2000s-02

Risques à grande échelle dans les systèmes en réseau : quelques interrogations

Erwann Michel-Kerjan

Série Scientifique
Scientific Series

CIRANO
Centre interuniversitaire de recherche
en analyse des organisations

Montréal
Janvier 2000

CIRANO

Le CIRANO est un organisme sans but lucratif constitué en vertu de la Loi des compagnies du Québec. Le financement de son infrastructure et de ses activités de recherche provient des cotisations de ses organisations-membres, d'une subvention d'infrastructure du ministère de la Recherche, de la Science et de la Technologie, de même que des subventions et mandats obtenus par ses équipes de recherche.

CIRANO is a private non-profit organization incorporated under the Québec Companies Act. Its infrastructure and research activities are funded through fees paid by member organizations, an infrastructure grant from the Ministère de la Recherche, de la Science et de la Technologie, and grants and research mandates obtained by its research teams.

Les organisations-partenaires / The Partner Organizations

- •École des Hautes Études Commerciales
- •École Polytechnique
- •Université Concordia
- •Université de Montréal
- •Université du Québec à Montréal
- •Université Laval
- •Université McGill
- •MEQ
- •MRST
- •Alcan Aluminium Ltée
- •Banque Nationale du Canada
- •Banque Royale du Canada
- •Bell Québec
- •Développement des ressources humaines Canada (DRHC)
- •Fédération des caisses populaires Desjardins de Montréal et de l'Ouest-du-Québec
- •Hydro-Québec
- •Imasco
- •Industrie Canada
- •Raymond Chabot Grant Thornton
- •Téléglobe Canada
- •Ville de Montréal

ISSN 1198-8177

Risques à grande échelle dans les sytèmes en réseau : quelques interrogations[*]

Erwann Michel-Kerjan[†]

Résumé / Abstract

La mise en connexion de réseaux complexes s'est accélérée au cours des dernières années de manière spectaculaire. Certains des avantages de cette utilisation grandissante sont bien connus et étudiés par la théorie économique (économie d'échelle de l'offre et de la demande et effet de club). Cependant, cette interconnexion a créé de nouveaux types de risques dont l'échelle des conséquences potentielles a elle-même évolué dans des proportions impensables quelques années auparavant. Cette note met en lumière de manière introductive quelques-uns des principaux risques en question dans une problématique théorique reposant sur des cas concrets. Le plus souvent, le réseau œuvre comme un moyen physique de propagation du sinistre qui atteint alors un nombre plus grand de victimes, plus rapidement, et de manière ubiquitaire. Ces spécificités sont dues principalement à la dépendance au réseau et à l'interdépendance entre les réseaux. La gestion de tels risques apparaît d'autant plus complexe que ces risques sont émergents dans leur forme actuelle.

During the last few years, the connection of complex networks has accelerated in a spectacular manner. Some of the advantages of this increasing use are well-known and are studied by theoretical works (network externalities). Nevertheless, this interconnection has created new types of risks where the potential consequences have themselves evolved into proportions that were unthinkable a few years ago. This note deals with the principle risks of interconnection using a theoretical and empirical approach. By examining concrete cases, we suggest that technological complexity may permit

[*] Adresse de l'auteur : Erwann Michel-Kerjan, CIRANO, 2020 rue University, 25[e] étage, Montréal, Qc, Canada H3A 2A5 Tél. : (514) 985-4000 Fax : (514) 985-4039 courriel : erwannmk@poly.polytechnique.fr
Je tiens à remercier Marcel Boyer, Dominique Henriet, Claude Henry, Patrick Lagadec, Nathalie de Marcellis, et Bernard Sinclair-Desgagné pour leurs commentaires et pour les nombreux échanges que nous avons eus sur le sujet. Ce cahier pose le cadre général de questionnements récents abordés par mes travaux de doctorat, et s'inscrit dans le cadre de recherches sur les risques à grande échelle, les ruptures, et sur la gestion de crise, recherches menées au CIRANO au sein du *Groupe Risques technologiques* dirigés par Bernard Sinclair-Desgagné et au Laboratoire d'économétrie (Ecole Polytechnique de Paris) au sein du *Groupe Engelberg* dirigé par Patrick Lagadec. Une version antérieure a été présentée lors d'un séminaire donné en juin dernier à Montréal. Cette note s'adresse à un large public, aussi est-elle volontairement non formalisée. Une approche mathématique modélisant certains des phénomènes économiques discutés ici fera l'objet de notes ultérieures. Ce travail a bénéficié du soutien de la *Fondation du Prix du Forum Engelberg* et de la *Compagnie Suisse de Réassurances*. Il est simultanément publié en France : E. Michel-Kerjan (1999), « Risques à Grande Echelle dans les Systèmes en Réseau », *Cahier du Laboratoire d'Econométrie de l'Ecole Polytechnique*, No 505, Paris.

[†] Université de la Méditerranée, GREQAM, Marseille, École Polytechnique, Laboratoire d'économétrie, Paris et CIRANO

vulnerabilities by allowing dependencies and interdependencies between networks to go unrecognized until a major failure occurs. Once a major failure takes place, the network reacts as a catalyst creating catastrophic consequences. The management of such risks appears even more complicated than these emerging risks in their actual form.

Mots Clés : Risque à grande échelle, catastrophe, réseaux, infrastructure, interdépendancee, vulnérabilité

Keywords: Large-scale risk, catastrophe, networks, infrastructure, interdependancy, vulnerability

Tempête climatique de janvier 98 au Canada : effondrement de réseaux en cascade.

Du 5 au 8 janvier 1998, le Canada a connu la plus grave tempête climatique de son histoire. Par vagues successives, des pluies verglaçantes se sont abattues sur plusieurs centaines de kilomètres dans le sud du Québec, l'Ontario, et le nord des Etats-Unis. Des épaisseurs de verglas dépassant deux fois les normes de sécurité ont été relevées sur des lignes électriques qui n'ont pu résister à un tel poids. Quatre des cinq lignes principales qui alimentent Montréal ont été coupées et plus de trois millions de canadiens privés d'électricité. Plus de 130 lignes du réseau ont été détruites (3000 kms de lignes), et 1400 relais de transmission endommagés ou entièrement détruits : un réseau électrique hors d'état.

Aucun scénario de crise n'avait prévu une catastrophe de cette ampleur. Statistiquement, ce risque était considéré nul. Car la tempête de verglas de janvier 98 à Montréal n'a pas été une simple panne de grande ampleur mais l'effondrement d'un réseau tout entier. Pire encore, par un effet de cascade dans les réseaux, cela a été l'effondrement de grands réseaux critiques nécessaires au bon fonctionnement de l'activité de la région (700 communes ont été touchées), un sinistre à grande échelle :

- le réseau électrique a été mis hors d'état ;
- l'approvisionnement en eau de Montréal a été sur le point de manquer ;
- les réseaux sociaux ont été fortement sollicités ;
- le réseau politique et diplomatique a également été affecté puisque le gouvernement a du prendre en charge la situation et faire intervenir l'armée américaine. Il a également été sur le point de demander une aide logistique à la Russie.

Outre les vulnérabilités propres à chacun des réseaux, de nouvelles vulnérabilités sont apparues du fait d'une interconnexion croissante de réseaux complexes les rendant interdépendants.

Les conséquences financières ont été catastrophiques, les dégâts avoisinant les 3 milliards de dollars.

Si de l'avis de tous, la compagnie *Hydro-Québec* a répondu avec efficacité (un mois après ce sinistre à grande échelle, la plupart du réseau était en état de fonctionnement), l'implication des citoyens a également été très positive. Ces facteurs ont sans aucun doute contribué à éviter le pire.

Le Gouvernement a ordonné un retour d'expérience et confié ce travail à la « Commission scientifique et technique chargée d'analyser les événements relatifs à la tempête de verglas survenue du 5 au 9 janvier 1998 ». Sous la présidence de Roger Nicolet, qui fut également à la tête de la Commission sur les inondations dans la région de Saguenay en 1997, cette Commission a été dotée d'un budget de fonctionnement de 7 millions de dollars. Plus de soixante experts canadiens et internationaux ont participé à ce retour d'expérience dont les résultats d'analyse font partie intégrante d'un rapport final publié l'été dernier.

Le mandat de la Commission s'est articulé autour de trois axes principaux : la tempête de verglas elle-même, l'interruption des approvisionnements en électricité, et le dysfonctionnement de certaines des infrastructures de la société qui en a résulté.

«Tout au long de ce rapport, près de 500 avis, conclusions, et recommandations, ont été formulés, toujours dans la perspective que le Québec soit mieux préparé pour faire face à un prochain sinistre ».

Ils s'articulent essentiellement autour de deux thèmes :

- adoption et mise en œuvre d'une *politique québécoise de sécurité civile* comportant l'établissement d'un *système de sécurité civile* et aboutissant à l'émergence d'une véritable *culture de sécurité civile*. Une partie importante du rapport est consacrée aux réformes et initiatives que devrait véhiculer une telle politique ;
- assurer les approvisionnements en énergie et renforcer la sécurité du réseau électrique, notamment en travaillant sur la configuration générale du réseau et en améliorant les caractéristiques structurales du réseau.

Introduction

Réseaux industriels, réseaux gouvernementaux, réseaux informatiques, réseaux sociaux, ou encore réseaux d'anciens élèves ou réseaux virtuels, le terme « réseaux » est aujourd'hui employé en langue française dans de très nombreux domaines. Aborder les réseaux - ou le réseau - doit alors se faire avec la plus grande prudence.

L'origine étymologique du terme « réseau » provient de l'ancien français *réseuil*, issu du latin *retiolus*, diminutif de *retis* qui signifie le « filet ». En anglais, le mot réseau se traduit par *network* qui signifie littéralement ouvrage (*work*) en filet (*net*). Cette image originale traduit bien l'idée de maillage constituant le réseau, et construit de lignes qui se croisent en des points d'intersection appelés « nœuds » du réseau.

Qu'il s'agisse de considérations historiques, mathématiques, technologiques ou économiques, et si l'approche réticulaire demeure transversale, la signification de ce maillage souvent complexe diffère suivant les domaines étudiés.

Sur le plan mathématique par exemple, l'étude formelle de ces réseaux trouve certainement son origine dans les travaux d'Euler. L'étude de leur topologie, ou « théorie des graphes », débute avec la publication de l'article d'Euler posant le fameux problème des ponts de Königsberg (Euler, 1736). La notion de *graphe* apparaît ici pour la première fois. Puis en 1878, Clifford introduit le terme « graphe » au sens algébrique où il est encore employé aujourd'hui.

Le mot « réseau » semble quant à lui être apparu dans son sens mathématique au cours des années 1930 avec les travaux du mathématicien français Sainte-Lagüe (Parrochia, 1993). Les mots *graphe* et *réseau* sont dans un premier temps utilisés comme synonymes, avant de prendre chacun une signification spécifique[1]. De nombreux problèmes mathématiques ont ainsi impliqué l'étude des graphes et procuré des solutions utilisées encore aujourd'hui pour des questions d'ingénierie de réseaux[2].

La théorie des graphes permet en particulier de représenter les réseaux. Formellement, le réseau est alors assimilé à un graphe défini par un ensemble de sommets (représentant les nœuds du réseau réel) et une relation de connexion entre les différents sommets, symbolisée par des branches (Economides, 1996). Suivant le domaine d'application, les nœuds et les branches symbolisent les caractéristiques du réseau réel que nous voulons étudier (Economides et White, 1993). Au-delà de la théorie même dont les fondements peuvent être assez complexes, une telle représentation permet des avantages de simplicité certains.

Dans une approche technologique, le réseau est souvent apparenté à l'interconnexion d'équipements dont le but premier est d'acheminer des flux d'un point à un autre (d'un sommet à un autre du graphe représentant l'infrastructure en réseau). Ces derniers peuvent être des flux énergétiques (réseaux électriques ou gaziers), informationnels (réseaux de télécommunication), et

[1] En particulier avec la publication de *Lattice Theory* par Birkhoff en 1948, dans laquelle le terme *réseau* traduit précisément la donnée d'un « ordre partiel sur un ensemble ».

[2] Un problème bien connu est celui du déplacement du cavalier dans le jeu d'échec : compte tenu des règles de déplacement définies par le jeu, un cavalier peut-il passer par toutes les cases de l'échiquier sans passer deux fois par la même ? Il s'agit ici d'un cas très particulier d'un problème de théorie de graphes : pour un graphe donné, est-il possible de proposer un chemin passant par tous les sommets une seule fois et dont le sommet initial est également le sommet final ? La solution a notamment été proposée par Hamilton au cours du 19° siècle. Le circuit solution, ou hamiltonien, est aujourd'hui utilisé dans de nombreux travaux de recherche de configuration optimale de réseau (par exemple, compte tenu d'un nombre de nœuds et de branches donnés, quelle configuration est la moins coûteuse ?).

plus généralement des flux de matières ou de personnes (réseaux de transports ferroviaires ou aériens).

Comme le souligne Curien (1993), les questions d'agencement des différents éléments constitutifs du réseau sont au cœur de l'approche technique, entretenue notamment par les ingénieurs.

Le réseau s'entend ici essentiellement comme réseau physique, réseau des grandes infrastructures.

Dans une approche économique, la configuration matérielle du réseau importe moins. Le réseau apparaît plus comme un moyen de diffusion, de mise en relation de fournisseurs et de consommateurs de biens et services. L'économiste mène sa réflexion à un niveau plus global : les aspects techniques du réseau sont traduits par des composantes agrégées permettant plus facilement la modélisation de problèmes économiques et sans pour autant diminuer de manière trop importante le degré de pertinence de l'analyse. Le réseau apparaît ici comme un moyen de mettre en relation différents agents économiques, un moyen d'allouer des ressources. En ce sens, il conviendrait de parler d'*intermédiation* plus que d'*interconnexion* lorsque l'on travaille sur une approche économique des réseaux. Dès lors, le concept de réseau dépasse les seuls réseaux d'infrastructures pour englober également les réseaux d'activité de services (Curien, 1992).

Ayant énuméré quelques-unes des nombreuses approches des réseaux, il apparaît dans la pratique que ces différents domaines ne sont pas déconnectés. Il convient alors de garder à l'esprit que l'approche économique des réseaux interagit avec des caractéristiques techniques ou encore avec une utilisation organisationnelle du réseau (non explicitée ci-dessus).

Nous abordons dans cette note un aspect restreint des questions de réseaux : celui des grands risques liés à leur utilisation. La note est organisée en quatre sections.

Dans la première section, nous présentons certains arguments de théorie économique qui justifient l'utilisation grandissante des réseaux dans la société. En particulier, les bénéfices liés aux économies d'échelle, aux effets d'envergure ou aux effets de « club » constituent un réel avantage de l'utilisation des réseaux. Cependant, et cela compose précisément le cœur de notre travail, cette évolution ne se fait pas sans risque.

Nous présentons dans la section 2 quatre exemples de risques à grande échelle (RGE) dans les réseaux que nous analysons brièvement :

- l'arrêt du satellite de télécommunication *Galaxy IV* en 1998;
- le tremblement de terre de Kobe en 1995 ;
- les risques liés à la modernisation des systèmes d'information dans le domaine public;
- le passage à l'an 2000 : risque exceptionnel ou risque canonique?

Dans la section 3, nous tentons de dégager certaines spécificités des risques à grande échelle :

- une probabilité d'occurrence incalculable;
- un phénomène de diffusion qui conduit à une réelle ubiquité du sinistre et à une propagation extrêmement rapide de celui-ci;
- des niveaux de risques décuplés par les réseaux eux-mêmes.

Notre analyse du phénomène porte principalement sur les questions de vulnérabilité des réseaux que nous développons également la section 3 : quelles sont les principales vulnérabilités

connues ? Quelles classifications sont utilisées ? Dans quel cadre sont-elles encore pertinentes face à des risques dont la nature a profondément évolué ?

La section 4 conclut en considérant certaines pistes pour des travaux de recherche. Certains sont actuellement en cours, d'autres devraient débuter dans les mois à venir.

1- Avantages économiques de l'utilisation des réseaux

A la question *pourquoi avons-nous de plus en plus recours à l'utilisation des réseaux ?* , une approche utilisant les résultats de la théorie économique permet un éclairage significatif. Les travaux académiques sur le sujet discutent principalement de l'intérêt économique de la mise en réseau qui réside dans ce que les économistes appellent les « rendements d'échelle » et les « externalités de réseau » (Curien, 1992 ; Perrot, 1997) :

- Les *rendements d'échelle* traduisent l'idée simple suivante : à capacité totale équivalente, un gros tuyau coûte moins cher que deux petits. Une généralisation de ces rendements d'échelle pour des firmes multi-produits est également discutée sur le plan théorique[3]. Il s'agit des *économies d'envergure* qui traduisent l'idée qu'il est préférable d'avoir sur le marché « une seule entreprise si le coût associé à la production d'un vecteur de biens par cette entreprise est inférieur au coût de production du même vecteur de biens par plusieurs entreprises. On peut alors mettre en évidence des effets sur les coûts dûs, non seulement à la taille de l'entreprise, mais aussi à des complémentarités dans les productions de biens différents» (Bouttes et Haag, 1992).
- L'existence d'*externalités de réseau* traduit le fait que la valeur intrinsèque pour un individu de devenir usager d'un réseau dépend du nombre d'utilisateurs déjà présents sur le réseau. Une externalité de réseau est dite *positive* si cette valeur s'accroît avec le nombre de consommateurs ou d'utilisateurs du réseau[4].

On parle dans ce cas d'« effet de club » (Katz-Shapiro, 1985 ; Farell-Saloner, 1986).

Il y a *externalité* car l'utilité d'un agent « membre » du club (utilisateur du réseau) dépend à la fois de sa propre volonté d'appartenir au réseau, mais aussi de la décision des autres agents potentiels. Il ne contrôle pas ces décisions qui lui sont donc bien externes (Curien et Gensollen, 1992).

Plus la taille du réseau est grande, plus les membres potentiels sont attirés et plus le réseau s'agrandit, et ainsi de suite[5]. L'externalité est ici directe[6].

---

[3] Une branche de la *théorie des marchés contestables*, essentiellement développée dans les années 70, discute de ces questions. Voir en particulier Baumol, Panzar et Willig (1982).

[4] Inversement, l'externalité est dite *négative* si cette valeur décroît avec le nombre d'agents présents sur le réseau. Les effets de congestion (en particulier les embouteillages) et les pollutions constituent des cas d'externalités de réseau négatives.

[5] Cet effet d'avalanche de la demande nécessite que le réseau ait déjà atteint une taille critique à partir de laquelle le processus s'enclenche.

[6] Une recherche plus récente s'intéresse aux « effets de réseaux indirects » ou « externalités d'offre ». L'idée repose sur la possibilité des offreurs de proposer des produits complémentaires formant un bien système. L'exemple de l'ordinateur et des logiciels est le plus significatif (paradigme du hardware-software) : d'un côté la quantité et la diversité de l'offre de logiciels dépendent du nombre de personnes possédant un ordinateur, d'un autre, l'intérêt de

Les réseaux de télécommunication constituent certainement l'exemple le plus parlant d'effet de club.

Il est d'autant plus intéressant pour un agent de s'abonner à un réseau téléphonique que le réseau relie déjà un grand nombre d'abonnés.

Que l'intérêt d'un recours au réseau soit direct ou indirect, l'approche économique explique donc en partie les raisons de l'évolution actuelle vers leur utilisation grandissante.

L'interconnexion de plusieurs réseaux d'un même secteur permet aux entreprises d'accéder à de nouveaux marchés, notamment par complémentarité dans l'offre, et donc d'accroître significativement le nombre de clients de leur réseau.

L'interconnexion peut également être nécessaire pour le fonctionnement même du réseau (exemple du réseau électrique qui alimente de nombreux autres réseaux).

Ces considérations économiques conduisent à deux conclusions : d'une part, il convient de construire un réseau desservant le plus grand nombre possible d'agents (idée d'un service universel), d'autre part, et puisque la technologie le permet, l'interconnexion de réseaux déjà complexes et internationaux devrait aller croissante. L'évolution grandissante des réseaux s'effectue actuellement clairement dans ce sens.

Ainsi la théorie économique étudie-t-elle essentiellement les aspects positifs de l'utilisation des réseaux, quand les risques inhérents à cette utilisation font l'objet de beaucoup moins d'attention théorique (Liebowitz et Margolis, 1994). Il se trouve justement que de nombreux sinistres sont liés à l'utilisation des réseaux :

- **Construire un réseau avec toujours plus d'agents utilisateurs signifie également construire un réseau avec plus d'agents dépendants de ce réseau.**
- **Interconnecter des réseaux signifie tout autant augmenter l'interdépendance entre ces réseaux.**
- **L'utilisation grandissante des réseaux conduit à accroître les risques, et surtout, comme nous le discutons par la suite, conduit à des niveaux de risques décuplés.**

La suite de cette note se focalise essentiellement sur certains des risques en question. Nous présentons en particulier dans la section suivante plusieurs cas concrets en tentant de mettre en avant les risques et leurs caractéristiques liées aux réseaux.

2- Quatre exemples de risques à grande échelle

Les quatre exemples de grands risques suivants (conséquences potentielles catastrophiques) dans les réseaux sont particulièrement illustratifs à cet égard. Ils ont été choisis ici[7] pour trois raisons principales :

- l'origine du risque peut être une panne technique, un événement naturel, une malveillance (ou autre), mais aussi une combinaison de plusieurs origines;

---

l'agent d'acheter ce type d'ordinateur dépend du nombre de logiciels compatibles avec celui-ci (voir l'article de Katz-Shapiro, 1994).

[7] Notons que pour les deux exemples de sinistre, il ne s'agit pas d'approfondir le retour d'expérience, ce qui demanderait un travail d'investigation beaucoup plus long.

- la diversité de ces situations montre à quel point les applications des questions discutées dans cette note sont multiples : réseaux technologiques, réseaux d'infrastructures, réseaux virtuels ou informationnels, le plus souvent enchevêtrés entre eux;
- enfin, les deux premiers exemples se sont réalisés (arrêt d'un satellite, tremblement de terre) et permettent de soulever des interrogations (on parle alors plutôt de sinistres à grande échelle ou de catastrophes) alors que les deux exemples suivants (réseaux informationnels, an 2000) ne se sont pas réalisés (deux cas de risques).

Exemple 1 – Réseau spatial, le cas des satellites de télécommunication.

En mai 1998, le satellite de communication G*alaxy IV*[8] a subi une avarie qui l'a mis hors d'usage. Or, ce satellite permettait d'envoyer de nombreuses ondes vers le territoire des Etats-Unis. Conséquence directe : " l'incident " a paralysé une grande partie du réseau d'ondes américain. Il s'est agit d'un sinistre d'origine accidentelle et interne au réseau (ici celui du satellite).

L'éventualité d'un dysfonctionnement étant prévue, il était convenu dans ce cas de rediriger les signaux à partir d'un autre satellite, *Galaxy I*. Cette manipulation a nécessité de réorienter manuellement des centaines de milliers d'antennes en direction du nouveau satellite émetteur. Cette modification a demandé le travail de trois mille personnes à plein temps pendant toute une semaine. A cela s'est ajouté le prix même de *Galaxy IV*, 250 millions de dollars. Les conséquences directes ont été nombreuses : les 45 millions de propriétaires de bipeurs n'ont pu recevoir de message, 600 stations de radio ont arrêté leurs programmes. Les liens avec les services d'urgence n'ont été rétablis que le lendemain, ainsi les médecins, les pompiers, et autres ambulanciers n'ont plus reçu aucune information sur leurs bipeurs pendant toute la journée qui a suivi la panne.

Il convient donc de prendre la mesure de l'incident qui n'a pas occasionné de pertes humaines. Alors qu'il ne s'agit que d'un seul satellite, la dépendance au réseau apparaît clairement, avec le nœud central du réseau qui est atteint.

Les conséquences directes auraient pu devenir très lourdes si plusieurs satellites étaient tombés en panne simultanément (déconnexion du réseau) ou si la possibilité de réorienter les signaux d'un satellite défectueux vers un autre n'avait pas été effective. Dans son ensemble, la gestion de crise a été très efficace.

Quant aux pertes indirectes, il est difficile de les mesurer.

Si les experts des entreprises concernées cherchent à présenter ce cas comme extrêmement rare, le risque n'en demeure pas moins réel et même croissant avec l'envoi de satellites plus nombreux dans les années à venir notamment avec de la constellation de satellites mise en place pour le système de communication *Iridium*[9] ou encore le GPS[10].

[8] Exemple donné dans Sinclair-Desgagné (1998).

[9] Iridium est un système de télécommunication qui ne nécessite pas de relais terrestre ; les récepteurs portables Iridium peuvent donc être installés partout sur la surface de la terre, ils ne sont reliés qu'aux constellations de satellites. Le système est actuellement dans sa première phase de commercialisation.

Exemple 2 – Un réseau d'infrastructures terrestres hors d'état : le tremblement de terre de Kobe (Japon).

Les événements naturels comme les tremblements de terre ou les tornades sont à même de détruire les infrastructures de la région où ils s'abattent. Il est certainement trop tôt pour tirer des conclusions objectives des conséquences désastreuses des séismes survenus ces derniers mois en Turquie[11], en Grèce[12] et à Taiwan[13]. Nous retenons alors celui du Japon survenu il y a près de quatre ans.

Le 17 janvier 1995, un tremblement de terre a dévasté la ville de Kobe au Japon. Les pertes humaines et financières ont été catastrophiques - on a compté plus de 5 500 morts et

350 000 blessés - et les pertes financières directes se sont élevées à 150 milliards de dollars. Toutes les infrastructures terrestres ont été au moins partiellement touchées : les routes, les ponts, le port, la distribution de l'eau et celle de l'électricité. Sur neuf axes routiers principaux que comptaient Kobe, un seul est resté praticable. La voie express qui surplombe la ville (Hanshin Expressway) a été détruite et les débris ont bloqué la circulation sur bon nombre des autres rues.

L'interdépendance des réseaux s'est faite cruellement sentir. Les services d'urgence n'ont pu se coordonner (réseau de télécommunication hors d'usage), ni se déplacer (réseaux des transports hors d'usage).

Aucun plan de crise n'avait prévu une telle mise en isolement : interdépendance de réseaux qui dépendent eux-mêmes d'autres réseaux.

---

[10] Le GPS (Système de Positionnement Global) est un système de navigation permettant de localiser la position et le mouvement des avions, voitures, bateaux … équipés du système de réception GPS. Il permet ainsi aux récepteurs de se localiser. L'appareil récepteur au sol est capable de suivre un itinéraire une fois qu'on lui a indiqué la destination choisie. Elaboré aux Etats-Unis, ce système fut d'abord réservé à un usage exclusivement militaire, utilisé en particulier pendant la guerre du Golfe. Il a été commercialisé par la suite dans le domaine civil, même si son fonctionnement repose aujourd'hui encore sur un réseau de 24 satellites militaires américains. En Amérique du Nord, il est utilisé par plus de 400 000 personnes.
Les Etats-Unis ont convenu d'utiliser exclusivement le système GPS d'ici 2010. Il constituera alors l'unique système de radionavigation de leur système aéronautique et spatial (le *National Airspace System*). Cette décision n'est pas sans risque puisqu'elle revient à faire reposer un système complexe de première importance pour le pays sur une seule technologie de réseau.

[11] Le tremblement de terre qui a dévasté la Turquie le 17 août dernier laisse derrière lui un triste bilan : le chiffre officiel est de 17 000 morts, 28 000 blessés et des centaines de milliers de sans-abris au début de l'hiver. Les dégâts matériels et les pertes financières sont estimés à 20 milliards de dollars. La baie d'Izmit est en effet la région la plus peuplée et la plus industrialisée du pays (45 % du potentiel industriel du pays). C'est donc tout le pays qui a été endommagé. Deux éléments sont à souligner : une gestion de crise par l'Etat assez discutable, et une absence totale d'une gestion globale de la sécurité du réseau de construction (selon la chambre de Commerce de Turquie, 60 % des constructions y sont bâties sans permis).

[12] Le séisme a frappé le 7 septembre dernier la capitale, Athènes, qui compte 4 millions d'habitants. Il constitue le plus violent tremblement de terre qu'ait connu la ville depuis deux siècles. Bilan : une centaine de victimes et 2000 blessés. Si l'événement a paralysé une partie des infrastructures de la ville (électricité et téléphone coupés par endroits, routes impraticables), la gestion de crise organisée par le gouvernement sous la direction du Premier ministre a été jugée efficace. Selon le Premier ministre, « la Grèce dispose d'une assez grande expérience des séismes. L'action de l'Etat montre aujourd'hui que nous pouvons dépasser les difficultés ».

[13] Deux semaines plus tard, un autre séisme s'abat, sur Taiwan cette fois. Le bilan officiel est de plus de 2 300 morts et 8 200 blessés. Une fois de plus la rupture des réseaux de communication (voies d'accès, électricité, téléphone) sur l'île isole les sinistrés et empêche les secours d'intervenir. Une fois de plus, la sécurité est en question : les habitations les plus récentes qui se sont effondrées ne respectaient pas les normes en vigueur. La mobilisation des autorités a été rapide et massive.

Une partie des grands réseaux d'infrastructure a été atteinte et en cascade, les autres réseaux sont devenus inutilisables.

Le gouvernement japonais a d'abord été critiqué pour la lenteur de réaction face à un sinistre à grande échelle. Il a cependant su mettre en place une organisation de gestion de sinistre efficace qui a été reconnue par la suite. Les réseaux de télécommunication ont été restaurés les premiers. En moins d'une semaine, l'électricité a été rétablie sur l'ensemble de la ville, alors que 70 % des lignes téléphoniques ont été remises en état à la fin du mois de janvier, soit deux semaines après la catastrophe. Les secours ont pu alors mieux s'organiser, les artères principales ont été dégagées et les trois quarts de la distribution de l'eau fonctionnaient de nouveau à la fin février (Deepack, Murray, et McCormack, 1996).

Cet exemple constitue certainement un cas limite dans la destruction des infrastructures (transport, énergie, eau, communication, services gouvernementaux et autres) puisque plus rien de fonctionnait ou presque.

Nous nous trouvons devant un cas de vulnérabilité du réseau externe et d'origine accidentelle.

La rupture des grandes infrastructures est toujours spectaculaire car en quelques minutes toute l'activité est stoppée. Dans cet exemple, l'origine du sinistre est accidentelle car naturelle. De récents travaux débordent la seule origine naturelle de la catastrophe et étudient l'éventualité d'attaques intentionnelles ciblées contre les grands réseaux d'infrastructures[14].

Exemple 3 – Modernisation des systèmes d'information dans le domaine public français : le Réseau Santé Social.

Nous changeons ici de sujet d'application et nous intéressons aux risques liés à l'évolution très rapide des systèmes d'information. Il nous a en effet paru utile à ce stade de l'étude de proposer un exemple puisé dans le cadre de la modernisation de l'administration en Europe qui est au cœur de réflexions actuelles.

Alors que les exemples précédents sont des exemples de sinistres (les risques se sont effectivement réalisés), l'exemple suivant n'est qu'hypothétique. Cependant, et à l'instar du tremblement de terre de Kobe, il présente l'avantage de montrer concrètement l'interconnexion croissante des systèmes et les risques liés à cette croissance. Les vulnérabilités pourraient provenir tant de menaces accidentelles qu'intentionnelles, en interne comme en externe.

L'interconnexion des réseaux internes dans l'administration française est ancienne mais a réellement pris son ampleur avec le lancement au niveau national en 1998 du *Programme d'Action Gouvernemental pour la Société de l'Information* (PAGSI). Cette interconnexion permet des gains financiers importants, une gestion plus rapide et uniforme sur le territoire.

En France, la création du réseau santé social (RSS), qui s'inscrit dans un souci de modernisation des systèmes d'information de la santé publique, illustre pleinement le niveau des enjeux.

La modernisation du secteur sanitaire et social doit compter sur l'organisation du grand réseau santé social. Celui-ci permet de relier instantanément les divers acteurs du domaine, la télétransmission des feuilles de soins, la constitution de banques de données médicales ou encore

[14] Concernant les réflexions américaines, voir *Computer Security Issues & Trends*, vol III., (1997), Computer Security Institute et le *FBI Computer Crime and Security Survey*, (1997).

de faciliter le remboursement des prescriptions médicales, à un coût moindre et identique sur l'ensemble du territoire. Le RSS apparaît donc également un outil de rentabilité économique ou tout au moins de recherche d'efficacité dans le domaine médical.

Ce réseau, mis en place en 1998, se veut un outil de simplification administratif et relie à ce jour professionnels de santé et caisses d'assurance maladie, obligatoire ou complémentaire, services de santé relevant de l'Etat, et autres institutions professionnelles (syndicats par exemple).

En Belgique, la banque de données du système de sécurité sociale, appelée *Carrefour*, a été élaborée en 1991. L'accès à Carrefour par les différents acteurs de santé a notamment permis l'économie de 30 millions d'extraits sur papier. Le fonctionnement du courrier électronique permet aux organismes de sécurité sociale d'être informés de l'ensemble des naissances, des décès, et des changements d'adresse.

Les atouts d'une installation en réseau sont donc nombreux.

Pourtant, une telle mise en réseau d'informations sur les personnes construit également de nouveaux risques. Ces « méga » bases de données contiennent des informations sur les personnes ou les entreprises. Un individu s'infiltrant intentionnellement dans le système aurait accès à des informations relevant du secret médical et pourrait porter atteinte à la liberté des personnes.

Le Réseau Santé Social français ou le système belge Carrefour sont assez révélateurs et ne constituent qu'un exemple parmi d'autres. Il suffit de penser aux informations sur les personnes détenues par le Ministère de la Justice (gestion des établissements pénitenciers, inscription aux registres des détentions, localisation des détenus, affaires juridiques en cours, témoignages … etc.) ou par le Ministère de l'Intérieur (réseau général de transport ou programme ACROPOL[15]).

Exemple 4 – Le passage à l'an 2000 : risque exceptionnel ou risque canonique?

Au début de l'ère l'informatique, pour faire face à des contraintes économiques (coût élevé de la mémoire informatique) et techniques (taille de la mémoire limitée), les informaticiens ont programmé les dates en retenant pour l'année uniquement les deux derniers chiffres, sans tenir compte du siècle[16].

Il faut alors revoir toutes les lignes de programmes et les corriger[17]. Pour comprendre l'ampleur du phénomène, il convient d'avoir à l'esprit que plus de 90 % des programmes font appel à des données

[15] Le programme ACROPOL a été lancé en 1993 dans la région Rhône-Alpes. Il s'agit d'un réseau numérique de communications de la Police Nationale qui devra compter à terme 600 relais pour plus de 40 000 terminaux de radiocommunications couvant l'ensemble du territoire français. Le programme sera achevé en 2007. Il permettra notamment un accès aux principaux fichiers détenus par la Police Nationale à partir de terminaux mobiles utilisant des moyens avancés de cryptologie.

[16] Ainsi, l'information déterminant la date a été construite sous le modèle JJ-MM-AA. Le 1er janvier 1980 était donc codé 01-01-80. Le problème se pose alors à compter du 1er janvier 2000 qui, sous l'ancienne configuration est codé 01-01-00, donc comme une date antérieure au 31 décembre 1999 (codée 31-12-99). Si sur les nouveaux systèmes, les dates sont codées sous la forme JJ-MM-AAAA, de nombreux programmes comportent l'ancienne version.

[17] A titre indicatif, une entreprise moyenne utilise 8 000 programmes, soit 12 millions de lignes de code devant être soumises à vérification parmi lesquelles 240 000 seront corrigées. Selon le cabinet *Gartner Group*, il s'agit de plus de 225 milliards de lignes de codes à vérifier à travers le monde.

de datation[18]. Ces mêmes programmes se trouvent à l'intérieur de systèmes plus complexes qui en dépendent. C'est le cas de l'automatisation ou de l'informatique de gestion. En cela, le problème du passage à l'an 2000 -on parle du bug de l'an 2000[19]- s'apparente à un risque de réseau.

Le caractère exceptionnel du risque est effectif pour plusieurs raisons :

- conséquences potentiellement très graves sur un plan financier;
- gestion très lourde des corrections en vue passage à l'an 2000[20];
- caractère inéluctable de son occurrence;
- échéance fixée (le temps devient l'ennemi premier, c'est un compte à rebours);
- tous les types d'organisation sont touchés.

Quant au montant des conséquences économiques, il est encore plus difficile à chiffrer puisqu'elles sont elles-mêmes indéterminées. Pour certains, le *Y2K*[21] n'est qu'une construction exagérée d'un problème d'informaticiens entretenu par des cabinets de conseil peu scrupuleux et qui n'aura pas de conséquence notable.

Pour les adeptes de l'alarmisme, il faut prévoir des répercussions d'une ampleur au moins égale à celles résultantes du premier choc pétrolier en 1973.

Entre deux extrêmes, les combinaisons sont nombreuses. Selon les économistes les moins pessimistes, il faut tout de même s'attendre à un ralentissement de l'activité économique au cours du premier semestre 2000, et cela dès le mois de janvier (on parle de « l'effet janvier »).

Le caractère exceptionnel du phénomène ne peut être discuté et le passage à l'an 2000 offre une fantastique prise de conscience générale de l'apparition de nouveaux types de risques que constituent les risques à grande échelle dans les organisations complexes et interdépendantes.

Au-delà de la dépendance au réseau, la dépendance entre réseaux est également en jeu. Trop souvent, elle est même absente des réflexions sur le passage à l'an 2000. Le discours ne se focalise que sur les conséquences directes de l'événement en interne. Connaître les actions menées par ses partenaires et ses fournisseurs devient impératif.

A titre indicatif, plus de 300 millions de PC sont connectés dans le monde par des systèmes internes de type intranet et au travers de l'Internet. La connexion entre ce dernier -ouvert au public- et le système interne, se situe dans une zone sensible.

Au premier janvier prochain, le risque pourrait bien venir de l'extérieur, par exemple d'un fournisseur (système Extranet) qui ne pourrait plus approvisionner l'entreprise car lui n'a pas effectué les démarches nécessaires pour contrôler son parc informatique et électronique. Toute inattention d'une compagnie peut d'abord lui être fatale, et en cascade, l'être également pour les autres organisations qui dépendent d'elle. Une étude réalisée par une dizaine de consultants et de

[18] Il ne s'agit donc pas seulement de la gestion des personnes nées au XXième siècle (pensions, retraites, … etc.) auquel cas le problème aurait été de la même dimension que pour le traitement des personnes nées au XIXième siècle, à savoir à la marge.

[19] *Bogue* est la traduction du mot anglais *bug* qui signifie « punaise ». Avant l'apparition des transistors, les punaises se plaçaient en dessous des lampes de calculateurs pour profiter de la chaleur et occasionnaient très souvent des courts-circuits. L'appellation *bug* a demeuré après l'avènement des transistors.

[20] A titre indicatif, la *Canadian Imperial Bank of Commerce* du Canada a alloué un budget de 120 millions de dollars aux mille personnes qui travaillent sur le projet. *AT&T* a déjà dépensé plus de 500 millions de dollars (De Jager, 1999). En France, le budget du passage à l'an 2000 d'une entreprise comme *France Telecom* s'élève à 1 milliard de francs.

[21] Abréviation anglaise couramment utilisée pour désigner le passage à l'an 2000.

professeurs de l'université américaine Harvard discute précisément de cette interdépendance[22]. Le réseau agit alors négativement, l'interconnexion permet la propagation du sinistre.

Le passage à l'an 2000 ne peut donc pas se concevoir uniquement au niveau local, il doit l'être aussi globalement. L'internationalisation des échanges a accéléré la mise en réseau des acteurs économiques. Ainsi, les défaillances peuvent également provenir de fournisseurs ou de partenaires étrangers qui ne sont pas au point[23]. C'est en partie ce qui rend difficile l'évaluation des conséquences. En ce sens, le passage à l'an 2000 illustre le phénomène de dépendance au réseau et d'interdépendance des réseaux que nous discuterons dans la section suivante d'analyse générale du problème.

Malgré cela, le cas du passage à l'an 2000 symbolise pour nous un RGE « simple ». En effet, la date de réalisation du risque est déterminée avec certitude, et nous connaissons les caractéristiques techniques de la réalisation.

Que se passerait-il si la date de réalisation devenait aléatoire pour chacun des systèmes informatiques ?

L'ampleur du phénomène serait certainement beaucoup plus catastrophique. Les risques à grande échelle dans les réseaux s'apparentent d'ailleurs le plus souvent à ce dernier cas.

Par exemple, la probabilité d'une attaque est elle-même très difficile à estimer. Nous sommes alors en situation d'incertitude probabiliste. Quant aux conséquences, elles dépendent en grande part du niveau d'intrusion et de détérioration.

Comme nous le discuterons en détail dans la section suivante consacrée à l'analyse du problème, ces risques ont donc :

- une probabilité d'occurrence indéterminée et quasi impossible à calculer avec certitude;
- une date d'occurrence inconnue;
- et des conséquences que nous commençons tout juste à appréhender.

De plus, et contrairement au cas *an 2000*, les organisations voulant conduire une politique interne de gestion de ces risques ne bénéficient pas du même élan de questionnements et de solutions rendues publiques à l'échelle internationale. Elles sont le plus souvent seules pour gérer les risques (Théry, 1999).

Comme l'illustrent ces quatre exemples, les RGE dans les systèmes en réseau ont des origines et des réalisations multiples. Les réseaux touchés diffèrent (infrastructures, organisations, services gouvernementaux, services d'urgence …), les origines possibles sont variées (technologique, naturelle ou malveillante). Chaque exemple le montre, les pertes sociales et financières sont de plus en plus importantes, sans doute parce que les réseaux en question regroupent un nombre croissant d'utilisateurs.

Dans aucun des cas, nous ne pouvons dégager un unique réseau touché. La rupture est effective car par interconnexion des réseaux, c'est le plus grand réseau dans son ensemble - la société- qui est touché.

[22] *Harvard Business Review*, July-August 1998.

[23] Certains experts prévoient également que des pirates pourraient envoyer le 1er janvier prochain des virus simulant les effets du bogue et conduisant à des pannes de réseaux ou de micro-réseaux.

3- Spécificités de ces risques à grande échelle et analyse

Il semble donc que nous assistions à l'apparition de risques et sinistres de grande ampleur, assez confus à cerner, d'une gestion très complexe : des risques inédits qui rendent inefficaces les approches classiques.

Nous avons choisi de discuter certaines pistes dans cette note :

- quelles sont les spécificités de ces risques?
- en quoi rendent-elles l'analyse difficile?
- quelles sont les vulnérabilités connues des réseaux?
- les approches classiques de gestion de risques ont-elles encore quelque utilité?

- Spécificités de ces risques -

- **Une probabilité d'occurrence incalculable**

Les réseaux sont devenus des éléments extrêmement complexes. Comme nous l'exposons plus bas, les vulnérabilités se sont diversifiées et la nature même du risque est devenue plus confuse encore.

De plus, les probabilités de ces risques sont très mal connues. Le plus souvent, la probabilité est incertaine voir ignorée. Le risque existe bien, mais il est impossible de fournir une distribution de probabilités sérieuse. Nous sommes dans une situation d'*incertitude radicale*[24] ou d'*ignorance* (Knight, 1921, et plus récemment Hogarth et Kunreuther, 1995).

Lorsqu'une probabilité est tout de même calculée, le risque apparaît improbable voir extrêmement improbable sur un plan statistique (une probabilité de l'ordre de 0.001 ou 0.0001 a une signification limitée pour les décideurs). Très vite, seuls de grands sinistres hautement médiatisés induisent une prise de conscience véritable de ces risques et la mise en place de mesures spéciales.

Le fait que la probabilité soit non significativement mesurable a des conséquences directes graves. Les sinistres en question peuvent en effet apparaître pour certains comme une fatalité.

Les comportements changent radicalement. On peut alors craindre l'émergence de comportements stratégiques spécifiques à ce type de situation. Cette dernière devient si complexe et si incertaine que certains préfèrent agir en occultant la réalité de la situation : le risque est ignoré (Tversky et Wakker, 1995). Si cette attitude est répétée à l'ensemble des sous-réseaux constituant le réseau, aucune gestion globale de risque ne peut être menée.

- **Un phénomène de diffusion**

Une des caractéristiques des sinistres en question est « l'effet de cascade » auquel nous assistons le plus souvent. L'événement déclencheur se diffuse au travers du réseau pour atteindre un

[24] Il existe trois niveaux de connaissance des possibles : celui où l'ensemble des possibles est déterminé et les probabilités sont connues, celui où les possibles sont connus mais pas leurs probabilités, enfin celui où il a présomption des possibles qui ne sont pas connus (Michel-Kerjan, 1998).
Dans ce dernier cas, on parle d'*incertitude radicale*.

nombre plus important de victimes. Cet *effet de diffusion* dans les réseaux possède deux spécificités claires :

- Ubiquité

L'évolution actuelle vers une hyper connexion des réseaux contribue à augmenter le pouvoir de diffusion du sinistre au travers des réseaux. Il faut donc réagir au sinistre à de multiples endroits.

L'ubiquité du sinistre est une spécificité de ces risques à grande échelle. La crise du verglas à Montréal illustre bien ce phénomène de diffusion.

- Rapidité de propagation du sinistre

En plus d'être touché dans son ensemble, le réseau subit un phénomène qui se propage à grande vitesse.

Il faut réagir très vite, prendre des décisions quasiment en temps réel avec une information qui est forcément réduite et non vérifiée en son intégralité.

- **Des niveaux de risques qui explosent**

Supposons un instant que la probabilité d'un sinistre soit connue. Un *niveau de risque* peut être défini par le produit d'un montant de pertes et d'une probabilité d'occurrence de ces pertes.

Pour les risques en réseau, trois facteurs directs font augmenter significativement ce niveau de risque :

- une dépendance accrue à des réseaux de plus en plus denses augmente le potentiel de diffusion d'un sinistre dans ce réseau et ainsi le montant des pertes potentielles;
- l'interdépendance entre réseaux amplifie l'impact de l'aléa en le diffusant d'un réseau aux autres réseaux qui en dépendent. Ainsi le montant des pertes potentielles est ici encore considérablement décuplé car il faut estimer les pertes consécutives à un sinistre touchant plusieurs réseaux[25];
- à la probabilité de défaillance interne au réseau lui-même, il faut aussi ajouter celle d'être touché par un effet indirect de diffusion provenant d'autres réseaux sinistrés.

Dans ces deux derniers cas, l'interdépendance des réseaux augmente significativement les niveaux de risque[26].

[25] A noter d'ailleurs que les conséquences sont sans commune mesure avec le coût de l'élément défaillant du réseau.

[26] Considérons le cas simpliste de deux réseaux, A et B, d'abord indépendants, chacun ayant une probabilité p d'être touché par un sinistre conduisant à des pertes de niveau L (état noté 1) sur le réseau. En regardant l'ensemble des deux réseaux, il y a donc quatre états du système (0/0 ;0/1 ;1/0 ;1/1).
Il vient que l'espérance des pertes égale 2Lp
Supposons ensuite les deux réseaux interdépendants et l'existence d'un potentiel de diffusion : un réseau atteint affecte l'autre réseau. Il a alors deux états possibles après diffusion : (0/0 ;1/1).
Il vient que l'espérance des pertes égale $2p(1-p)(2L) + p^2(2L)$, soit $2Lp[2-p] > 2Lp$.

Nous sommes donc face à une situation complexe, des sinistres dont les conséquences explosent du fait même d'un effet de diffusion lié à l'utilisation de systèmes en réseau, et face à des risques non probabilisables.

Il faut gérer en temps réel un sinistre en propagation qui touche simultanément tout un ensemble de réseaux.

La gestion de tels sinistres présente des aspects inusités qu'il faut expérimenter en pleine crise. Il faut gérer des sinistres inédits[27].

- Analyse -

En plus de vulnérabilités bien connues, des nouvelles vulnérabilités sont apparues. Apparues récemment et très rapidement, on ne les a pas vraiment considérées sérieusement. Elles en sont d'autant plus dangereuses. Il conviendrait donc de les placer dorénavant au cœur de la réflexion.

- **Des vulnérabilités bien connues**

Plusieurs vulnérabilités sont connues, parmi lesquelles certaines ne sont pas spécifiques aux risques dont nous discutons. Les réseaux deviennent justement vulnérables du fait des menaces qui peuvent les affecter (un élément du réseau, un sous-réseau ou tout le réseau).

Pour aller à l'essentiel des approches les plus répandues, nous reprenons ici deux classifications très utilisées.

- Les menaces susceptibles de peser sur les systèmes en réseau sont regroupées en quatre origines : la menace interne versus la menace externe, la menace accidentelle versus intentionnelle, chaque combinaison pouvant exister comme l'illustre la matrice suivante.

-

	Menace interne	**Menace externe**
Menace accidentelle	accident interne	accident externe
Menace intentionnelle	malveillance interne	malveillance externe

Sources : SCSSI, 1994.

La menace interne provient de l'organisation elle-même. Comme le souligne une récente enquête, elle paraît trop souvent sous-estimée : on évalue à 50 % la part des sinistres informatiques ayant comme origine une malveillance interne (De Marcellis et Gratacap, 1999).

Dans les politiques de gestion de risques classiques, cette dichotomie interne/externe est toujours fondamentale. Cela est compréhensible, il convient de traiter différemment les menaces internes mettant directement en cause la responsabilité de l'organisation et de ses responsables, et les menaces externes pour lesquelles les responsabilités ne sont pas toujours clairement définies.

[27] Voir Lagadec (1997) et Lagadec (2000).

Les catastrophes naturelles (séismes, tornades, orages, vents violents, grêles, inondations … etc.) constituent certainement la première source de menaces accidentelles d'origine externe. Classiquement, les incendies, coupures de courant ou de téléphone, d'origine interne ou externe, rendent également les réseaux vulnérables.

Enfin, le manque d'entretien des systèmes peut menacer les réseaux internes de la firme.

- En France, le *Service Central de la Sécurité des Systèmes d'Information* (S.C.S.S.I)[28] utilise une typologie des menaces intentionnelles en quatre classes de risques : la menace stratégique, la menace terroriste, la menace ludique, et la menace cupide (cf. annexe).

Compte tenu d'un caractère extrême de complexité, de l'évolution grandissante de la taille des réseaux, et d'une interdépendance nettement accrue, nous pouvons nous demander si ces diverses classifications, typologies et autres matrices sont encore pertinentes?

Prenons deux exemples.

Avec la croissance des réseaux virtuels, que devient la dichotomie menace interne versus menace externe? Le réseau est omniprésent. Les « entrées » du réseau sont multiples et par conséquent une tentative malveillante peut être organisée à partir de n'importe quel endroit du globe avec un accès au réseau informatique[29].

Alors que les groupes dits *terroristes* sont aujourd'hui constitués le plus souvent de réseaux hybrides, que devient la classification proposée par le SCSSI incluant une menace terroriste?[30]

- **De nouvelles vulnérabilités jaillissent**

On l'aura bien compris, l'utilisation grandissante des réseaux change totalement les données. Vouloir gérer ces risques comme des vulnérabilités classiques est le meilleur moyen de courir à la catastrophe. D'une part les sources de vulnérabilité sont plus nombreuses, plus confuses, et engendrent des conséquences sans commune mesure avec les pertes précédemment enregistrées, mais surtout les réseaux apportent avec eux de nouvelles menaces.

Prenons de nouveau un exemple. Il présente un aspect clair du problème, mais un aspect seulement.

Nous assistons depuis quelques années à l'émergence et à l'évolution exponentielle de services financiers en ligne et à celle du commerce électronique, encore dénommé E-Trading. La création

[28] Le service central de la sécurité des systèmes d'information a été créé en 1986 auprès du Premier ministre. Il est chargé d'apprécier le niveau de protection des systèmes d'information. Il participe aux activités de recherche relatives aux procédés de protection, coordonne les études et développements de protection des systèmes d'information gouvernementaux.

[29] L'exemple suivant illustre la situation actuelle. Il m'a été rapporté par l'un des membres de la *Commission présidentielle américaine sur la protection des infrastructures critiques.*
Pendant l'été 1997, l'armée américaine a mis en place un programme de simulations d'attaques informatiques dans les réseaux du Ministère de la Défense. Il s'agissait de savoir si l'on pouvait infiltrer les réseaux gouvernementaux et être alors en mesure de porter atteinte à la sécurité nationale. Le résultat a été des plus concluant : en moins de trois mois, l'équipe mise en place a réussi à pénétrer plus d'une centaine d'ordinateurs du Ministère. De plus, cette intrusion n'a requis que des « outils » disponibles légalement sur Internet !

[30] Rappelons que l'appellation « acte terroriste » est réservée à « un ensemble des actes de violence, des attentats, des prises d'otages civils qu'une organisation politique commet pour impressionner un pays ». (Cf. Annexe)

d'ECN (Electronic Crossing Networks) permet des transactions en continu, quasi instantanées, et nettement moins chères (en moyenne 15$ pour une transaction en ligne contre 1 500$ en mode classique pour un montant de 50 000$ avec 3 % de commission). D'après les travaux de Suret (voir Lagadec, 2000), on estime par exemple à 100 milliards de dollars les montants échangés en ligne en 1996, 375 en 1999, et 3100 sont prévus pour 2003. L'évolution est donc fulgurante et elle commence à toucher d'autres secteurs comme l'assurance (souscription et indemnisation en ligne) et le commerce. Dans chacun de ces cas, le réseau est au cœur de l'évolution.

Il semble donc que nous assistions à une révolution qui ne se fera pas sans risque dans un monde de réseaux virtuels entremêlés qui opèrent en temps réel sur une échelle planétaire.

Pour chaque entreprise le premier souci sera de faire face, elles devront s'adapter à ces changements brutaux ou disparaître (voir l'article de Peter Drucker sur la question dans le second numéro d'octobre de *The Economist*).

Les fraudes, les pannes de secteur ou du réseau lui-même (défaillances du système) ont déjà occasionné des pertes importantes[31] et pourraient conduire à des pertes colossales. L'échelle à considérer est devenue très étendue (par conception même il n'y a plus de frontière, ni pour les consommateurs, ni pour les pirates).

Il apparaît clairement dans cet exemple que les approches existantes au mieux ne peuvent suffirent, au pire sont inutilisables. Les outils de gestion de risques traditionnels n'évoluent pas avec la même vitesse. Nous sommes passés très rapidement de menaces sur des réseaux physiques à des menaces sur des réseaux physiques et virtuels. Les risques à grande échelle liés à l'*économie virtuelle* (notion qui déborde alors la seule finance) sont encore aujourd'hui considérés à la marge car ce sont des risques émergents.

Mais ces risques « inédits » constitueront demain, avec les grandes catastrophes naturelles qui s'abattent sur des régions fortement industrialisées, deux potentialités majeures de sinistres à grande échelle.

4- Conclusion et perspectives de recherche

L'utilisation des réseaux est croissante car elle procure de nombreux avantages comme nous l'avons brièvement exposé dans la section 1, notamment des économies d'échelle significatives. L'évolution grandissante de réseaux toujours plus complexes et denses pourrait pourtant contribuer à construire des sinistres aux conséquences accrues par l'existence même du réseau.

A l'image de la boule de feu qui grossit car elle trouve sur son passage de quoi la rendre plus dévastatrice encore, le sinistre se propage au travers du réseau pour atteindre un nombre de victimes accru par la forte dépendance au réseau et surtout par l'interconnexion des réseaux. La dépendance entre réseaux se traduit par une corrélation positive des risques. Une même menace pourrait affecter dans des temps très rapprochés et de manière ubiquitaire plusieurs réseaux dont certains agents dépendent simultanément ou de manière complémentaire.

L'utilisation inconsidérée de réseaux immenses peut alors présenter un versant bien plus sombre, le réseau augmentant de fait les externalités, négatives dans ce cas.

[31] Exemple du E-Trade de Palo-Alto (Californie), "planté" durant trois jours en février dernier : 700 000 comptes à gérer, tous gelés.

Les questions de vulnérabilité des réseaux (hier physiques, aujourd'hui physiques et virtuels) s'intensifient donc. Un arbitrage économique entre les bénéfices apportés par l'interconnexion des réseaux et l'échelle catastrophique des pertes en cas de sinistre (liée à l'interdépendance des réseaux) doit être maintenant considéré avec une attention particulière.

Les questions de complexité et des liens d'interconnexion constituent selon nous le mot d'ordre des risques à grande échelle et phénomènes de rupture émergents et à venir.

Perspectives

- Il y a une véritable nécessité d'enquête sur le terrain pour comprendre ce que sont ces nouveaux risques, et quelles approches sont à privilégier pour traiter ce type de risques. Il apparaît assez urgent de construire une première base opérationnelle.

Nous entreprendrons dans les mois à venir une étude sur le sujet auprès des *risks managers*, des analystes, et des instances de régulation. Cette étude se fera en partenariat avec les compagnies de réassurance avec lesquelles nous collaborons actuellement[32], et les firmes souhaitant se joindre au projet.

- Dans un autre registre, les Américains ont été les premiers à réagir au plus haut niveau pour connaître l'ampleur des vulnérabilités liées à l'utilisation croissante de grands réseaux physiques et virtuels. Ils l'ont fait au niveau régional et national en analysant la vulnérabilité des infrastructures considérées vitales pour le bon fonctionnement de leur économie. L'enquête a impliqué à la fois des institutions, des entreprises publiques et des firmes privées[33].

A notre connaissance, aucune étude de ce genre n'a été menée et publiée en Europe. Il apparaît donc pertinent de travailler au plus vite sur le sujet pour obtenir un retour d'expérience approfondi. En ce sens, nous sommes entrés en contact avec certains membres de cette Commission. Il conviendra alors d'étudier dans quelles conditions il est envisageable et bénéfique de reproduire l'expérience en Europe (pays ou groupement de pays) et à plus petite échelle (organisation) ?

- Comme nous l'avons écrit, peu de travaux de théorie économique traitent de ces questions. La littérature économique des réseaux s'intéresse davantage aux questions relatives à la pertinence de l'utilisation d'un réseau ou d'une technologie donnée plutôt qu'aux questions de taille optimale de réseau ou de redondance des outils de gestion de risques. Nous travaillons actuellement à l'élaboration d'un modèle mathématique prenant en compte les questions de vulnérabilité, de dépendance au réseau et d'interdépendance entre réseaux, et formalisant certains arbitrages économiques. Ce modèle devrait constituer une première contribution théorique pour rendre compte de ces risques inédits et apporter des solutions de gestion afin d'en limiter l'occurrence et l'ampleur des conséquences.

[32] En particulier la *Compagnie Suisse de Réassurances* à Zürich.

[33] Les travaux de la Commission présidentielle mise en place à cet effet ont été rendus publics en octobre 1997. Ils posent clairement la question de ces nouveaux risques. La mise en place de cette Commission d'enquête s'est inscrite dans un souci affirmé des domaines publics et privés de comprendre la situation actuelle sur les risques à grande échelle qu'ils encourent. Ces risques sont notamment liés à l'utilisation des nouvelles technologies de l'information, à l'expansion de l'informatique et de l'électronique au sein des infrastructures jugées "critiques" (secteur de l'énergie, des transports et télécommunications, les organes gouvernementaux, les secteurs bancaires et financiers entre autres). Qu'il s'agisse de pannes technologiques, des conséquences de catastrophes naturelles ou encore d'attaques délibérées contre les Etats-Unis, les organisations ou les entreprises américaines, les vulnérabilités existent déjà.

Bibliographie

W. Baumol, Panzar JC., et Willig R. (1982), *Contestable Markets and the Theory of Industry Structure*, Harcourt Brace Jovanovich, New York.

G. Birkhoff (1948), *Lattice Theory*, New York : American Mathematical Society.

JP. Bouttes et D. Haag (1992), « Economie des réseaux d'infrastructure », in N. Curien, éd., *Economie et Management des entreprises en réseau*, ENSPTT, Economica, pp. 3-30.

Comité interministériel pour la société de l'information (CISI) (1998) : *Préparer l'entrée de la France dans la société de l'inform@tion : Programme d'action gouvernemental pour la société de l'information (PAGSI)*, Paris : Comité interministériel pour la société de l'information.

Computer Security Institute (1997) : *Computer Security Issues & Trends*, vol III, San Francisco : Computer Secutity Institute.

N. Curien, éd. (1992), *Economie et Management des entreprises en réseau*, ENSPTT, Economica, Paris, pp. 211.

N. Curien (1993), *Economie des services en réseau*. Leçon inaugurale, Chaire d'Economie et de Politique des Télécommunications, Conservatoire National des Arts et Métiers.

N. Curien et Gensollen M., éds. (1992), *Economie des télécommunications*, ENSPTT, Economica, Paris, pp. 318.

C. Debaert, Legrand N., et E. Michel-Kerjan (1997), *L'Organisation face aux risques technologiques majeurs*, Publication Cirano, Montréal : CIRANO, pp. 178.

P. Drucker (1999), « Innovate or die », *The Economist*, 25 septembre-1er octobre, pp. 27-34.

P. de Jager (1999), « Y2K : So Many Bugs … So Little Time », *Scientific American*, January.

N. Economides (1996), « The Economics of Networks », *International Journal of Industrial Organization*, vol. 14, No 2.

N. Economides and LJ. White (1993), « One-Way Networks, Two-Ways Networks, Compatibility, and Antitrust », Discussion Paper EC-93-14, Stern School of Business.

J. Deepack, W. Murray, and R. McCormack (1996), « Dealing with Disaster : the Recovery in Kobe », *Risk Management*, pp. 64-69.

N. De Marcellis et A. Gratacap (1999), "TIC et Gestion des Risques : bilan et perspectives assuranciels pour l'entreprise", *Communication & Stratégies*, No 33.

L. Euler (1736), Solutio problematis ad geometriam situs pertinentis, *Commentarii Academiae Scientiarum Imperialis Petropolitanae 8.*

J. Farrell et S. Garth (1986), « Installed Base and Compatibility : Innovation, Product Preannoucements, and Predation », *American Economic Review*, vol. 76, pp. 940-955.

Federal Bureau of Investigation (1997) : *FBI Computer Crime and Security Survey*, Washington : Federal Bureau of Investigation.

RM. Hogarth et H. Kunreuther (1995), « Decision Making under Ignorance : Arguing for Yourself », *Journal of Risk and Uncertainty*, vol. 10, pp. 15-36.

F. Knight (1921), *Risk, Uncertainty and Profits*, Houghton, Mifflin & CO.

M. Katz et C. Shapiro (1985), « Network Externalities, Competition, and Compatibility », *American Economic Review*, vol. 75, No 3, pp. 424-440.

M. Katz et C. Shapiro (1994), « Systems Competition and Network Effects », *Journal of Economic Perspectives*, vol. 8, No 2, pp. 93-115.

M. Kretzschmar (1999), « Modeling Network Structure : Implications for Spread and Prevention of HIV-Infection », mimeo.

P. Lagadec (2000), *Ruptures créatrices*, Editions d'Organisation, Paris (à paraître en janvier).

P. Lagadec (1997), "Urgences, Crises, Ruptures : des théâtres de vulnérabilité en mutation", *Préventique-Sécurité*, No 36, pp. 14-23.

P. Lagadec (1993), *Apprendre à gérer les crises - Société vulnérable, acteurs responsables*, Editions d'Organisation, Paris.

P. Lagadec (1988), *Etats d'urgence – Défaillances technologiques et déstabilisation sociale*, Editions du Seuil, Paris, pp. 406.

S. Liebowitz et S. Margolis (1994), « Network Externality : An Uncommon Tragedy », *Journal of Economic Perspectives*, vol. 8, No 2, pp. 133-150.

E. Michel-Kerjan (1998), « Peut-on assurer le risque à grande échelle ? », *Bulletin de liaison sur le risque*, CIRANO, vol. 2, No 2.

RL. Nolan et al. (1998), « Connectivity and Control in the Year 2000 and Beyond », *Harvard Business Review*, July-August 1998, pp.149-166.

OCDE (1998) : *Le problème de l'an 2000 : incidences et actions*, Paris : OCDE.

Office Parlementaire d'Evaluation des Choix Technologiques (1998) : *Le passage à l'an 2000 : Rapport de Gérard Théry*, Paris : Office Parlementaire d'Evaluation des Choix Technologiques, Sénat-Assemblée Nationale.

Commission Nicolet (1999), *Rapport de la Commission Nicolet*, 5 volumes, Publications du Québec, Montréal : Commission Nicolet.

D. Parrochia (1993), *Philosophie des réseaux*, PUF, Paris, pp. 300.

A. Perrot, éd. (1997), *Réglementation et Concurrence*, Economica, Paris, pp.175.

President's Commission on Critical Infrastructure Protection (1998), *" Critical Foundations, Protecting America's Infrastructures "*, Washington : President's Commission on Critical Infrastructure Protection.

Service Central de la Sécurité des Systèmes d'Information (1994) : *La menace et les attaques informatiques*, N° 650/DISSI/SCSSI, Paris : Service Central de la Sécurité des Systèmes d'Information.

B. Sinclair-Desgagné (1998), « Large Networks Can Induce Large Risks », article non publié présenté lors de la Conférence de Toulouse sur l'économie des réseaux.

JM. Suret (1999), « Le commerce électronique et le secteur financier: ruptures au cœur du système économique », in P. Lagadec (2000), *Ruptures créatrices*, Editions d'Organisation, Paris.

Rapport de G. Théry - Comité interministériel pour la société de l'information (CISI) – (1999) : *Mise en œuvre du PAGSI, état d'avancement après un an (janvier 1998-janvier 1999),* Paris : Comité interministériel pour la société de l'information.

A. Tversky and P. Wakker (1995), « Risk Attitudes and Decision Weights », *Econometrica*, vol. 63, No. 6, pp. 1255-1280.

Annexe

- Typologie des menaces intentionnelles -
Service Central de la Sécurité des Systèmes d'Information.

- **la menace stratégique**

Il peut s'agir de concurrence industrielle ou d'espionnage entre Etats. L'accès à certaines banques de données ou à certaines informations confidentielles de l'entreprise apparaît stratégique, offrant la possibilité aux concurrents « pirates »[34] de disposer des plans de développement ou des listes clients de la société piratée. A un autre niveau, il peut s'agir de neutraliser les infrastructures vitales d'un pays pour le rendre plus vulnérable. Les menaces stratégiques pour un pays regroupent les actions susceptibles de porter atteinte à la sécurité de l'Etat ou au secret de défense.

- **la menace terroriste**

Dans ce cas, il s'agit souvent de frapper l'opinion publique au travers d'une action hautement médiatisée afin de créer un climat national de peur. Les pirates peuvent être des groupes organisés voire parfois des Etats.

- **la menace ludique**

Il ne s'agit pas ici de porter réellement atteinte à autrui mais plus de défier les systèmes de sécurité d'organismes importants reconnus inviolables. Le piratage s'apparente plus à un jeu.

- **la menace cupide**

Le but est ici clairement de détourner à son profit des montants financiers. Les principaux systèmes touchés sont ceux des institutions bancaires ou autres compagnies d'assurance. On parle également de « délinquance en col blanc ».

[34] Nom donné habituellement; traduction de l'anglais *hackers.*

Liste des publications au CIRANO *

Cahiers CIRANO / *CIRANO Papers* (ISSN 1198-8169)

99c-1 Les Expos, l'OSM, les universités, les hôpitaux : Le coût d'un déficit de 400 000 emplois au Québec — Expos, Montréal Symphony Orchestra, Universities, Hospitals: The Cost of a 400,000-Job Shortfall in Québec / Marcel Boyer

96c-1 Peut-on créer des emplois en réglementant le temps de travail? / Robert Lacroix

95c-2 Anomalies de marché et sélection des titres au Canada / Richard Guay, Jean-François L'Her et Jean-Marc Suret

95c-1 La réglementation incitative / Marcel Boyer

94c-3 L'importance relative des gouvernements : causes, conséquences et organisations alternative / Claude Montmarquette

94c-2 Commercial Bankruptcy and Financial Reorganization in Canada / Jocelyn Martel

94c-1 Faire ou faire faire : La perspective de l'économie des organisations / Michel Patry

Série Scientifique / *Scientific Series* (ISSN 1198-8177)

2000s-01 Wealth Distribution, Moral Hazard, and Entrepreneurship / Sanjay Banerji et Ngo Van Long

99s-48 A New Class of Stochastic Volatility Models with Jumps: Theory and Estimation / Mikhail Chernov, A. Ronald Gallant, Eric Ghysels et George Tauchen

99s-47 Latent Variable Models for Stochastic Discount Factors / René Garcia et Éric Renault

99s-46 Sequential Auctions with Multi-Unit Demand: Theory, Experiments and Simulations / Jacques Robert et Claude Montmarquette

99s-45 American Options: Symmetry Properties / Jérôme Detemple

99s-44 What Is Happening in the Youth Labour Market in Canada? / Paul Beaudry, Thomas Lemieux et Daniel Parent

99s-43 The Valuation of Volatility Options / Jérôme Detemple et Carlton Osakwe

99s-42 Labour Market Outcomes and Schooling in Canada: Has the Value of a High School Degree Changed over Time? / Daniel Parent

99s-41 Travail pendant les études, performance scolaire et abandon / Marcel Dagenais, Claude Montmarquette, Daniel Parent et Nathalie Viennot-Briot

99s-40 Recursive Intergenerational Utility in Global Climate Risk Modeling / Minh Ha-Duong et Nicolas Treich

99s-39 Transition vers le marché du travail au Canada : Portrait de la situation actuelle et perspective historique / Daniel Parent

99s-38 Program Evaluation Criteria Applied to Pay Equity in Ontario / Morley Gunderson et Paul Lanoie

---

* Vous pouvez consulter la liste complète des publications du CIRANO et les publications elles-mêmes sur notre site Internet à l'adresse suivante :

http://www.cirano.umontreal.ca/publication/documents.html