent donc deux problèmes sérieux : D'abord le maintien du système dans sa fonctionnalité, c'est à dire la sauvegarde des données dans leur disponibilité et intégrité ; et ensuite la protection contre la lecture indélicate.
Sur le premier, les normes ITSEC et le référentiel sur les prestations de service pour la sauvegarde à distance[7] ont fait largement avancer les choses… Il reste fondamentalement à développer une culture de sécurité de l'information qui reste extrêmement rare.
Les pistes de recherche sont alors dans les éléments d'organisation, de « Knowledge Management », de communication interne ou de coût de revient par exemple.
Sur le second, évidemment, les choses sont plus compliquées et cela demande des travaux importants encore. Si nous pouvons retrouver là des éléments communs aux deux points, il y a des considérations tout à fait spécifiques qui relèvent par exemple du cryptage, ou de la traçabilité, ou encore du droit et des poursuites possibles avec recherche de l'auteur et constitution de preuves. Le bouleversement concerne aussi les problèmes de responsabilité des collaborateurs et les derniers rebondissements judiciaires sur les questions touchant aux clauses de non concurrence ou aux conditions d'utilisation des réseaux Internet d'entreprise à des fins personnelles relancent largement le débat.
On voit bien que le sujet est d'importance en tout cas.

B. Intelligence Economique

La discipline est en train de trouver ses marques et elle fédère un certain nombre de pratiques tantôt bien spécifiées et organisées, tantôt plus floues dans les concepts et donnant lieu à des pratiques peu harmonisées. Parmi ces pratiques citons principalement les outils de veille, le benchmarking, la créativité et la gestion de l'innovation, et de nombreux outils de protection de l'information déjà.
L'I.E. se définit comme un ensemble de concepts et de méthodes rassemblées vers un objectif d'optimisation de la stratégie concurrentielle de l'entreprise en vue de l'obtention d'avantages compétitifs décisifs.

[5] Fabrice LEBRATY, Nice, Décembre 2001, colloque "Communication d'entreprise: regards croisés SDG/SIC". Voir aussi : Claude LEBOEUF « La fin du Groupware » 2001.
[6] Op cit

[7] Voir les différentes dispositions sur le site de la DCSSI et le référentiel AFAQ « service confiance » développé par Christian FERRAND.

La richesse cognitive globale de l'entreprise étant ici considérée comme la base du développement de l'outil, se posent alors deux questions importantes, la première sur l'élément humain proprement dit, et la seconde sur la valeur produite par ce travail d'I.E. au sein d'une entreprise.

Le facteur humain

Si l'entreprise fait ce passage tant vanté « d'une information distribuée à une information partagée », elle accroît d'autant plus ses points de faiblesse quant à la question sécuritaire.

D'une part les connexions externes à l'entreprise font de chaque collaborateur un point de fragilité, et d'autre part la relative volatilité de la main d'œuvre rend tout départ potentiellement dangereux, d'une part du fait de la perte de mémoire qu'il représente, et d'autre part du fait du risque de dissémination d'informations potentiellement utiles pour la concurrence et donc dangereuse pour l'entreprise .

On ne peut concevoir d'I.E. sans cela. Il faut donc accompagner très sérieusement le développement de ces méthodes en surveillant le niveau de sécurité du S.I..

Il faut « remettre l'humain au centre » de l'entreprise, certes, mais tout en se félicitant de cette démarche et en lui reconnaissant dans le cadre de l'I.E. une pertinence croissante, il nous faut bien reconnaître que cela suppose une nouvelle réflexion sur la question relative aux informations détenues.

La base de données est exposée

La « Guerre de l'Info » ou « Infoguerre » est engagée et les entreprises qui veulent la gagner doivent réellement travailler sur les côtés offensifs comme défensifs. Sur ce dernier plan, la sécurité de l'information est une exigence primordiale.

Au delà des considérations humaines il faut comprendre que les informations recueillies et traitées par la mémoire et l'analyse de la fonction I.E. constituent un contenu stratégique qui deviendra de plus en plus essentiel au fur et à mesure que la discipline se répandra dans les entreprises.

Pour être dynamique cette base de données doit fonctionner sans arrêt et doit manipuler en permanence les contenus en tissant les liens nécessaires. Ces liens sont eux mêmes autant d'opportunités potentielles qui résultent du travail de l'entreprise comme ils conditionnent sur le long terme la réussite de ses stratégies.

Autrement dit, plus le savoir faire dans ce domaine est grand, plus l'entreprise peut être l'objet d'attaques, et plus la confidentialité de ces informations vitales est menacée.

Si l'on veut que les concepts et méthodes si performants de l'I.E. se développent, la sécurité de l'Information doit être une préoccupation majeure.

Si le bien informationnel prend maintenant une place telle que sa protection devient une préoccupation au même titre que l'a toujours été la protection des biens en général on voit que les pistes de recherche sont nombreuses dans ce domaine. C'est là donc déjà, un enjeu majeur.

Parler de sécurité de l'Information sans parler de la sécurité elle même serait sans doute passer à côté d'une composante essentielle du monde économique et social du début du 3°millénaire.

II. La sécurité : un objectif sociétal essentiel

Les questions de sûreté ou de Sécurité, qui intéressent aujourd'hui de manière prioritaire les citoyens et les pouvoirs publics, s'incarnent facilement et logiquement dans les manifestations portant atteinte aux biens et aux personnes, depuis l'incivilité jusqu'aux catastrophes naturelles en passant par toutes les menaces et agressions qui pèsent sur les citoyens et les atteignent en tant que personnes ou à travers leurs possessions.

L'exercice serait intéressant de réfléchir à la place de cette notion au moment où elle fait la une des sondages et des programmes politiques avec les bouleversements et les incompréhensions que cela suscite dans tous les milieux sociaux et politiques. Un aspect au moins de cette question nous intéresse pour savoir si nous sommes dans un phénomène conjoncturel ou bien s'il s'agit d'un mouvement de fond.

On nous a traditionnellement présenté la société moderne comme poursuivant successivement, et au fur et à mesure des étapes de son développement, des objectifs fondamentaux constituant la base du consensus social.

Ce fut d'abord le développement et la croissance qui devaient nous conduire à une ***société de « consommation de masse »*** selon le modèle en 5 étapes de l'Américain ROSTOW. Ce niveau de vie était atteint par une grande quantité de citoyens à partir de la fin des années 60, sauf évènements conjoncturels de crises ou politiques de guerres. Il fallait un relais dans les objectifs sociétaux et l'on a alors parlé de ***« civilisation des loisirs ».*** Le développement du tourisme, la réduction du temps de travail, la mondialisation et le développement considérable des moyens de transport pour une majorité de nos concitoyens, chez nous comme dans les pays de niveau comparable, constitue très certainement une caractéristique remarquable de la fin du 20° siècle.

Comme la société ne pouvait se passer de chercher « toujours plus et toujours mieux » Un nouveau type d'objectif devait émerger. Il vient sur une base objective de montée de l'insécurité réelle et mesurable ; mais chacun sait bien, d'une part la relativité de la notion d'*insécurité*, et d'autre part que celle-ci repose d'abord sur le concept de « *sentiment d'insécurité* ». Voilà donc un nouvel objectif social

ou plutôt sociétal qui prend le relais du loisir **: *la sécurité.***

Nous devons aussi évoquer et c'est sans doute plus pertinent les théories de MASLOW sur la progression des besoins humains selon une pyramide dont la base est représentée par les besoins physiologiques suivis des besoins de sécurité. Au delà des besoins élémentaires, les besoins se déclinent dans la pyramide vers le besoin d'appartenance puis celui de l'épanouissement personnel, le schéma est bien connu. L'analyse était sans doute pertinente au milieu des années 50, années durant lesquelles les besoins élémentaires avaient encore à progresser dans les sociétés industrialisées. Il semble bien qu'aujourd'hui son actualité ne soit plus si claire. Le règne est désormais celui du « principe de précaution » qui concerne tous les secteurs de la vie. Logement, loisirs, consommations alimentaire, monde des jouets, automobile, secteur médicale, éducation/école…
A la base de cette culture sécuritaire en plein développement : l'information et la traçabilité. Cela concerne la vie quotidienne dans ses aspects les plus habituels.
Il est en effet connu de tous que les indications de l'étiquette deviennent la critère premier de la qualité et donc du prix. Qualité et sécurité se retrouvent naturellement, ici comme ailleurs.
Notre premier point sera ici de développer un peu sur ce thème pour cibler des enjeux actuels. Nous verrons ensuite que les NTIC sont en train également de bouleverser le mode de fonctionnement du marché. C'est le deuxième aspect de cet enjeu sociétal.

A. L'information dans les circuits traditionnels

Les divers secteurs d'activité sont directement touchés par la place de plus en plus prépondérante de l'information.
L'exemple le plus ancien est celui du ***nucléaire*** qui se trouve en première ligne des enjeux souvent pour deux raisons : La première est la nécessité de contrôler la sécurité des informations technologiques en vue de la préservation des performances de l'industrie nationale d'une part et dans le but d'éviter le diffusion d'informations dangereuses pour la paix mondiale d'autre part.
Parmi les effets de cette protection, ont été observées les réactions négatives de l'environ-nement social qui recherche une protection contre les risques réels ou supposés tels de cette activité. Le lien entre sécurité et information est tout à fait net. Tant la rétention que l'utilisation d'informations déformées porte des conséquences sociétales importantes. Il s'agit bien d'une question d'Intelligence au sens évoqué plus haut avec les aspects défensifs de la discipline.
L'industrie et le commerce ***agro-alimentaires*** sont un secteur également caractéristique. Point n'est besoin de démontrer cela aujourd'hui (ESB, mouvements divers en direction du commerce équitable et contre les excès de la mondialisation…). A chaque fois la place de l'information est primordiale. Cela passe par des certificats, labels, normes et attestations qui reposent sur des circuits d'information validés. On montre facilement que les enjeux liés à la protection des systèmes et des circuits de l'information sont dominants.
Prenons un dernier exemple, peut être le plus frappant : celui de ***l'information médicale***. Les enjeux sont là multiples : Yves DESWARTE, responsable du laboratoire LAAS de Toulouse, qui pilote avec Ernst et Young le projet MP6 sur la sécurité de l'information médicale du Réseau National de Recherche Technologique, insiste sur ce point en disant que se posent dans ce cas précis tous les aspects en même temps de la sécurité de l'information.
Probablement là plus que partout ailleurs, les progrès technologiques doivent apporter des solutions aux questions scientifiques et techniques en même temps qu'ils doivent permettre des économies considérables. Mais c'est aussi dans ce domaine que les questions de sécurité sont les plus sensibles, à la fois pour des raisons de confidentialité, aspect loin d'être résolu et qui semble prioritaire aujourd'hui, et pour des raisons de fiabilité. Les échanges d'information sur un patient pourraient permettre d'éviter des doubles emplois systématiques. On imagine facilement les risques que pourrait courir une population dont les données sanitaires seraient manipulables ou échangeables… des exemples de « piratage » de systèmes d'Information de cliniques ont été vus aux Etats Unis et pour le moment, seul l'aspect confidentialité a été atteint.

Nous ne voulons pas insister davantage pour montrer que la sécurité de l'information met en jeu des aspects très largement ouverts et concernant toutes les populations. Et encore n'avons nous pas parlé des aspects traditionnels de la protection des informations secrètes au niveau national, militaire ou civil. On estime que plus de la moitié des questions de défense nationale aujourd'hui concernent les problèmes de sécurité de l'information[8].
Dans la nouvelle information il faut évidemment citer le E-Business.

B. Les nouvelles donnes de l'information commerciale

Le sujet étant déjà abondamment et régulièrement traité, il nous suffira ici de souligner quelques aspects.

La sécurité des paiements.
Le développement de l'E-Commerce est sans doute une perspective tout à fait intéressante et les taux de croissance autour de 400% récemment observés sont très prometteurs.

[8] Tristan LECOQ, chargé de mission SGDN, au colloque IHEDN/IHESI, Paris, janvier 2002

Les mentalités évoluent lentement et les principaux freins ne sont plus d'ordre culturel ou psychologique mais tiennent essentiellement aux garanties offertes dans le traitement des informations mises en ligne par le client, notamment pour le paiement.

La confidentialité des données personnelles.
Les cookies contiennent des informations passionnantes sur les clients et même si l'on n'utilise pas cet outil pratique, les sites de commerce en ligne traitent régulièrement nombre d'informations concernant leurs clients qui permettront une meilleure performance dans le CRM ou suivi de clientèle. Il n'est pas forcément évident que ces informations soient toujours récoltées en accord avec les personnes concernées.

La garantie de bonne livraison.
Les piratages de données sur les e-business, s'ils sont possibles, permettent par exemple de détourner une commande prise et réglée par un client vers un autre destinataire.

Ces exemples ne sont qu'une partie des cas possibles et, au delà de l'E-commerce stricto sensu, on peut citer par exemple le problème général des nouveaux systèmes de paiement comme les incontournables cartes bancaires, ou bien le piratage des téléphones mobiles…

Sans avoir besoin d'aller plus loin il est évident que l'information est partout présente comme l'élément moteur et central qui conditionne le développement du commerce et de l'économie toute entière.

PARTIE II
RISQUES ET VULNERABILITES D'AUJOURD'HUI

De nouvelles fragilités liées à cette information sont également apparues.
Notre société est devenue dépendante de son espace « informatique ».
Elle est donc sujette à des vulnérabilités liées aux utilisations frauduleuses ou criminelles de cet espace que ce soit pour l'acquisition d'informations essentielles afin de gagner la bataille de la connaissance, faciliter des entreprises criminelles classiques ou assurer un plus concurrentiel à des entreprises privées. Ces vulnérabilités sont la conséquence d'actions volontaires affectant les matériels, les ressources et les réseaux.
Ces actions se traduisent par des destructions physiques, des sabotages immatériels ou la corruption de données. [9]

La menace pèse également sur les équipements physiques (ordinateurs et périphériques), les ressources logiques et virtuelles (vol de fichiers, altération ou duplication de logiciels, destructions de données par infections informatiques ou sabotage manuel) et les réseaux (moyens de liaisons entre les équipements informatiques).
Les deux concepts de risque et de vulnérabilité sont bien distincts et la recherche aura intérêt à travailler dans cette distinction. Une entreprise qui court de gros risques pourra être invulnérable (théoriquement !), alors qu'on pourra observer une atteinte malgré un très faible risque sur une entreprise vulnérable.
Un troisième point sera de donner une idée de la mesure du phénomène à travers quelques exemples, chiffrés ou non, des conséquences possibles des atteintes à l'Information.

I. Quelques mots sur les risques

Nature et origine seront de bons critères de classement ; mais notre ambition ne va pas plus loin ici qu'une évocation.

A. Atteintes volontaires externes

Les résultats des études du CLUSIF montrent qu'elles sont ressenties exagérément par les usagers et nous rejoignons ici le constat bien connu de l'IHESI qui parle de la Sécurité Intérieure davantage comme d'un sentiment, d'un « ressenti », que d'un constat et d'une mesure objective. Les circonstances politico-sociales, qui sont tout à fait caractéristiques de ce phénomène en Europe, nous ont appris aussi cela. La communication aura sans doute un rôle considérable à jouer en la matière.
En citant les chiffres donnés par Gilles DANAN[10] dans son interview à la revue « CYBER-GESTION » (DBR mai 2002), Chiffres empruntés au CLUSIF, on remarque trois exemples flagrants :

- Pour les ***vols et sabotages physiques***, risque le plus facile à mesurer sans doute, on observe déjà un écart important : cela est perçu comme représentant près de ***20%*** des atteintes, alors que le chiffre de la sinistralité (probablement assez proche de la réalité sur ce sujet) est inférieur, tout compris à ***9%.***

- Pour les ***infections virales***, la perception situe le risque à ***41%*** des atteintes alors que la réalité est seulement de ***11,5%,*** ce qui est déjà, somme tout important compte tenu des protections disponibles.

- Pour les ***attaques logiques*** ou intrusions, aux ***50%*** de risques perçus, il faut opposer les ***1,8%*** réels. A dire vrai dans ce cas, les détections d'intrusions sont très largement sous estimées et on peut penser que dans ce cas la sinistralité déclarée est

[9] Le cabinet d'audit américain Ernst &Young évalue les pertes globales, occasionnées par la criminalité informatique mondiale à environ 5 billions de dollars par an en 1998.

[10] PDG de BACKUPAVENUE, société spécialisée dans la sauvegarde à distance des données numériques.

peu significative. Nous serions dans un cas particulier où la perception, bien que très supérieure aux chiffres réels connus, apparaisse comme plus juste.

Il y a en tout cas clairement un mécanisme identique à celui qui est généralement perçu en matière de Sécurité Intérieure : le sentiment d'insécurité ne dépend pas seulement des attaques reçues ; mais aussi très largement des attaques simplement « connues » et arrivées aux autres !

Dans les trois exemples donnés, le premier ne relève pas d'un type de délinquance bien original puisque aussi bien nous retrouvons purement et simplement des comportements déviants classiques.
Il en va différemment des deux domaines qui suivent et qui concernent spécifiquement les TIC ;
Nous ne développerons pas ce nouveau type de risque tant il est vrai qu'il est « à géométrie variable » en fonction des populations concernées : les informations détenues par les citoyens sont en effet de sensibilités différentes selon qu'il s'agit de données privées et sans implication ou sans valeur spéciale ou qu'il s'agit au contraire de données « sensibles » comme le sont les informations techniques ou scientifiques détenues et utilisées par les entreprises de haute technologie ou dans des professions sensibles comme les médecins par exemple. Le degré de sensibilité mesure alors l'enjeu réel.

B. Les atteintes « de l'intérieur » et involontaires

De la même manière qu'en matière de sécurité routière, le simple comportement individuel ou collectif plus ou moins inconscient peut revêtir des aspects de dangerosité qui constituent largement une qualification d'insécurité.
Ce mécanisme est plus insidieux car il présente une auto atténuation sous deux angles : Le premier est celui du caractère facilement admis comme habituel ou normal de l'erreur humaine. Au-delà du côté positif de ce qui relève de la vertu de tolérance, il s'agit bien aussi de considérer le fait comme « négligeable». Cela ne serait rien si dans le domaine de l'information cette atténuation bien naturelle ne risquait de comporter des conséquences graves. On sait bien dans certaines activités particulières que les procédures doivent suppléer la défaillance humaine au- delà de la simple marge d'erreur acceptable sous l'adage latin « errare humanum est ».
L'enquête du CLUSIF est tout à fait révélatrice à ce sujet : les simples ***pannes ou erreurs*** de conception et d'utilisation des technologies représente dans la réalité mesurée de la sinistralité près de ***60%*** des sinistres alors que la perception de cet état de choses ressort comme explicative au maximum à ***5%.*** Cet écart considérable donne la mesure d'un phénomène contre lequel la lutte est d'autant plus difficile : on sait la difficulté de lutter contre la « criminalité routière » alors que la quasi-totalité des conducteurs de voiture se considère comme « excellents conducteurs » !

Nous en venons naturellement aux populations concernées car il est en effet impossible de réfléchir sur les risques eux-mêmes en les détachant des citoyens ou agents économiques concernés.
Il s'agit bien alors de mesurer les vulnérabilités.

II. Les populations concernées et leurs vulnérabilités

On pourrait être tenté de diviser en « sécurité publique » et « sécurité privée » ; mais ce serait ignorer que les enjeux de Sécurité Intérieure concernent aussi les intérêts privés des personnes : il est clair par exemple que le secret médical, s'il concerne des informations privées et justement pour cela d'ailleurs, est un enjeu de sécurité publique. La CNIL est le meilleur exemple d'organisme public destiné à défendre les intérêts privés.
Pour éviter cet écueil nous parlerons d'intérêt national et d'intérêt privé.

A. Informations d'intérêt national

Il n'est pas question ici de faire le catalogue de tous les agents ou organismes détenant des informations dans cette catégorie. L'évocation de deux grandes catégories suffira à notre démonstration.

- Les ***organismes publics*** exerçant la puissance publique à proprement parler (administrations publiques) sont évidemment les premiers concernés ; et, dans l'histoire, le concept de « SECRET DEFENSE » restera sans doute le premier exemple d'information dont la protection relève d'un enjeu de « Sécurité Publique ». Comment ne pas comprendre en effet que les intérêts nationaux dépendent de la confidentialité des opérations diplomatiques, militaires ou judiciaires. Cela est pourtant souvent considéré, à tort ou à raison, comme contradictoire avec les principes de base de la démocratie ; mais les choses avancent sur ce point et les mesures prises par exemple pour assurer plus de transparence sur les « Fonds Spéciaux » montrent les progrès de la démocratie sur ce terrain. Il reste que bien souvent la condition de l'efficacité de l'action publique repose sur la discrétion. Mais les atteintes ne sont pas à limiter aux seuls aspects de confidentialité de l'information : elles se présentent aussi et peut-être, surtout sous la forme de désinformations ou manipulations qui sont sans doute plus dangereuses encore. Les attaques contre les Systèmes d'Information eux-mêmes sont surtout à craindre tant il est vrai que leur fonctionnement sans faille conditionne la pertinence des décisions prises à tous les niveaux. Les « HACKERS » ne s'y trompent pas et attaquent le plus souvent des sites publics pour faire preuve de leur ingéniosité nuisible. Les intérêts nationaux ne se limitent pourtant pas à cela et c'est évident si l'on songe seulement par exemple aux enjeux considérables que représente la recherche

publique. La politique de plus en plus suivie de protection des résultats de la recherche publique, démarche non naturelle en France, est significative de l'évolution là aussi. Il s'agit de préserver les conditions de la compétitivité de l'économie nationale.

- Les ***entreprises***, force vitale de la nation, sont également de plus en plus susceptibles d'une attention particulière sur ce plan. Parmi de nombreux auteurs, Bernard BESSON et Jean Claude POSSIN[11], ainsi que Thibault du MANOIR de JUAYE[12], ont mis l'accent ces dernières années sur les risques courus par l'Information compte tenu de son intérêt stratégique grandissant pour les entreprises. L'explication en est simple et tient aux trois constats classiques : d'abord mondialisation par le développement des TIC, puis importance croissante de l'Information Technologique et Stratégique dans un univers économique de concurrence exacerbée et de plus en plus turbulent, et enfin vulnérabilité accrue due au développement de l'Internet. Le GDS de la session régionale IHESI 1999/2000, « Nouvelles Technologies et Sécurité », sous la présidence de Danièle PUJAZON[13], faisait remarquer judicieusement que les entreprises aujourd'hui doivent s'ouvrir ou mourir ! Elles sont évidemment exposées et rendent vulnérables la collectivité entière aussi au titre des informations scientifiques qu'elles échangent notamment avec les services publics de recherche et développement.

La prise en compte des vulnérabilités de ces divers agents, et notamment au titre des données concernant directement ou indirectement des enjeux économiques, est actuellement assurée par les services du haut fonctionnaire de défense au MINEFI. Le service Intelligence Economique de ce ministère éminemment stratégique sur le plan national assure là une mission primordiale à la fois dans la partie offensive et en matière de Sécurité de l'Information.
Il s'agit bien de « Sécurité Publique » dans la mesure où la responsabilité des services publics d'Etat est en première ligne. On voit bien cependant que la frontière entre Sécurité Intérieure et Défense Nationale se fait plus ténue. La notion de frontière est en effet plus délicate à déterminer et l'on sait bien les difficultés ressenties par les forces de sécurité du fait de la « mondialisation » de cette nouvelle délinquance qu'est la cybercriminalité. La note signée par Alain AUMONIER en 2001, énumère les neufs potentialités criminelles nouvelles liées aux NTIC. Il s'agit dans chaque cas d'atteintes à la Sécurité de l'Information. Il y évoque aussi la coopération internationale sur le sujet et les travaux de l'OCDE sont une tentative de traiter ces questions « au-delà des frontières ».

B. Informations d'intérêt privé

Cette même note d'Alain AUMONIER évoque les trois catégories d'agents que sont les administrations, les entreprises et les particuliers. Tristan LECOQ, chargé de mission au SGDN, lors de la rencontre IHEDN/IHESI de janvier 2002 évoquait la part croissante des préoccupations concernant les « intérêts vitaux » de la nation. Il précisait que les problématiques traditionnelles liées au concept de protection du « sanctuaire » national, entendu au sens territorial étaient effectivement totalement dépassées, tandis que la préoccupation des responsables de l'Etat s'oriente de plus en plus vers des atteintes moins classiques aux intérêts nationaux, facilitées par les nouvelles donnes de la mondialisation. Il y a certes les nouvelles organisations terroristes internationales qui peuvent frapper au delà des frontières. Au-delà de cette question préoccupante, les intérêts vitaux pris pour cibles sont de plus en plus des éléments non militaires dont la destruction ou la mise hors d'état de fonctionner peut atteindre la France au cœur : on pense aux structures industrielles majeures comme le réseau de centrales nucléaires par exemple. Plus insidieuses et peut être plus dangereuses sont les actions liées aux systèmes vitaux fondamentaux des populations nationales, telles que des opérations d'empoisonnement par pollution des eaux ou par des opérations du type « guerre bactériologique » comme on a pu le voir avec le bacille du charbon ou comme on le redoute à propos des installations découvertes en IRAK. Mais tout ceci ne concernerait apparemment l'information que comme moyen ou conséquence.

Pourtant, de récents accidents survenus aux Etats Unis montrent que des attaques sur des systèmes d'information touchant directement les personnes privées comme les informations médicales sont parfaitement possibles et peuvent avoir des conséquences dramatiques.
Les moyens techniques actuellement disponibles autorisent par exemple des attaques sur le système d'information médical (SIM) en France, attaques pouvant prendre différentes formes dont les plus anodines sont la diffusion des informations, et les plus dangereuses les modifications de données ou échanges de données entre dossiers. Le Ministère de la Recherche, via le réseau national de recherche sur les Télécommunications a lancé un programme sur deux ans (projet MP6) pour appuyer la mise au point de moyens et d'outils destinés à faire monter le niveau de sécurité du SIM. De plus en plus en effet les progrès de la médecine impliquent la coopération entre divers spécialistes et divers établissements au chevet des patients, et cette circulation de données pour la mise en commun des informations ouvre grande la porte aux risques. L'obligation faite au

[11] « Du renseignement à l'Intelligence Economique », 2° édition, DUNOD 2001.
[12] « Intelligence Economique : utilisez toutes les ressources du Droit » 2001.
[13] Rapport GDS, 7°session régionale IHESI, juin 2000.

corps médical libéral de s'informatiser avant la fin de l'année 2000 introduit des technologies souvent peu ou mal maîtrisées et les praticiens eux-mêmes reconnaissent les dangers de ces pratiques. L'Union Professionnelle des Médecins Libéraux du Languedoc-Roussillon, consciente du phénomène, a entamé un travail en profondeur, en liaison avec MP6, pour détailler les conditions actuelles de fonctionnement des réseaux et préparer la mise en œuvre sur le terrain de nouveaux modes d'organisation des réseaux qui permettent l'optimisation de l'usage des NTIC dans des conditions optimales de sécurité. Cette étude se fait avec l'appui de notre équipe de recherche.

On comprend facilement que le SIM pourrait être une cible idéale pour des intérêts hostiles aux intérêts nationaux français.
Si le domaine de l'Information médicale est un exemple caractéristique, on peut facilement comprendre que de nombreuses autres cibles sont possibles sur des données qui ne concernent que des intérêts particuliers.
A cela ajoutons que l'accroissement très rapide du parc des ordinateurs personnels constitue en lui-même une menace car l'utilisation par les HACKERS de ces appareils sur lesquels ils peuvent prendre la main à travers des logiciels apparemment anodins.

PARTIE III
DES IMPACTS IMPORTANTS

Dans leur livre « L'INFOGUERRE », Philippe GUICHARDAZ, Pascal LOINTIER et Philippe ROSE[14] montrent à quel point l'information est devenue aujourd'hui un des objets majeurs du combat concurrentiel, international notamment. La compétitivité des entreprises en dépend directement.
On sait parfaitement, par ailleurs, que l'économie est fragilisée par la concentration des moyens informatiques.
Les activités d'interception d'Information, tout à fait répandues, ont des conséquences significatives à partir d'une certaine échelle. On peut légitimement penser que le seuil est atteint alors que l'on voit s'allumer partout des clignotants d'alerte. Les Dirigeants d'entreprise s'inquiètent de plus en plus ouvertement des atteintes ou des risques d'atteintes à leur information technologique ou stratégique. Les citations seraient trop nombreuses pour être intéressantes ; mais l'intervention de Jean François DEHECQ aux 4° rencontres nationales de l'Intelligence Economique était très significative, tandis que Philippe BALLADUR, responsable de la sécurité au groupe CEGETEL nous faisait remarquer que toute la sécurité d'un tel groupe aujourd'hui se structure autour de la sécurité de l'Information.

Les assurances commencent à enregistrer des sinistres directement liés à la perte d'information ; mais les contrats sont difficiles à généraliser et les déclarations largement en dessous des sinistres réels. Il faut aussi noter du côté des assurances l'entrée sur le marché de services performants de sauvegarde à distance qui constituent de véritables assurances de restitution intégrale des données et de ce fait rendent inutile toute forme d'assurance spécifique, sauf cas très particuliers.
On peut aussi remarquer que la perte de données informationnelles ne constitue pas une nouveauté du monde des NTIC. Il faut cependant relever que ce qui constituait autrefois un risque classique d'atteintes aux biens mobiliers et immobiliers (incendies, inondations…) qui se traduisait accessoirement par des pertes d'information, se trouve décuplé par les risques spécifiques de l'informatique et par l'importance croissante des actifs incorporels.

I. Les attaques spécifiques

Les déclarations de sinistres enregistrés pour pertes d'information aux assurances représentent en France de 2 à 3 milliards d'€ par an chiffre à multiplier par 3 ou 4 si l'on veut approcher les coûts réels (déclarations non faites notamment). Nous tenons là une évaluation concrète intéressante.

Le FBI dans sa dernière étude avec le CSI publiée en avril 2002 rappelle les chiffres déjà évoqués dans les rapports précédents sur les pertes financières des entreprises : en moyenne près de 500 millions de dollars en 2001 pour les 223 entreprises ayant donné des informations précises sur le sujet : c'est considérable et justifie sans doute une préoccupation nationale ! La première source de coûts identifiée dans les questions de sécurité informatique est celle de la perte d'informations techniques et économiques, et la deuxième la fraude financière.

Une des principales causes de perte de données est tout simplement la perte ou le vol (évidemment plus vraisemblable !) d'ordinateurs portables. Chaque année aux Etats-Unis sont concernés environ 200000 appareils dont la valeur matérielle est négligeable au regard de la perte des informations contenues estimées à plus de 50 millions de dollars.
La valeur des informations contenues peut aussi s'exprimer par les conséquences de leur perte. Le CLUSIF constate à ce propos que plus des trois quarts des entreprises subissant un sinistre majeur (perte totale de plus de 75% des données) déposent leur bilan dans les deux ans.

Les activités délinquantes se développent et représentent plusieurs types d'actions :

[14] « L'Infoguerre », **Philippe GUICHARDAZ, Pascal LOINTIER, Philippe ROSE**, DUNOD, 1998

A. Le vol d'informations

Aujourd'hui, on vole moins un « PC » pour sa technologie que pour les informations qu'il contient. De même un réseau est pénétré, plus pour accéder à une banque de données que par esprit ludique. D'interne la menace tend à devenir externe.

Les détournements d'informations représentaient en 1996 déjà 58% des sinistres informatiques commis en France selon le CLUSIF [15].

Ces sinistres informatiques sont évalués au total **à 11,56 milliards de francs en 1995** pour la seule France..

B. Les attaques sur les systèmes d'information

•Le poste « **malveillance » représente** 6.8 milliards de francs et la fraude 1,67 milliards de francs de pertes.

• les **attaques logiques** (1.24 milliard de francs) se taillent la part du lion **soit 9.74 milliards de francs** et **85 %** des pertes dues …à condition qu'elles soient identifiées et signalées ! !

Or, une attaque dite « institutionnelle » sur vingt cinq le serait aux USA, d'après le Pentagone.

Ce chiffre est à rapprocher des 90% de fraudes informatiques signalées aux sociétés d'assurance en France mais non déclarées aux services de Police en France, selon le CDIA [16].

Ces trois formes de criminalité informatique devraient croître fortement avec l'essor prévisible de l'informatique, de l'exploitation des communications mais également avec la poursuite de la crise, l'insécurité de l'emploi et la crise propre au secteur informatique et son corollaire de conséquences pour les informaticiens (déstabilisation de certaines fonctions, budgets restrictifs, concurrence accrue).

Une enquête de la « Fondation pour la Recherche Sociale » de 1996 fait apparaître une augmentation des préjudices liés au crime informatique de 7 à 10% par an jusqu'en 2005.

Cela représente une projection envisageable **de 20 milliards de francs de préjudice identifié en 2005**.

II. Une tendance à l'externalisation et à l'adaptation de délits connus par le biais de l'informatique : un développement inquiétant

Avec la tendance à l'externalisation du crime informatique, il est logique de voir surgir de nouveaux acteurs. Le crime organisé ne peut que s'intéresser au crime informatique [17].

Si le rôle des mafias russes dans les fraudes informatiques est devenu révélateur voire prépondérant[18], nous accordons une attention toute particulière aux formes de criminalité suivantes :

A. Piratages et contrefaçons

En 1994, 57 % des logiciels utilisés en France sont des copies contrefaites constate le BSA [19] . Cela représente un manque à gagner ou des pertes financières lourdes de **4 milliards de francs** en 1996 pour les développeurs et les éditeurs de logiciels nationaux.

- Le détournement des communications de téléphones mobiles qui est rendu possible par l'intégration de l'informatique et de l'électronique dans ces outils de communication [20], soit un préjudice de 600 millions de dollars aux USA en 1997.
- Le vol et commerce de microprocesseurs et de mémoires.
- Le blanchiment d'argent électronique par les serveurs et les réseaux [21]
- Le dévoiement des autoroutes informatiques d'Internet par :
    - les réseaux pédophiles internationaux
    - les « narco trafic »
    - les hold-up informatiques (intrusions dans les systèmes de transferts de fonds électroniques des banques et détournements de monnaie « électronique »)
    - les sites de casinos virtuels électroniques délocalisés dont le C.A, d'environ **4 0** milliards de dollars par an. échappe aux taxes et législations nationales [22].
    - les magasins virtuels mettant à dispositions des produits localement interdits tels que médicaments classés, drogues et produits dopants acheminés par courrier postal banalisé.
    - le ré encodage des cartes de crédit servant au règlement des transactions en cash à partir de comptes électroniques (portefeuille créé à partir du disque dur des ordinateurs particuliers).

Or, le marché français de « l'achat en ligne » comme nous l'avons déjà vu, est en croissance exponentielle et passa de 42 millions de francs d'achat de produits ou de services sur les sites Internet en 1997 à 400 millions de francs en 1998. L'augmentation du volume des transactions électroniques (+850% en un an) qui peut être considérée comme un indicateur valable en terme de volume et de progression de l'activité illicite s'y rattachant, démontre que toute une économie illicite et

[15] Club de la Sécurité des Systèmes d'Information Français

[16] Centre de Documentation et d'information de l'Assurance.

[17] Discours de Louis FREEH , Directeur du FBI, à l'International Association of Chiefs of Police, Albuquerque 18Octobre 1994.

[18] Selon M. FREEH, il existe dès 1996, 25 gangs russes spécialisés dans la fraude informatique, implantés dans 17 villes US et comptant environ 2000 membres ….

[19] Le Business SoftWare Alliance, organisation mondiale regroupant les éditeurs de logiciels.

[20] Re Programmation de portables avec des numéros de lignes affectées et interceptées par scanner.

[21] Exemple de l'European Union Bank, banque internationale Internet dont l'adresse électronique le domicilie dans le paradis fiscal d'Antigua depuis 1994.

[22] 160 cyber-casinos clandestins ont été répertoriés sur le WEB en 1998.

galopante fonctionne déjà sur un marché mondial incontrôlé pour l'instant.
Ainsi, dès 1997, le Trésor Fédéral US estimait à environ **100 milliards** de dollars, les préjudices subis dans ce pays, imputables uniquement aux hold-up informatiques, ventes et reventes de fichiers –clients des grandes sociétés, destructions de données commerciales au profit de concurrents et à l'utilisation frauduleuse de numéros de cartes de crédit et de comptes via l'informatique (cette dernière activité lucrative est promise malheureusement à un bel avenir d'après le CLUSIF).

B. Des enjeux stratégiques encore mal appréciés

Nous comprenons bien que les évaluations soient très délicates et nous sommes très certainement en dessous de la réalité : moins de la moitié de plus grandes entreprises américaines est capable de donner un chiffre.
Ce qui est certain c'est que les enjeux économiques deviennent considérables.

Confrontés à ces vulnérabilités et à ces ordres de grandeur, toute action de sécurité sur les systèmes d'information doit intégrer les quatre points fondamentaux suivants :

1. Les systèmes d'information sont par nature difficiles à surveiller parce qu'ils sont organisés en réseaux interdépendants et ignorent les frontières.
2. La dépendance de nos sociétés à l'égard de ces systèmes va croissant et notre société devient une société de l'information, cette dernière s'avérant aussi vitale que l'énergie.
3. Le problème de sécurité le plus nouveau et le plus décisif est de nature économique et financière, donc stratégique.
4. Le droit de la sécurité des systèmes d'information se doit de concilier la sécurité des systèmes avec la sécurité juridique.

PARTIE IV
LES MOYENS D'ACTION ET LEUR EVOLUTION

Les actions sont orchestrées par la combinaison d'instruments permettant un équilibre et autorisant un degré tolérable de pratiques « border law » en échange d'une exploitation créative de la technologie.
Nous verrons d'abord le rôle direct des citoyens avant d'en venir aux moyens d'action publique.

I. Les actions émanant de la société civile .

Ainsi furent mis au point des logiciels spécialisés dans des contenus adaptés à la consommation des familles, logiciels bloquant l'accès à des sites « douteux », logiciels de classement et de filtrage de type « Platform for Internet Content Selection ». Ce dernier exemple est révolutionnaire dans la mesure ou pour la première fois un instrument de contrôle global et généralisé est intégrable au média …
Puis se développèrent le marché de la réparation des dégâts causés par les attaques des systèmes de télécommunication (équipes informatiques de traitement d'urgence – SAMU « informatique »), le marché des solutions de sauvegarde de confiance sur le commerce électronique d'Internet (bombes logiques utilisées contre le vol de la propriété intellectuelle).

Au deuxième degré, les forces du marché peuvent exercer un contrôle par le biais du principe de proportionnalité des primes d'assurance aux mesures de protection prises par les entreprises assurées contre le piratage et les actes de vandalisme informatique.

A. L'autorégulation par les fournisseurs de service et les compagnies de télécommunications.

Elle induit des codes de bonne de conduite et le respect de certains protocoles entre l'utilisateur et ces organismes pour limiter les risques d'abus dans le cyberespace. La sanction de ceux -ci est une rupture de contrat.

B. La coproduction citoyenne.

Elle aboutit à des formes privées de contrôle et de surveillance du cyberespace (ex : le Centre Simon Wiensenthal et des Cyber Angels) aux fins de déceler et de dénoncer toute information à caractère raciste, antisémite, pornographique ou contribuant au piratage informatique, au développement des virus, fabrication d'explosifs. L'information est alors transmise aux autorités compétentes. C'est un exemple de coopération visant à résoudre les difficultés classiques du contrôle légal réservé aux plus sérieuses atteintes.

C. L'autoprotection des victimes potentielles

Elle passe par l'intégration de procédures de sécurité (restriction d'accès, « firewalls », sécurité bio-métrique, programme de détection des anomalies) et l'association des fournisseurs de service aux responsabilités découlant des infractions.

D. Les solutions commerciales fondées sur le marché

Au premier degré, elles sont l'offre des fournisseurs de services qui ont très vite intégré leur intérêt à « surfer » sur les nouveaux marchés :
Mais, les formes nouvelles de régulation des illégalités et de protection dans le cyberespace peuvent avoir des effets pervers comme, par exemple, l'effet « fruit défendu » ou l'émergence de sites miroirs quant on bloque l'accès à un site « douteux » et l'essaimination

dans des juridictions plus permissives servant de points d'accès aux matériaux en cours.

Enfin, deux logiques semblent s'affronter dans la conception, le développement et la mise en œuvre des défenses ci-dessus évoquées :

D'une part, un impératif de dérégulation caractérisant les économies avancées et d'autre part, la nécessité d'exercer un contrôle minimum des aspects les moins licites des nouveaux domaines.
Trop de régulation et d'interdits n'aboutirait qu'à freiner le développement des nouvelles technologies, source de croissance économique (relation entre l'impact des NTIC et de la croissance des PIB dans les pays avancés) au risque de piètres résultats et de coûts prohibitifs.
De plus, toute limitation des investissements et de l'innovation prive ces mêmes autorités de contrôle des futurs instruments de connaissance et des armes dont on peut être sûr que les autres acteurs ne se priveront pas.

E. Les structures privées de surveillance et de contrôle

Nous pouvons leur joindre un acteur économique tel que France Telecom qui mène une politique de surveillance des serveurs Minitel évoluant vers une déconcentration au niveau régional et se trouve de fait à la charnière entre les services de surveillance et les institutions. Il s'agit de réagir *a posteriori* aux courriers adressés au Conseil Supérieur de la Télématique et cette institution ne vise qu'à surveiller la partie publique du Minitel et non les boites aux lettres accessibles par mot de passe soumises au secret des correspondances. Son arme suprême se limite aux dispositions contractuelles permettant de couper tout serveur ne respectant pas la loi .

Pour sa part, le **CLUSIF** oriente son action vers la recherche et le développement en sécurité des systèmes information .
Il est constitué de constructeurs, de sociétés de service et d'ingénierie, de cabinets d'audit et de conseil, d'assureurs et de juristes.

L'association pour la Protection des Programmes (**APP**) enregistre sous certaines conditions, les logiciels créés par les développeurs leur permettant ainsi en l'absence de « brevet » comparable aux inventions technologiques classiques, de bénéficier d'un droit d'antériorité lors d'un litige postérieur à la commercialisation du produit.

Enfin, le syndicat des éditeurs de logiciels de loisirs (**SELL**) organise la profession des éditeurs et édite un code de déontologie de la profession destiné à protéger les acheteurs.

On voit clairement que, si la responsabilité citoyenne est première, elle se trouve souvent largement dépassée et contrainte de faire appel à des moyens extérieurs, sous forme d'offres commerciales certes ; mais qui n'exonèrent pas les autorités de contrôle de leurs responsabilités et ce d'autant plus que bien souvent la nécessaire harmonisation des modes d'action suppose une référence publique (comme le système de normalisation ou de certification…).

II. L'arsenal juridique national et les outils de répression et de contrôle

A. Les principaux textes français en la matière

Loi 78-17 du 6 janvier 1978 « Loi Informatique et Libertés » réprimant la création des fichiers clandestins, l'enregistrement ou la conservation illicite d'informations nominatives, le détournement de finalités d'informations nominatives, la divulgation illicite d'informations nominatives, la collecte d'informations sans information préalable des personnes interrogées.

- Loi 85-660 du 3 juillet 1985 dite « Loi sur la protection des logiciels » qui punit toute reproduction de logiciel autre que pour les nécessités de sauvegarde.

Ce fait répréhensible est devenu un délit prévu par l'article 332 du Code de la Propriété Intellectuelle. La loi assimile un logiciel à un contrat de licence.

- Loi 88-19 du 02 janvier 1988 dite « Loi Godfrain » réprimant l'accès frauduleux aux systèmes informatiques, le maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données, le fait de fausser ou d'entraver intentionnellement un système, l'introduction, la suppression ou la modification intentionnelle directe de données dans un système de traitement automatisé, la falsification de documents informatisés et leur usage intentionnel.
- Le décret 86-250 du 18 février 1986 définissant et réglementant les moyens de cryptologie (matériel ou logiciels conçus pour transformer à l'aide de conventions secrètes des informations claires ou des signaux en informations ou signaux inintelligibles).

Ce texte prévoit l'autorisation préalable à l'utilisation sur le territoire français du Service Central de la Sécurité des Systèmes Informatiques.

- L'article 28 de la loi du 29 décembre 1990 relative à la réglementation des télécommunications tolérant le cryptage de la signature et de la certification d'intégrité d'un message mais interdisant le cryptage du message (sauf accord très restrictif du S.C.S.S.I)
- L'article 17 de la Loi du 26 juillet 1996 sur la réglementation des Télécommunications assouplit les dispositions légales en la matière en définissant le nouveau régime de la cryptologie. Il est possible désormais d'utiliser librement la cryptologie pour authentifier et contrôler l'intégrité des messages informatiques. En revanche, pour assurer la confidentialité des contenus, il faut recourir à « des tiers de confiance » agréés par le Premier Ministre et soumis au secret professionnel. Le but est de permettre la protection de l'information, le développement des communications et des transactions sécurisées tout en

préservant les intérêts de la défense nationale et de la sécurité intérieure et extérieure de l'Etat. A terme, l'on évolue vers une libéralisation complète en la matière.

La jurisprudence
En développant un travail d'imagination face aux nouvelles facettes du crime informatique, il s'agit de faire évoluer la jurisprudence des tribunaux civils en matière de contrats informatiques vers une plus grande responsabilité des fournisseurs d'accès (assimilation à un intermédiaire technique) et une obligation des utilisateurs d'informer le fournisseur quant à l'utilisation du produit.

B. La mise en œuvre de services spécialisés

Si l'émergence de services spécialisés dans la lutte contre les nouvelles formes de criminalité utilisant les nouvelles technologies de l'Information et de la Communication, se traduit par une action répressive, elle fait également intervenir les Renseignements Généraux et la Direction de la Surveillance du Territoire qui assurent également une surveillance du Web par le biais de sections spécialisées dans le renseignement informatique et la dotation de capacités autonomes et puissantes de décryptage jusque là réservées à la Direction Générale de la Sécurité Extérieure.
Ces actions bénéficient ou génèrent un fort développement des technologies modernes liées à la sécurité informatique.

Les services répressifs .
Le Service d'Enquêtes sur les Fraudes aux Technologies de l'Information (**SEFTI)** appartenant à la Sous –Direction des affaires économiques de la direction régionale de la police judiciaire de la Préfecture de Police de Paris.
Il mène des enquêtes judiciaires relatives aux infractions visant ou utilisant les systèmes informatiques, les modes de traitement automatisés, le stockage et la communication de l'information.
Pratiquement son action se traduit par le démantèlement des réseaux de faussaires de logiciels, la lutte contre les vols physiques de matériels et de composants et l'utilisation de logiciels sans licence. Ce service apporte également son concours technique aux autres services de police qui le sollicitent et mène des actions de formation et d'information sous forme de conférences auprès des organismes publics et privés demandeurs .

L'Office Central de Répression de la Criminalité Informatique (**OCRCI**) dont la mission consiste à gérer le bureau central national Interpol pour la fraude informatique, assurer des missions d'enquêtes judiciaires au niveau national, coordonner les enquêtes diligentées en matière de délinquance informatique par les autres services et assister les services centraux ou extérieurs dans l'approche des systèmes informatiques rencontrés dans le cadre de procédures financières ou criminelles.

Le Service Informatique de l' Institut de Recherches Criminelles (**IRCGN)** de la Gendarmerie Nationale est aussi mis à contribution lors des enquêtes concernant les nouveaux outils de communication et de traitement de l'information (notamment les réseaux pédophiles sur Internet).

Les structures publiques de surveillance ou de contrôle .
Au niveau gouvernemental, il existe un organisme en charge des dossiers concernant la sécurité informatique : le Service Central de la Sécurité des Systèmes d'Information. En l'état actuel de la législation, ce service n'a pas à motiver ses décisions de rejet ou de demandes d'autorisation de cryptage qui lui sont obligatoirement adressées. Cet organisme est l'autorité dans l'attribution des normes ITSEC[23] des logiciels de chiffrement disponibles sur le marché français.

C. La mise en place d'une coopération internationale

La proposition FILLON à l'Organisation pour la Coopération et le Développement Economique en octobre 1996 prévoyait une charte de coopération internationale axant ses dispositions autour de l'établissement d'un code de bonne conduite et un accroissement de la coopération policière internationale pour lutter contre les délits liés aux NTIC. Elle s'inscrit dans l'action d'institutions telles :
Le **G7/P8** (les sept pays les plus développés plus la Russie) dont le Plan d'Action contre la criminalité High-Tech adopté en décembre 1997 a pour objet :
- L'adaptation des législations nationales pour permettre la condamnation des utilisations anormales des systèmes informatiques et de télécommunications;
- Le renforcement des capacités techniques permettant de localiser et d'identifier les criminels en coopération avec les opérateurs et fournisseurs d'accès à Internet;
- L'amélioration de l'entraide judiciaire en vue de collecter les éléments de la preuve;
- L'engagement des ressources pour la formation et l'équipement du personnel.

L'Organisation Internationale de Police Criminelle et son groupe de travail européen sur la criminalité liée aux technologies de l'information porte particulièrement ses efforts sur des stages de formation adaptés aux nouveaux types de délinquance destinés aux magistrats et policiers des pays européens.

Le Comité PC CY du Conseil de l'Europe et sa finalisation de projet de convention internationale relative au cyberespace en matière pénale. Ce projet couvre le fond du droit pénal (création d'incrimi-nation

[23] Critères d 'évaluation de la sécurité des systèmes d'information .

de fond), la procédure pénale (dispositions spécifiques sur la valeur probante des preuves électroniques), la compétence juridictionnelle (règlement des conflits de compétence entre les juridictions) et les aménagements des législations nationales susceptibles de faciliter la coopération internationale (régime des responsabilités et notamment celui des fournisseurs d'accès).

Les USA, le Japon et le Canada participent à ces travaux et sur de nombreux points les réflexions menées au sein du G8 rejaillissent sur l'activité du Conseil de l'Europe. Les questions en suspens des perquisitions et des saisies transfrontalières dans les réseaux, de la saisie des mails restent entiers.

La problématique centrale en matière de stratégie d'action est de chercher un équilibre qui autoriserait un degré tolérable d'illégalité en échange d'une exploitation créative de la technologie et du développement de l'économie numérique, moteur fondamental de l'économie.

Cet équilibre serait la résultante des préférences assignées au marché émises par les gouvernements, les groupes d'intérêts et les consommateurs –citoyens. Les solutions adoptées en réponse à ces signaux, si elles devaient être plus efficaces que les réponses traditionnelles étatiques, n'excluent pas une coopération internationale organisée.

Cela contribuera peut-être à garder dans la sphère du politique les capacités à organiser et structurer un ordre international, facteur de sécurité pour toutes les entités dans un contexte où la révolution de l'information, la puissance des grands groupes, financiers, économiques et de haute technologie pèse de plus en plus lourd sur la constitution des équilibres planétaires régionaux, locaux, sectoriels à venir.

On peut aussi signaler l'initiative de l'OCDE qui a lancé une opération de sensibilisation des gouvernements et de suivi de leurs actions dans ce domaine.

CONCLUSION

A travers ces exemples, on peut dire aujourd'hui que les questions de Sécurité de l'Information sont un point de passage indispensable pour permettre le développement des nouvelles technologies de l'information comme des nouveaux outils de management privé et public.

Les champs de recherche sont extrêmement nombreux, dans des disciplines variées, et les retombées à attendre sont très facilement valorisables étant donnés les coût observables de la non-sécurité.

Il y a beaucoup de travail et pas assez de chercheurs.

BIBLIOGRAPHIE

- **AUMONIER A. et Bruté de Rémur D.** L'information : un enjeu de Sécurité Globale, A paraître, Cahiers de la Sécurité Intérieure, printemps 2003.
- **BESSON B., POSSIN J.C.** : « Du renseignement à l'Intelligence Economique », 2° édition, DUNOD 2001.
- **FERRAND Christian** : « Le management de la qualité appliqué à la Sécurité de l'Information », mémoire de DEA, Sciences de l'Information et de la communication, UM1, octobre 2002.
- **GUICHARDAZ Ph., LOINTIER P., ROSE Ph.**, « L'Infoguerre », DUNOD, 1998
- **LACOUR Jean Philippe**, La tribune, 18 juillet 2000
- **LEBOEUF Claude** « La fin du Groupware » 2001.
- **LEBRATY Fabrice**, Nice, Décembre 2001, colloque "Communication d'entreprise: regards croisés SDG/SIC".
- **MASLOW A.M.** « Motivation and personality » Harper, N.Y. 1954
- **Du MANOIR de JUAYE Thibault :** « Intelligence Economique : utilisez toutes les ressources du Droit » 2001.
- **PUJAZON Danièle** (sous la présidence de..) : Rapport GDS, 7°session régionale IHESI, juin 2000.
- **VIVANT Michel**, Ensemble des travaux. Faculté de Droit de Montpellier, UM I.

Réflexions sur la communication publique entre PME et Commission Européenne en matière de sécurité de l'information. Les premières pistes pour un projet de thèse.

Eleni Boursinou
Doctorat en SIC (1ère année)
Boursinou.eleni@wanadoo.fr
Tél. 04.67.63.21.62

Résumé : Le présent article est un questionnement sur la communication publique de la sécurité de l'information en Europe. Il ne s'agit pas d'un simple échange d'information mais elle s'inscrit dans la perspective d'agir ou de tenter agir sur les organisations. La communication publique représente l'un des meilleurs indicateurs du progrès et il est impératif d'enrichir ses théories et ses pratiques pour la promotion d'une valeur comme la sécurité.

Mots clés: communication publique/institutionnelle, sécurité de l'information, systémique, Europe

Abstract: This paper presents the challenge of public communication in Europe as far as information security is concerned. It is not a simple exchange of information but an effort to make organisations more active in the matter. Public communication represents one of the vital signs of progress and the improvement of its methods and practices in order to promote a value such as security is urgent.

Key words: public/institutional communication, information security, systemic, Europe

Introduction

Un néophyte en Sciences de l'Information et de la Communication est invité à faire un choix de sujet/projet pertinent et des choix méthodologiques importants pour acquérir la posture du chercheur. Une palette de possibilités s'ouvre devant lui de manière étonnante car le choix est immense. Comme le note J.L Le Moigne les chercheurs doivent être aptes à réfléchir et répondre aux termes d'un contrat social « que ces chercheurs réfléchissent scrupuleusement à leurs réponses aux trois questions fondatrices de l épistémologie et du statut de la connaissance : quoi ? , Comment ? , Pourquoi ? .»

Une problématique sur le rôle de l'Union européenne à une culture de sécurité de l'information est-elle une problématique de SIC ? Nous voulons analyser comment la distribution de l'information est faite et quel est le processus pour arriver aux PME. Nonobstant nous ne voulons pas se contenter à une description des faits. Bourdieu dit sur la communication « qu'il suffit provisoirement de prendre claire conscience du fait qu'une perspective d'analyse matérialiste doit sans arrêt nier l'apparence que se donne la sphère des communications : elle n'est pas un miroir où se refléterait l'actualité, elle n'est pas une place publique, même électronique, comme le dit MacLuhan, elle constitue le lubrifiant général des rapports sociaux de production, de consommation, d'échange, de reproduction. Pour dire autrement la même chose, communiquer ne sert pas seulement à communiquer ou alors on se contente de décrire des phénomènes. »

Le sujet est typiquement transversal aux Sciences de Gestion et chaque discipline est concernée dans ses contenus. L'approche en amont de la problématique fait sortir la question du seul domaine de compétence des concepteurs et réalisateurs d'outils aptes à protéger les informations ou les systèmes : si l'approche n'est pas globale, toutes les dispositions prises ou à prendre s'avèrent inefficaces.

La sécurité de l'information est un sujet passionnant. Le fait qu'aujourd'hui il y ait très peu de sensibilisation et que c'est l'insécurité qui règne à sa place est un paradoxe. Il s'agit bien sur d'un problème de nature complexe.
Notre but dans cet article est de suivre le conseil d'Edgar Morin « de mettre de l'ordre dans les phénomènes, en refoulant le désordre, d'écarter l'incertain, c'est à dire de désambiguïser, clarifier, distinguer, hiérarchiser… », en vue de dégager les tendances d'un projet européen d'e-sécurité.

L'originalité du sujet réside au traitement de l'Union européenne comme milieu organisationnel. L'objet d'étude est le fonctionnement des échanges entre les hommes et les entreprises à travers les messages et les effets éventuels sur les récepteurs.

En d'autres termes, la communication est traitée comme lieu de la constitution sociale des phénomènes que l'analyse sociale se donne pour tâche de décrire et d'expliquer, comme « milieu » dans lequel émergent et se maintiennent les objets et les sujets, les individus et le collectif, le monde commun et la société.

Comme toute organisation, l'Union européenne a une structure hiérarchique selon laquelle les décisions sont prises. « Les directions ne peuvent décider de l'innovation, elles ne peuvent qu'y inciter car elles ne contrôlent pas la définition du sens et de l'efficacité du travail; elle est en fait amenée à arbitrer entre des forces de défense des règles antérieures et des forces d'innovation. (la «destruction créatrice »)

Pourquoi l'Europe ?

D'après Dominique Wolton[24], « l'Europe est pour un chercheur travaillant sur le rapport entre communication et société, un terrain d'expérimentation des théories et un lieu d'observation empirique essentiel. Elle offre une leçon de modestie quant à l'efficacité du modèle rationaliste de l'information. Il ne suffit pas d'informer, de communiquer, de faire pression sur les opinions publiques, d'ouvrir les cultures les unes sur les autres pour créer de l'intérêt mutuel… »

L'Europe nous permet en réalité de reprendre une question théorique fondamentale, celle des rapports entre communication et communauté. « Penser le rôle de l'information par rapport à l'Europe, c'est le situer par rapport à un projet. Et tout le problème vient de la bien trop faible clarté de ce projet. On y trouve pour le moment beaucoup de réalité institutionnelle et peu de réalité symbolique. »

« D'autre part, il faut bien avoir conscience qu'il n'y a pas d'Europe sans communication. Impossible au citoyen d'adhérer à ce projet sans un rôle essentiel de l'information et de la communication qui sont des moyens normatifs, et non fonctionnels de dépasser les clivages actuels. »

Dans tous les cas la construction européenne illustre les limites, comme facteur de mobilisation, du rôle de l'information et de la communication. La dynamique communicationnelle est une façon d'analyser l'action de communiquer dans le temps. Elle considère ce qui se passe auparavant, pendant et après l'échange de signes. Notre projet suit cette même logique.

Notre ambition coïncide avec l'ambition de la systémique qui est *de penser la globalité, les interactions entre les éléments plutôt que les*

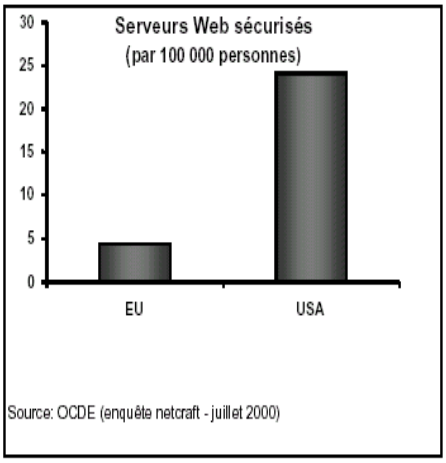
[24] Wolton D., *Penser la communication*, Flammarion, 1997

causalités, d'appréhender la complexité des systèmes comme des ensembles dynamiques aux relations multiples et changeantes.

L'interaction est la clé de voûte de ce qu'on a appelé après les apports systémiques et constructivistes de l'école de Palo Alto « la nouvelle communication. »
L'intelligibilité du système (de communication) doit être trouvée, non seulement dans le système lui-même, mais aussi dans sa relation avec l'environnement et cette relation n'est pas une simple dépendance, elle est constitutive du système. Le fait de nous rendre familier de ce terrain tout en demeurant indépendant et à distance est une difficulté majeure selon Bruno Latour et aussi un défi à réaliser les années à venir.

Pour conclure, il ne fallait jamais oublier que la communication y est étudiée comme action située: située dans un cadre, un contexte qui englobe l'échange et qui constitue un ensemble de « marques » permettant l'attribution de sens. Goffman (1974), par exemple, a montré que des individus placés en situation de co-présence sont soumis à des règles et que leur action a lieu à l'intérieur d'un cadre (frame), ce « dispositif cognitif et pratique d'attribution de sens qui régit l'interprétation d'une situation et l'engagement. » (Joseph, 1998) Il existe donc, selon lui, un ordre de l'interaction, ordre dans lequel la communication est un acte social régulé auquel on participe. Les acteurs sont actifs et peuvent déformer, bloquer, détourner l'information ou bien l'utiliser comme une arme : proposer une image favorable aux partenaires, faciliter le changement, protéger la confidentialité, etc.

L'objectif est de faciliter la compréhension d'un phénomène qu'on pourrait appeler la politisation de la communication des entreprises. Autrement dit quel est le dispositif réglementaire de l'Union Européenne pour communiquer avec les entreprises.



Le tableau nous aide à comprendre l'écart entre la réalité américaine et celle en Europe. L'Europe est confrontée à plusieurs problèmes particulièrement urgents : la nécessité d'une sécurité à toutes épreuves, d'une protection des attaques virtuelles contre ses réseaux et des attaques physiques contre son infrastructure informatique.

Pour le projet de thèse, on voudrait exploiter trois notions principales : l'environnement socio-politique de l'Union; sa responsabilité sociale, politique et éthique ainsi que la gestion de sa communication externe. Il est également question de souligner qu'on considère l'Union Européenne comme une organisation avec tous les éléments caractéristiques. Cette partie inspiré par le livre de I. Nonaka et H. Takeushi « la Connaissance créatrice »[25] De Boeck Université, 1997 part de la croyance que l'entreprise ne traite pas seulement la connaissance mais la « crée » aussi. On va explorer *la connaissance explicite celle qui peut être articulée en langage formel comprenant les énoncés grammaticaux, les expressions mathématiques, les spécifications, les manuels* et ainsi de suite. Il s'agit des connaissances qui sont devenues conscientes et qui sont exprimées en forme de rapports, de propositions ou de décisions de la Commission, du Conseil et du Parlement.

Dans le cadre d'une analyse systémique on devrait considérer les éléments dans leur ensemble les uns vis-à-vis des autres et dans leur rapport à l'ensemble. « Un système est constitué d'un ensemble d'éléments en interaction dont chacun concourt à l'objectif commun ou finalité du système ». [26]Pour faire une telle approche, il est essentiel d'inclure dans notre analyse les autres acteurs du système à part l'Union Européenne (le rôle des états et des régions) pour chercher à comprendre comment chaque élément contribue à la finalité du système en préservant sa propre identité. Cette méthodologie nouvelle qu'on veut adopter pour le projet de thèse nous permet de dépasser des blocages liés à une représentation cartésienne et séquentielle de l'information et des actes.

L'Europe en tant qu'organisation *intelligente*

Au sein de l' Union européenne, certains États membres ont déjà mis en place des unités spécialisées dans la criminalité informatique. La Commission estime que la création de ces unités est une privilège des États membres et incite vivement ces derniers à prendre des mesures dans ce sens. Les pouvoirs publics devraient fixer des priorités et prendre les décisions politiques qui s'imposent par l'achat des tous derniers matériels et logiciels ainsi que la formation de leur personnel. Les expériences des unités existant déjà dans quelques États membres

[25] I. Nonaka et H. Takeushi, La Connaissance créatrice, De Boeck Université, 1997
[26] A. Yatchinovsky, L'approche systémique pour gérer l'incertitude et la complexité, ESF éditeur, 1999

pourraient être particulièrement précieuses et la Commission prendra des mesures pour encourager l'échange de ces pratiques.

La Commission pense également qu' Europol peut contribuer à une valeur ajoutée supplémentaire au niveau communautaire, par des actions de coordination, d'analyse et d'autres formes d'assistance menées auprès des unités nationales spécialisées. Elle supportera par conséquent l'extension du mandat d' Europol à la cybercriminalité.

Certains États membres ont mis sur pied des initiatives pour former le personnel des autorités chargées de l'application des lois aux hautes technologies. Les autres États membres qui n'ont pas encore pris de mesures similaires devraient être incités à suivre leur exemple.

Divers projets allant dans ce sens, qui se présentent sous la forme d'échanges d'expériences, de séminaires consacrés aux challenges communs auxquels se heurtent les catégories de professionnels concernées, ont été lancés avec l' appui de programmes gérés par la Commission (en particulier, les programmes STOP, FALCONE et GROTIUS). Celle-ci va faire de recommandations pour d'autres activités dans ce domaine, notamment en ce qui concerne la formation en informatique et en ligne. Europol a pris l'initiative d'accueillir une session de formation d'une semaine destinée au personnel des autorités chargées de l'application des lois des États membres, qui a eu notamment pour thème la pornographie enfantine. Le champ de ce type d'action pourrait être élargi de manière à englober la criminalité informatique en général.

Le but d'une initiative de sensibilisation des citoyens, des administrations et des entreprises serait donc de fournir des informations accessibles, objectives et fiables sur la sécurité des réseaux et de l'information. Lorsque cette sensibilisation aura eu lieu, les personnes seront libres de faire leurs propres choix quant au niveau de protection qui leur convient.

Les États membres doivent lancer une campagne d'information et d'éducation du public et il convient de renforcer les travaux en cours à l'aide d'une campagne médiatique et des actions s'adressant à toutes les parties intéressées. Une campagne d'information bien conçue et efficace est coûteuse. L'élaboration d'un contenu qui décrit le risque sans alarmer inutilement le public et sans encourager les pirates potentiels exige une planification rigoureuse. Dans le cadre du programme eEurope 2005, un nombre des propositions ont été suggéré pour arriver à un niveau de sensibilisation.

Premièrement les États membres soutenus par la Commission devraient promouvoir l'utilisation des meilleures pratiques en matière de sécurité sur la base des mesures existantes telles que la norme ISO/ IEC DIS 17799 (*code of practice for information security management*.) Il convient de cibler plus particulièrement les petites et moyennes entreprises.

En deuxième lieu la sécurité devrait être enseignée dans les écoles. Les systèmes éducatifs des Etats membres devraient mettre davantage l'accent sur les cours sur la sécurité. L'élaboration de programmes éducatifs à tous les niveaux, comme par exemple la formation en matière de risques pour la sécurité sur les réseaux ouverts et les solutions efficaces, devrait faire partie de l'enseignement de l'informatique dans les écoles.

Un système européen d'alerte et d'information

L'élaboration d'un système européen d'alerte et d'information serait un moyen pour les Etats membres de renforcer leurs équipes d'intervention en cas d'urgence informatique (CERTs) et d'améliorer la coordination entre elles. La Commission examinera avec les Etats membres la meilleure façon d'organiser au niveau européen, la collecte des données, l'analyse et le planning des réponses à donner aux menaces de sécurité actuelles et futures.

Même lorsque les utilisateurs sont conscients des risques pour la sécurité, il faudra toujours les avertir de nouvelles menaces. Les pirates trouveront presque inévitablement de nouvelles vulnérabilités pour échapper aux meilleures méthodes de protection. L'industrie développe constamment de nouveaux services et logiciels offrant une meilleure qualité, rendant l'Internet plus attrayant, mais créant en même temps involontairement des vulnérabilités et des risques nouveaux.

Même les ingénieurs de réseau expérimentés et les experts en sécurité sont souvent étonnés par la nouveauté de certaines attaques. Par conséquent, il est nécessaire de disposer d'un système de détection précoce qui peut rapidement alerter tous les utilisateurs, ainsi que d'une source de conseils rapides et fiables sur la manière de lutter contre les attaques. Quant aux entreprises, elles ont besoin d'un mécanisme confidentiel leur permettant de rendre compte des attaques sans risquer de perdre la confiance du public. À cela doit s'ajouter une analyse de sécurité prospective plus complète, qui rassemble des données et évalue les risques, avec l'avantage d'une vision plus large. Beaucoup d'efforts sont faits dans ce domaine par les équipes publiques et privées d'intervention en cas d'urgence informatique (CERT) ou les organismes semblables.

La Commission propose d'inclure la sécurité dans le futur 6ème programme-cadre, qui est actuellement à l'étude au Conseil et au Parlement. Pour optimiser ces dépenses, il faut établir un lien avec une stratégie plus large en matière de sécurité des réseaux et de l'information. *La recherche soutenue par ce*

programme devrait relever les défis que représentent, en matière de sécurité, le "tout numérique" et la nécessité de sauvegarder les droits des individus et des communautés. Elle sera centrée sur des mécanismes de sécurité fondamentaux et leur interopérabilité, des processus dynamiques de sécurisation, des méthodes de cryptographie avancées, le renforcement du respect de la vie privée, des technologies de traitement des actifs numériques et des technologies garantissant la fiabilité à l'appui de fonctions économiques et organisationnelles au sein de systèmes dynamiques et mobiles.

La certification des processus d'entreprise et des systèmes de gestion de la sécurité des informations est soutenu par le Guide de coopération européenne pour l'accréditation EA17. L'accréditation des organismes de certification renforce la confiance dans leur compétence et leur impartialité, ce qui favorise l'acceptation des certificats à travers le marché intérieur.

C'est pourquoi les activités actuelles de normalisation et de certification doivent être mieux coordonnées afin de suivre l'introduction de nouvelles solutions pour la sécurité. L'harmonisation des spécifications entraînera à la fois une plus grande interopérabilité et une mise en œuvre accélérée par les acteurs du marché.

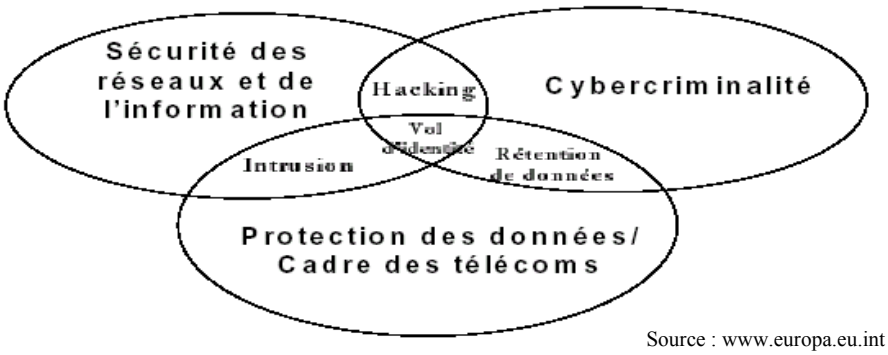
Il est préférable pour les organismes européens de normalisation qu'ils accélèrent leur travail sur les produits et services interopérables et sécurisés selon un calendrier ambitieux et bien défini.

La Commission continuera à soutenir, notamment à travers ses programmes IST et IDA, l'utilisation des signatures électroniques, la mise en œuvre de solutions PKI interopérables et conviviales, ainsi que la poursuite du développement des protocoles Ipv6 et IPSec.

En 1999, la société Deloitte & Touche, dans une évaluation, a émis l'avis suivant:
« Les Euro Info Centres sont évalués de façon positive. Leur impact quantitatif et qualitatif est important. Ils témoignent également d'un effet de "réseaux" croissant, et leur apport en valeur ajoutée aux PME va bien au-delà de leur rôle traditionnel de fournisseurs d'informations sur les affaires européennes. »

La gamme de services des EIC s'étend à l'Info service, l'assistance et le conseil.
Diffuseurs d'information, les EIC mettent à la disposition des entreprises un grand nombre de documents. Organisateurs de séminaires et de conférences, ils participent activement à des manifestations de forte mobilisation sur des thèmes prioritaires dans les pays de l'Union européenne, les PECO et le bassin méditerranéen. Dans le cadre de la campagne d'information 1999-2000 sur l'euro, les EIC organisent plus de 270 actions auprès des PME. En 1998, les EIC ont poursuivi la campagne de sensibilisation en matière de santé et de sécurité sur le lieu de travail dans les PME lancée en 1997. Les EIC seront amenés à coopérer à des actions de sensibilisation dans le cadre de l'initiative eEurope («go digital») visant à faire accéder le plus grand nombre possible de PME au commerce électronique.

La sécurité des réseaux et de l'information est un problème dynamique



Source : www.europa.eu.int

En raison de sa rapidité, l'évolution technologique lance en permanence de nouveaux défis : les problèmes d'hier sont résolus et les solutions à ces problèmes sont caduques. Presque quotidiennement, des applications, des services et des produits nouveaux sont offerts sur le marché. Mais il est évident que certains développements présenteront des défis majeurs pour une politique de la sécurité privée et publique.

La nature même des infractions informatiques pose, sur les scènes nationales et internationales, le problème des procédures applicables, dans la mesure où des souverainetés, des compétences et des législations différentes s'opposent. Plus que pour toute autre forme de criminalité transnationale, la rapidité, la mobilité et la flexibilité de la criminalité informatique défient les règles existantes du droit pénal procédural.

L'asymétrie d'information

Les réseaux deviennent de plus en plus complexes et atteignent un marché plus large comprenant de nombreux utilisateurs qui connaissent mal la technologie ou ses dangers potentiels. Cela signifie que les utilisateurs ne seront pas totalement conscients de tous les risques de sécurité tandis qu'un grand nombre d'opérateurs, de vendeurs ou de fournisseurs de services ont du mal à évaluer l'existence et l'ampleur des vulnérabilités. De nombreux services, applications et logiciels nouveaux offrent des caractéristiques attrayantes, mais celles-ci sont souvent la source de nouvelles vulnérabilités (par exemple, le succès du World Wide Web est partiellement dû à l'éventail des applications multimédias qui peuvent être facilement téléchargées, mais ces "plug-ins" constituent aussi une porte d'entrée pour les attaques.) Alors que les bénéfices sont visibles, les risques ne le sont pas, et les fournisseurs sont plus enclins à offrir de nouvelles caractéristiques qu'une plus grande sécurité.

Dans la société de l'information, les réseaux mondiaux contrôlés par l'utilisateur remplacent progressivement l'ancienne génération des réseaux de communication nationaux. L'une des raisons qui expliquent le succès de l'Internet est qu'il a donné aux utilisateurs l'accès aux technologies les plus modernes. La loi de Moore prédit que la puissance de calcul doublera tous les 18 mois. Or, les technologies de communication connaissent des progrès encore plus rapides. L'une des conséquences de cette évolution est que le volume de données transportées via l'Internet double à intervalles de moins d'un an.

Cette observation a été formulée en 1965 par Gordon Moore, cofondateur de l'entreprise Intel, à propos du rythme de progression du nombre de transistors sur un circuit intégré. À l'heure actuelle, ce nombre double quasiment tous les dix-huit mois, ce qui a une influence directe sur le prix et les performances des puces informatiques. Nombre d'experts pensent que cette loi se vérifiera encore pendant les dix prochaines années au moins.

Dans un contexte tellement mutant le besoin de sécurité devient de plus en plus impératif.

Dans ce cadre et après des études empiriques, on pourrait constater qu'il y a un écart énorme entre la décision prise par la commission et son entrée en vigueur ainsi que l'information pour les entreprises. Pourquoi existe ce décalage ? Est-ce que la communication tue l'information ?
Il s'agit des questions qu'on voudrait explorer pendant notre projet.

La sécurité et la pyramide de Maslow

La théorie des besoins de Maslow (1954) a une origine spéculative et s'appuie sur son expérience clinique. Elle repose sur plusieurs postulats :

Il existe cinq catégories de besoins : les besoins physiologiques élémentaires (se nourrir par exemple), les besoins de sécurité, (besoin de protection contre le danger ou la menace, sécurité de l'emploi par exemple) les besoins d'estime (certains concernent l'estime de soi, d'autres la reconnaissance par autrui), les besoins de réalisation de soi.

Ces différents besoins s'ordonnent selon une hiérarchie. Les besoins physiologiques sont au plus bas de la hiérarchie, les besoins de réalisation de soi au sommet. Les besoins de niveau supérieur ne constitueront une source de motivation que si les besoins de niveau inférieur ont été raisonnablement satisfaits. Ainsi, une personne qui ne mange pas à sa faim ne sera pas motivée par le souci du développement personnel et de la réalisation de soi dans le travail.

Cette théorie a le mérite de la simplicité. C. Louche souligne le fait qu'elle a suscité des critiques : on a questionné le caractère universel de la typologie des besoins retenue par Maslow parce que des variations culturelles sont possibles et ont d'ailleurs été démontrées (Clark, Mc Cabe, 1970.) Ensuite on ne peut pas exclure que des besoins de niveau différent agissent de manière concomitante pour motiver l'individu. Les validations empiriques sont de plus très limitées. *« On n'a observé ni corrélation négative entre la force d'un besoin et le niveau de satisfaction le concernant, ni corrélation positive entre la satisfaction d'un besoin et la force du besoin qui le suit dans la hiérarchie »*[27]. Enfin le découpage en 5 besoins a_t discuté par Alderfer (1972) avec sa théorie ESC (existence, sociabilité, croissance) qui reconnaît l'existence de 3 besoins. Les besoins d'existence concernent le plan physiologique et

[27] Levy-Leboyer., *Satisfaction et motivation : Théories et recherche*., p. 93, (1994)

matériel. Ils correspondent aux besoins physiologiques et de sécurité de la pyramide de Maslow. Ils se traduisent par le désir d'améliorer ses conditions d'emploi, son salaire ou ses avantages sociaux. Les besoins de sociabilité correspondent aux besoins d'appartenance et aux besoins d'estime de soi définis par Maslow. Le besoin de croissance se rapproche du besoin de réalisation de soi.

Il y a au niveau du découpage des besoins de fortes similitudes entre Maslow et Alderfer (sans que le recoupement ne coïncide d'ailleurs parfaitement.) C'est au niveau de la dynamique des besoins que ces auteurs se séparent nettement. Maslow avançait l'idée d'une progression des niveaux inférieurs vers les niveaux supérieurs. Pour Alderfer, l'idée d'une présence hiérarchique est abandonnée. Toute frustration ressentie au niveau d'un besoin pourra amener un déplacement vers d'autres besoins. Ce déplacement ne s'opère pas dans le cadre du respect d'une hiérarchie ascendante ou descendante.

Conclusion

Après un effort d'analyse de l'impact de l'Union européenne à l'environnement des entreprises dans la matière de l'innovation et de la sécurité informatique, nous avons dressé un bilan sur les initiatives communautaires sur le sujet. A travers la lecture de textes, il paraît que les mesures proposées par l'Union européenne sont très bien définies. Mais qu'est-ce qui se passe vraiment dans la réalité qu'on a vécue ?

Pour arriver à répondre à cette question il fallait qu'on prenne une posture anthropologique. L'image proposée par Bateson convient parfaitement pour caractériser cette posture. « L'anthropologie de la communication est un regard 'binoculaire' sur le monde social. Un regard de l'extérieur' et un regard de l'intérieur: par une démarche dite « ethnographique », l'observateur peut se faire participant, le temps de comprendre le milieu qu'il étudie depuis le point de vue de ceux qui y vivent. ».

A un moment où la sécurité informatique est l'une des premières priorités de nombreuses entreprises européennes, on constate que toutes les organisations n'ont pas pris conscience des avantages certains que représente la sécurisation tant au niveau de leur infrastructure que de leur propriété intellectuelle. Notre démarche vise à trouver le meilleur moyen possible pour communiquer la sécurité afin de favoriser la responsabilité européenne qui donnera lieu à une politique de sécurité de l'information en Europe.

Bibliographie

- Besson B. Possin J, C Du renseignement à l'intelligence économique, Dunod, 2001
- Coriat B et Weinstein O, Les nouvelles théories de l'entreprise, Librairie Générale Française, 1995
- Di Rupo E., *La société de l'Information*, in Libertés, Droits et Réseaux dans la Société de l'Information, éditions Bruylant, 1996, Bruxelles
- Eric de Grolier, *L'organisation des systèmes d'information des pouvoirs publics*, Unesco, 1978
- Ferry J.M, La question de l'état européen, Gallimard, 2000
- Gabay M., La nouvelle communication de crise, éditions stratégies, 2001
- Golvers Luc. , *La société de l'information : sécurité et insécurité, in* Libertés, Droits et Réseaux dans la Société de l'Information, éditions Bruylant, 1996, Bruxelles
- Hassid L. Jacques-Gustave P. Moinet N, Les PME face au défi de l'intelligence économique, Dunod, 1997
- Lawrence P., Lorsch J., *Adapter les structures de l'entreprise*, Paris, Editions d'Organisation, 1989
- Louche C. Psychologie Sociale des Organisations, Armand Colin, 2001
- Martinez-Fortun, Manager la sécurité, INSEP Consulting Éditions, 2001
- Maslow A.M, *Motivation and personality*, New York, Harper en prow, 1954
- Michaud C. et Thoenig J-C. Stratégie et sociologie de l'entreprise, Editions Village Mondial, Paris/Pearson Education France, 2001
- Morin E., *Introduction à la pensée complexe*, ESF, 1990
- Mucchielli A., *Approche systémique et communicationnelle des organisations*, A. Colin, 1998
- Mucchielli A., *La nouvelle communication*, A. Colin, 2000
- Queré Louis, D'un modèle épistémologique de la communication a un modèle praxéologique, Réseaux n°46-47, CNET 1991
- S/dir Cova B., Wickham S, Stratégies d'incertitude, Economica, 1996
- www.europa.eu.int
- www.csrc.lsc.ac.uk/People/Angell/WinnerLoser.htm

ORBAC : un modèle de contrôle d'accès basé sur les organisations

Anas Abou El Kalam[1] Rania El Baida[2] Philippe Balbiani[2]
Salem Benferhat[3] Frédéric Cuppens[2] Yves Deswarte[1]
Alexandre Miège[4] Claire Saurel[5] Gilles Trouessin[6]

CRIL[3] ENST[4] Ernst & Young Audit[6] IRIT[2] LAAS-CNRS[1] ONERA[5]

Résumé : Les modèles de contrôle d'accès comme DAC, MAC, RBAC, TBAC ou TMAC ne permettent de modéliser que des politiques de sécurité qui se restreignent à des permissions statiques. Ils n'offrent pas la possibilité d'exprimer des règles contextuelles relatives aux permissions, aux interdictions, aux obligations et aux recommandations. Ce type de règle est particulièrement utile pour exprimer des politiques de sécurité dans le domaine médical. Dans cet article, nous proposons un nouveau modèle qui permet de spécifier de telles politiques de sécurité contextuelles. Ce modèle appelé Organisation Based Access Control (ORBAC) s'appuie sur un langage formel basé sur la logique du premier ordre.

Abstract: None of the classical access control models such as DAC, MAC, RBAC, TBAC or TMAC is fully satisfactory to model security policies that are not restricted to static permissions but also include contextual rules related to permissions, prohibitions, obligations and recommendations. This is typically the case of security policies that apply to the health care domain. In this paper, we suggest a new model that provides solutions to specify such contextual security policies. This model, called Organization based access control, is presented using a formal language based on first-order logic.

[1] Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, 7 avenue du Colonel Roche, 31077 Toulouse Cedex 4.
2 Institut de Recherche en Informatique de Toulouse, Université Paul Sabatier, 118 route de Narbonne, 31062 Toulouse Cedex 4.
3 CRIL – Université d'Artois, Rue Jean Souvraz, SP18, 62307 Lens.
4 Ecole Nationale Supérieur des Télécommunications, 46 rue Barrault, 75634 Paris Cedex 13.
5 Office National d'Etudes et de Recherches Aérospatiales - Centre de Toulouse BP 4025, 31055 Toulouse Cedex 4.
6 Ernst & Young Audit, 1 place Alphonse Jourdain, 31000 Toulouse.

Introduction

Plusieurs modèles de contrôle d'accès ont été proposés : DAC [14], MAC [2, 6], RBAC [15, 12, 11], TBAC [17] ou TMAC [18]. Aucun de ces modèles n'est entièrement satisfaisant au regard des difficultés rencontrées pour mettre en œuvre, au sein d'une organisation, une politique de sécurité qui prendrait en compte les points suivants :

1. Des règles qui spécifient des permissions ou des interdictions contextuelles. En effet, il est fréquent d'avoir des règles de sécurité spécifiques à un certain contexte. Dans le domaine médical par exemple, les médecins ont des permissions spéciales dans des contextes spécifiques comme l'urgence (voir section 5).
2. Des règles qui spécifient des obligations ou des recommandations. Les modèles de contrôles d'accès classiques sont généralement restreints aux permissions. Certains incluent des interdictions, et plus récemment des modèles de politique de sécurité ont ajouté des obligations [9,5].
3. Des règles spécifiques à l'organisation. En particulier, l'organisation peut être structurée en plusieurs sous organisations qui ont chacune leur propre politique de sécurité. Le modèle devra ainsi proposer un moyen de spécifier au sein d'une même organisation plusieurs politiques de sécurité.

L'objet de cet article est de présenter un modèle qui tente de prendre en compte ces différents points. Le concept d'organisation est central dans ce nouveau modèle. L'organisation est un des paramètres des règles de sécurité de sorte qu'il soit possible de gérer à la fois plusieurs politiques de sécurité associées à différentes organisations. Le modèle n'est pas restreint aux permissions mais permet également de définir des interdictions, des obligations et des recommandations.

L'article est organisé comme suit : les sections 2 et 3 présentent des modèles de contrôle d'accès discrétionnaire et basé sur les rôles. La section 4 décrit notre modèle ORBAC. Dans la section 5, nous définissons un langage basé sur la logique du premier ordre utilisé pour définir une politique de sécurité ORBAC. La section 6 développe un exemple de politique de sécurité basé sur ce langage. Dans la section 7 nous évoquons comment exprimer différents types de contraintes. Enfin, la section 8 conclut l'article.

Le contrôle d'accès discrétionnaire

Harrison, Ruzzo et Ullman [13] définissent un modèle de politique de sécurité, le modèle HRU, qui s'applique sur des sujets, des objets et des actions. De manière intuitive, un sujet est une entité active alors qu'un objet est un conteneur d'information. Dans le contexte d'un système d'information, les sujets incluent les utilisateurs du système et généralement les processus exécutés pour le compte de ces utilisateurs. De plus, l'ensemble des objets inclut les entités actives, ainsi que les entités passives telles qu'un système d'information, des fichiers ou des répertoires. Les actions offrent aux sujets un accès direct aux objets. Elles correspondent généralement à des actions élémentaires comme "lire" ou "écrire". Dans ce modèle, la politique de sécurité est réduite à l'expression des permissions ; ces dernières étant des relations entre les sujets, les objets et les actions. Elles sont représentées dans la matrice A des permissions. Si s est un sujet et o est un objet alors, $A(s, o)$ définit l'ensemble des actions α que le sujet s est autorisé à faire sur l'objet o.

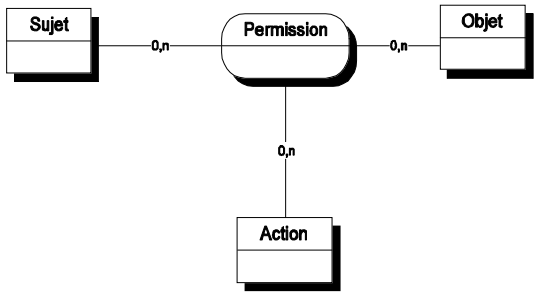


Figure 1 : le modèle HRU

Dans le modèle HRU, la politique de sécurité s'exprime à travers l'énumération dans la matrice des permissions de tous les triplets $<s, o, \alpha>$. Si de nouveaux objets, de nouveaux sujets ou de nouvelles actions sont ajoutés au système d'information, il est alors nécessaire d'enregistrer toutes les permissions accordées à ces nouvelles entités. Par conséquent, la mise à jour d'une politique de sécurité exprimée par ce modèle est quelque peu fastidieuse. Enfin, ce modèle ne permet pas d'exprimer des interdictions, des obligations ou des recommandations.

Le contrôle d'accès basé sur les rôles

Dans le modèle de contrôle d'accès basé sur les rôles, ou RBAC, la politique de sécurité ne s'applique pas directement à des utilisateurs comme dans le modèle précédent. Le rôle est ici le concept central de la politique de sécurité [12]. D'un côté des permissions sont accordées aux rôles ; de l'autre les utilisateurs se voient affecter un ou plusieurs rôles.

Les utilisateurs obtiennent les permissions accordées aux rôles qu'ils jouent (figure 2).

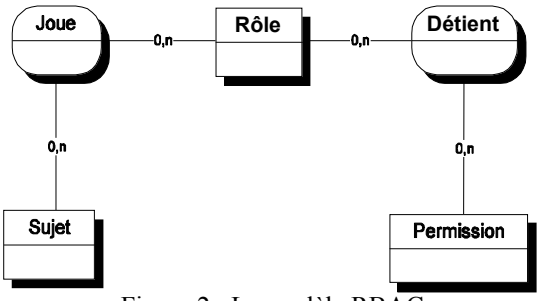


Figure 2 : Le modèle RBAC

Il est possible de raffiner ce modèle en incluant les concepts de session et de hiérarchie de rôles. Dans une même session, un utilisateur a la possibilité de ne pas activer tous ses rôles, mais uniquement le sous-ensemble de ses rôles nécessaires à la réalisation de la tâche à accomplir. La hiérarchie de rôles a cela d'utile qu'elle permet de mettre en place un mécanisme d'héritage des permissions entre les rôles et simplifie d'autant l'administration de ce modèle. Le modèle RBAC est complété par des contraintes. La séparation des pouvoirs, par exemple, peut être exprimée à l'aide d'une contrainte indiquant qu'un utilisateur n'est pas autorisé à jouer simultanément certains rôles dans une même session, comme ceux d'anesthésiste et de chirurgien lors d'une opération.

Les inconvénients du modèle RBAC sont les suivants. Tout d'abord, le concept de permission est primitif. En effet, dans le modèle RBAC, rien n'est dit sur l'usage ou la structure des permissions, considérant qu'ils sont dépendants de l'application concrète du modèle. Nous pensons à l'inverse qu'il serait préférable d'ajouter au modèle une structure générique de permission. Le concept de hiérarchie de rôles est quelque peu ambigu. Il est en général incorrect de considérer que la hiérarchie de rôles correspond à la hiérarchie organisationnelle. Par exemple, le directeur d'un hôpital a un rôle administratif supérieur au rôle de médecin. Pour autant, un directeur d'hôpital n'est pas nécessairement un médecin. Ainsi, il serait incorrect de considérer que le directeur de l'hôpital hérite des permissions du rôle de médecin, comme celle d'opérer par exemple. Enfin, la distinction entre le concept de rôle et celui de groupe est floue. Le groupe est un concept qui a été introduit avant la définition du modèle RBAC. Il y eut beaucoup de discussion à propos des différences entre le contrôle d'accès basé sur les groupes et RBAC. Le modèle ORBAC propose, dans la section 4, de clarifier ce point.

Ajoutons qu'il n'est pas possible dans le modèle RBAC d'exprimer des permissions qui dépendent du contexte. Plus précisément, si une certaine permission est accordée à un rôle, alors tous les utilisateurs qui jouent ce rôle héritent de cette permission. Par conséquent, il n'y a aucun moyen de spécifier qu'un médecin n'a la permission d'accéder au dossier médical d'un patient que si ce dernier est son patient [1, 7]. De plus, comme nous l'avons déjà évoqué dans le cas du modèle HRU, il est uniquement possible de définir des permissions. Enfin, l'application du modèle RBAC à la définition d'une politique de sécurité d'un système contenant plusieurs organisations fait apparaître d'autres limites de ce modèle.

Le contrôle d'accès basé sur l'organisation

Dans cette section, nous présentons notre modèle ORBAC en s'appuyant sur un langage diagramatique basé sur le modèle entité-relation. La section 5 présente le même modèle en utilisant un langage formel basé sur la logique du premier ordre. En conformité avec le modèle entité-relation, des attributs peuvent être associés aux entités et aux relations. Considérant que ces attributs sont généralement spécifiques au domaine d'application, nous n'en faisons pas état ici.

Les organisations

L'entité centrale dans notre modèle est l'*organisation*. Dans le domaine médical, nous pouvons considérer les organisations suivantes : "la clinique privée du Languedoc", "le service des urgences de l'hôpital Purpan", "l'unité des soins intensifs de l'hôpital Rangueil", etc. Une organisation peut être vue comme un groupe structuré d'entités actives, c'est-à-dire de sujets jouant certains rôles. Notons qu'un groupe de sujets n'est pas nécessairement considéré comme une organisation. Autrement dit, le fait que chaque sujet joue un rôle dans l'organisation correspond à un certain accord entre les sujets pour former une organisation.

Les sujets et les rôles

L'entité *Sujet* est utilisée différemment selon les modèles de sécurité. Dans notre modèle ORBAC, un sujet peut être soit une entité active, c'est-à-dire un utilisateur, soit une organisation. Par exemple, "Jean", "Marie", "Pierre", etc., peuvent être des sujets, tout comme les organisations "département comptable de la clinique privée du Languedoc", "le service des urgences de l'hôpital Purpan", etc. Dans notre modèle, l'entité *Rôle* est utilisée pour structurer le lien entre les sujets et les organisations. Dans le domaine médical, les rôles "cardiologue", "infirmière" ou "médecin", sont joués par des utilisateurs alors que les rôles "service des urgences" ou "unité des soins intensifs" sont joués par des organisations. Comme les sujets jouent des rôles dans des organisations, nous introduisons une relation entre ces entités : la relation *Habilite* (figure 3). Si *org* est une organisation, *s* est un sujet

et *r* est un rôle, alors *Habilite*(*org*, *s*, *r*) signifie que *org* habilite le sujet *s* à jouer le rôle *r*.

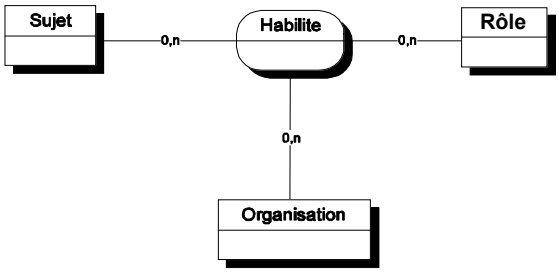


Figure 3 : La relation *Habilite*

Contrairement aux modèles TMAC et RBAC qui ne considèrent que des relations binaires entre les organisations et les sujets ou entre les sujets et les rôles, notre modèle définit une relation ternaire entre les organisations, les sujets et les rôles. Les deux exemples suivants illustrent le fait que les sujets sont soit des utilisateurs, soit des organisations :

- *Habilite*(*Purpan*, *Jean*, *cardiologue*) : "l'hôpital Purpan habilite Jean dans le rôle cardiologue" et
- *Habilite*(*Rangueil*, *ICU31*, *unité_des_soins_intensifs*) : "l'hôpital Rangueil habilite l'unité ICU31 dans le rôle d'unité des soins intensifs".

Les objets et les vues

Dans notre modèle, l'entité *Objet* représente principalement les entités non actives comme les fichiers, les courriers électroniques, les formulaires imprimés, etc. Dans le domaine médical, nous aurons ainsi à considérer des objets comme les dossiers administratifs, les dossiers médicaux et les dossiers chirurgicaux des patients. Les rôles nous permettent de structurer les sujets et de faciliter la mise à jour de la politique de sécurité quand un nouvel utilisateur est ajouté. Dans la mesure où il est également nécessaire de structurer les objets et d'ajouter de nouveaux objets au système, nous considérons qu'une entité comparable au rôle pour les sujets est nécessaire pour les objets. Nous l'appelons : entité *Vue*. De manière intuitive, une vue correspond, comme dans les bases de données relationnelles, à un ensemble d'objets qui satisfait une propriété commune. Par exemple dans un système de fichier administratif, la vue "dossiers administratifs" correspond à l'ensemble des dossiers administratifs des patients, alors que la vue "dossiers médicaux" correspond aux dossiers médicaux des patients. Dans la mesure où les vues caractérisent la manière dont les objets sont utilisés dans l'organisation, nous avons besoin d'une relation qui lie ces trois entités : la relation *Utilise* (figure 4). Si *org* est une organisation, *o* est un objet et *v* est une vue, alors *Utilise*(*org*, *o*, *v*) signifie que *org* utilise l'objet *o* dans la vue *v*.

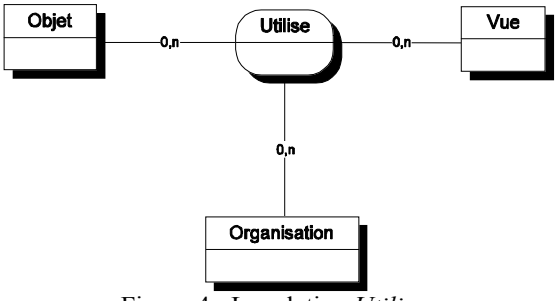


Figure 4 : La relation *Utilise*

Notre modèle définit donc une nouvelle relation ternaire entre les organisations, les objets et les vues. Ainsi une même vue peut être définie différemment suivant l'organisation considérée. Le but est de caractériser des organisations qui donnent des définitions différentes à une même vue. La vue "dossier médical" peut être définie à l'hôpital Purpan comme un ensemble de documents Word, et comme un ensemble de documents Latex à l'hôpital Rangueil :

- *Utilise*(*Purpan*, *F31.doc*, *dossier_médical*) : "L'hôpital Purpan utilise F31.doc comme un dossier médical" et
- *Utilise*(*Rangueil*, *F32.tex*, *dossier_médical*) : "L'hôpital Rangueil utilise F32.tex comme un dossier médical".

Les actions et les activités

Les politiques de sécurité spécifient les accès autorisés aux entités passives par des entités actives et régulent les actions opérées sur le système. Dans notre modèle, l'entité *Action* englobe principalement les actions informatiques comme "lire", "écrire", "envoyer", etc. De la même manière que dans les sections 4.2 et 4.3 où les rôles et les vues sont des abstractions des sujets et des objets, nous définissons une nouvelle entité utilisée comme abstraction des actions : l'entité *Activité*. Ainsi, les rôles associent des sujets qui remplissent les mêmes fonctions, les vues regroupent des objets qui satisfont une propriété commune et par analogie les activités correspondent à des actions qui ont un objectif commun. Dans notre modèle, les activités pourront être "consulter", "modifier", "transmettre", etc. Dans la mesure où des organisations différentes peuvent considérer qu'une même action est employée à la réalisation d'activités différentes, la relation *Considère* (figure 5) sera utilisée pour associer les entités *Organisation*, *Action* et *Activité*. Plus précisément, si *org* est une organisation, α est une action et *a* est une activité, alors *Considère*(*org*, α, *a*) signifie que l'organisation *org* considère l'action α *comme* faisant partie de l'activité *a*.

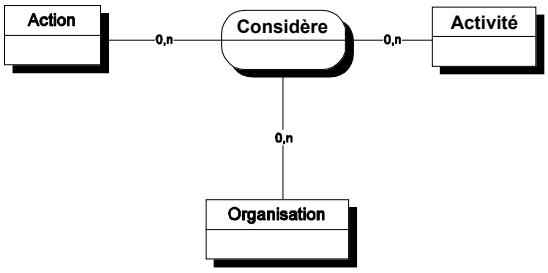


Figure 5 : La relation *Considère*

Remarquons que là encore nous définissons une relation ternaire. L'objectif est de pouvoir caractériser des organisations qui structurent différemment les mêmes activités. Si nous considérons l'activité "consultation". Cette activité peut correspondre, dans l'organisation hôpital Purpan, à l'action "lire" un fichier, mais peut tout aussi bien correspondre à l'action "select" sur une base de données dans l'hôpital Rangueil.

- *Considère*(*Purpan*, *lire*, *consultation*) : "l'hôpital Purpan considère *lire* comme une consultation" et
- *Considère*(*Rangueil*, *select*, *consultation*) : "l'hôpital Rangueil considère *select* comme une consultation".

Politique de sécurité (première définition)

En utilisant les entités et les relations introduites dans les sections précédentes, nous pouvons à présent définir des politiques de sécurité appliquées à telle ou telle organisation. Une politique de sécurité réglemente les accès au système à travers des permissions, des interdictions, des obligations et des recommandations. Nous ne traitons que les permissions, en considérant que les mêmes raisonnements s'appliquent aux interdictions, aux obligations et aux recommandations. L'objectif est ici d'ajouter une nouvelle entité *Permission* afin de relier entre eux les organisations, les rôles, les vues et les activités. Plus précisément, si *org* est une organisation, *r* est un rôle, *a* est une activité et *v* est une vue, alors *Permission*(*org*, *r*, *a*, *v*) signifie que l'organisation *org* accorde au rôle *r* la permission de réaliser l'activité *a* sur la vue *v*. Prenons l'exemple de l'hôpital Purpan qui accorde au rôle "secrétaire médicale" la permission de réaliser l'activité "création" sur la vue "dossier administratif". Cette règle de sécurité est exprimée comme suit : *Permission*(*Purpan*, *secrétaire_médicale*, *création*, *dossier_administratif*). Considérons à présent la règle suivante : *Permission*(*Purpan*, *médecin*, *consultation*, *dossier_médical*) ; elle indique que l'hôpital Purpan permet aux médecins de consulter les dossiers médicaux. Pourtant, il est très probable que l'hôpital Purpan ne souhaite pas exprimer exactement cette règle, mais plutôt que dans des circonstances normales, un médecin à la permission de consulter les dossiers médicaux de ses propres patients uniquement. Le modèle ORBAC ne permet pas en l'état d'exprimer une telle règle. Nous proposons, pour résoudre ce problème, d'ajouter une nouvelle entité à notre modèle : l'entité *Contexte*.

Les contextes

Les contextes sont utilisés pour spécifier les circonstances concrètes dans lesquelles les organisations accordent des permissions de réaliser des activités sur des vues. Dans le domaine médical, une nouvelle entité *Contexte* permettra d'exprimer des circonstances telles que "urgence", "médecin traitant", etc. Les contextes peuvent être vus comme des relations ternaires entre les sujets, les objets et les actions définis dans une certaine organisation. Par conséquent, les entités *Organisation*, *Sujet*, *Objet*, *Action* et *Contexte* sont liées par une nouvelle relation appelée *Définit* (figure 6) telle que : si *org* est une organisation, *s* est un sujet, α est une action, *o* est un objet et *c* est un contexte, alors *Définit*(*org*, *s*, α, *o*, *c*) signifie qu'au sein de l'organisation *org*, le contexte *c* est vraie entre le sujet *s*, l'objet *o* et l'action α.

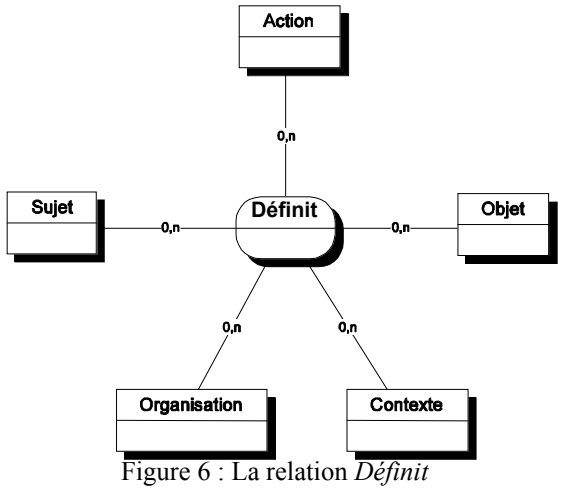


Figure 6 : La relation *Définit*

Les conditions requises pour qu'un contexte donné soit lié, dans une certaine organisation, aux sujets, aux objets et aux actions sera formellement spécifié par des règles logiques. Ceci sera abordé dans la section 5. Pour l'heure, considérons les faits suivants : *Définit*(*Purpan*, *Jean*, *lire*, *F31.doc*, *urgence*) et *Définit*(*Rangueil*, *Marie*, *lire*, *F32.tex*, *médecin_traitant*). Si le premier fait est vrai, alors Jean n'a pas besoin d'être le médecin traitant du patient correspondant au dossier médical F31.doc pour consulter son dossier. En effet, il est raisonnable de considérer que dans un contexte d'urgence, les médecins ont un accès immédiat à tous les dossiers médicaux. Si le second fait est vrai, alors Marie doit être le médecin traitant du patient dont le dossier médical est F32.tex : dans un contexte normal comme "médecin traitant", les médecins ont uniquement l'autorisation de consulter les dossiers médicaux de leurs patients.

Politique de sécurité (définition finale)

Maintenant que nous avons présenté l'entité *Contexte*, nous pouvons à présent donner la définition finale d'une politique de sécurité dans le modèle ORBAC. La relation *Permission* correspond à une relation entre les organisations, les rôles, les vues, les activités et les contextes. Les relations *Interdiction*, *Obligation* et *Recommandation* sont définies de la même manière (figure 7). Si *org* est une organisation, *r* est un rôle, *a* est une activité, *v est* une vue et *c* est un contexte, alors *Permission*(*org*, *r*, *a*, *v*, *c*) signifie que l'organisation *org* accorde au rôle *r* la permission de réaliser l'action *a* sur la vue *v* dans le contexte *c*.

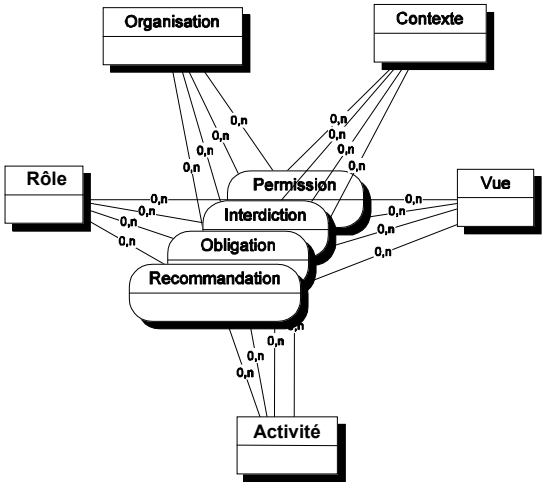


Figure 7 : Les relations *Permission*, *Interdiction*, *Obligation* et *Recommandation*.

Par exemple, la politique de sécurité de l'hôpital Purpan peut comporter les faits suivants : *Permission*(*Purpan*, *médecin*, *consulter*, *dossier_médical*, *urgence*) qui signifie que "l'hôpital Purpan accorde aux médecins la permission de consulter n'importe quel dossier médical dans le contexte de l'urgence" et *Permission*(*Purpan*, *médecin*, *consulter, dossier_médical*, *médecin_traitant*) qui signifie que "l'hôpital Purpan accorde aux médecins la permission de consulter les dossiers médicaux des patients dont ils sont les médecins traitants".

Les autorisations concrètes

La relation *Permission* permet à une organisation donnée de spécifier les permissions accordées suivant le contexte. De telles permissions correspondent à une relation entre les rôles, les vues et les activités. Pour autant, le contrôle d'accès bas niveau doit permettre de décrire les actions concrètes que réalisent les sujets sur les objets. Dans le but de modéliser des permissions concrètes, nous introduisons dans notre modèle la relation *Est_permis* entre les sujets, les objets et les actions : si *s* est un sujet, α est une action et *o* est un objet, alors *Est_permis*(*s*, α, *o*) signifie que le sujet *s* a la permission de réaliser l'action α sur l'objet *o*. Les relations *Est_interdit*, *Est_obligatoire* et *Est_recommandé* sont définies de la même manière. Notre relation *Est_permis* est similaire à la notion de permission évoquée dans le modèle HRU (voir section 1). Il y a tout de même une différence de taille : dans le modèle HRU, les triplets d'autorisation <*s*, α, *o*> doivent être explicitement décrit ; alors que dans notre modèle, les triplets, qui sont des instances de la relation *Est_permis*, sont dérivés logiquement des permissions accordées aux rôles, aux vues et aux activités par la relation *Permission*. Ceci est modélisé par une règle générale présentée dans la section 5. Les instances explicites de la relation *Est_permis* peuvent être considérées comme des exceptions à la politique de sécurité générale spécifiée par la relation *Permission*.

La figure 8 résume notre modèle de sécurité. Il contient huit entités (*Organisation*, *Sujet*, *Rôle*, *Objet*, *Vue*, *Action*, *Activité* et *Contexte*) et douze relations (*Habilite*, *Utilise*, *Considère*, *Permission*, *Interdiction*, *Obligation*, *Recommandation*, *Est_permis*, *Est_interdit*, *Est_obligatoire*, *Est_Recommandé* et *Définit*).

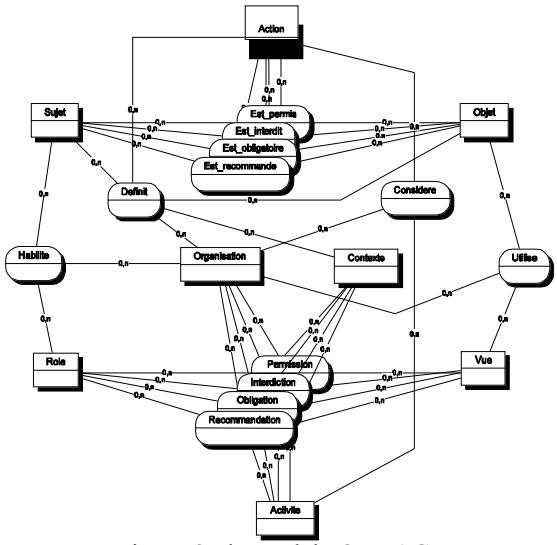


Figure 8 : le modèle ORBAC

Langage et axiomatique

L'objet de cette section est de présenter un cadre logique qui nous offre des outils d'aide au raisonnement sur les permissions, les interdictions, les obligations et les recommandations. L'objectif est d'associer un langage du premier ordre _ au diagramme entité-relation décrit précédemment. Notre langage du premier ordre doit fournir une syntaxe permettant d'exprimer les instances des relations existantes entre les entités. Chaque expression de _ contiendra des symboles extraits d'un vocabulaire particulier classés en quatre groupes : les symboles de constante, les variables individuelles, les symboles de relation et les symboles de fonction.

Les symboles de constante correspondent aux instances des entités du diagramme. Ainsi, il y aura autant de type _ de symboles de constante que d'entités dans notre diagramme, c'est-à-dire huit : *Organisation*, *Sujet*, *Objet*, *Action*, *Rôle*, *Vue*, *Activité* et *Contexte*. Nous aurons par exemple les symboles de constante de type *Organisation* comme *Purpan*, *Rangueil*, *ICU31*, etc., les symboles de constante de type *Sujet* comme *Jean*, *Marie*, *ICU31*, etc, les symboles de constante de type *Objet* comme *F31.doc*, *F32.doc*, *F33.tex*, etc., les symboles de constante de type *Action* comme *lire*, écrire, *consulter*, etc., les symboles de constante de type *Rôle* comme *médecin*, *infirmière*, *unité_des_soins_intensifs*, etc., les symboles de constante de type *Vue* comme *dossier_administratif*, *dossier_médical*, *dossier_chirurgical*, etc., les symboles de constante de type *Activité* comme *lecture*, *écriture, consultation*, etc. Les constantes seront notées par des lettres minuscules comme *a*, *b* et *c*.

De la même manière, il y aura des variables individuelles pour chaque type _. Elles seront notées par des lettres latines minuscules comme *x*, *y* et *z*. Pour tous les types _, les symboles de constante de type _ et les variables individuelles de type _ seront appelés termes-_.

Les symboles de relation de _, notées par des lettres majuscules *P*, *Q*, *R*, etc., correspondront aux douze relations de notre diagramme. Chaque symbole de relation *P* de _ est considéré comme un type de relation. Plus précisément, *Habilite* est un symbole de relation de type (*Organisation*, *Sujet*, *Rôle*). *Permission*, *Interdiction*, *Obligation* et *Recommandation* sont symboles de relation de type (*Organisation*, *Rôle*, *Vue*, *Activité*, *Contexte*). *Est_permis*, *Est_interdit*, *Est_obligatoire*, *Est_recommandé* sont des symboles de relation de type (*Sujet*, *Objet*, *Action*).

En utilisant les termes et les relations, nous construisons les formules atomiques de _ comme suit : si t_1 est un terme-$_1$, …, t_n est un terme-$_n$ et *P* est une relation de type ($_1$, …, $_n$), alors $P(t_1, \ldots, t_n)$ est une formule atomique. *Habilite*(*Purpan*, *Jean*, *médecin*) et *Permission*(*Rangueil*, *secrétaire_médicale*, *création*, *dossier_administratif*, *normal*) sont des formules atomiques.

A ce stade, notre langage n'est pas assez expressif pour pouvoir comparer des entités. Dans de nombreuses applications, nous désirons dériver des informations concernant certaines propriétés des entités. D'un point de vue formel, des symboles de fonction seront utilisés pour décrire les attributs de ces entités. Les symboles de fonction seront notés par des lettres minuscules comme *f*, *g* et *h*. A chaque symbole de fonction *f* sont associés un domaine et un co-domaine (encore appelé domaine image de la fonction). Le domaine et le co-domaine d'un symbole de fonction dépendent de la nature des attributs qui lui sont associés. Si un symbole de fonction correspond à l'attribut *Nom*, alors son domaine est de type *Sujet* et son co-domaine est un ensemble de noms. De même, le domaine d'un symbole de fonction correspondant à un attribut *Age* sera de type *Sujet* et son co-domaine sera un ensemble d'entiers positifs. Enfin, le domaine d'un symbole de fonction correspondant à l'attribut *Groupe_sanguin* sera de type *Sujet* et son co-domaine {*A*, *AB*, *B*, *O*}. Dans la mesure où il est possible que des sujets n'aient pas de nom ou que leur groupe sanguin soit inconnu, les symboles de fonction du langage _ pourront n'établir qu'une correspondance partielle entre les domaines et co-domaines associés. Dans de nombreuses situations, il nous est impossible d'attribuer une valeur unique à certains attributs d'une entité. Pour répondre à une telle situation d'un point de vue conceptuel, nous utiliserons des symboles de fonction unaires ayant pour co-domaine l'ensemble des parties d'un ensemble (*Power Set*). Pour illustrer ceci, il nous suffit de mentionner le cas de l'attribut *médecin_traitant* : le domaine du symbole de fonction associé est de type *Sujet* et le co-domaine associé est un ensemble d'ensembles finis de noms.

Afin de dériver les informations représentées par les symboles de fonction, nous devons introduire des relations binaires concrètes, notées par _, _ et _ entre les domaines. Le type d'une relation binaire concrète est le couple correspondant aux domaines sur lesquels la relation s'applique. L'égalité est probablement la relation binaire concrète la plus simple que nous aurons à traiter. Considérons les exemples suivants :

- Si *t* et *u* sont des termes de type *Sujet*, alors *médecin_traitant(t) = médecin_traitant(u)* signifie que les sujets *t* et *u* ont les mêmes médecins traitants,
- Si *t* et *u* sont des termes de type *Sujet*, alors *Âge(t) = Âge(u)* signifie que les sujets *t* et u ont le même âge et
- Si *t* et *u* sont des termes de type *Sujet*, alors *Groupe_sanguin(t) = Groupe_sanguin(u)* signifie que les sujets *t* et *u* ont le même groupe sanguin.

Bien évidemment, il existe certains cas où d'autres relations binaires doivent être considérées. Par exemple :

- Si *t* et *u* sont des termes de type *Sujet*, alors *médecin_traitant(t) _ médecin_traitant(u)* $\neq \varnothing$ signifie que les sujets *t* et *u* ont un médecin traitant en commun,
- si *t* et *u* sont des termes de type *Sujet*, alors *Âge(t) < Âge(u)* signifie que le sujet *t* est plus jeune que le sujet *u* et
- si *t* et *u* sont des termes de type *Sujet*, alors *Groupe_sanguin(t) ~ Groupe_sanguin(u)*

signifie que les groupes sanguins de t et u sont compatibles.

Ces types de formules seront aussi considérés comme des formules atomiques. Ainsi les formules de _ sont définies comme suit :

- Une formule atomique est une formule,
- si A est une formule alors $\neg A$ "non A" est une formule,
- si A et B sont des formules alors $(A \wedge B)$ "A et B" et $(A \vee B)$ "A ou B" sont des formules et
- si A est une formule et x est une variable individuelle alors $\forall xA$ "pour toutes les valeurs possibles de x, on a A" et $\exists xA$ "il existe des valeurs possibles de x telles que A" sont des formules.

Comme d'habitude, les connecteurs logiques $\rightarrow$ et $\leftrightarrow$ sont définis de la façon suivante : $(A \rightarrow B)$ est équivalent à $(\neg A \vee B)$, et $(A \leftrightarrow B)$ est équivalent à $((A \rightarrow B) \wedge (B \rightarrow A))$. Nous omettrons volontairement les parenthèses quand aucune ambiguïté ne sera possible. Voici deux exemples de formules :

- $\forall s$ (*Habilite*(*Rangueil*, s, *médecin*) $\rightarrow$ *Habilite*(*Rangueil*, s, *personnel_soignant*)) : "tous les médecins de l'hôpital Rangueil sont aussi habilités comme personnel soignant" et
- $\forall r \forall v \forall a$ (*Permission*(*Rangueil*, r, a, v, *médecin_traitant*) $\rightarrow$ *Permission*(*Rangueil*, r, a, v, *urgence*)) "si l'hôpital Rangueil accorde au rôle r la permission de réaliser l'activité a sur la vue v dans le contexte "*médecin_traitant*", alors il accorde aussi cette permission dans le contexte d'urgence.

La valeur de vérité d'une formule est déterminée par les valeurs de ses sous formules dans un modèle donné. Les modèles pour notre langage consistent en huit ensembles non vides correspondant aux huit entités de notre diagramme et en douze relations correspondant aux douze relations de notre diagramme. Comme nous utilisons dans la suite la définition classique de la valeur de vérité d'une formule, il ne nous semble pas nécessaire de la rappeler ici.

Les axiomes d'une théorie du premier ordre sont habituellement divisés en axiomes logiques et axiomes propres. Les axiomes logiques fournissent les bases pour démontrer tous les théorèmes de la logique classique du premier ordre alors que les axiomes propres correspondent à des règles particulières. Nous supposons que toutes les politiques de sécurité seront basées sur la liste suivante d'axiomes propres pour toutes les organisations *org* :

1. $\forall s \forall \alpha \forall o \forall r \forall a \forall v \forall c$
   Permission(*org*, r, a, v, c) $\wedge$
   Habilite(*org*, s, r) $\wedge$
   Utilise(*org*, o, v) $\wedge$
   Considère(*org*, α, a) $\wedge$
   Définit(*org*, s, α, o, c) $\rightarrow$ *Est_permis*(s, α, o) : "si l'organisation *org*, dans le contexte c, accorde la permission au rôle r de réaliser l'activité a sur la vue v, si *org* habilite le sujet s dans le rôle r, si *org* utilise l'objet o dans la vue v, si *org* considère l'action α comme faisant partie de l'activité a et si au sein de l'organisation *org* le contexte c est vraie entre s, α et o, alors le sujet s a la permission de réaliser l'action α sur l'objet o",
2. $\forall r \forall a \forall v \forall c$ (*Obligation*(*org*, r, a, v, c) $\rightarrow$ *Recommandation*(*org*, r, a, v, c) : "toutes les obligations sont aussi des recommandations",
3. $\forall r \forall a \forall v \forall c$ (*Recommandation*(*org*, r, a, v, c) $\rightarrow$ *Permission*(*org*, r, a, v, c) : "toutes les recommandations sont aussi des permissions",
4. $\forall r \forall a \forall v \forall c$ (*Permission*(*org*, r, a, v, c) $\rightarrow$ $\neg$*Interdiction*(*org*, r, a, v, c) : "une permission implique une non interdiction".

L'axiome 1 décrit comment des permissions abstraites entre des rôles, des vues et des activités peuvent être transformées en permissions concrètes entre des sujets, des objets et des actions. Les axiomes pour les obligations, les recommandations et les interdictions sont définis de la même manière.

Exemple de politique de sécurité

Dans cette section nous montrons comment exprimer un exemple simple de politique de sécurité dans notre langage.

Les sujets et les rôles

Dans cet exemple, nous ne considérons que l'organisation "hôpital Purpan" (figure 9). Nous supposons que l'hôpital Purpan habilite plusieurs sujets : Jean dans le rôle de directeur, Marie dans le rôle d'assistante administrative, ST1 dans le rôle d'équipe chirurgicale et RT2 dans le rôle d'équipe radiologique. Dans notre langage, ces faits sont représentés par des instances de la relation *Habilite* :

- *Habilite*(*Purpan*, *Jean*, *directeur*),
- *Habilite*(*Purpan*, *Marie*, *assistante_administrative*),
- *Habilite*(*Purpan*, *ST1*, *équipe_chirurgicale*) et
- *Habilite*(*Purpan*, *RT2*, *équipe_radiologique*).

Dans ces faits, *directeur*, *assistante_administrative*, *équipe_chirurgicale* et *équipe_radiologique* sont des rôles.

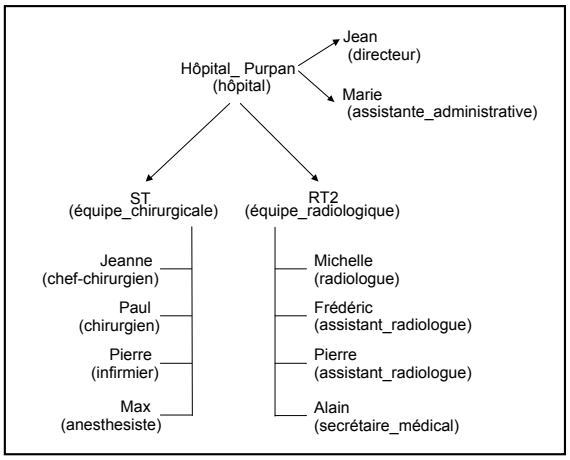


Figure 9 : Exemple d'organisation

La sous organisation ST1 habilite d'autres sujets : Jeanne dans le rôle de chef de l'équipe chirurgicale, Paul dans le rôle de chirurgien, Pierre dans le rôle d'infirmier et Max dans celui d'anesthésiste. Nous obtenons ainsi de nouvelles instances de la relation *Habilite* :

- *Habilite*(*ST1*, *Jeanne*, *chef_chirurgien*),
- *Habilite*(*ST1*, *Paul*, *chirurgien*),
- *Habilite*(*ST1*, *Pierre*, *infirmier*) et
- *Habilite*(*ST1*, *Max*, *anesthésiste*).

De la même manière, des sujets sont habilités par RT2, l'équipe radiologique. De plus, nous considérons qu'un attribut *Patient* associé à l'entité *Sujet* indique quels sont les patients d'un sujet. Par conséquent, notre langage inclut une fonction partielle *Patient* ayant pour domaine *Sujet* et pour co-domaine un ensemble d'ensembles finis de noms.
Par exemple, les fonctions *Patient(Purpan)* et *Patient(Michelle)* retournent respectivement la liste des patients de l'hôpital Purpan et de Michelle.

Les objets et les vues

Considérons les objets appartenant aux vues suivantes :

- *dossier_administratif* : Les objets qui appartiennent à cette vue fournissent des informations administratives concernant les patients comme leur nom, leur adresse, leur âge, etc,
- *dossier_médical* : Cette vue correspond au dossier médical des patients et,
- *dossier_chirurgical* : Cette vue correspond aux dossiers confidentiels gérés par l'équipe chirurgicale.

Nous supposons que les objets appartenant à ces vues ont un attribut *Nom*. Ainsi, si *F31.doc* est un dossier appartenant à une de ces vues, alors *Nom*(*F31.doc*) fournit le nom du patient correspondant. Nous supposons également que les dossiers sont directement gérés par l'hôpital Purpan, dans une base de données relationnelle par exemple. Ceci se traduit dans notre modèle par des faits de la forme :

- *Utilise*(*Purpan*, *F31.doc*, *dossier_administratif*),
- *Utilise*(*Purpan*, *F32.doc*, *dossier_médical*) et
- *Utilise*(*Purpan*, *F33.tex*, *dossier_chirurgical*).

ST1, l'équipe chirurgicale et RT2, l'équipe radiologique, partagent la même base de données gérée par l'hôpital Purpan. Cela signifie qu'elles utilisent les mêmes vues que l'hôpital. Ceci peut s'exprimer de la manière suivante :

- $\forall o \forall v$ (*Utilise*(*Purpan*, *o*, *v*) → *Utilise*(*ST1*, *o*, *v*)),
- $\forall o \forall v$ (*Utilise*(*Purpan*, *o*, *v*) → *Utilise*(*RT2*, *o*, *v*)).

A partir des trois vues *dossier_administratif*, *dossier_médical*, *dossier_chirurgical*, nous définissons une quatrième vue, appelée *dossier_patient*. Nous supposons qu'elle a trois attributs *dossier_administratif*, *dossier_médical* et *dossier_chirurgical* tels que :

- $\forall o$ (*Utilise*(*Purpan*, *o*, *dossier_patient*) ↔
  $\exists o_1 \exists o_2 \exists o_3$
  (*Utilise*(*Purpan*, o_1, *dossier_administratif*) ∧
  Utilise(*Purpan*, o_2, *dossier_médical*) ∧
  Utilise(*Purpan*, o_3, *dossier_chirurgical*) ∧
  dossier_administratif(o) = o1 ∧
  dossier_médical(o) = o2 ∧
  dossier_chirurgical(o) = o3 ∧
  Nom(o1) = Nom(o2) = Nom(o3)).

La vue *dossier_patient* correspond au dossier médical complet du patient. Dans une base de données relationnelle, nous obtiendrions le dossier patient par une jointure des vues *dossier_administratif*, *dossier_médical*, *dossier_chirurgical* suivant l'attribut *Nom*.

Les actions et les activités

Nous ne considérons ici que les activités correspondant à des accès directs aux dossiers, c'est-à-dire la création, la consultation et l'écriture, etc. Si nous supposons que les dossiers sont gérés par l'hôpital dans une base de données relationnelle, ces activités correspondent respectivement aux actions *insert*, *select*, *update*, etc. Ceci est représenté par les trois faits suivants :

- *Considère*(*Purpan*, *select*, *creation*),
- *Considère*(*Purpan*, *select*, *consulter*) et
- *Considère*(*Purpan*, *update*, *écriture*).

Les contextes

Nous modélisons trois contextes dans notre exemple : "médecin traitant", "équipe traitante" et "urgence". Le contexte "médecin traitant" est défini dans ST1, l'équipe chirurgicale, comme suit :

- $\forall s \forall o \forall \alpha$ (*Définit*(*ST1*, *s*, α, *o*, *médecin_traitant*) $\leftrightarrow$ *Nom*(*o*) $\in$ *Patient*(*s*)) : dans ST1, le contexte "médecin traitant" est vrai entre le sujet *s,* l'action α et l'objet *o* si et seulement si *s* joue un rôle dans ST1 et si *o* est un dossier correspondant à un patient traité par le sujet *s*.

Le contexte "équipe traitante" est défini de la manière suivante :

- $\forall s \forall o \forall \alpha$ (*Définit*(*ST1*, *s*, α, *o*, *equipe_traitante*) $\leftrightarrow$ $\exists r$ (*Habilite*(*ST1*, *s*, *r*) $\wedge$ *Nom*(*o*) $\in$ *Patient*(*ST1*)) : dans ST1, le contexte "équipe traitante" est vrai entre le sujet *s*, l'action α et l'objet *o* si et seulement si *s* joue un rôle dans ST1 et si *o* est un dossier correspondant à un des patients traité par l'organisation ST1.

De même, le contexte "urgence" est définit comme suit :

- $\forall s \forall o \forall \alpha$ (*Définit*(*ST1*, *s*, α, *o*, *urgence*) $\leftrightarrow$ vrai): dans ST1, le contexte "urgence" est toujours vrai entre les sujets, les actions et les objets.

La politique de sécurité

Nous ne pouvons dans cet article entrer dans le développement complet de la spécification d'une politique de sécurité d'un établissement hospitalier. Nous ne présentons que quelques exemples illustrant comment une telle politique de sécurité peut être exprimée à l'aide de notre modèle. Considérons les trois permissions suivantes :

- *Permission*(*RT2*, *médecin*, *consulter*, *dossier_médical*, *medecin_traitant*),
- *Permission*(*RT2*, *médecin*, *consulter*, *dossier_médical*, *équipe_traitante*) et
- *Permission*(*RT2*, *médecin*, *consulter*, dossier*_chirurgical*, *équipe_traitante*).

La première permission indique que l'organisation RT2 permet aux médecins de consulter les dossiers médicaux des patients dont ils sont les médecins traitants. Les deuxième et troisième permissions spécifient que l'organisation RT2 permet aux médecins de consulter un dossier médical ou chirurgical si ce dossier correspond à un patient de RT2. Notons que les permissions associées aux rôles médecin peuvent changer d'une organisation à une autre, et les contextes respectifs sont aussi susceptibles d'être différents. Cette possibilité est en particulier intéressante dans notre exemple dans la mesure où les conditions dans lesquelles un médecin à la permission de consulter un dossier peut varier selon s'il exerce dans une équipe chirurgicale ou une équipe radiologique.

Les hiérarchies

Jusqu'à présent nous n'avons pas abordé la notion de hiérarchie de rôles. Cette notion à d'abord été introduite dans le modèle RBAC [15]. L'idée est de mettre en place un mécanisme d'héritage des permissions à travers la hiérarchie de rôle. Dans notre approche, la hiérarchie de rôle n'est pas considérée comme un concept de base. L'héritage des permissions dans ST1 entre un rôle r_1 (par exemple médecin) et un rôle r_2 (par exemple chirurgien) est spécifié par la règle suivante :

- $\forall a \forall v \forall c$ (*Permission*(*ST1*, r_1, *a*, *v*, *c*) $\rightarrow$ *Permission*(*ST1*, r_2, *a*, *v*, *c*).

Nous pouvons ajouter à notre langage une relation *Sous-rôle*(*ST1*, r_1, r_2). Les instances d'une telle relation étant simplement définies par la règle que nous venons de définir. Précisons toutefois que dans notre modèle il est possible de spécifier que l'héritage entre deux rôles donnés ne s'applique qu'à certaines organisations. Nous pouvons par exemple spécifier qu'à l'hôpital Purpan, le rôle directeur hérite des permissions du rôle médecin. :

- $\forall a \forall v \forall c$ (*Permission*(*Purpan*, *médecin*, *a*, *v*, *c*) $\rightarrow$ *Permission*(*Purpan*, *directeur*, *a*, *v*, *c*)).

Bien sur, nous n'aurions pas cette règle si, au lieu de considérer l'hôpital Purpan, nous considérons un autre établissement au sein duquel le directeur n'est pas un médecin. Il est également possible d'exprimer dans notre modèle l'héritage, entre rôles, d'interdictions, d'obligations et de recommandations. Nous pouvons également une hiérarchie entre les vues et considérer que les permissions sont héritées à travers cette hiérarchie. Le même principe peut être appliqué à une hiérarchie entre les activités. Par exemple, les vues *dossier_administratif*, *dossier_médical* et *dossier_chirurgical* sont des sous vues de la vue *dossier_patient*. Ainsi, un rôle qui a la permission de réaliser une activité sur la vue *dossier_patient*, a également la permission de réaliser la même activité sur les sous vues précédemment citées. Ceci s'exprime dans notre langage par la règle suivante :

- $\forall r \forall a \forall c$ (*Permission*(*Purpan*, *r*, *a*, *dossier_patient*, *c*) $\rightarrow$ *Permission*(*Purpan*, *r*, *a*, *dossier_administratif*, *c*)).

Il en est de même pour les vues *dossier_médical* et *dossier _chirurgical*.

Les contraintes

L'utilisation de contraintes a été proposée dans le modèle RBAC [15]. Les contraintes sont exprimées dans notre modèle par des règles s'appliquant à diverses relations. Nous donnons ici quelques exemples :

- $\forall s$ (*Habilite*(*Purpan*, *s* , *équipe_chirurgicale*) $\rightarrow$ ($\exists s_1$ *Habilite*(*s, s_1, chirurgien*) $\wedge$ $\exists s_2$ *Habilite*(*s, s_2, anesthésiste*) $\wedge$ $\exists s_3$ *Habilite*(*s, s_3, infirmier*)) : Cette règle indique que si l'hôpital Purpan habilite *s* comme équipe chirurgicale, alors *s* habilite un chirurgien, un anesthésiste et une infirmière.
- $\forall s$ $\neg$(*Habilite*(*Purpan*, *s*, *chirurgien*) $\wedge$ *Habilite*(*Purpan*, *s* , *anesthésiste*)) : Au sein de l'hôpital Purpan, aucun sujet *s* ne peut être habilité à la fois comme chirurgien et comme anesthésiste.
- $\forall s \forall s'$ *Habilite*(*Purpan*, *s*, *directeur*) $\wedge$ *Habilite*(*Purpan*, *s'*, *directeur*) $\rightarrow$ *s* = *s'* : Au sein de l'hôpital Purpan, un seul sujet *s* peut être employé comme directeur.

Il est ainsi possible d'exprimer de nombreuses contraintes sur les relations *Utilise*, *Considère*, *Définit*, *Permission*, *Obligation*, *Interdiction*, *Prohibition* ou *Recommandation*.

Conclusion

Dans cet article, nous avons présenté un nouveau modèle de politique de sécurité dont le but est d'apporter des réponses aux limites des modèles existants. Ce modèle, appelé ORBAC, est centré sur le concept d'organisation. En effet, tous les autres concepts que nous avons définis et qui permettent de spécifier une politique de sécurité dépendent d'une organisation donnée :

- Le concept de *Rôle* permet de modéliser comment l'organisation habilite les sujets,
- le concept de *Vue* permet de modéliser comment l'organisation utilise les objets,
- le concept d'*Activité* permet de modéliser comment l'organisation réalise des actions, et
- la relation *Définit* permet de modéliser comment l'organisation définit des contextes dans lesquels des utilisateurs réalisent des actions sur des objets.

En s'appuyant sur ces concepts, nous pouvons exprimer une politique de sécurité comme un ensemble de permissions, d'interdictions, d'obligations et de recommandations. Une permission correspond à un fait ayant la forme $Permission(org, r, a, v, c)$ qui signifie que l'organisation *org*, dans le contexte *c*, permet au rôle *r* de réaliser l'activité *a* sur la vue *v*. Les faits *Interdiction*, *Obligation* et *Recommandation* sont définis de façon analogue. Nous avons également montré comment dériver des permissions, des interdictions, des obligations et des recommandations concrètes qui s'appliquent à des sujets, des actions et des objets.

Plusieurs problèmes n'ont pas été abordés dans cet article. Tout d'abord, des conflits peuvent apparaître dans la politique de sécurité. Par exemple, pour un sujet donné, une action donnée, et un objet donné, il nous faut détecter et résoudre une situation dans laquelle il serait possible de dériver à la fois une permission et une interdiction. Cette question a fait l'objet de diverses propositions [4, 10, 18]. L'approche que nous suggérons s'appuie sur la logique possibiliste, et doit permettre de dériver automatiquement des niveaux de priorité entre les règles de la politique de sécurité [3]. Si nous n'avons pas discuté ici de la question de l'administration de la politique de sécurité, il est bien évidemment nécessaire de développer un modèle complet incorporant l'administration. Un tel modèle a été présenté avec ARBAC [16] pour l'administration du modèle RBAC. Le modèle d'administration de notre modèle sera abordé dans un futur article. Enfin, il nous faut aussi montrer comment spécifier des propriétés de sécurité dans le modèle ORBAC. En particulier, nous devons définir des moyens pour détecter une violation de la politique de sécurité et spécifier la décision à prendre dans un tel cas ; comme par exemple dans le cas d'un sujet qui ne remplirait pas ses obligations.

Remerciements

Le travail présenté dans cet article a été effectué dans le cadre du projet RNRT MP6 (***M***odèles et ***P***olitiques de ***S***écurité des ***S***ystèmes d'***I***nformations et de ***C***ommunication en ***S***anté et en ***S***ocial).

Bibliographie

- [1] J. Barkley, K. Beznosoz et J. Uppal. Supporting Relationships in Access Control Using Role Based Access Control. *Proceeding of the ACM workshop on RBAC*, Fairfax, Virginia, USA, 28-29 Octobre 1999.
- [2] D. E. Bell et L. J. LaPadula. Secure computer systems: Unified exposition and multics interpretation. Technical Report ESD-TR-73-306, The MITRE Corporation, Mars 1976.
- [3] S. Benferhat, R. El Baida et F. Cuppens. Modélisation des politiques de sécurité dans le cadre de la théorie des possibilités. *Rencontres Francophones de la Logique Floue et ses Applications*, Montpellier, France, Octobre 2002.
- [4] E. Bertino, S. Jajodia et P. Samarati. Supporting Multiple Access Control Policies in Database Systems. *IEEE Symposium on Security and Privacy*, Oakland, USA, 1996.
- [5] C. Bettini, S. Jajodia, X. S. Wang et D. Wijesekera. Obligation Monitoring in Policy Management. *International Workshop, Policies for Distributed Systems and Neworks (Policy 2002)*, Monterey CA, 5-7 Juin 2002.
- [6] K. J. Biba. Integrity consideration for secure computer systems. Technical Report MTR-3153, The MITRE Corporation, Juin 1975.
- [7] E. C. Cheng. An Object-Oriented Organizational Model to Support Dynamic Role-based Access Control in Electronic Commerce Applications. *32nd Annual Hawaii International Conference on System Sciences (HICSS-32)*, Maui, Hawaii, 5-8 Janvier 1999.
- [8] F. Cuppens, L. Cholvy, C. Saurel et J. Carrère. Merging Regulations: analysis of a practical example. *International Journal of Intelligent Systems*, 16(11), Novembre 2001.
- [9] N. Damianou, N. Dulay, E. Lupu et M. Sloman. The Ponder Policy Specification Language. *International Workshop, Policies for Distributed Systems and Neworks (Policy 2001)*. Bristol, UK, 29-31 Janvier 2001.
- [10] G. Dinolt, L. Benzinger et M. Yatabe. Combining Components and Policies. *Proceedings of the Computer Security Foundations Workshop VII*, Franconia, USA, 1994.
- [11] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn et R. Chandramouli. Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security*, 4(3):222-274, Août 2001.
- [12] S. I. Gavrila et J. F. Barkley. Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management. *Third ACM Workshop on Role-Based Access Control*, pages 81-90, 22-23 Octobre 1996.
- [13] M. A. Harrison, W. L. Ruzzo et J. D. Ullman. Protection in Operating Systems. *Communication of the ACM*, 19(8):461-471, Août 1976.
- [14] B. Lampson. Protection. *5th Princeton Symposium on Information Sciences and Systems*, pages 437-443, Mars 1971.
- [15] R. Sandhu, E. J. Coyne, H. L. Feinstein et C.E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38-47, 1996.
- [16] Ravi Sandhu, Bhamidipati et Qamar Munawer. The ARBAC97 Model for Role-Based Administration of Roles. *ACM Transactions on Information and System Security*, 2(1), Février 1999.
- [17] R. Thomas et R. Sandhu. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *11th IFIP Working Conference on Database Security*, Lake Tahoe, California, USA, 1997.
- [18] Roshan K. Thomas. TMAC: A primitive for Applying RBAC in collaborative environment. *2nd ACM, Workshop on RBAC*, pages 13-19, Fairfax, Virginia, USA, 6-7 Novembre 1997.

Etude sur la sécurité du système d'information dans le milieu médical en Languedoc Roussillon

Francis GARCIA
Professeur Ensam
Université Montpellier II
Département Sécurité de l'Information (CRIC)

Résumé : Persuadée que l'introduction des nouvelles technologies aggrave la responsabilité du médecin vis à vis de la loi, l'Union Professionnelle des Médecins Libéraux a demandé au département « sécurité de l'information et intelligence économique du CRIC » de réaliser une expertise auprès des médecins libéraux de la région Languedoc-Roussillon afin de vérifier ces inquiétudes. Une longue enquête à laquelle ont répondu des centaines de médecins confirme toutes ces craintes et met en évidence une plus grande vulnérabilité des informations médicales. Ce travail propose toute une série d'actions à mener afin de réduire les risques. Mais au delà d'une réponse au problème spécifique de sécurité, ce travail pose un grand nombre de questions mettant en lumière plusieurs pistes de recherche en matière de sécurité des systèmes d'information.

Introduction

Le médecin a l'obligation d'assurer la confidentialité des informations médicales qui lui sont confiées par ses patients (article 4 et 73 du code de déontologie médicale) ainsi que la protection de leur intégrité et de leur disponibilité (article 226-17 du code pénal)[ALLAERTA F.A, 1999]. La révélation d'une information à caractère secret par une personne qui est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire est punie (article 226-13 du code pénal).

Les informations médicales relatives aux patients sont des informations protégées en France depuis 1978 par la loi "Informatique et libertés" et depuis 1998 par la directive Européenne " relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette protection s'applique à des informations banales telles que l'âge, le sexe ou le lieu d'habitation dans la mesure où elles ont été recueillies à l'occasion d'une consultation médicale [DUCROT H. 1996].

L'ordonnance N° 96-345 du 24 avril 1996 a ouvert le marché de l'informatisation des cabinets médicaux libéraux et de nombreux éditeurs de logiciels proposent des produits aux médecins sans toujours maîtriser les spécificités de l'information médicale , leurs implications légales et déontologiques.

Cette loi autorisant l'enregistrement et le traitement automatisé de ces informations aggrave les responsabilités des médecins. En effet les articles 226-13, 226-21 et 226-22 du code pénal prévoient de lourdes sanctions pour ceux qui de manière directe ou indirecte, volontaire ou involontaire contribuent à la divulgation d'informations médicales nominatives [VERLYNDE P. 2001].
Ainsi en cas de malversation à l'encontre des données personnelles de leurs patients, même si elle n'est pas de leur fait, les médecins pourront se voir reprocher de s'être montrés négligents dans le choix de leur équipement, si celui-ci ne comporte pas les sécurités requises par l'exercice médical. Or, les atteintes à l'intégrité et à la disponibilité des informations résultent non seulement de malveillances mais le plus souvent d'accidents techniques ou de maladresses.

Il est important de rappeler que toute connexion dans un réseau comporte un risque d'intrusion d'une personne extérieure et que dans ce contexte les liaisons Internet doivent être étroitement protégées [VENOT A., 1997)].

Dans un système d'information, les possibilités d'atteinte à la confidentialité sont nombreuses[ANDERSON R. 1996]:
- le vol de tout ou partie des informations
- les erreurs de manipulation adressant par erreur des informations à des personnes non autorisées
- les accès indiscrets
- les copies illégales de fichiers
- les interceptions de transmissions

En conséquence les logiciels et équipements diffusés pour l'informatisation du cabinet médical doivent intégrer les protections nécessaires pour assurer la sécurité des informations médicales et permettre ainsi aux médecins de satisfaire à leurs obligations.

C'est dans ce contexte que le Département Sécurité de l'Information du CRIC à été mandaté par l'Union afin de réaliser une expertise du système d'information médical en région Languedoc Roussillon et mettre en évidence les défauts de sécurité .

La suite de ce document présente l'enquête réalisée, fait la synthèse des réponses , décrit les faiblesses du système d'information et présente une réflexion sur les principales actions à mener pour limiter les risques.

I - L'enquête

I.1 – Objectifs recherchés et méthode de travail

Ce travail commandité par l'Union s'était fixé deux objectifs majeurs :

1. Mettre en évidence les failles dans la sécurité du système
2. Proposer un plan d'action de manière à réduire ces failles

Le principal problème dans ce travail était de mettre en place une méthode efficace pour un recueil significatif des informations. En effet l'autonomie des personnes et leur dispersion géographique rendait difficile une étude exhaustive de chaque médecin. Rapidement nous nous avons opté pour réaliser un sondage d'une partie de cette population au travers d'un questionnaire. Un comité de pilotage composé de médecins de l'Union et de membres de l'équipe serait chargé de mettre au point le questionnaire et de suivre l'avancement du travail.

La version finale de ce questionnaire n'était obtenue qu'après plusieurs semaines de travail. Une première esquisse était proposée aux médecins du comité de pilotage et modifiée à partir des remarques formulées. Cette pré-version permit de

faire une première collecte d'information auprès d'un groupe de médecins volontaires. L'analyse des résultats et la forme des réponses contribua à compléter le questionnaire et à améliorer la présentation pour aboutir à la version finale.

L'enquête serait effectuée auprès de 500 médecins de la région et de tous ceux qui disposaient d'une adresse électronique. Le choix des destinataires du document fut fait de telle sorte que :

- la proportion de médecins généralistes et de spécialistes sondés reste conforme à la répartition générale
- le questionnaire soit envoyé à au moins un médecin de chaque ville ou village de la région.

I. 2 – Forme et contenu du questionnaire

Le principal souci était de réaliser un questionnaire rapide à compléter, en effet l'introduction de l'informatique étant vécue par beaucoup de médecins comme une charge de travail supplémentaire et une perte de temps nous ne souhaitions pas conforter cette vision des choses. Pour cette raison le questionnaire se présente sous la forme d'un QCM pour les questions principales mais avec la possibilité de s'exprimer librement s'ils le souhaitent.

Ce questionnaire devait être le plus complet possible pour nous permettre de mieux connaître cette population ainsi que le niveau d'utilisation des nouvelles technologies afin d'en déduire les risques potentiels.

Plusieurs parties étaient analysées :

Généralités sur l'activité du médecin : Il s'agissait de déterminer le mode de fonctionnement du médecin indépendamment des outils utilisés. Travaille-t-il seul ou en groupe ? A-t-il une secrétaire pour l'aider ? Se contente-t-il de conserver uniquement le dossier médical de ses patients ou intègre-t-il d'autres données telles que les résultats d'analyses ou compte-rendus fait par d'autres cabinets ? Gère-t-il des données autres que médicales comme par exemple les données comptables ?

L'équipement et les applications informatiques : On détermine si le médecin dispose d'un équipement informatique ou pas. Le questionnaire permet de préciser pour quelles raisons il n'en possède pas ou bien demande des précisions sur les matériels et logiciels possédés ainsi que sur la maintenance et la formation.

Télétransmission des données et Internet : Dans un premier temps cette partie fait le point sur la transmission des feuilles de soins électroniques qui est une obligation légale. Elle s'intéresse ensuite à l'utilisation ou pas de l'internet. L'objectif est de connaître les types d'applications utilisées , le temps passé et les attentes vis à vis de ce réseau.

Sécurité : dans cette partie les questions s'articulaient autour de 3 axes :

- protection et accès aux locaux,
- protection des systèmes informatiques (mot de passe, sauvegarde des données, antivirus, et autres problèmes),
- problèmes rencontrés

I. 3 – Diffusion et retour des questionnaires

Les questionnaires ont été diffusés :

- par e-mail, à tous les médecins référencés comme ayant une adresse électronique (soit près de 700 personnes)
- par courrier, à 500 médecins choisis aléatoirement dans la région. Il a été expédié au moins un questionnaire dans chaque ville et village de la région où est implanté un médecin.

Pour les expéditions par e-mail près de 100 adresses se sont révélées incorrectes ou non utilisées. Ceci ramène le nombre effectif de questionnaires ayant atteint leur destinataire à 600. Nous comptabilisons 31 réponses soit 5% des personnes contactées. Ce chiffre est d'autant plus intéressant que seulement 6 questionnaires ont été retournés via la messagerie électronique, les autres ayant été imprimés puis renvoyés par courrier. Il semble que les médecins maîtrisent mal ce type d'outil .

En ce qui concerne les expéditions par courrier, 125 questionnaires ont été retournés soit plus de 25%. Ce chiffre montre l'intérêt du médecin pour l'informatique et d'une façon générale pour les nouvelles technologies.

Les médecins de l'Hérault et du Gard ont mieux répondu que ceux de l'Aude et des P .O. Le faible taux de réponses de la Lozère s'explique par la population dans ce département.

Les réponses émanent pour 70% de généralistes et 30% de spécialistes. Cette répartition est conforme à l'appel initial .

Il faut noter que la plupart des médecins (81%) qui ont participé à cette enquête n'avaient pas répondu à un questionnaire antérieur sur l'informatique réalisé par l'Union . Cette situation montre bien

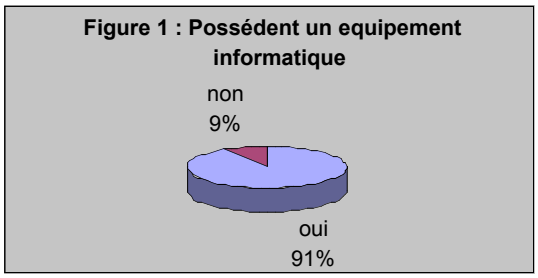
l'intérêt que portent les médecins à l'utilisation des nouveaux outils de traitement de l'information .

II – Résultats de l'enquête

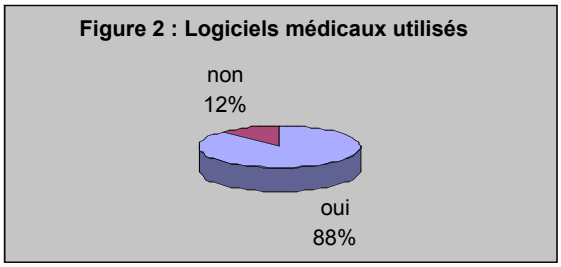
II . 1 - Généralités sur l'activité du médecin

Sur la région il semble que les médecins travaillent seuls (50%) ou regroupés en cabinet pour une même spécialité (47%). Très peu de spécialités différentes s'associent (3%).

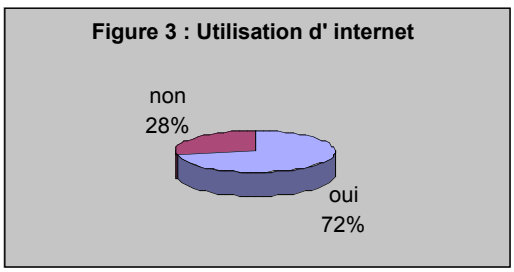
Malgré les obligations légales, 26% déclarent ne pas utiliser la télétransmission . Ceci n'est pas dû à l'absence de matériel car 91% des médecins possèdent et utilisent un équipement informatique (figure 1).



L 'utilisation de l'outil informatique est aujourd'hui (figure 2) une réalité avec 88% des personnes qui ont opté pour des logiciels médicaux dans l'exercice de leur profession. On dénote d'ailleurs que 40% des cabinets possèdent plusieurs machines reliées en réseau. Ceci sous entend une structure technique lourde et une organisation particulière du travail [FORMMEL 2000].



Les médecins se sont massivement ouverts vers l'extérieur (72%) grâce à l'internet (figure 3).



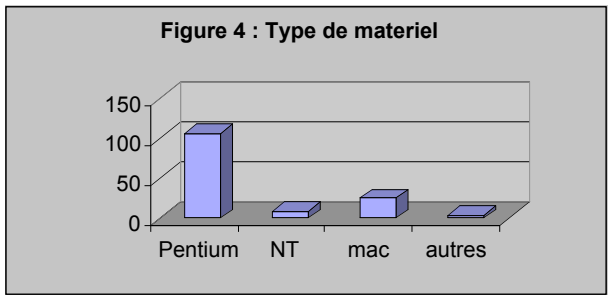
On peut enfin dire qu'ils sont généralement sensibilisés à la notion de risque informatique puisque 77% déclarent réaliser systématiquement des sauvegardes de leur données et que 73% disent utiliser un anti-virus.

Les raisons de non-utilisation d'équipement informatique mettent aussi en évidence des différences entre les généralistes et les spécialistes. Les spécialistes dénoncent tout particulièrement les aspects techniques (compliqués, vulnérables) et financiers de ces équipements (trop onéreux), alors que les généralistes se plaignent tout particulièrement d'un manque de temps et de formation nécessaires à une utilisation correcte de ces outils.

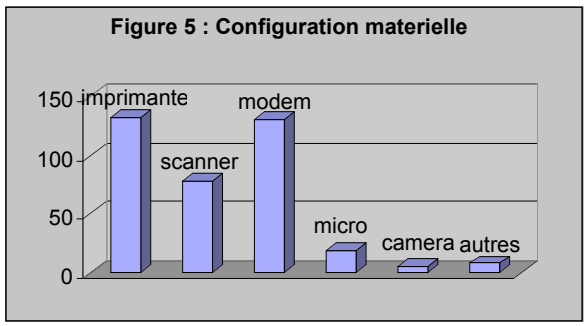
II.2- L'équipement et les applications informatiques

Configuration des machines

La configuration informatique est des plus classique, un pentium (figure 4) ou équivalent sous windows avec une imprimante et un modem (figure 5) pour la télétransmission ou l'internet. Beaucoup utilisent aussi un scanner pour le stockage de documents externes concernant les patients.

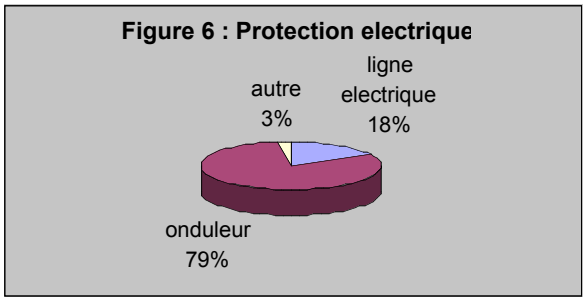


On relève quelques systèmes sous Windows NT et sur Linux, mais généralement leur utilisation reste marginale et concerne des médecins dans le milieu hospitalier.



Il est intéressant de noter l'utilisation en quantité non négligeable de machines de type Mac.

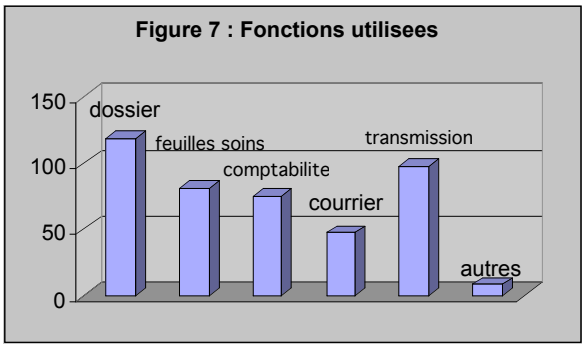
Cet équipement est généralement protégé par un onduleur et parfois par une ligne électrique spécifique (figure 6) . On note cependant que près de 30% de cabinets ne disposent d'aucune protection électrique .



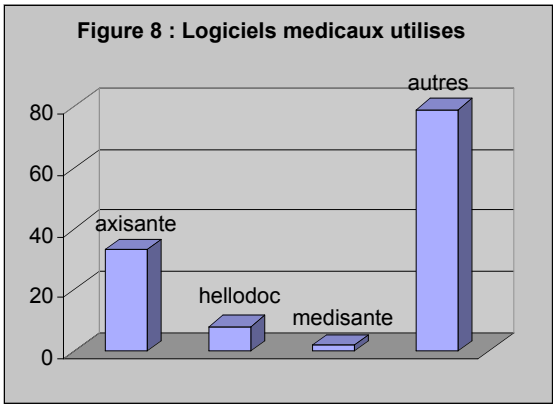
Logiciel médical

Si la gestion du dossier patient et la télétransmission sont les fonctions les plus utilisées dans les applications médicales (figure 7) , on peut noter que les médecins essayent d'exploiter au mieux cet outil, même s 'ils le considèrent parfois comme difficile [FRACHET B. 2002]. Par exemple ils saisissent et éditent les ordonnances sur ordinateur ce qui ne déplaît pas aux patients qui disposent de documents lisibles. D'autres fonctions plus annexes sont également utilisées comme la comptabilité ou le courrier électronique.

L'élément marquant est la grande hétérogénéité des logiciels médicaux utilisés (figure 8). Le questionnaire proposait trois noms : « axisante », « hellodoc » et « médisante » qui, d'après les magazines spécialisés, étaient les plus vendus et complets en France. Or aucun de ces logiciels ne se détache . Ceci est la résultante de l'indépendance du milieu médical vis à vis d'autorités supérieures,



mais cela ne place pas le médecin en position de force par rapport à son éditeur de logiciel et rend difficile les comparaisons et les échanges d'informations entre cabinets.



Autres logiciels

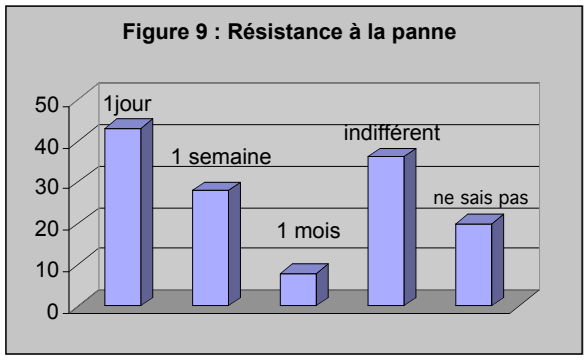
Beaucoup de médecins utilisent les standards de Windows pour :

- la réalisation de rapports et de courrier avec Word
- la consultation d'informations et le courrier électronique via Internet avec « Internet Explorer ».

On notera que quelques personnes utilisent un logiciel de comptabilité spécifique mais cela reste assez peu fréquent.

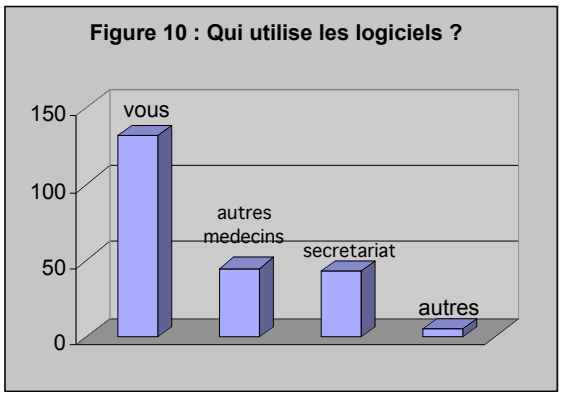
Dépendance vis à vis de l'outil informatique

A la question « Combien de temps estimez-vous pouvoir fonctionner sans ordinateur et sans danger pour vos patients ? » les réponses sont sans appel : un jour , au plus une semaine (figure 9) . Même si un tiers des médecins estiment pouvoir revenir à une gestion du dossier totalement manuelle du jour au lendemain, nombreux sont ceux qui deviennent dépendants des nouvelles technologies.



La réponse à la question « qui utilise les logiciels ? » peut nous laisser perplexe puisque 60% des médecins disent être seuls à utiliser les applications (figure 10). Cette situation est normale dans le cas d'une personne qui exerce seule, mais lorsqu'il apparaît que 50% des médecins exercent conjointement avec d'autres collègues cela pose

problème. Cela sous entend que dans le cas de regroupement de plusieurs personnes, l'un d'eux se spécialise dans l'informatique ce qui peut être dramatique en cas de défaillance de ce dernier.

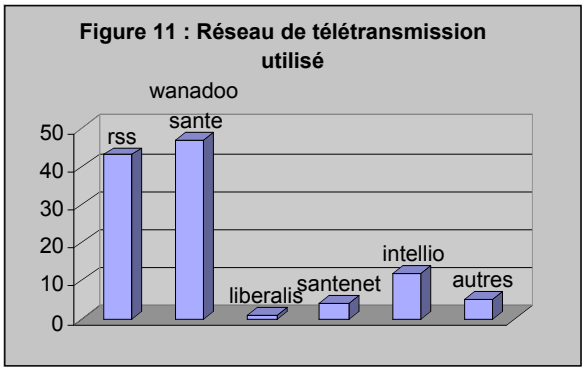


Si l'on se réfère à l'utilisation des logiciels médicaux, on constate ici que les généralistes sont de grands « consommateurs » avec 94% contre 72% pour les spécialistes. Cet écart par contre n'est pas surprenant, il semble en effet que les éditeurs de logiciel se soient surtout intéressés au corps le plus important « les généralistes », délaissant des activités plus marginales (en nombre) donc moins rentables économiquement.

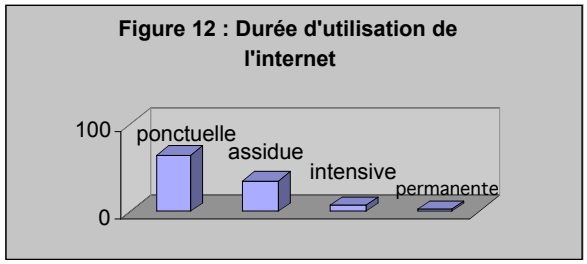
II. 3 - Télétransmission des données et Internet

Comme cela a déjà été noté précédemment, seulement 74% des médecins utilisent la télétransmission pour expédier automatiquement les feuilles de soins électroniques. C'est , à quelques exceptions près , la seule utilisation qui est faite.

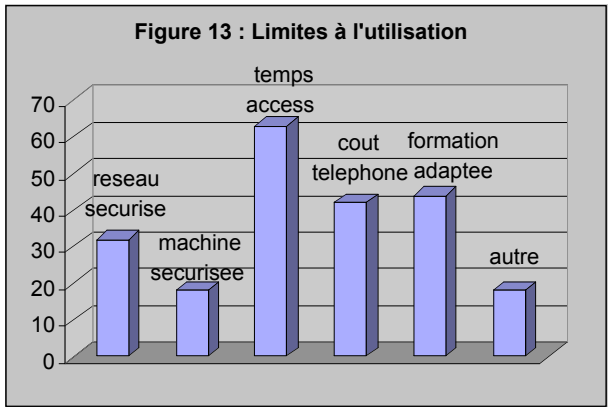
Ils utilisent principalement deux types de réseaux de transmission « RSS » ou « Wanadoo Santé » (figure 11). Localement les médecins ont fait installer une ligne téléphonique spécifique ou réservent une ligne dans les cas où ils disposent d'un groupe de lignes. Cette configuration permet, le cas échéant, une liaison permanente des équipements informatiques avec l'extérieur, même si peu de médecins disent exploiter cette possibilité [LE BEUX P. 2001]. En fait la plupart transmettent les informations en fin de journée, laissant ainsi les lignes disponibles pour l'utilisation d'internet.



L'internet fait une entrée en force dans le milieu médical. Même si pour l'instant l'utilisation ne semble que ponctuelle (figure 12) seulement quelques minutes par jour , il est utilisé massivement pour consulter des informations et échanger des messages.



Les principaux freins à une meilleure utilisation du « net » sont dans l'ordre : le temps d'accès élevé , les coûts élevés des communications téléphoniques et le manque de formation (figure 13) . Le manque de sécurité dans ce type de réseau n'est pas, a priori, une préoccupation. Or la présence de fonctions de communication sur l'ordinateur couplés avec une ligne téléphonique spécifique et un modem intégré rendent les équipements accessibles depuis l'extérieur dès qu'ils sont allumés.



Les généralistes ont recours à 71 % à la télétransmission contre 61% pour les spécialistes. Cette différence de 10 points est suffisamment significative pour que l'on s'intéresse à elle. L'enquête ne permet pas d'apporter une réponse valable à cet écart. Cela peut faire l'objet d'une étude complémentaire. En ce qui concerne l'utilisation de l'internet les chiffres s'inversent ici. Les spécialistes disent l'utiliser à 82% contre 68% pour les généralistes. Ici aussi ces résultats ne surprennent pas, l'internet est utilisé dans l'exercice de la profession pour la recherche et l'échange d'informations spécifiques.

II. 4 – Documentation et formation

Documentation

80% des médecins possèdent la documentation de leur équipement informatique et/ou des applications utilisées. Cela signifie encore que 20% d'entre eux n'ont aucun support de référence en cas de problème de fonctionnement. Parmi ceux qui disposent de notices, ils sont 69% à les posséder toutes (machine, système, application médicale et/ou télétransmission). On note cependant que 18% ont les guides de la machine mais pas des applications médicales et/ou télétransmission et que 13% possèdent une aide pour leur applications mais pas pour le matériel. En fait trop de médecins ne disposent pas d'une aide documentaire suffisante pour faire face à des problèmes, même mineurs.

La formation

Ils sont 46% à n'avoir suivi aucune formation pour l'utilisation de leur équipement ni des applications. Pour ceux qui ont pu le faire, 41% se sont formés (ou informés) sur le matériel ou le système d'exploitation (Windows, Linux, ..) et seulement 54% ont appris le fonctionnement de leur application médicale et/ou logiciel de télétransmission. En fait moins de 25% des médecins qui utilisent un équipement informatique et des applications se sont préparés à leur utilisation. Cela fragilise la profession qui ne possède pas les connaissances techniques suffisantes pour faire face aux divers problèmes quotidiens.

Les raisons de non formation

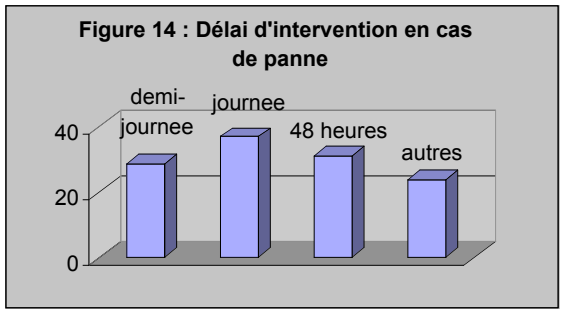
Pourquoi les médecins ne se forment-ils pas ? 40% évoquent le manque de temps ou la technicité des produits (12%), ils pensent ne pas avoir les connaissances de base suffisantes pour suivre ces types de formation. D'autres dénoncent la trop grande complexité des applications par rapport à leur besoin, ils n'utilisent que très peu de fonctionnalités parmi toutes celles proposées . Se former sur des produits dont ils n'utilisent qu'une petite partie ne présente aucun intérêt (11%), se former sur des fonctions qu'ils maîtrisent bien aujourd'hui ne présente pas plus d'intérêt (24%).

Cela veut-il dire que les médecins ne souhaitent pas de formation ? non bien sûr, ils sont 90% à en réclamer. Cependant ils ne désirent pas se former n'importe comment et à n'importe quoi. Pour eux (28%) une bonne connaissance de l'informatique générale est indispensable. Ces acquis leur permettront de mieux comprendre les applications médicales qu'ils utilisent dans le cadre de leur profession (26%) puis de découvrir les possibilités du système Windows ou équivalent (20%).

II. 5 - Sauvegardes et sécurité

Protection des équipements

Généralement un contrat de maintenance matériel et/ou logiciel à été passé avec le fournisseur ou une société spécialisée. Ces contrats prévoient généralement des délais d'intervention très courts de l'ordre d'une journée au maximum et rarement au delà de 48 heures (figure 14). Ces chiffres sont à prendre avec beaucoup de précautions , car la plupart du temps les médecins n'ont encore jamais rencontré de problèmes. Dans le cas contraire il s'agit de problèmes mineurs qui ont pu être réglés rapidement par le médecin lui-même ou parfois un ami.



Dans tous les cas cette situation pose un problème de confidentialité car une intervention sur matériel ou logiciel implique des essais et souvent un libre accès à l'ensemble des fichiers de la machine, donc aux données des patients.

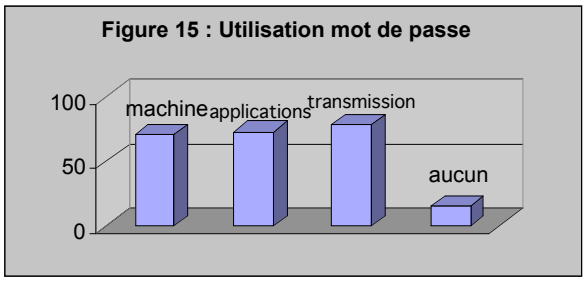
Sécurité des locaux et des équipements

Ici le constat est accablant , peu ou pas de précautions sont prises. Lorsqu'on sait que les équipements informatiques possèdent toutes les données des patients et que les copies de sauvegarde sont généralement conservées sur place, seulement 14% des cabinets sont équipés d'alarmes. Ceci rend les données excessivement vulnérables en cas d'effraction du cabinet.

Sécurité des applications

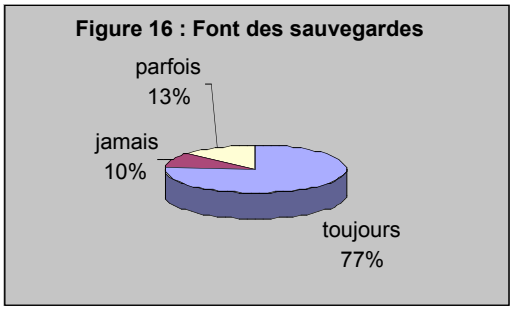
Si la plupart des applications médicales ou de télétransmission sont protégées par un mot de passe (figure 15) , peu de machines disposent d'une protection logique lors de la mise en route et trop d'équipements ne possèdent aucune protection.
Lorsqu'un mot de passe protège l'accès à une application il n'est souvent connu que par une seule personne ou alors il est divulgué à tous les employés du cabinet et parfois même à l'extérieur. Il est même des cas ou les codes d'accès sont communiqués à la « femme de ménage » ! ! !

Il semble même que le changement de mot de passe ne soit pas chose courante, ceci peut poser des problèmes lorsqu'on le communique à du personnel temporaire (remplaçants) .

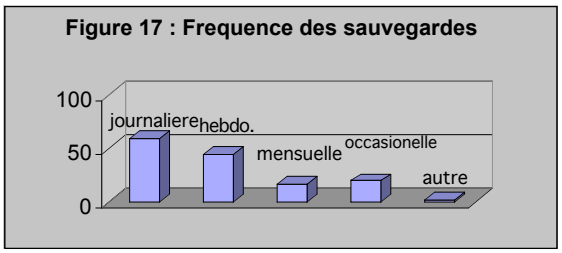


Sauvegarde des données

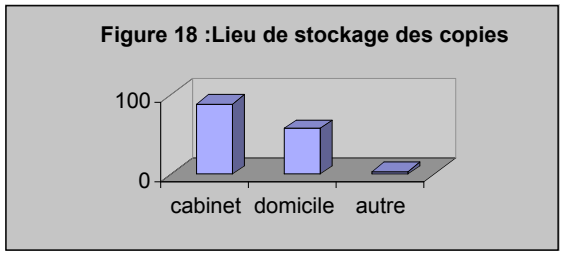
77% des médecins réalisent systématiquement des sauvegardes (figure 16) . Ils effectuent généralement une copie des seules données modifiées du système .



Cependant moins de 50% des cabinets font des copies journalières, beaucoup ne réalisent des sauvegardes qu'une fois par semaine voire une fois par mois (figure 17). Une part non négligeable de médecins n'attache pas d'importance aux copies de sécurité puisqu'ils n'en font qu'occasionnellement.



Copiés sur des supports externes « zip » ou « CD gravés », les sauvegardes sont souvent conservées dans le cabinet médical ou à proximité de la machine (figure 18) . Ceci ne garantit pas une protection efficace en cas de vol ou de catastrophe naturelle.



Incidence des problèmes rencontrés sur le comportement des médecins

Principaux problèmes

La relative jeunesse des équipements dans les cabinets ne permet pas d'observer les problèmes majeurs de l'informatique tels que :

- panne d'un disque dur et perte totale des données et des applications existantes,
- changement d'équipement avec transfert de données sur une nouvelle machine et une nouvelle application.

On signale cependant un certain nombre de problèmes que nous pouvons qualifier de mineurs :

- 34% de médecins disent avoir perdu des données
- 73% affirment avoir eu des pannes de matériel (modems, disque, imprimante, …)
- 10% ont été victimes de vol, essentiellement de matériel (imprimante, ordinateur,…)

Malgré les faibles impacts de ces problèmes sur le fonctionnement quotidien, il semble que la gêne occasionnée ait été suffisante pour amener des changements notables de comportement chez ceux qui en ont été victimes .

Impact de la perte des données

85% des personnes ayant perdu des données disent faire des sauvegardes régulières de leur fichiers contre 71% pour ceux qui n'ont jamais rencontré ce type de problème. Ils ne sont plus que 4% à ne pas faire de copies contre 15% dans l'autre cas de figure.

Fait encore plus marquant, même si 47% ne vérifient pas encore les sauvegardes malgré des pertes de données, ce chiffre est bien inférieur aux 71% qui ne le font pas.

Impact des pannes de matériel

Même si toutes les pannes de matériel n'ont pas comme conséquence une perte des données stockées elles permettent de prendre conscience du risque indirect qui existe.

Parmi les personnes victimes de pannes, 80% disent faire des sauvegardes régulières et seulement 7% s'obstinent à ne prendre aucune précaution . Ces chiffres montrent bien une prise de conscience du risque puisque en l'absence de panne ils ne sont que 67% à faire des copies régulières et 19% à ne rien faire.

Impact des vols

La conséquence d'un vol a bien plus d'impact sur le comportement des médecins que les autres types de problèmes. Après un tel événement 92% déclarent faire des copies de leur données contre 71%. Mais on note surtout que 67% des médecins déposent les copies hors de leur cabinet (généralement à leur domicile) alors qu'en moyenne seulement 36% externalisent leurs sauvegardes.

III - Synthèse de l'enquête

Lorsque les pouvoirs publics ont obligé le médecin à automatiser le cabinet, certainement par soucis d'amélioration des procédures, ils n'ont pas donné à cette profession les moyens techniques, financiers et informationnels d'exploiter ces outils [NETIZEN 1995].

La profession se retrouve souvent face à une technologie nouvelle qu'elle ne maîtrise pas toujours .

L'enquête réalisée met en évidence un grand nombre de dysfonctionnements tant au niveau technique qu'humain. La suite de ce chapitre reprend les principaux problèmes recensés pouvant mettre en cause de manière directe ou indirecte le système d'information donc la responsabilité du médecin.

III.1 - Confidentialité des données

Peu de machines disposent d'une protection logique (mot de passe) lors de la mise en route et trop d'équipements ne possèdent aucune protection. Lorsque des mots de passe existent, ils ne sont souvent connus que d'une seule personne ce qui peut être une cause de blocage en cas de défaillance de cette dernière. Il semble même que le changement de mot de passe ne soit pas chose courante et que l'on utilise le « post-it » pour ne pas oublier les codes d'accès.
La plupart des équipements étant sous maintenance auprès de prestataires extérieurs, cela pose un problème de confidentialité car une intervention sur le matériel ou le logiciel implique des essais, soit un libre accès à l'ensemble des données de la machine, donc aux données des patients.

III.2 - Pérennité et conservation des données

L'élément marquant est la grande hétérogénéité des logiciels utilisés **,** cela ne place pas le médecin en position de force vis à vis de son éditeur de logiciel et rend difficile les échanges d'informations entre cabinets.
Cette situation est d'autant plus préoccupante que les évolutions des équipements ne garantissent pas une compatibilité avec les versions antérieures. Cela laisse présager des problèmes dans le futur avec des équipements qui ne pourront plus lire les anciennes sauvegardes. En particulier dans un proche futur lorsqu'il faudra renouveler les équipements informatiques dans les cabinets [QUANTIN C. 1997].

III. 3 - Sauvegardes

Moins de 50% des cabinets font des copies journalières, beaucoup ne réalisent des sauvegardes qu'une fois par semaine voire une fois par mois. Une part non négligeable de médecins n'attache pas d'importance aux copies de sécurité puisqu'ils n'en font qu'occasionnellement.
Les médecins n'ont d'ailleurs aucune garantie sur la validité de leur sauvegarde, puisque très peu disent vérifier les copies.
Les sauvegardes sont souvent conservées dans le cabinet médical ou à proximité de la machine. Ceci ne garantit pas une protection efficace en cas de vol ou de catastrophe naturelle.
Cette situation est inquiétante , beaucoup de médecins ne seront pas en mesure de récupérer les données en cas de grave problème, ils ne pourront pas dans ce cas faire face à leur responsabilités vis à vis des patients.

III. 4 - Sécurité des transmissions

Si la plupart des outils de télétransmission sont sécurisés (mot de passe, cryptage, …) cela n'est pas le cas pour l'accès à l'internet. Or le manque de sécurité dans ce type de réseau n'est pas, à priori, une préoccupation pour le médecin. La présence de fonctions de communication sur l'ordinateur couplées avec une ligne téléphonique spécifique et un modem intégré rendent les équipements accessibles depuis l'extérieur dès qu'ils sont allumés.

III . 5 - Résistance aux attaques

La résistance des équipements aux infections par virus est quasiment nulle . Trop d'équipements ne sont pas protégés par des anti-virus et, pour ceux qui le sont, la mise à jour de ces protections est rarement faite.
En général les équipements sous internet font souvent l'objet d'attaques (hacking) extérieures

ayant pour but de visiter la machine ou de détourner des données. Les protections contre ce type d'action sont très difficiles à mettre en œuvre, elles passent par des mises de droits d'accès et des limitations dans les applications. A priori aucune protection de ce type n'est mise en œuvre sur les machines des médecins.

III . 6 - Protection des équipements

En ce qui concerne la sécurité des locaux et des équipements le constat est accablant . Peu ou pas de précautions sont prises, seulement 14% des cabinets sont équipés d'alarmes. Ceci rend les données excessivement vulnérables en cas d'effraction du cabinet, d'autant plus que matériel et support de sauvegarde sont très rarement mis sous clé et que les codes d'accès sont souvent visibles.
On note aussi que près de 30% des cabinets ne disposent d'aucune protection électrique , ceci peut entraîner des pertes de données en cas de perturbations électriques.

III . 7 - Maîtrise du système

Moins de 25% des médecins qui utilisent un équipement informatique et des applications se sont préparés à leur utilisation. Cela fragilise la profession qui ne possède pas les connaissances techniques suffisantes pour faire face aux divers problèmes quotidiens.
Les éditeurs de logiciels ne sont pas étrangers à ce manque de maîtrise. En voulant faire des applications médicales très générales et adaptables au plus grand nombre, ils proposent des produits très complexes à utiliser contenant un très grand nombre de fonctions souvent inutiles.
Trop de médecins ne disposent pas d'une aide documentaire suffisante pour faire face à des problèmes, même mineurs.

IV - Actions à mener

Les problèmes de sécurité rencontrés par les médecins au niveau de leurs appareils ne sont pas différents de ceux des autres professions . Les professionnels des nouvelles technologies ont d'ailleurs apporté au fil des années des solutions à la plupart des problèmes connus. Le monde médical profite (ou pourra profiter) de toutes ces protections matérielles et logicielles.

Cela n'est bien sûr pas suffisant car, dans un système d'information (l'enquête le met bien en évidence), c'est bien souvent le facteur Humain qui est la cause des défaillances pouvant mettre en cause la responsabilité des médecins. C'est à ce niveau qu'il faut agir afin de réduire les risques d'erreurs et de pertes d'informations.

Même s'il est illusoire d'envisager un système sécurisé à 100%, la mise en œuvre des mesures ci-dessous devraient permettre une réduction importante du risque, réduisant par la même occasion la responsabilité du médecin vis à vis de leur système d'information.

Le travail à faire pour envisager une sécurisation du système d'information est très important.
Quatre grands axes peuvent être définis :

- La sensibilisation et formation du médecin.
- L'automatisation et l' externalisation des sauvegardes.
- La standardisation des applications médicales et des procédures informatiques.
- La modification du comportement.

IV . 1 - Sensibilisation et formation du médecin

Le médecin a obligation d'assurer la confidentialité des informations médicales qui lui sont confiées par ses patients.
Mais le médecin a-t-il réellement conscience du risque encouru avec l'introduction des nouvelles technologies ? La réponse est visiblement non ! Or l'application de ces procédures ne sera effective qu'après cette prise de conscience.
Il est donc important d'informer le médecin mais en s'adaptant à lui, à sa disponibilité, à son manque de familiarisation avec les outils informatiques. Il est possible d'envisager plusieurs formes d'information :

- une campagne d'information très ludique avec la création de films présentant les principaux risques
- des conférences-débats où les médecins pourraient partager leur expériences.
- …

Il est nécessaire de mettre en œuvre une politique d'information et de formation adaptée [HUYNH F., ALLOUET J.M. 2001]. Ces programmes devront tenir compte de trois préoccupations : le manque de temps, le coût souvent élevé des formations externes, la technicité du domaine. Ici l'Union peut jouer un grand rôle en mettant en place ces types de formation … à méditer !

IV . 2 - Automatisation et « externalisation » des sauvegardes.

Il est du devoir et de l'intérêt du médecin de réaliser régulièrement des sauvegardes avec l'aide de logiciels appropriés.
Pourquoi ne pas automatiser les sauvegardes et délocaliser les copies ? La solution à ce problème consiste à rendre transparente cette action en intégrant dans les applications informatiques des procédures automatiques de sauvegarde à distance.
La définition d'une norme spécifique à ce type de

métier permettrait ainsi de « déresponsabiliser » le médecin en transférant la responsabilité de la sauvegarde vers des prestataires extérieurs.

IV.3- Standardisation des applications médicales et des procédures informatiques.

Si les systèmes actuels garantissent une conservation du dossier médical sur les supports informatiques, la durée légale de 30 ans n'est pas compatible avec l'évolution actuelle des logiciels et matériels informatiques [MASKENS A. ET GEBOERS J. 1998]. En moins de 20 ans nous sommes passés de la bande magnétique au « gravage » de CD en passant par des disquettes de différents formats. Il est quasiment impossible de nos jours de trouver un équipement (grand public) capable de lire des supports datant de plus de 10 ans.
Il est fondamental de normaliser les formats des données utilisées ainsi que les fonctionnalités des applications médicales et de prévoir le cas échéant des procédures de migration entre les systèmes.

Si les atteintes à l'intégrité et à la disponibilité des informations résultent non seulement de malveillances mais le plus souvent d'accidents techniques ou de maladresses ceci est la conséquence d'un manque de formation des médecins mais aussi d'un manque d'harmonisation des produits proposés sur le marché.
La réalisation d'un cahier des charges des besoins (normes) spécifique aux applications informatiques devrait aboutir à une meilleure harmonisation des produits. Ces normes imposées aux éditeurs de logiciels aboutiraient à des applications médicales standardisées et plus faciles à utiliser.

IV . 4 - Modification du comportement.

Face à toutes ces propositions il faut envisager une modification du comportement des personnes en définissant des procédures pour l 'utilisation des équipements. En effet dans le paragraphe II-5, il à été montré comment divers problèmes rencontrés ont influés sur le comportement des médecins, il s'agit souvent de réactions instinctives et prévisibles .
Il serait intéressant de mener une étude pour évaluer les conséquences, visibles ou prévisibles, de l'informatisation sur le comportement du médecin.

IV . 5 - Méthodologie

Nous constatons que chaque tâche est indépendante et contribue à une plus grande sécurisation du système. C'est l'Union et elle seule qui décidera du ou des modules à mettre en œuvre ainsi que de l'ordre et des dates de leur réalisation.

En effet la mise en œuvre d'un système d'information sécurisé peut s'apparenter à un jeu de construction. Il s'agit de mettre en œuvre différents modules dont chacun contribuera à une meilleure protection du système. Chaque module doit rester indépendant , sa mise en œuvre et son contenu dépendront de la politique de sécurité définie par la structure. En conséquence les investissements nécessaires à la sécurisation d'un système dépendent du niveau de sécurité que l 'on désire atteindre.

Conclusion

Ce travail montre comment l'introduction de nouvelles technologies peut fragiliser un système d'information . Dans le cas particulier du milieu médical, la sécurisation du système devient un enjeu stratégique, dans la mesure ou les informations concernées ont un caractère confidentiel et sont protégées par la loi.

Les solutions à mettre en œuvre ne peuvent s'articuler autour du seul équipement informatique ni se résumer à la mise en place d'outils spécifiques qui limitent les accès aux machines et aux données. Elles doivent aussi prendre en compte les aspects humains et organisationnels du système.

Mais au delà d'une réponse au problème spécifique de sécurité des médecins de la région , ce travail pose un grand nombre de questions mettant en lumière plusieurs pistes de recherche en matière de sécurité des systèmes d'information.

Il s'agit de définir la notion de sécurité même. Comment évaluer le niveau de sécurité d'un système ? Peut-on définir des critères suffisamment précis et fiables à partir desquels il serait possible de déduire la vulnérabilité d'un système ? Ces critères sont-ils applicables à toutes les organisations ?

Il faut aussi aborder la phase d'étude. Comment faire un audit de sécurité ? Peut-on modéliser un audit adapté aux problématiques de la sécurité ? Quels critères étudier ? Pour quelles organisations ?

Le travail fait pour l'Union peut-il se transposer aux médecins des autres régions voire même à d'autres secteurs d'activité? Peut-on s'appuyer sur les méthodes de conception de systèmes existantes ou doit-on définir une méthode spécifique pour la conception de systèmes sécurisés ? Quel doit-être le contenu d'un cahier des charges pour la sécurité ?

Un dernier axe peut s'intéresser à la prévision du risque : Peut-on anticiper les risques et évaluer une politique de sécurité ? Les critères pour l 'évaluation de la sécurité évoqués précédemment sont-ils utilisables ici ? Sous quelles conditions et dans quelles limites ? Peut-on introduire la notion de qualité au niveau des solutions ou au niveau du système ?

Il apparaît clairement que la recherche de solutions efficaces aux problématiques de sécurité de l'information fait appel à des processus complexes et concerne des disciplines transverses telles que la technologie informatique, les sciences humaines , les sciences de gestion et de la communication.

Dans les mois à venir les membres de l'équipe s'attacheront à explorer différentes voies parmi celles évoquées.

Références bibliographiques

- **ALBERT A., ROGER-FRANCE F.H., DEGOULET P. ET FIESCHI M**.(1998), *SANTE ET RESEAUX INFORMATIQUES* , VOLUME 10

- **ALLAERTA F.A,B, DUSSERRE C, QUANTIN C.** (1999) *EVOLUTION DU CADRE JURIDIQUE DE L'INFORMATISATION DU CABINET MEDICAL* , A CEN BIOTECH, DIJON

- **ANDERSON R.** (1996) *SECURITE DANS LES SYSTEMES MEDICAUX INFORMATISES*
- COMPUTER LABORATORY, UNIVERSITY OF CAMBRIDGE

- **DUBOIS O.** (1997) *RECOMMANDATIONS DU CONSEIL NATIONAL DE L'ORDRE DES MEDECINS, CONCERNANT LA DEMARCHE D'INFORMATISATION DU DOSSIER MEDICAL*
- CONSEIL NATIONAL DE L'ORDRE DES MEDECINS

- **DUCROT H.** (1996) *LE DOSSIER MEDICAL INFORMATISE FACE A LA LOI FRANÇAISE* , BIAM, BOULOGNE

- **DUSSERRE L., GOLDBERG M. ET SALAMON R** .(1996) *INFORMATION MEDICALE :ASPECTS DEONTOLOGIQUES, JURIDIQUESET DE SANTE PUBLIQUE* SPRINGER-VERLAG , PARIS

- **FORMMEL** (2000) *„APPORT DE L'INFORMATIQUE DANS LA PRATIQUE MEDICALE,* FORMMEL N° 26 , FRANCE

- **FRACHET B.** (2002) , *NOTES POUR BIEN CHOISIR SON LOGICIEL INFORMATIQUE* , SFORL, FRANCE

- **HUYNH F.** , **ALLOUET J.M.** (2001*), LA SENSIBILISATION DES COLLABORATEURS A LA SECURITE DES INFORMATIONS* , ARTHUR ANDERSEN , FRANCE

- **LE BEUX P.** (2001) *INFORMATIQUE MEDICALE ET TECHNOLOGIES DE COMMUNICATION* LABORATOIRE INFORMATIQUE MEDICALE, FRANCE

- **MASKENS A. ET GEBOERS J.** (1998*) L'EVOLUTION DU SYSTEME GEHR POUR LES RESEAUX INFORMATIQUES DE SANTE,* HEALTH DATA MANAGEMENT PARTNERS , BRUXELLES

- **NETIZEN** (1995) *LE SECRET MEDICAL A LA MERCI DU SCSSI* NGROUPS : FR.NETWORK.DIVERS, FR.COMP.INFOSYSTEMES ...

- **QUANTIN C.** (1997) *SECURITE DES INFORMATIONS MEDICALES* ,ACTUALITES CANCEROLOGIQUES , CENTRE G.F. LECLERC, FRANCE

- **VENOT A.** (1997) *INTELLIGENCE COLLECTIVE ET SYSTEME D'INFORMATION DE SANTE*, SPRINGER-VERLAG , PARIS

- **VERLYNDE P.** (2001) *L'ACCES AU DOSSIER MEDICAL*, ORDRE DES MEDECINS

Partenariat interfirmes et securité des systèmes d'informations

Prémisses d'une réflexion

Abdelmalik Kaiel
Doctorant en Sciences de gestion
sous la direction de Damien Bruté de Rémur
6, rue des Jonquilles
34430 St Jean de Védas

a.kiel@tiscali.fr
Tél : 04.67.42.26.07

Résumé :

La course à la sécurisation des systèmes d'informations a poussé les entreprises à se méfier encore plus de leurs concurrents. Cependant, cet article pose la question de savoir si, dans ce secteur bien particulier, il est possible de former des « partenariats sécurité » ou « parsecs » invitant des firmes concurrentes à partager des informations liées à la sécurité de leurs systèmes d'informations et relatives à leur environnement commun (menaces potentielles, définition de nouveaux virus, partage de connaissances inhérentes aux systèmes de protection…). Mais dans quel but ?

Le partage d'informations peut théoriquement aider chaque firme à mieux protéger ses frontières de sorte que chacune contribue à la protection du secteur. Cependant, il reste encore à définir quels types d'informations méritent d'être partagés ; car s'il est vrai que la coopération implique que tous les membres fonctionnent comme une seule entité, il ne faut néanmoins pas oublier de préciser que la cellule se divise lorsqu'il s'agit de réaliser des affaires !

Mots clés : Sécurité de l'information, Partenariat interfirmes, Stratégie d'entreprise, Intelligence économique.

Abstract :

Running after information systems security has lead firms to pay much more attention to their competitors. However, in this article, we try to know if, in this particular economic sector, it is possible to create "security partnerships" or "parsecs" which invite competitors to share information about their information systems and their common environment (potential menaces, new virus definitions, knowledge share about security...). But what is the goal ?

Sharing information can theoretically help each firm to better protect their boundaries so that each of them contribute to protect the economic sector. However, the types of information to be shared must be defined. If it is true that cooperation means that all the members work as a unique entity, we must not forget to mention that this entity is dividing when the business must be done !

Key words : Infosecurity, Partnership between firms, Firm strategy, Economic intelligence.

Introduction

Les valeurs acquises par les entreprises sont la plupart du temps représentées par de l'information, qu'elle soit technologique (confidentialité de l'innovation comme condition importante du maintien de la force compétitive des entreprises), stratégique (informations sur l'environnement, les concurrents…), ou empirique (études, essais, réseaux de relations, savoir faire divers...). Aujourd'hui, les firmes comprennent de mieux en mieux que l'information accroît sa valeur par le partage ou plus particulièrement par le travail en réseau qui permet d'appuyer leurs projets et leurs actions sur la coopération. En effet, *« la puissance communicationnelle d'un réseau numérique est dans son potentiel : il permet la construction d'un nouvel espace d'intermédiations qui positionne autrement les acteurs, inter-acteurs »*[28]. C'est dans l'action que se dévoile sa complexité car il autorise la prolifération des situations de communications. *« Générateur d'intermédiations »*, le réseau numérique qui est à la fois média de diffusion et média interactif, permet d'organiser la coopération sur des complémentarités efficientes, transforme les mécanismes de diffusion et dynamise les modes de réception (interactivité).

On comprend bien dans ce cas que la performance de cette forme de coopération dépend fortement de la gestion de l'information[29] : répartition, temps de circulation, traitement et mise à disposition, toutes tâches qui demandent un système d'information performant. Cependant, *« plus on veut un système efficace, et plus on prend de risques*. *Le risque est celui de la dimension du réseau, de la « chaîne » et de la fragilité de son maillon le plus faible »* [Bruté de Rémur, 2001]. Ce risque concerne donc directement la sécurité de l'entreprise qui s'inscrit dans un nouveau dilemme à savoir dynamiser son système d'information tout en le sécurisant au maximum.

Ce modeste essai a pour but de proposer une alternative originale qui puisse aider les firmes à satisfaire ce double objectif. Ainsi, puisque « l'union fait la force », la coopération interfirmes s'annonce comme une option attractive. Encore faut-il déterminer dans quelle mesure ; ce choix n'ayant pas été validé scientifiquement, en tout cas dans le domaine de l'infosec, nous nous proposerons seulement d'identifier les apports potentiels d'une telle forme de partenariat.

La sécurité : un problème plus humain que technique

Les firmes qui souhaitent sécuriser leur SI le font dans le but de pouvoir utiliser les réseaux en toute sûreté. Au moindre problème, les firmes attribuent ce phénomène à une déficience du réseau. Pourtant, le réseau est conçu pour que de l'information y circule. Comment lui reprocherait-on de faire ce pour quoi il a été conçu ? La sécurité est donc bel et bien un problème humain avant d'être un problème technologique ; ce sont les individus qui contournent les fonctions du réseau pour « espionner le voisin ». Par conséquent, ce qui sous-tend du « toujours plus de technologie » revendiqué par les responsables, c'est qu'ils estiment ainsi plus aisé de changer de technologie que de changer le comportement de l'individu. Or, force est de constater que quelque soit le degré de technicité de la technique, l'individu reste à même d'en exploiter les failles.

« Depuis que la technologie règne dans les entreprises, ces dernières tendent à graviter autour du type d'information « auquel la technique leur donne le plus facilement accès »[30], c'est-à-dire les données automatisées plutôt que l'information proprement dite, car ces données sont rarement converties en information ou en connaissance. On comprend donc aisément que la technologie n'est pas le secret d'une information de qualité, mais qu'il est nécessaire de se recentrer sur le facteur humain comme précédemment cité. Or, la plupart des chefs d'entreprise ne connaissent pas la nature de la relation entre les individus et l'information, le type d'information nécessaire aux différentes personnes au sein de l'entreprise, comment amener les salariés à se mettre d'accord sur la signification d'une information donnée, ou encore ce qui incite les individus à partager ou, au contraire, à stocker l'information.

En pratique, les entreprises disposent à la fois d'informations et de connaissances, mais elles ont quelques difficultés à faire la distinction entre les deux. *« La connaissance, c'est de l'information qui prend du sens dans un certain contexte »*[31]. Représenter la connaissance, c'est donc représenter cette information avec le ou les sens qui lui sont attachés et le ou les contextes dans lesquels ses sens peuvent être compris ». L'objectif d'une coopération interfirmes dans ce domaine qu'est la sécurité des SI est bel et bien de partager es informations et non pas des connaissances ; il appartiendra ensuite à chaque membre de transformer les informations récoltées en connaissances utilisables. En effet, ce qu'une firme x

[28] **Broche M.**, *Les technologies de l'information et de la communication bousculent-elles vraiment les organisations ?, Actes 5ème colloque du CRIC (Nice 6-7 décembre 2001).*

[29] **Lesca H. et E.**, *Gestion de l'information, qualité de l'information et performances de l'entreprise, Litec, 1995*.

[30] **Davenport T. H.**, Privilégier l'information sur la technologie, Les Echos 01/10/1999.

[31] **Ermine J.L.**, *Capter et créer le capital savoir, Réalités Industrielles, Annales de l'Ecole des Mines, Novembre 1998, pp 82-86*.

considère comme une connaissance n'en est pas systématiquement une au regard d'une firme y.

« Dès lors que l'on intègre la connaissance au centre des valeurs stratégiques de l'entreprise, il convient de s'interroger sur la valeur réelle de la connaissance en particulier et de l'information en général », et de *« prendre en compte* [non seulement] *la valeur intrinsèque* [de cette dernière] *mais surtout sa valeur extrinsèque »*. En effet, *« la prise en compte de la certitude est dépassée par la potentialité de l'hypothèse »*[32]. On s'intéresse autant si ce n'est plus à ce qui risque de se produire qu'à ce qui s'est déjà produit. Ainsi, si deux faits isolés sont appréhendés séparément, alors nous nous trouvons confrontés à deux informations distinctes. Mais si l'on relie ces deux évènements de manière à en déduire un troisième avec certitude, alors ce dernier sera une connaissance qui permettra par exemple d'anticiper un fait. Cette *« posture mentale »* est un gage de compétitivité qui traduit l'état d'esprit des firmes dans lequel *« la recherche et l'interprétation des signaux faibles deviennent un corollaire indispensable à un mode d'action basé sur la conception d'une manœuvre économique »*.

Le problème des entreprises est donc de reconnaître ces informations qu'elles soient réparties en son sein ou chez ses partenaires proches, et de les exploiter intelligemment, tout en sachant les distinguer des *« manœuvres de désinformation exécutées par leurs concurrents »*. Lourde tâche en effet, qui nécessite à la fois des moyens financiers conséquents et des compétences de veille hors paires. Une des alternatives possibles envisagée par cet article est de permettre à un ensemble de firmes de collaborer pour se répartir les fonctions de « veille sécuritaire ». En réalisant ainsi une dichotomie de leur environnement commun et en partageant leurs résultats, elles seront à même de l'appréhender plus facilement. Utopie ? Nous allons tenter de prouver à travers ce modeste essai qu'il n'en est rien !

Coopérer pour mieux sécuriser ?

Pour accéder à des informations importantes à l'extérieur, il est nécessaire pour la firme d'ouvrir son système d'information (SI) et donc de prendre des risques et de s'exposer. Ainsi, la pérennité de l'entreprise sera assurée au prix de son ouverture. Et cela implique une démarche incontournable en termes de sécurité de l'information car *« c'est en cherchant à perfectionner la gestion de l'information, par les nouvelles technologies, par le développement des échanges et des réseaux comme par la recherche et le traitement du maximum d'informations que l'entreprise commence à prendre des risques sérieux »*[33].

C'est pourquoi les entreprises d'aujourd'hui sont amenées à se faire concurrence et à coopérer tout à la fois. Coopérer, c'est gagner ensemble et comprendre les rapports de concurrence autrement qu'en termes d'affrontements. Cette nouvelle conception du « concurrent-partenaire » risque de remettre en question les stéréotypes traditionnels qui font école en la matière. Cependant, il n'est pas évident de vivre « intelligemment » une situation de concurrence mais cela s'applique également à la coopération. En effet, l'approche « gagnant-gagnant » qui encourage les firmes à s'engager sur cette voie n'est plus vérifiée lors de la négociation à l'issue de laquelle l'une gagne plus que l'autre. Il arrive donc que la coopération dérive en stratégie de contrôle conduisant la firme la plus importante à « aliéner » son partenaire. C'est pourquoi il sera difficile pour des concurrents de se vivre en partenaires capables de combiner leurs efforts et leurs moyens, sans pour autant négliger leurs intérêts et d'accepter, pour le plus faible, d'y « perdre au change ».

Pourtant une troisième voie est ouverte aux firmes informatiques indécises face au dilemme « faire ensemble » plutôt que « faire seul ou faire contre ». Il s'agit de concilier compétition et coopération : ce que Ray Noorda, fondateur de Novell, a formalisé sous le terme de « coopétition ».

Ainsi, de plus en plus d'entreprises informatiques se lancent dans des coopérations leur permettant d'être plus compétitives. Plutôt que de s'affronter à l'autre, on utilise sa force ; plutôt que de vouloir « tuer l'ennemi », on s'associe à lui temporairement. S'associer pour développer un marché, en fonder un nouveau, ou se liguer contre un ennemi commun est, en effet, une pratique dont le développement s'est accentué ces dernières années. Comme le disait le *Wall Street Journal* en *1995: « Co-Branding is not recent, but it has bloomed anew...»* (Le partenariat n'est pas récent, mais il s'est totalement régénéré). Ainsi, Marco Landi, ancien directeur général d'Apple, déclarait lors de la signature d'accords avec « l'ennemi » Microsoft : « *Dans ce monde, il n'est pas possible d'être seulement des concurrents. Il faut comprendre que l'un de nos rivaux d'hier peut être aujourd'hui notre meilleur associé ... ».*

La voie de la coopétition *« s'inscrit donc bien dans une stratégie de contrôle intelligente fondée sur une recherche de puissance mesurée dans un réel esprit de partage qui préserve des libertés d'action et augmente logiquement les chances mutuelles de profit (financier comme relationnel) »*. C'est donc sur cette forme toute particulière d'interaction que repose le concept de parsec par lequel une entreprise tente essentiellement d'obtenir que le partenaire réalise tout

[32] **Harbulot C.**, *Frappes informationnelles contre les entreprises : l'offensif prime sur le défensif, http://www.strategic-road.com/intellig/infostrategie/pub/frappes_informationnelles_txt.htm*.

[33] **Bruté De Rémur D**., Un nouveau champ de recherche : La Sécurité de l'Information, Une illustration du concept de « champ sécant », Actes 5ème colloque du CRIC (Nice 6-7 décembre 2001).

ce qui sera en son pouvoir pour la soutenir, en cas d'agression par un tiers. Le parsec ou partenariat interfirmes en matière de sécurité des systèmes d'information se définit comme l'espace dans lequel les entreprises peuvent partager les informations qu'elles détiennent sur leur « environnement agressif » respectif. Il ne s'agit donc pas ici de dévoiler des informations déterminant la stratégie d'une firme et qui, si elles venaient à être dévoilées, risqueraient de mettre en péril sa compétitivité et sa position stratégique sur le marché. En effet, nous comprenons bien que même si ces firmes collaborent pour élaborer une base de données en temps réel, interactive et commune, elles demeurent néanmoins concurrentes puisqu'elles se positionnent et coexistent sur un marché commun. Par conséquent, la question se complique dès lors qu'on souhaite amener plusieurs firmes à coopérer car cette coopération ne sera effective et efficace que si les intérêts de chaque participant sont représentés, demeurent saufs et plus encore, s'accroissent.

Ainsi, dans le cas qui nous préoccupe, une firme n'adhèrera au parsec que si cela lui permet d'améliorer le niveau de sécurité de son système d'information (SI). Mais son engagement sous-entend en contrepartie qu'elle participe à la vie du parsec et lui fasse profiter de ses compétences. D'un autre côté, les autres membres du parsec n'accepteront son adhésion que s'ils y voient la perspective d'un apport conséquent. Nous constatons donc que la constitution d'un parsec repose sur une double acceptation : l'acceptation du parsec par la firme candidate et de cette dernière par le parsec lui-même.

Une approche en terme de cadres

Il s'agit de raisonner en terme de cadre général englobant toutes les firmes appartenant au système coopératif, sans omettre les « micro-cadres » qui correspondent aux évolutions respectives de chaque firmes ou autrement dit, de chaque partie du nouveau système car les caractéristiques individuelles demeurent importantes, ainsi que leurs relations, leurs variations historiques et leurs échanges spécifiques avec l'environnement. Ces systèmes peuvent coopérer s'ils *« entrent en résonances, et par leurs couplages forment des assemblages harmonieux »*[34]. Ces couplages et ces assemblages varient en fonction de leurs caractéristiques propres et des relations qu'ils entretiennent avec un environnement changeant.

On comprend aussi, que si ces systèmes souhaitent former des « assemblages harmonieux », il est préférable que les caractéristiques individuelles propres à chaque « sous-système » ne soient pas à l'opposé l'une de l'autre. En effet, il est difficile de concevoir un « assemblage harmonieux » résultant d'une coopération en matière de sécurisation des systèmes d'information entre un géant informatique et une ferme du Poitou ! Les alliances interfirmes se comprennent par une volonté commune de partager des savoirs relativement à des projets et des besoins communs dans un domaine de compétences partagé, comme c'est le cas dans le sujet qui nous intéresse. On en déduit donc que ce type de partenariat ne fonctionnera efficacement que s'il se composent de firmes intervenant sur un secteur d'activité identique et par conséquent directement ou indirectement concurrentes. En effet, la pertinence des informations varie selon le secteur d'activité auquel on se rattache ; on n'imagine donc mal une coopération efficiente si elle se confronte à l'incompatibilité structurelle et sectorielle des firmes qui la composent.

Quels types d'informations partager ?

Reste encore à définir quel type d'information mérite d'être partagé ou plus exactement il est possible et crédible de partager. Il est évident que seules les informations sensibles méritent d'être protégées ; il n'est donc pas nécessaire de protéger la totalité du patrimoine informationnel de la firme. Reste à identifier, dans le méandre des données qui transitent par l'entreprise lesquelles méritent de l'être. La sensibilité d'une information peut être définie en fonction de son degré de pertinence par rapport à la stratégie d'une entreprise. Si cette information est déterminante ou autrement dit « stratégique », alors elle méritera d'être protégée. Si son dévoilement risque de mettre en péril la position stratégique de la firme sur son marché, elle sera dite sensible. On distinguera deux types d'informations dites sensibles transitant dans et par l'entreprise :

- *les informations relatives à la firme elle-même* : ce sont toutes les informations qui concernent la firme, sa structure, ses activités, sa stratégie… Elles ne représentent pas la totalité du patrimoine informationnel d'une firme étant donné que ce dernier se compose d'informations non sensibles qui ne risquent pas de nuire à l'entreprise si elles venaient à être dévoilées.

- *les informations relatives à l'environnement « agressif »* : qui traduit la dimension spatio-temporelle dans laquelle se multiplient toutes les actions susceptibles de représenter une menace potentielle pour le système d'information d'une firme. Cela comprend aussi bien les menaces dites « privées » (hack teams…) que les menaces dites « concurrentielles » résultant de l'espionnage industriel (firmes concurrentes, Etats…).

Les informations de deuxième type participe à la protection des premières. En effet, une information détenue sur l'activité subversive d'un acteur _ (tentative d'intrusion, espionnage…) est primordiale pour permettre à une firme d'identifier à la fois un agresseur éventuel et les données auxquelles il s'intéresse, afin d'être en mesure d'éradiquer la

[34] **Côté C.**, *La Systémique et l'intervention, historique de la Systémique 1920-1998, L'approche systémique en santé mentale, Presses de l'Université de Montréal et Fidès, 1999, p 17.*

menace à temps. On peut finalement reformuler ces deux types d'informations en distinguant les informations sur l'intérieur (informations internes) susceptibles d'intéresser l'extérieur, des informations sur l'extérieur aidant à la protection de l'intérieur. Cette distinction nous permet de comprendre la firme comme un système à la fois ouvert et fermé : ouvert sur l'extérieur via ses capacités de communication et d'« écoute » ; fermé car le système, délimité par des frontières qui le distinguent des autres systèmes, agit pour ses propres intérêts. Autrement dit, l'entreprise est un système ouvert, dans ses échanges avec l'environnement, et fermé, pour maintenir son identité et son autonomie.

Le bon fonctionnement du parsec est relatif aux modes de relations adoptés par les différents acteurs du système qui utilisent les informations reçues de l'environnement en autant qu'elles correspondent *« à ce qu'ils estiment acceptable, recevable, et utilisable »*, c'est-à-dire adaptable à la structure du système, pour procéder à des changements. Il est nécessaire que ce changement corresponde à ce que le système soit à ce moment. Un changement trop brusque laisserait les acteurs « sur le carreau » ; à l'inverse, un changement trop lent démotiverait les acteurs et pourrait susciter leur envie de quitter le système pour un autre, plus ouvert au changement. C'est pourquoi, si les dites règles internes sont souples et ouvertes, le changement se fait harmonieusement, facilement et avec cohérence; si elles sont rigides et fermées, le changement se fait difficilement et avec tensions. Par conséquent, sécuriser le système d'information d'une firme correspond bien à un changement dans le cadre. Cependant, dans une optique de partenariat interfirmes, on assistera à la fois à un changement dans le cadre inhérent à chaque partenaire, mais également à un changement de cadre (entreprise - groupe d'entreprises). Ce système fonctionne donc grâce à un niveau élevé d'échanges d'informations[35]. On en déduit par conséquent, qu'une altération ou une dégradation (volontaire ou non) de cet échange d'informations conduirait à mettre en péril ce système. L'importance de la communication interpreunariale ayant été soulignée, il s'agit d'appréhender la coopération *« sous l'angle interactionniste de la communication ce qui constitue un axe fondamental de recherche »*.

Comme une chaîne, la force d'un système de sécurité informationnelle est égale à celle de son plus faible maillon[36]. Par conséquent, chaque firme a intérêt à soutenir son partenaire afin qu'il ne s'affaiblisse pas et qu'il n'entraîne pas le reste du parsec dans sa chute.

Prémisses d'une modélisation

Ce qui nous intéresse ici, c'est ce que la l'alliance interfirmes peut apporter en terme d'amélioration de la sécurisation des systèmes d'information, et de lutte contre le piratage et dans quelle mesure elle permettrait d'identifier plus rapidement leur(s) auteur(s). La coopération est perçue ici comme un moyen de communiquer plus vite les informations non pas en accélérant le débit de transfert des données via un intranet mais tout simplement en partageant les informations « détenues » par chaque firme avec ses partenaires au lieu de les conserver dans ses archives confidentielles. Tout simplement car une information acquise par une firme x et qui lui semble inutile ou inexploitable pourra être utile à une firme y ou servir à une firme z. Ainsi, dans un partenariat xyz, l'information d'origine x circulera plus vite vers y et z plutôt que si ces deux derniers tentaient de la trouver par leur propres moyens.

Si aujourd'hui, ce type de partenariat émerge à peine, c'est parce que les entreprises du secteur ont longtemps raisonner sous l'adage « un prêté pour un rendu » ; autrement dit, si la firme x souhaitait obtenir une information sur son concurrent y, il lui fallait donner en échange une information sur elle-même. Ce phénomène étant toujours d'actualité, il représente un frein majeur à l'élaboration de politiques de sécurité efficaces, étant donnée que certaines firmes sont tentées d'obtenir des informations sur leurs concurrents par le biais de l'espionnage industriel pour ne pas avoir à « se livrer » en retour. Ces firmes peu scrupuleuses ont recours à la politique du miroir sans teint qui permet à la victime de voir son agresseur sans être vue par lui à la différence qu'ici l'agresseur se trouve du mauvais côté du miroir en épiant son concurrent sans que ce dernier émette le moindre soupçon. Le parsec, en tant qu'alliance stratégique, peut présenter une alternative intéressante pour se prémunir du regard indiscret de ses concurrents et éviter de recourir soi-même à cette pratique.

Il est difficile d'établir une définition unique de l'alliance stratégique à partir des connaissances actuelles. Pour la majorité des spécialises en stratégie, le qualificatif "stratégique" n'intervient que pour caractériser une *« association entre plusieurs entreprises concurrentes[37] »*. Cependant, certains chercheurs considèrent que *« lorsque les activités, les métiers ou les compétences concernées par la coopération viennent de concurrents, la coopération est qualifiée d'alliance. L'adjectif "stratégique" lui est habituellement adjoint lorsque l'alliance doit aboutir à un nouvel avantage concurrentiel partagé[38] »*. Ainsi, *"l'existence d'une dimension stratégique"*

[35] **Boss P., Doherty W., Larossa R., Schumm W. et Steinmetz S.**, *Sourcebook of Family Theories and methods, A contextual Approach, New-York, Plenum Press, 1993, p 328-330.*

[36] **Cohen, F. B**., (1995), Protection and security on the Information Superhighway, John Wiley & Sons, inc., New York, 301 p.

[37] **Dussauge P. et Garrette B.**, *Alliances stratégiques mode d'emploi , Revue Française de Gestion, 1991, p 4.*

[38] **Nalleau G.,Vasseur J.**, *Deux modèles d'alliance gagnants, L'Expansion Management Review, 1998, p 74.*

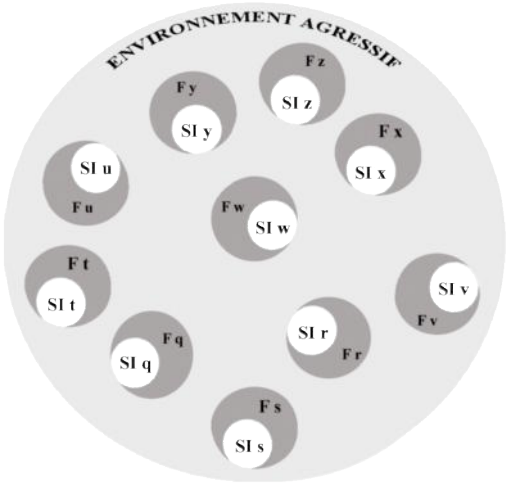
représente-t-elle la dimension fondamentale de ce type d'accord[39].

La difficulté majeure relative à la mise en œuvre d'une telle alliance réside dans le fait que les alliés sont davantage préparés à gérer leurs propres structures que celles qui les unissent à un concurrent[40]. En effet, *« l'entreprise est par nature une entité* [autonome] *qui est capable de fonctionner par elle-même »*[41]. Ainsi, doit-elle apprendre à gérer une situation paradoxale : travailler avec un concurrent [Dussauge et Garrette, 1991]. Il est possible de confier la responsabilité de l'alliance à l'un des partenaires, mais responsabilité ne veut pas dire contrôle[42] ; celui-ci étant partagé par les différents membres du parsec. La relation avec les concurrents doit faire l'objet d'une attention particulière ; toute entorse à l'accord peut conduire à la perte de la confiance que les parties se portent et aboutir à sa rupture.

Le changement de cadre s'avère être une solution possible pour permettre aux firmes de coopérer en matière de sécurité des systèmes d'information. En effet, en élargissant le cadre d'analyse ce qui se traduit sur le terrain par le regroupement de firmes prêtes à collaborer, la frontière avec l'environnement extérieur devient plus grande, et par conséquent l'alliance bénéficie d'un poids beaucoup plus important. En effet, les entreprises partenaires fonctionnent dans notre exemple comme une seule firme. Rappelons qu'il ne s'agit ici que de coopérer en matière de sécurité, les activités commerciales, productives… propres demeurant sous le contrôle de chaque firme (même s'il n'est pas exclu que ces firmes coopèrent à la fois sur le plan de la sécurité et forment en même temps un partenariat stratégique ou de savoir-faire). Par conséquent, alors qu'auparavant, les firmes se préoccupaient de protéger leurs frontières respectives, elles ne surveilleront désormais que le segment de frontière qui les rattache à l'environnement agressif commun (par exemple, la firme x ne se préoccupera que de la zone aa'b'b (Schéma 2) alors qu'auparavant (Schéma 1) il lui fallait « sur-veiller » l'environnement agressif dans sa totalité. On comprend dès lors, que les menaces d'intrusion qui occupent l'espace grisâtre ont été contenues autour de la frontière commune abcdefghij. Ce type de partenariat a permis de structurer l'environnement de manière à identifier beaucoup plus facilement les menaces d'intrusion ; chaque firme (ou sous-système) protégeant une partie du système coopératif abcdefghij. En se partageant « le travail » chaque firme peut ainsi réduire sérieusement son niveau de menaces.

Schéma 1 : Un partenariat traditionnel
(dans lequel chaque firme est appréhendée indépendamment de l'autre)

Laissons maintenant l'aspect stratégique de côté pour nous focaliser sur le contenu communicationnel. De ce point de vue, on remarque très nettement une amélioration entre les deux étapes. Tout d'abord, les firmes fonctionnent désormais comme une seule firme, chaque sous-système pouvant être assimiler à



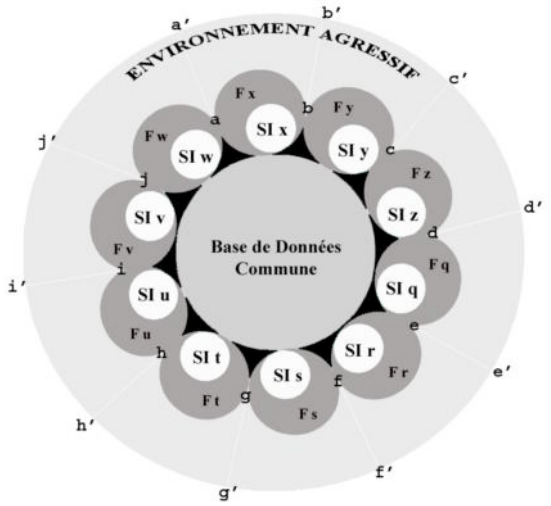
un département comme on trouve un département Marketing, Relations publiques, G.R.H… dans une entreprise classique. Par conséquent, la communication est évidemment beaucoup plus facile entre les divers départements d'une même firme qu'entre firmes concurrentes. Nous n'omettons pas ici que tous les firmes composant le parsec sont effectivement concurrentes l'une de l'autre, mais nous nous intéressons ici au système d'un point de vue communicationnel. De ce point de vue, les firmes sont des partenaires et le fait qu'elles puissent communiquer entre elles à la manière d'une seule entreprise limite très nettement les risques de désinformation inhérents à ce secteur. En effet, une information captée par la firme x dans la zone aa'b'b'pourra être immédiatement partagée avec tous ses partenaires par le biais d'une base de données « sécurité » commune. Ainsi, la firme z pourra profiter de l'information captée par la firme x, alors qu'il lui aurait fallu, dans un schéma traditionnel, attendre que l'information qui se trouve dans la zone aa'b'b, se déplace jusqu'à la zone cc'd'd pour être en mesure de l'exploiter. Nous constatons donc qu'une collaboration « interpreunariale » en matière de communication des données sensibles à un moment donné, peut nettement améliorer le niveau de protection du SI de chaque membre du parsec,

[39] **Urban S. et Vendimini S.**, Alliances stratégiques coopératives européennes, Ed. DeBoeck, 1994.
[40] **Balantzian G.**, *L'avantage coopératif, Les Editions d'Organisation, 1997.*
[41] **Chauzal C.**, *Discours des dirigeants et alliances stratégiques, Actes 5ème colloque du cric (Nice 6-7 décembre 2001).*
[42] **Ohmae K.**, *Pourquoi les alliances échouent-t-elles ?, Harvard L'Expansion, n°56, 1990, p 74.*

prévenir contre d'éventuelles attaques et « guérir » des dégâts potentiels.

Cependant, on pourrait penser qu'une pénétration de la frontière abcdefghij menacerait toutes les firmes partenaires et mettrait en péril le système dans sa globalité alors qu'auparavant une seule firme en aurait payé le prix. En réalité, les systèmes d'information individuels demeurent avec une protection propre à chaque firme ; une sorte de frontière dans la frontière. Par conséquent, les partenaires sont toujours des firmes à part entière, avec leur propre structure, leur administration… leur SI propre. Ainsi, si jamais quelqu'un parvient à franchir la frontière abcdefghij, le ou les membres affectés en premier n'auront qu'à se « déconnecter » de la base de données commune qui elle seule relie toutes les firmes entre elles. Ainsi, le parsec continuera de fonctionner à n-1 ou n-m membres. Prenons un exemple ; si un pirate parvient à infiltrer le SI de la firme x via la frontière ab, alors certes la firme x sera en situation de danger potentiel, mais pas ces partenaires puisque la menace ne se limite qu'aux limites de la firme x, celle-ci s'étant déconnecté du système. Si ce pirate souhaite ensuite infiltrer la firme z, il lui faudra pénétrer le système de protection propre à la firme z qui se déconnectera aussitôt du système pour ne pas que la menace s'étende au parsec tout entier.

Schéma 2 : L'émergence du parsec
(après recadrage ; les partenaires fonctionnent désormais comme une seule entité)



Dans ce scénario, le seul risque est que la menace se propage si rapidement qu'elle parvienne jusqu'à la base de données commune. Là en effet, toutes les firmes seraient directement exposées au danger ; l'ultime échappatoire serait alors que toutes les firmes se déconnectent de la base de données commune. Mais il faudrait, pour que l'intrus parvienne à infiltrer cette base de données commune que la firme exposée ne s'en soit volontairement pas déconnectée.

On imagine donc que si une telle chose arrivait, les firmes décident d'un commun accord de suspendre momentanément les accès à la base de données commune puisque si cette dernière était effectivement « contaminée », le virus pourrait se transmettre d'une firme à l'autre dès que l'une d'entre elle la consulterait.

Conclusion

L'aspect communicationnel du problème qui nous occupe est primordial, car il s'agit de comprendre comment l'information relative à une menace potentielle, identifiée et détenue par la firme x, parvient aux différents partenaires. Par ailleurs, si la firme x est sujette à une menace d'intrusion, on peut imaginer que ses canaux de transmission de données numériques (intranet, Internet) le soient aussi. C'est pourquoi, la firme x doit faire preuve de vigilance, si elle veut diffuser cette information à ses partenaires sans que le pirate ne puisse capter l'information au passage. Nous ne faisons ici que soumettre une hypothèse sans avoir la prétention de proposer une technologie de substitution adéquate, ceci étant la préoccupation des centres de R&D.

Ainsi, chacune des entreprises impliquées a un rôle majeur à jouer dans la *« gestion des flux de communication interne sur l'alliance »*[43]. La coopération est alors perçue comme un moyen de cacher ses faiblesses et répond donc momentanément à un problème momentané. Chaque membre de l'alliance doit pouvoir trouver dans celle-ci les intérêts et avantages auxquels il aspire. L'un des membres ne doit pas dominer l'autre, aucune des parties ne doit se sentir lésée.

Cependant, il est évident que notre réflexion n'en est qu'à ses débuts, ces hypothèses n'ayant pas encore été vérifiées dans la réalité. De plus, puisque le parsec propose que chaque partenaire réalise tout ce qui sera en son pouvoir pour soutenir un des « siens » en cas d'agression par un tiers, il reste encore à déterminer comment ce soutien pourrait se matérialiser.

[43] **Chauzal C.**, *Discours des dirigeants et alliances stratégiques, Actes 5ème colloque du CRIC (Nice 6-7 décembre 2001).*

Bibliographie

- Balantzian G., *L'avantage coopératif, Les Editions d'Organisation, 1997*.

- Boss P., Doherty W., Larossa R., Schumm W. et Steinmetz S., *Sourcebook of Family Theories and methods, A contextual Approach, New-York, Plenum Press, 1993, p 328-330*.

- Broche M., Les technologies de l'information et de la communication bousculent-elles vraiment les organisations ?, Actes 5ème colloque du cric (Nice 6-7 décembre 2001).

- Bruté De Rémur D., *Un nouveau champ de recherche : La Sécurité de l'Information, Une illustration du concept de « champ sécant », Actes 5ème colloque du CRIC (Nice 6-7 décembre 2001).*

- Chauzal C., *Discours des dirigeants et alliances stratégiques, Actes 5ème colloque du cric (Nice 6-7 décembre 2001).*

- Côté C., *La Systémique et l'intervention, historique de la Systémique 1920-1998, L'approche systémique en santé mentale, Presses de l'Université de Montréal et Fidès, 1999, p 17.*

- Cross S., directeur du *Software Engineering Institute*, Université Carnegie Mellon, devant le Congrès américain, 23 février 2000.

- Davenport T. H., *Privilégier l'information sur la technologie, Les Echos 01/10/1999.*

- Dussauge P. et Garrette B., *Alliances stratégiques mode d'emploi, Revue Française de Gestion, 1991, p 4.*

- Ermine J.L., *Capter et créer le capital savoir, Réalités Industrielles, Annales de l'Ecole des Mines, Novembre 1998, pp 82-86*.

- Harbulot C., *Frappes informationnelles contre les entreprises : l'offensif prime sur le défensif, http://www.strategic-road.com/intellig/infostrategie/pub/ frappes_informationnelles_txt.htm*.

- Lesca H. et E., *Gestion de l'information, qualité de l'information et performances de l'entreprise, Litec, 1995*.

- Nalleau G.,Vasseur J., *Deux modèles d'alliance gagnants, L'Expansion Management Review, 1998, p 74.*

- Ohmae K., *Pourquoi les alliances échouent-t-elle ?, Harvard L'Expansion, n°56, 1990, p 74.*

- Urban S. et Vendimini S., Alliances stratégiques coopératives européennes, Ed. DeBoeck, 1994.

La prise en compte des émotions peut trouver une place dans la planification stratégique de la sécurité d'un système d'information ?

Dimitri Zalonis zalonis@yahoo.fr
DEA en science et technologie de l`information et de communication et médiation des connaissances, université de Montpellier I

Résumé : L'émotionnel a été induit dans le monde économique. Bien que son utilité peut être facilement comprise dans l'objectif de la vente des biens et des services, ce n'est pas le cas pour la gestion des systèmes à risque. L'émotion a été approchée en tant qu'un mécanisme adaptatif de réponse d'un organisme à son environnement. Il s'agit d'essayer de montrer en quoi la prise en compte des émotions peut être bénéfique pour la sécurité d'un système d'information. Pour cela on se base sur le lien entre la sécurité et le système d'information et on réalise une introspection des émotions de l'organisation d'abord comme une variable stratégique et ensuite comme un outil de gestion de l'organisation.

Mots clés : émotions, sécurité, système d'information, résonance, performance, risque, organisation.

Abstract: The emotional factor was inducted in the economic world. It's utility in order to sell goods and services can be easily understood contrary to its vital role for risk management. We approached emotion as an organism's response to its environment. It's an effort to make clear how beneficial the consideration of emotions could be for prevailing security in an information system. Therefore, we focus on the bond between security and information system. We first make an introspection of organisational emotions as a strategic factor and then as the key instrument for organisational management.

Keywords: emotions, security, information system, resonance, performance, risk, organisation.

Introduction.

Pendant longtemps la théorie économique était fondée sur le modèle néoclassique qui voulait l'organisation comme une boîte noire. Henderson et Quandt ont, plus tard (1967), défini l'organisation par son objectif principal. Ainsi l'entreprise est donc définie par sa fonction essentielle, son métier, la production des biens et des services. L'abandon de l'analytique et le développement de la systémique ont induit March et Simon de proposer un organisationnel basé sur le comportement. Morin a approfondi et a développé ses idées en s'investissant sur le potentiel de gérer « la logique collective ».

Toutes les théories économiques pendant plusieurs années ont voulu l'homme et son comportement, baptisé irrationnel, comme un handicap à l'optimisation des processus et à la validité des modèles proposés. Les émotions ou les actes qui en découlent ont souvent été placés au cœur de cette conduite nuisible, qui mettait en péril le résultat des organisations. L'homme est la cause dominante des événements accidentels (au sens large du terme).

Ceci car le rationnel a graduellement été imposé au mode de vie occidental. Pourtant les modèles ont touché leurs limites. Argyris et Schön se renvoient à un mécanisme psychosociologique qui régit l'organisation. On se demande si les émotions sont une cause c'est-à-dire un symptôme de nuisance (et donc il faudra les éliminer) ou font elles partie structurel du système (et donc trouver les moyens pour les optimiser) ?

Le développement des technologies d'information et de communication a propulsé le poids des services dans le système économique. La valeur matérielle des produits se sacrifie à la perception donc le client fait allusion. L'émotionnel a été impliqué dans le monde économique. Bien que l'utilité de la notion des émotions peut être facilement comprise pour la vente des biens et des services ce n'est pas le cas pour la gestion interne.

Mais en quoi les émotions peuvent être utiles pour l'organisation ? Afin de répondre à cette question on doit d'abord se demander en quoi, primitivement, les émotions sont-elles utiles ? Scherer décrit l'émotion comme un mécanisme adaptatif de réponse d'un organisme à son environnement[44].

Si on synthétise les différentes études menées en psychologie on voit qu'elles ont montré que l'émotion servait les fonctions suivantes : (a) l'évaluation de l'environnement, (b) l'adaptation de l'organisme, (c) la planification des actions à mener , (d)l'exécution, (e) la communication des réactions et des intentions ,(f)le besoin de fournir une action optimale à la situation perçue et (g) la prise de conscience de l'expérience émotionnelle elle-même (mémorisation)[45].

En comparant ces actions à celles menées par les différents responsables de sécurité, on voit qu'il s'agit de procédés banals et rationnels. L'évolution des technologies d'information et de communication a radicalement modifié la conception non seulement des produits et des services, mais du monde. Doit-on donc apprendre à adopter cette action naturelle et mener une politique de sécurité inspirée par celle qui inclura en plus les émotions ressenties par les membres de l'entreprise ?

La restructuration du modèle économique, autrement dit le passage de l'économie à la net – économie, nous a poussé à introduire la notion de la crise. Comment gérer une situation délicate? De quelle manière doit-on parler aux personnes impliquées et gérer leurs émotions, les représentations ? Goleman et Boyatzis essayent de traiter ces questions et introduisent la notion d'intelligence émotionnelle dans les lieux de travail.

Dans la première partie on met en rapport les notions de la sécurité et du système d'information. Au fil du temps les différents systèmes vivants arrivent à s'adapter à l'environnement et à dominer les dangers qui les menacent. Mais pour réussir dans ce combat continu, il faut mettre en place des mécanismes plus ou moins élaborés qui seront stratégiquement capables d'y faire face.

La deuxième partie s'intéresse à l'analyse des éventuelles possibilités de gérance des émotions. On les place à l'épicentre du plan stratégique. On réalise une introspection des émotions de l'organisation d'abord comme une variable stratégique et ensuite comme un outil de gérance de l'organisation.

Avant tout on doit comprendre les règles qui régissent l'environnement de l'objet observé, même si cela parait difficile.

[44] Scherer, K. R.(1984a). On the nature and function of emotion: A component process approach. In K. R. Scherer & P. Ekman (Eds), *Approaches to emotion*. Hillsdale, NJ: Lawrence Erlbaum Associates Inc, pp. 293-317.

[45] Pascal Richard Pierre Edwards, Etude empirique de déterminants de la différenciation des émotions et de leur intensité, thèse présentée à la Faculté de Psychologie et des Sciences de l'Education de l'Université de Genève, 1988.

I. La complexité de la sécurité du système d'information.

A ce stade on essaie de montrer que la protection d'un sous–système, en référence au système d'information, est délicate quand le dernier fait partie d'un sous–système ouvert, et donc doté de complexité.

L'âge de l'organisation indique sa résistance et ses capacités d'adaptation. Elle témoigne alors d'un processus évolutif qui peut nous mener à penser à une forme d'intelligence.

A. La sécurité est un indice d'intelligence pour l'organisation.

Cette partie évalue le système de sécurité en tant qu'une piste d'apprentissage organisationnel. Elle aboutit finalement à le considérer comme un indice d'intelligence.

La sécurité est une mission primordiale pour les organismes. Dès l'apparition des premiers groupements on a remarqué la formation de mécanismes de défense plus ou moins élaborés. Le premier mécanisme est la mémoire, l'expérience[46]. On constate que les caractéristiques souvent attribuées à l'intelligence en référence l'anticipation, l'adaptation et la synthèse[47], ont permis aux organismes de se développer[48] pour s'intégrer dans un environnement hostile. Ainsi on est arrivé au point de différencier les organisations selon leur degré de sécurisation. Une organisation est intelligente si elle arrive à anticiper et à contrôler son environnement. L'enjeu est important et les variables chaotiques. Contrairement à certains stratèges qui pensent que la stratégie est une tâche continue dans les organisations en fonction de leur taille[49];

Il s'agit d'une procédure d'apprentissage informelle et intuitive[50]. Mais on n'en reste pas là. On pense ainsi à la maîtrise des événements (réactions) qui se produisent au sein de l'organisation. Les derniers composent un bruit à la performance et donc un obstacle de caractère opérationnel[51]. Autrement, une organisation est intelligente si elle dispose des mécanismes qui lui permettront de capter et analyser les signaux émis, endogènes ou/et exogènes[52]. Car de cette manière, elle permet d'évaluer les éventuels risques et de planifier les actions nécessaires pour y faire face.

Un grand nombre d'opérations a été investi sur la capture des signaux différents afin de constituer d'importantes bases de données. Ces investissements ont contribué à la production des opérations de contrôle à caractère massif[53]. Cependant ces données ne sont pas toujours traitées de manière optimale. On constate une fragmentation au niveau de l'ampleur : on n'arrive pas à inclure des facteurs qui sont *a posteriori* importants et la plupart du temps non quantifiables. Parfois ces données sont trop riches et le temps de raffinage devient pénalisant au niveau stratégique. Finalement je mentionne la surqualification des données transmises[54]. On peut trouver plusieurs raisons à cela mais la nature du problème est indiscutablement stratégique.

Le caractéristique de la sécurité c'est qu'elle n'est pas une science exacte[55]. Si elle l'était, il n'y aurait pas d'*accidents*. On ne peut pas éliminer le risque, mais on peut le diminuer et le maîtriser.

On a montré que la sécurité est un processus inné. Il consiste à mettre en place un procédé adaptatif capable de contrarier les attaques provenant de l'environnement hostile pour protéger l'organisation.

Ensuite on s'intéresse au système d'information car dans notre regard il s'agit du centre opérationnel de l'organisation.

B. Le système d'information est pluridimensionnel.

Afin de pouvoir estimer l'enjeu on met en valeur le caractère polyvalent du système d'information.

Un système d'information est constitué de technologies, d'organisation et de gestion[56]. Tous ses

[46] Aristote, Métaphysique A, 1.
[47] Hachette multimédia, mesure de l'intelligence et étude des activités mentales.
[48] Aristote, Les parties des animaux, § 10, 687 b, éd. Les Belles Lettres, trad. P. Louis, pp. 136-137.
[49] M. Porter: « …la planification stratégique se produit rarement de façon spontanée tout particulièrement dans les organisations de grande taille. La planification formelle donnait la discipline permettant de s`arrêter de façon occasionnelle pour penser à des questions stratégiques », Choix stratégiques et concurrence : technique d`analyse des secteurs et de la concurrence dans l`industrie, Paris, Economica, 1987.
[50] Grandeur et décadence de la planification stratégique, Henry Mintzberg, Dunod, 1994, page 277.
[51] Stratégie et sociologie de l`entreprise, Claude Michaud et Jean-Claude Thoenig, Village Mondial, 2001, page 130.
[52] J. Piatrat : « un système intelligent doit et peut observer son propre comportement », an intelligent system must and can observe its own behavior, afcet, 1991, pages 337.
[53] Echelon, projet américain installé à l`U.K.
[54] Grandeur et décadence de la planification stratégique, Henry Mintzberg, dunod, 1994, page 270.
[55] Manager la sécurité, Alain Martinez - Fortun, ed. INSEP consulting, 2001, page 7.
[56] Les systèmes d`information de gestion, Kenneth C. Laudon et jane P. Laudon, Pearson Education, 2000, page 12.

éléments contribuent également à la procédure de développement stratégique de l'organisation[57]. Dans tous les systèmes on peut définir la variance et le coefficient de corrélation. Ainsi la sécurité en tant que système dispose un degré de dépendance des facteurs qui varient selon les cas. Mais, les règles d'entropie contribuent fortement à la fluctuation des variables. L'intelligence permet au système de réduire l'entropie par le biais de la croissance de l'information. De telle manière on se trouve en face de la restructuration du système qui se manifeste par la complexification[58].

On distingue deux grandes familles d'approche des systèmes d'information modernes : les approches techniques et les approches comportementales[59]. Les premières s'orientent vers l'analyse des phénomènes dans la perspective d'apporter des solutions techniques. Quant aux autres, elles s'orientent vers le changement d'aptitudes qui découle de la mise en place et l'utilisation des systèmes d'information. Plutôt anthropocentriques, elles ne négligent pas la technologie[60].

Pourtant, jusqu'à maintenant, le coût élevé des investissements matériels a poussé les organismes à surévaluer les performances des machines[61]. L'éventuel gain de ses investissement techniques dépendra des capacités et des performances des salariés qui utiliseront cette technologie. Face à ce défi, le poids stratégique s'est orienté vers la relation homme–machine. Le facteur humain est un facteur qualifié à risque et par conséquence les compétences des agents sont mises en question[62].

Les solutions techniques ont permis une baisse considérable des accidents et du coût opérationnel[63]. Néanmoins, les dépenses liées à la sécurité du système d'information ne cessent d'augmenter. L'environnement du travail devient de plus en plus complexe en incitant une augmentation marginale d'investissement. Pourtant la gestion de la sécurité contrairement aux autres systèmes est corrélée à la gestion[64].

Le chiffre d'affaire pour la sécurité de l'information en Europe est estimé à cinq milliards de dollars. Les budgets annuels des entreprises consacrent progressivement une partie plus importante au SI. Par ailleurs, des études menées en France ont montré la prise de conscience de l'importance du système d'information par les directions générales. L'essor stratégique du système d'information a été évalué. Le directeur du système d'information voit la revalorisation de sa mission. « Il est responsable de tout et de rien »[65]. Sa mission polyvalente est étroitement liée à l'évolution de l'organisation[66]. Pourtant la singularité architecturale des systèmes opérants est flagrante. Celui-ci se manifeste par l'écart constaté entre l'importance et les possibilités d'évolution attribuées par les DG et les DSI. [67]

Dans un contexte ou le capital de l'organisation s'oriente du matériel vers l'immatériel, l'enjeu de la protection de l'information devient majeur. La numérisation de la vie oblige tous les partenaires du système à s'y adapter. Le travail se métamorphose en révélant le facteur humain[68]. Les salariés sont des travailleurs de la connaissance dont la productivité consiste à la vulgarisation de l'information. Le travail est fortement spécialisé et la productivité dépend de la coordination de l'équipe dont ils font partie.[69] L'entreprise devient un domaine psychothérapique[70]. Les dangers prennent d'autres formes, plus complexes.

Jusqu'à maintenant on a fait le rapport entre le système d'information et la sécurité. Par confrontation de ces notions deux autres concepts sont ressortis : l'intelligence et la pluridimensionnalité.

On a montré que la nature polyvalente du système d'information nécessite un surcroît d'effort en métier de sécurité. Mais aussi on note que plus l'organisation est sécurisée plus elle est intelligente et donc pluridimensionnelle.

Dans la deuxième partie on s'intéresse aux intérêts stratégiques que l'organisation peut tirer par la gestion des émotions.

---

[57] Political Issues in the Use of Cryptography, Petri Puhakainen, Department of Computer Science and Engineering, Helsinki University of Technology, December 4th, 1998.

[58] Passage des résolutions linéaires aux résolutions jacobéen.

[59] Laudon et Laudon., 2000, page 15.

[33] The computers package: dynamic complexity in computers and politics, rob kling and William H. Dutton, Columbia university press, 1982.

[61] The real problem with computers, Michael Schrage, Harvard Business Review, 1/9/97.

[62] La conduite de systèmes à risques, René Amalberti, PUF, 1996, page 25.

[63] Notamment en matière militaire, le transport du personnel, de la logistique.

[64] Alain Martinez – Fortun 2001.

[65] 01 Informatique, 8/11/2002.

[66] Hubert d`Erceville, Le bon DSI est d`abord un opérateur du changement, 01 Informatique, 29/11/02.

[67] Le monde informatique, Le DSI en quête de sens stratégique, n°962, 6/12/2002.

[68] Joanna Pomian et Claude Roche, Connaissance capitale, L'Harmattan 2002.

[69] Peter Drucker, The age of Social Transformation, in the Atlantic monthly, November 1994.

[70] Pierre Hurstel, L`entreprise réparatrice ou le nouvel épanouissement, ed Maxima, 2002.

II. La gestion des émotions: un objectif stratégique.

La problématique présentée lors de cette deuxième partie est d'étudier la faisabilité de la gestion des émotions. Peut-on instaurer des indices et des outils, qui seront par la suite mis à la disposition des différents organismes dans le but de permettre la gestion du climat émotionnel ?

La question à laquelle cette partie s'intéresse est de voir d'abord s'il est possible de gérer les émotions et ensuite comment on pourrait l'envisager.

On va montrer que les émotions ont un coté pragmatique qui les rend gérables.

A. Les émotions ne sont pas abstraites, sont précises et donc maîtrisables.

Les analyses des psychologues ne prenaient pas en compte les sentiments. Les behavioristes considèrent que seul le comportement des objets peut être observé, contextualisé et analysé. D'autre part, les sciences cognitives sont orientées vers les ordinateurs pour analyser divers phénomènes. Les systèmes artificiels ont été mis au point pour analyser les habitudes des humains mais finalement elles sont limitées à des observations qu'on peut qualifier comme des statistiques. Des études menées sur le cerveau humain ont montré que les réactions sentimentales jouent un rôle primordial. Même si leur poids par rapport à l'intellectuel n'est pas plus important, elles constituent un élément primordial. Le défi qu'on peut lancer à un système d'information est de voir s'il est capable de sentir les événements pour accélérer les opérations adéquates.

« L'homme est le miroir de l'univers dans lequel il vit …»[71]. Bien que l'intellect et les émotions soient deux fonctions différentes, elles sont étroitement liées. Toutes les deux se logent dans un système global, le cerveau. En situation de crise les centres émotionnels réquisitionnent la procédure de fonctionnement du cerveau. L'explication de cette action est normative. Tout l'intellect est bâti sur la primitive qui utilise largement l'émotionnel.

Les études psychiatriques ont montré que l'intellectuel n'est pas influencé par le psychique[72]. Le cerveau des objets est capable de saisir des données et les traiter. Les informations sont ensuite stockées dans la mémoire. On constate l'indépendance entre la capacité de collecte des informations et l'équilibre psychique. « Cette réalité neurologique sépare clairement ces compétences des capacités purement cognitives comme l'intelligence, le savoir technique ou l'expérience professionnelle ».

Bien sûr la maîtrise des émotions demande la combinaison d'éléments très divers. Par conséquent on doit insister sur la mise en place de synergies qui vont permettre d'aboutir à un objectif qui n'est autre que l'autocontrôle.

Ensuite on parlera des bases du mode de gestion des émotions. La difficulté à détecter les vibrations de l'organisation manifeste le manque de médiatisation; c'est une difficulté à laquelle il faudrait remédier.

B. La gestion de résonance.

Dans cette partie on décrit les opérations et on repère les éléments d'analyse adéquate.

La réussite d'une stratégie dépend non seulement de la planification et de la mobilisation des équipes mais, de la manière dont elle se réalisera. Autrement dit, il s'agit de la façon de commander: est-ce qu'il y a un impact émotionnel capable d'aligner les objectifs du projet avec ceux des participants ? S'inspire-t-il d'optimisme, de motivation, d'implication, de confiance ou d'orientation ?

Le défi est de conduire les émotions collectives dans une direction positive et d'éliminer la partie des émotions négatives[73]. Quand on favorise la restauration d'un climat émotionnellement positif, c'est à dire éclore le meilleur de chacun, il s'agit de la résonance. Au contraire, quand la partie négative est favorisée on parle de dissonance. De cette façon « on ébranle les fondations émotionnelles de l'implication, et donc de la performance individuelle»[74].

Afin de canaliser les émotions de l'organisation vers la direction voulue, les compétences d'organisation en terme d'intelligence émotionnelle sont déployées. D'une part la gestion de ses propres émotions, on parle donc d'intelligence intrapersonnelle et d'autre part leurs relations avec autrui, on parle alors d'intelligence interpersonnelle.

L'équilibre émotionnel n'est pas une mission facile. Car il s'agit d'un système ouvert en interaction. Les individus sont en contact continu. Ce frottement peut être catalytique car il peut rassurer ou émettre un signal d'alarme mais il peut aussitôt déstabiliser et endormir le système de défense.

---

[71] Newell et Simon, 1972.

[72] Antonio Damsio, university of Iowa College of Medecine, communication personnelle; Reuven Bar-On, entretien sur des données préliminaires collectées avec Antoine Bechara et Daniel Tranel.

[73] Pierre Livet, émotions et rationalité morale, PUF, 2002, page 145.

[74] Goleman,Boyatzis et McKee, 2002.

«Plus les individus sont en résonance les uns avec les autres, moins leurs interactions sont statiques. La résonance minimise le bruit dans le système. Ce qui soude les individus dans une équipe, et qui les implique dans une entreprise, ce sont les émotions qu'ils éprouvent.[75]»

Conclusion.

A partir du sous-système imbriqué du cerveau humain on a constaté l'évolution du système cognitif. On procède de la même manière pour approcher les organisations. On a traité la question posée de façon épidermique car l'objectif n'était que d'identifier le cadre général. Il s'agissait d'étudier la possibilité d'intégrer les émotions dans les processus de gestion.

L'approche pivote entre la théorie de Shannon–Weaver et celle de Newel–Simon. Car elle essaye de grouper des éléments d'horizons considérés par le grand public comme opposés. D'un coté, on trouve les méthodes de sécurité dites classiques qui sont dans une grande partie techniques et de l'autre coté, des procédés qui mettent l'accent sur l'homme et sa façon d'apparaître dans une structure. On décline vers le courant qui veut qu'il y ait une corrélation entre la façon dont l'organisation est gérée et la création du savoir. L'enjeu stratégique de ce postulat est majeur et se manifeste d'une façon encore plus flagrante (importante) quand il s'agit de la sécurité. Autrement dit, la possibilité de la continuité de l'organisation face à un événement inattendu qui entrave le fonctionnement normal. L'opérationnel doit être assuré dans tout les cas et face à tout problème.

Pour cela on s'est intéressé à une étude qui vise les fonctionnalités psychologiques. L'opérationnalité des actions doit être plus efficace. Autrement dit, il s'agit d'étudier non la compétence mais la performance de l'organisation. Ainsi ce n'est plus mise en cause le comportement en tant qu'expression mais en tant que fonction d'expression.

Le concept d'intelligence émotionnelle constitue un outil d'approche d'un phénomène complexe non par les ressources ou les structures mais, par la relation entre la stratégie et la performance.

La planification d'un système de sécurité vise non seulement à affronter les accidents potentiels ou probables mais aussi, de rassurer l'organisation et son relationnel de sa pérennité. La sécurité est un sentiment.

Les émotions sont présentes lors des relations. Le défi consiste à capter les signaux émis. Pour cela on doit étudier les canaux qu'ils utilisent. Il ne faut donc pas négliger de vérifier les réseaux informels qui se construisent. Car ils peuvent représenter un enjeu à la délibération de la stratégie.

Comment doit-on gérer le relationnel ? La sécurité se construit par la mise en place des scénarios qui sont en partie fantastiques et en partie d'expérience. Ses scénarios sont soit de provenance externe soit interne. Dans le premier cas des experts en relation - client avec l'organisation interviennent. Dans le deuxième, les experts internes ou le personnel posent les bases. Il ne faut pas négliger que les relations sont plus fortes, le langage est commun ainsi que les représentations.

L'écart qui s'installe entre les deux types d'élaboration des scénarios doit être géré. On doit faire appel à un *mix* d'intelligence émotionnelle qui permettra d'accentuer les processus d'échange des connaissances.

Il y a un espoir dans le fait que les organisations à grand risque ont déjà mis au point des systèmes de simulation de gestion de crise qui ne prennent en compte que l'implication émotionnelle[76]. Dans ce cadre, la notion d'intelligence émotionnelle pourrait faire partie des principes du management de la qualité.

[75] B.E. Ashforth and R.H. Humphrey, emotions in the workplace: a reappraisal, human relation 48, 1995.

[76] The N.Y. Times on the web, Game Simulations for the Military to Make an Ally of Emotion, de Kathie HAFNER, 21 juin 2001.

Bibliographie.

Ouvrages :

- AMALBERTI R., La conduite de systèmes à risques, Puf, 1996.
- GOLEMAN D., BOYATZIS R. et MCKEE A., L'intelligence émotionnelle au travail, Editions Village Mondial/ Pearson Education France, 2002.
- GOLEMAN D., BOYATZIS R., MCKEE A., L'intelligence émotionnelle au travail, Editions Village Mondial/ Pearson Education France, 2002.
- GOLEMAN D., L'intelligence émotionnelle, Robert Laffont, 1995.
- LAUDON K., LAUDON J., Les systèmes d'information de gestion: Organisations et réseaux stratégiques, Editions Village Mondial/ Pearson Education France, 2001.
- LOUCHE C., Psychologie sociale des organisations, Armand Collin, 2001.
- MEINDL J-R., STUBBART C., PORAC J-F., Cognitions within and between organizations, sage, 1996.
- MICHAUD C., THOENIG J-C., Stratégie et Sociologie de l'entreprise, Editions Village Mondial/ Pearson Education France, 2001.
- MINTZBERG H., Le management, Editions d'organisation, 1999.
- MINTZBERG H., Planification stratégique, Dunod, 1994.
- MORIN P., DEVALEE E., Le manager à l'écoute du sociologue, édition d'organisation, 2002.
- NONAKA I., TAKEUSHI H., The knowledge creating company, Oxford University Press, 1995.
- PIERSON M-L., L'intelligence relationnelle, Editions d'Organisation, 1999.
- POMIAN J., ROCHE C., Connaissance capitale : Management des connaissances et organisation du travail, L'Harmattan et les éditions Sapientia, 2002.

Revues:

- Harvard Business Review, Boosting Your Emotional Intelligence, DAVID STAUFFER, October 1997.
- Harvard Business Review, V-S. DRUSKAT, S-B.WOLFF, Building the Emotional Intelligence of Groups, Mar 2001.
- Harvard Business Review: Le knowledge management, Editions d'organisation, 1999.
- La Documentation Française, Management et organisation des entreprises, Cahiers français nº 287, juillet septembre 1998.
- Sloan Management Review 3, S.GOSHAL, C.BARTLETT, P.MORAN, A new manifest for management, 1999.
- Sloan Management Review 3, C.KIM, R.MAUBORGNE, Strategy value innovation and the knowledge economy, 1999.

Ouvrages collectifs:

- Le business émotionnel, questions des dirigeants, Editions Village Mondial/ Pearson Education France, 2001.
- Science de l'information et de la communication, Larousse, 1993.

Quelques ouvrages récents

Voici une sélection des derniers ouvrages non techniques parus dans le domaine de la sécurité (Années 2002-2003). Chaque numéro des cahiers intègrera les derniers ouvrages parus depuis, ainsi qu'une sélection bibliographique plus ancienne concernant le domaine.

SOCIOLOGIE DE LA SECURITE
Auteur : Collectif
janvier 2003
Editeur : Armand Colin
Collection : SOCIOLOGIES AU QUOTIDIEN
Prix éditeur : 13,50 euros / 88,55 FRF
ISBN : 2200262833 - EAN13 : 9782200262839

LA SECURITE EN ENTREPRISE - SENSIBILISATION DES PERSONNELS ET MISE EN OEUVRE D'UN PLAN D'ACTION
Auteurs : Chaboud / Jean-Pierre Mouton
janvier 2003
Editeur : Dunod
Prix éditeur : 25,00 euros / 163,99 FRF
ISBN : 2100064525 - EAN13 : 9782100064526

THEORIES DE LA SECURITE (1ère EDITION)
Auteurs : J-J Roche / CH-P. David
décembre 2002
Editeur : L.G.D.J Montchrestien
Prix éditeur : 11,00 euros / 72,16 FRF
ISBN : 2707613355 - EAN13 : 9782707613356 - Nombre de pages : 160

LA SECURITE INFORMATIQUE
Auteur : J. Claviez
octobre 2002
Editeur : JCI INC.
Prix éditeur : 24,00 euros / 157,43 FRF
ISBN : 2921599805 - EAN13 : 9782921599801

COMPRENDRE ET GERER LES RISQUES
Auteur : Moreau
juillet 2002
Editeur : Editions d'Organisation
Prix éditeur : 38,00 euros / 249,26 FRF
ISBN : 2708127845 - EAN13 : 9782708127845

SOLUTIONS DE SECURITE INFORMATIQUE
Auteur : LOINTIER
juin 2002
Editeur : Dunod
Prix éditeur : 38,00 euros / 249,26 FRF
ISBN : 2100051563 - EAN13 : 9782100051564

SECURITE INFORMATIQUE - RISQUES, STRATEGIES ET SOLUTIONS
Auteur : Didier Godart
février 2002
Editeur : EDITIONS DE LA CHAMBRE DE COMMERCE ET D'INDUSTRIE DE LIEGE
Prix éditeur : 36,00 euros / 236,14 FRF
ISBN : 2930287217 - EAN13 : 9782930287218 - Nombre de pages : 334.

LES POLITIQUES DE SECURITE ET PREVENTION
Auteur : Dominique Duprez
janvier 2002
Editeur : GEORG
Genre : SCIENCE POLITIQUE
Prix éditeur : 18,29 euros / 119,97 FRF
ISBN : 2825707651 - EAN13 : 9782825707654

LA SOCIETE DU RISQUE
Auteur : Ulrich Beck
Editeur : Aubier
Collection : ALTO
Prix éditeur : 21,50 euros / 141,03 FRF

MANAGER LA SECURITE - UNE VOLONTE, UNE CULTURE, DES METHODES
novembre 2001
Auteur : ALAIN MARTINEZ-FORTUN
Editeur : Insep
Prix éditeur : 27,00 euros / 177,11 FRF
ISBN : 2914006101 - EAN13 : 9782914006101