A paraître dans *Flux – Cahiers Scientifiques Internationaux Réseaux et Territoires*
Forthcoming in *Flux – International Scientific Quarterly on Networks and Territories*

Risques catastrophiques et réseaux vitaux : de nouvelles vulnérabilités[1]

Erwann MICHEL-KERJAN[2]

Novembre 2002

Adresse pour correspondance :

Erwann MICHEL-KERJAN

Center for Risk Management, The Wharton School

Jon M. Huntsman Hall, Suite 500

3730 Walnut Street, Philadelphie, PA, 19104-6340, United-States.

Email :erwannmk@wharton.upenn.edu.

[1] L'écriture de cet article a bénéficié du soutien scientifique et financier du programme IDS joint Wharton-Columbia, de l'Institut Vivendi Environnement, et de l'Ecole Polytechnique.

[2] Center for Risk Management, The Wharton School (USA) et Laboratoire d'économétrie de l'Ecole Polytechnique (Paris).

Abstract

Large-scale terrorism, natural hazards with extreme consequences, major technological disasters in highly industrialized and densely populated areas, malevolent acts are examples of events relatively disconsidered a decade ago but that call today for much more attention and specific analysis.

In parallel to such an evolution, we can observe –for well-known economic reasons- a great development of large-scale infrastructure networks that are increasingly interdependent. Citizens or organizations are also more and more dependent on those critical infrastructures. The combination of the two trends leads to new vulnerabilities with possible extreme consequences on the economic and social activity of countries. The paper illustrates that phenomenon through three cases (failure of a telecommunication satellite, natural disaster hurting am electric distribution, terrorism).

Because of that change in the scale of possible consequences, it is become necessary to redefine some risk mitigation approaches: moving from numerous local programs, most of them disregarding the other, to a global approach of risk assessment and risk mitigation taking into account the interdependencies among several networks. Few organizations do still operate in that way.

However, this paper shows that those risks present some similarities. Better understanding those common characteristics could allow organizations (private as well as private) being more prepared.

At a national level, there is an urgent need to the development of collective initiatives on issues related to extreme events. France could appreciate the recent initiatives launched in North America, some of which are discussed here.

Key words: Large-scale risks – Critical Networks – Interdependence – Risk Management

Résumé

Terrorisme de masse, désastres naturels d'ampleur exceptionnelle, catastrophes industrielles majeures, actes de malveillance à grande échelle…, autant de sinistres hier considérés comme des scénarios impossibles, qu'il convient aujourd'hui de traiter avec beaucoup plus d'attention.

En parallèle de ces nouveaux risques, on assiste – pour des raisons économiques légitimes – à une croissance fulgurante des grands réseaux d'infrastructures, ainsi qu'à leur interconnexion. Or, précisément, ces nouvelles vulnérabilités touchent avant tout les grands réseaux vitaux à l'activité économique et sociale d'un pays. Nous l'illustrons par trois exemples d'effondrement ou d'utilisation malveillante (télécommunication, distribution électrique, terrorisme).

Puisque l'échelle des potentialités de sinistres s'est considérablement étendue, cela nécessite de repenser leur prévention : passer d'une sécurité locale à des programmes de gestion de risques à une échelle nationale et internationale. Or, à ce jour, peu d'organisations se sont engagées dans cette voie.

Nous montrons pourtant que ces risques présentent des régularités et des caractéristiques communes. Il est donc possible de préparer les dirigeants des entreprises et des organisations (privées comme publiques) à y faire face.

A une échelle nationale, il y a urgence à créer de l'apprentissage collectif sur ces sujets qui restent complexes à appréhender et à solutionner, sous peine, à court terme, de devoir subir des catastrophes plus nombreuses, plus coûteuses, et plus dramatiques encore. Si la France demeure bien frileuse encore, des initiatives collectives sont à souligner, notamment en Amérique du Nord. Elles pourraient constituer des exemples à suivre ou à améliorer.

Mots clés : Gestion de risques à grande échelle – Interdépendance – Réseaux vitaux

1. Introduction

Les attentats du 11 septembre 2001 contre les Etats-Unis ont créé un véritable électrochoc dans la communauté internationale : alors que

nombreux actes de terrorisme ont déjà été perpétrés contre des populations civiles, aucun attentat contre un Etat en paix n'avait jamais tué ni blessé autant de civils à la fois.

Les dommages matériels ont également été catastrophiques. De fait, ces attentats constituent un point de rupture pour l'assurance et donc pour la continuité de certaines activités. Ces attentats, avec des montants de remboursement par les compagnies d'assurance et de réassurance dépassant les 40 milliards de dollars, constituent en effet l'événement le plus coûteux de toute l'histoire de l'assurance mondiale[3].

Mais ces attaques ne constituent pas seulement une déstabilisation pour l'industrie de l'assurance[4]. La configuration même des attentats ne relève pas d'actes de terrorisme « traditionnels » tels que l'explosion d'une voiture ou d'un colis piégé. En effet, dans ce cas précis, un des grands services vitaux d'un pays –le transport aérien– a été détourné de son usage traditionnel pour atteindre un nombre beaucoup plus important de victimes : détournement d'avions de lignes privées, pour s'écraser sur des biens privés, les deux tours du *World Trade Center*[5].

Quelques semaines plus tard, ce fut la crise de l'anthrax. Là encore, un autre réseau était détourné de son usage à des fins de malveillance : les services postaux. Avec la paralysie des services postaux de nombreux pays, ces opérateurs ont du affronter un nouveau type de risques et des coûts financiers se chiffrant en centaines de millions d'euros.

Ces événements nécessitent une réflexion de fond sur la gestion de la sécurité des grands services vitaux au bon fonctionnement d'un pays. Que l'on pense aux réseaux de distribution (eau, électricité, gaz, pétrole), de transport de personnes et de marchandises (aérien, ferroviaire, routier, maritime), aux réseaux de communication (services postaux, téléphonie,

[3] Swiss Re (2002), *Terrorism-dealing with the new spectre*. Zurich.

[4] Sur la question des politiques de couverture des conséquences matérielles d'actes de terrorisme en France et à l'étranger, voir Michel-Kerjan (2002), « Terrorisme à grande échelle : partage de risques et politiques publiques », *Wharton Center for Risk Management*, working paper, décembre 2002.

[5] Voir le dernier chapitre de O. Godard, C. Henry, P. Lagadec et E. Michel-Kerjan (2002), *Traité des nouveaux risques. Précaution, Crise, Assurance.* Paris, Editions Gallimard, coll. Folio-Actuel, 620p.

transport de l'information, télévision, Internet), aux maillages complexes des réseaux bancaires et financiers ou encore aux réseaux gouvernementaux de sécurité nationale.
Le simple fait que les scénarios du pire que nous nous étions fixés, comme étant une limite théorique qui ne serait jamais atteinte, soient non seulement réalisés mais dépassés, nous oblige à considérer une limite catastrophique encore supérieure, comme ce fut le cas ces dernières années lors de grandes catastrophes d'origine naturelle tels que des séismes (Northridge, Kobe, Izmit) ou des tempêtes d'ampleur extrême (Mireille, Andrew, Lothar et Martin).

Au-delà de ces épisodes plus récents, il s'agit aussi de reconnaître aujourd'hui que la vulnérabilité des grands réseaux a été démultipliée en l'espace de 10 ans. Et le paradoxe est important. D'un point de vue technologique, des avancées importantes ont été réalisées dans le domaine de l'ingénierie pour offrir une plus grande fiabilité technique aux grands ouvrages de réseaux. En parallèle de ces améliorations techniques, le recours à des réseaux de très grande taille et leur interconnexion ont permis des réductions de coûts substantielles grâce aux économies d'échelle et d'envergure réalisées. Néanmoins, on ne peut occulter un versant plus sombre de l'utilisation des grands réseaux. Lorsqu'ils sont mis en défaut de fonctionnement, le sinistre touche alors un très grand nombre de personnes et d'entreprises et, en cascade, d'autres réseaux. De plus, de nouvelles sources de déstabilisation apparaissent, et sont beaucoup plus difficiles à appréhender que les défaillances techniques : confrontations des grands réseaux à des événements climatiques d'une ampleur sans précédent, émergence significative d'actes de malveillance interne aux entreprises[6], actes de malveillance externe et « terrorisme de masse ». Aux impacts directs pouvant affecter un réseau en particulier, il faut donc aussi tenir compte de l'interdépendance croissante des réseaux entre eux et d'une dépendance largement accrue des populations, entreprises et autres institutions, au bon fonctionnement quotidien des grandes infrastructures.

En d'autres termes, les risques ne relèvent plus aujourd'hui de simples mesures de sécurité locales. Il faut considérer des risques globaux dont les sources potentielles ont été multipliées en interne, et plus encore en externe. Cette globalisation des risques appelle une **gestion globale** des nouvelles vulnérabilités. La catastrophe de Toulouse comme les grands

[6] A titre illustratif, dans une étude publiée en 1999 sur les risques informatiques au sein des entreprises, les auteurs estimaient ainsi à 50% la part des sinistres informatiques due à un acte de malveillance interne à l'entreprise ; De Marcellis et Gratacap, (1999), « TIC et Gestion des Risques : bilan et perspectives assurantiels pour l'entreprise », *Communication & Stratégies*, N° 33.

épisodes d'inondation ou les tempêtes de décembre 1999 auraient du constituer autant d'alertes sérieuses[7]. Or, à ce jour, ces sujets demeurent relativement peu analysés en France[8].

Cet article offre un éclairage sur la question émergeante des sinistres à grande échelle touchant les grands services vitaux.

Dans un souci de pragmatisme et afin de rendre cette problématique directement plus concrète pour le lecteur, trois exemples sont discutés dès la section 2 de l'article :

- l'arrêt brutal d'un satellite de télécommunication qui a touché plus de 45 millions d'américains en mai 1998 ; défaillance technologique locale.
- l'effondrement du réseau de distribution électrique lors de la grande tempête de verglas qui a dévasté l'Amérique du Nord, et plus particulièrement le Québec, en janvier 1998 ; catastrophe naturelle à l'échelle nationale.
- la question du terrorisme de masse ; utilisation malveillante de réseaux mondiaux.

Dans la section 3, nous montrons notamment pourquoi l'approche traditionnelle de gestion de risques, fondée sur le seul critère des pertes espérées, est inadaptée pour traiter nos nouvelles vulnérabilités.

Lorsque ces scénarios se réalisent, ils sont porteurs d'un fort pouvoir de déstabilisation dans l'entreprise qui doit y faire face, la gestion de crise est particulièrement difficile, les pertes humaines et/ou financières potentiellement catastrophiques. De telles caractéristiques nécessitent la mise en place d'outils de réflexion stratégique à l'usage des décideurs du secteur privé et du secteur public[9]. Cela passe par la reconnaissance de nouvelles sources de déstabilisation et par un apprentissage collectif sur ces questions complexes. Il y a aujourd'hui une nécessité pressante de développer de véritables éléments de gouvernance : dans les entreprises (EDF le fit avant les tempêtes de 1999) comme à l'échelle d'un pays.

Or, à ce jour, seuls les Etats-Unis ont considéré cette atteinte des grands services vitaux comme une source nouvelle des futures catastrophes. Les travaux de la Commission présidentielle mise en place par le Président Clinton et rendus publics 1997 et 1998

[7] Comme le souligne le rapport de la Commission de retour d'expérience sur les tempêtes de 1999 Sanson, sans une volonté affirmée de les étudier et de les solutionner, au moins partiellement, on peut craindre la recrudescence d'événements paralysant le pays ou tout un secteur industriel en particulier ; voir Sanson (2001), *L'évaluation des dispositifs de secours et d'intervention mis en œuvre à l'occasion des tempêtes des 26 et 28 décembre 1999*, Rapport complémentaire à la mission interministérielle, Paris.

[8] Sur la question de la sécurité des grands sites chimiques dans les zones industrialisées, voir notamment l'éditorial du Journal *Le Monde* du 21 septembre 2002, «AZF, connais pas ! ».

[9] D. Moss (2002), *When All Else Fails: Government as the Ultimate Risk Manager*. Cambridge: Harvard University Press.

s'inscrivent pleinement dans cette voie, une initiative que les Européens pourraient vouloir considérer avec intérêt. Ces éléments font l'objet de la section 4.
Une dernière section conclut l'article.

1. Grands réseaux, grands sinistres : trois exemples

2.1. Réseau de télécommunication hors d'état aux Etats-Unis : défaillance technologique locale

En mai 1998, le satellite de communication G*alaxy IV*, qui permettait d'envoyer de nombreuses ondes vers le territoire des Etats-Unis, subit une avarie qui le met hors d'usage. " L'incident " paralyse alors une grande partie du réseau d'ondes américain : les 45 millions de propriétaires de « bipeurs » ne peuvent plus recevoir de message, 600 stations de radio arrêtent leurs programmes, de très nombreux terminaux bancaires ne fonctionnent plus, …etc. 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.
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.
Quant aux pertes indirectes, il est difficile de les mesurer.

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 et d'une panne interne prévisible, la dépendance au réseau apparaît ici clairement.
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.
Si les experts des entreprises concernées cherchent à présenter ce cas comme extrêmement rare, le risque de nouveaux « blackouts » de nature similaire pourrait s'accroître sensiblement

avec l'envoi de satellites plus nombreux dans les années à venir, notamment avec la constellation de satellites mise en place pour le système de communication GPS[10].

En effet, l'accumulation importante de « déchets » dans la stratosphère (par exemple, des satellites ne fonctionnant plus ou ayant quitté leur orbite) augmente la probabilité que, lors de l'envoi d'un nouveau satellite dans l'espace, celui-ci percute les déchets existants. Une nouvelle collision fait de nouveaux déchets et accentue le phénomène.

Dans les années à venir, on peut donc craindre un nombre croissant d'incidents de cette nature : la perte –momentanée ou définitive– de l'usage de certains réseaux de télécommunication par satellites.

2.2. Tempête de verglas au Canada : effondrement de réseaux en cascade à l'échelle nationale.

Le Canada a connu la plus grave tempête climatique de son histoire en janvier 1998. Par vagues successives, des pluies verglaçantes se sont abattues sur plusieurs centaines de kilomètres, paralysant 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 alimentaient Montréal ont été coupées et plus de trois millions de canadiens privés d'électricité au plus fort de la crise. 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 (avec des températures de l'ordre de –25°C).

Aucun scénario de catastrophe n'avait prévu un événement de cette ampleur. Statistiquement, ce risque était considéré nul. Car la tempête de verglas de janvier 1998 au Québec n'a pas été une simple panne de grande ampleur, ce fut l'effondrement d'un réseau tout entier. Pire encore, par un effet de cascade dans les réseaux, de grands réseaux critiques nécessaires au bon fonctionnement de toute l'activité de la région ont du stopper leur activité (700 communes ont été touchées), un sinistre à grande échelle :

- le réseau électrique a été mis hors d'état ;

[10] 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

- 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~~ demander l'aide de l'armée américaine et a été sur le point de demander une aide logistique à la Russie.

Outre les vulnérabilités propres à chacun des réseaux, et des dégâts avoisinant les 3 milliards de dollars, cet épisode a révélé de nouvelles vulnérabilités liées à une interconnexion croissante de réseaux complexes les rendant interdépendants, et la dépendance exclusive des populations à l'énergie électrique.

De l'avis de tous, la compagnie *Hydro-Québec* a répondu avec efficacité à cette situation soudaine en assumant publiquement sa responsabilité sociale d'entreprise en situation de monopole, en faisant état quotidiennement de son engagement dans la crise et en communiquant –par la voie de son PDG– sur les avancées effectuées par ses équipes. Un mois après ce sinistre à grande échelle, une grande part du réseau était en état de fonctionnement. L'implication des citoyens, très ancrée dans la culture nord-américaine, a tout autant contribué à une gestion efficace, par l'auto-organisation locale et régionale, et permis d'éviter le pire.
Un tel événement devait impérativement faire l'objet d'une analyse approfondie *a posteriori* afin de tirer des leçons d'une telle catastrophe à l'échelle du pays et, nous le verrons plus bas, pour constituer une base de réflexion pour d'autres entreprises.

Quelques mois seulement après l'événement, le Gouvernement a alors 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 "[11] qui a été dotée de moyens conséquents (budget de fonctionnement de 7 millions de dollars).
Le mandat de la Commission s'est articulé autour de trois axes principaux : le phénomène naturel en lui-même, les raisons de l'interruption des approvisionnements en électricité, et le dysfonctionnement de certaines des infrastructures avec les impacts pour les citoyens et les

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] Commission Nicolet (1999), *Rapport de la Commission Scientifique et technique sur la crise du verglas de janvier 1998* , 5 volumes, Publications du Québec, Montréal : Commission Nicolet.

entreprises (études économiques, assurance, programmes d'indemnisation, responsabilités, etc.).

Ce travail a permis de formuler près de 500 avis, conclusions, et recommandations, dans la perspective que le Québec soit mieux préparé pour faire face à un prochain sinistre. Ils s'articulent essentiellement autour de deux thèmes principaux :

- 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 ;
- adopter et mettre en œuvre 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 face à des vulnérabilités d'ampleur nouvelle.*

Une partie importante du rapport est consacrée aux réformes et initiatives que devrait véhiculer une telle politique (et qu'il ne s'agit bien évidemment pas de discuter ici).

Et c'est là une des leçons essentielles de cette « crise du verglas » : à travers une consultation approfondie au niveau local, national et international, permettre de cicatriser les impacts physiques et psychologiques dus à la catastrophe ; cela par l'adoption de mesures concrètes suivant les recommandations d'une commission d'évaluation autonome scientifiquement et financièrement[12].

Notons enfin que la crise du verglas dépassait tous les scénarios de catastrophes imaginées par Hydro-Québec et les services de sécurité du pays avant l'événement. En ce sens, ils n'étaient pas « préparés » à affronter spécifiquement cette tempête. Il s'agissait certainement plus d'une préparation de fait à affronter des situations imprévues, plus ancrée en Amérique du Nord qu'elle ne peut l'être en Europe et cela depuis les comportements des citoyens jusqu'au plus haut niveau de direction. La responsabilité collective face à un événement extrême fut déterminante dans l'issue de cet épisode qui demeure encore marquée, après cinq ans, dans l'esprit de tous les Québécois.

2.3. Actes terroristes : nouvelle potentialité avérée de sinistres à grande échelle

Nous le soulignions en introduction, les scénarios actuellement analysés en matière de terrorisme envisagent des niveaux d'attaques extrêmes. En cela, ils vont bien au-delà du

terrorisme « traditionnel » (colis piégés par exemple), au delà d'attentats ponctuels qui n'en sont pas moins dramatiques qu'ils touchent un nombre plus limité de victimes[13]. En effet, on assiste depuis plusieurs années à une montée des potentialités d'actes de terrorisme (organisation de réseaux terroristes nationaux et internationaux). Comme nous avons pu le constater avec les attentats du 11 septembre mais aussi lors l'explosion de l'usine AZF de Toulouse, ces potentialités ne sont plus le fruit de penseurs à l'imagination débordante, mais sont devenus bien réelles. D'autant qu'au travers des médias, ne sont relatés que les événements qui ont effectivement eu lieu et non pas ceux qui furent évités. Le seul fait que nous ayons été incapables pendant plusieurs mois de savoir si l'explosion d'AZF était un accident ou un acte volontaire illustre assez bien la pauvreté de nos connaissances actuelles face à ce type de vulnérabilités ; cela nécessite, de fait, des interrogations fortes pour l'ensemble des infrastructures vitales d'un pays.

Le terrorisme n'est pas cependant un risque nouveau puisque depuis trente ans, des milliers de personnes ont été tuées ou blessées dans le monde, victimes d'actes de terrorisme[14]. La conférence « Terrorisme et responsabilité pénale internationale », organisée par l'association SOS Attentats, qui s'est tenue en février 2002 à l'Assemblée Nationale (Paris), témoigne de cette évolution. Un des enseignements fondamentaux de cette manifestation est la nécessité d'une coopération internationale sur ces questions, qui devient d'autant plus impérative que le développement de réseaux terroristes de toute sorte s'est considérablement accéléré ces récentes années[15]. Fondée sur cette réalité, toute analyse de prospective, même optimiste, fait craindre la recrudescence de nouvelles formes d'actes de terrorisme.
Or, les cibles ne sont plus seulement des bâtiments gouvernementaux, mais peuvent tout aussi bien être des entreprises représentant les intérêts économiques du pays à déstabiliser. Les attentats perpétrés au Pakistan (Karachi) le 09 mai 2002 contre des employés français de la direction des constructions navales qui ont tué 14 personnes dont 12 français, ainsi que la

[12] P. Lagadec et E. Michel-Kerjan (2000), « D'un continent à l'autre », Journal *Le Monde*, mardi 11 janvier.
[13] En France, l'association SOS Attentats est particulièrement active pour la reconnaissance des victimes d'actes de terrorisme : SOS Attentats, Hotel National des Invalides, escalier K, corridor de Metz, 75700 Paris Cedex 07 SP – www.sos-attentats.org ; voir notamment F. Rudetski (2002), « Terrorisme. La primauté du droit, pour les victimes », dans X. Guilhou et P Lagadec (2002), *La fin du risque zéro*. Paris, Eyrolles Société.
[14] T. Vareilles (2001), *Encyclopédie du terrorisme international*. Paris, Editions l'Harmattan, coll. 'culture du renseignement'.
[15] Assemblée Nationale, (2002), *Livre noir. Contributions à la conférence internationale « Terrorisme et responsabilité pénale internationale »,* Paris.

forme de ces actes (opération suicide), témoignent d'une évolution certaines de ces risques dont on sait aujourd'hui qu'ils peuvent tout aussi bien frapper à une très grande échelle[16].

Pour ce qui a trait aux vulnérabilités des grands réseaux vitaux, nous devons aujourd'hui considérer les potentialités d'atteinte aux infrastructures vitales d'un pays en changeant radicalement de référentiel. Cela est non seulement vrai parce que l'ampleur des événements du 11 septembre 2001 révèle une capacité à toucher des zones particulièrement peuplées et à forte concentration de biens, mais aussi parce qu'elle témoigne d'une volonté délibérée de frapper à une toute autre échelle.

La forme de telles attaques pourra bien différer à l'avenir. Par exemple, l'introduction de gaz toxique dans les circuits d'air conditionné d'immeubles de grande hauteur constitue un scénario probable. A une échelle bien plus large, tout opérateur de réseau d'alimentation d'eau potable n'est pas à l'abri de devoir gérer une crise aiguë : l'utilisation de son réseau à des fins d'intoxication à grande échelle par l'introduction de bactéries (le cas de l'anthrax illustre bien la paralysie immédiate de tout un réseau) ou, pire encore, de virus. La pollution du réseau de distribution d'eau par un agent pathogène hautement toxique, voire mortel, paraît bien plus simple à réaliser que le détournement simultané de trois avions de ligne privés. Et il ne s'agit évidemment pas de poster à un gardien à tous les endroits susceptibles d'être attaqués : cela est économiquement impossible.

Les opérateurs doivent néanmoins impérativement se préparer à de tels scénarios, par de la réflexion stratégique sur ces questions nouvelles et la formation de leurs équipes, du plus haut niveau de la hiérarchie (en cas de crise, les médias –et plus tard les juges– interrogeront immédiatement le PDG de la compagnie touchée pour connaître son degré de préparation à ce type d'événement que « nul ne pouvait plus ignorer après le 11 septembre »~~)~~ jusqu'aux ouvriers qui travaillent chaque jour sur le réseau.

Il est impératif de développer une culture du risque qui ne relève plus seulement des bonnes vieilles procédures de sécurité – totalement inadéquates pour ce type de risques catastrophiques – mais bien une attention et une préparation, assumée collectivement, pour limiter une utilisation malveillante du réseau pouvant conduire à de véritables catastrophes

[16] Les attaques bio-terroristes ne sont pas à exclure des scénarios liés aux nouvelles vulnérabilités. Or, le degré de préparation pour gérer de telles attaques est bien pauvre. Aux Etats-Unis, une étude récente a analysé le degré de préparation de plus de 200 services d'urgence (cliniques, hôpitaux, pompiers, …) à des scénarios d'attaque bioterroriste de faible taille et, qui plus est, locale. A la question « disposez-vous d'un plan d'urgence et l'avez-vous expérimenté ces deux dernières années », à peine 7% de ces services ont répondu –sous la base de déclaration volontaire- par l'affirmative. Voir R. Fricker, J. Jacobson et L. Davis (2002), « Measuring and

humaines et financières. Nous l'avons déjà mentionné, il ne s'agit plus de faire face à des risques majeurs locaux, mais bien à de véritables risques à grande échelle. Ce changement radical d'échelle par rapport à une culture de la sécurité « traditionnelle » nécessite, pour y faire face, d'adapter les solutions connues et d'inventer de nouvelles procédures.

3. Spécificités de ces risques à grande échelle

Quelles caractéristiques communes, quelle régularité, ces différents cas de sinistres à grande échelle touchant ou utilisant les réseaux vitaux présentent-ils? Il semble bien que nous soyons face à des risques et sinistres de grande ampleur, assez confus à cerner dans leur ensemble, et dont la gestion se révèle très complexe : des risques inédits qui rendent inefficaces les approches classiques relevant d'un traitement local de la sécurité.

3.1. Effets domino : des niveaux de sinistres qui explosent.

Une des caractéristiques des sinistres en question est " l'effet de cascade " auquel nous assistons le plus souvent, qui peut être interne ou externe.

Il est interne à l'organisation lorsque l'événement déclencheur se diffuse au travers du réseau pour atteindre un nombre plus important de victimes utilisatrices de ce réseau. C'est l'*effet de diffusion interne*.

Il peut également être externe : l'évolution actuelle vers une hyper connexion des réseaux contribue à augmenter le pouvoir de diffusion du sinistre au travers d'autres réseaux, avec un effet boule de neige. Supposons un instant que la probabilité d'un sinistre soit connue. Une courbe de *niveau de risques* peut être définie comme l'ensemble des scénarios associés au même niveau (produit d'un montant de pertes et d'une probabilité d'occurrence) de pertes espérées.

A cause de l'interdépendance entre réseaux, en plus de la probabilité de défaillance interne au réseau lui-même, il faut aussi tenir compte de celle d'être touché par un effet indirect de diffusion provenant d'autres réseaux sinistrés. Ainsi, l'interdépendance des réseaux augmente significativement les niveaux de risque[17]. Or, peu d'analyses tiennent compte de ces pertes

---

Evaluating Local Preparedness for a Chemical or Biological Terrorist Attack », Issue Paper, Publication de la *Rand Corporation*. Une telle étude n'existe pas en France.

[17] 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

provoquées par des défaillances extérieures[18]. Le plus souvent on s'en tient aux défaillances interne ou aux effets de la nature sur le dit réseau.

3.2. Limite de l'approche probabiliste

Comme nous l'avons montré plus haut, les sources de vulnérabilité se sont diversifiées et la nature même du risque à appréhender (et à réduire) est devenue plus confuse encore.

Nous disposons pour certains risques bien connus de données historiques et de données scientifiques –comme les tremblements de terre ou certains risques industriels majeurs– pour les traiter.

Il est ainsi possible de tracer des courbes de niveau de risques de type (pertes ; probabilité associée). L'espérance des pertes se calcule alors comme le produit de ces deux nombres qui caractérisent un événement particulier de type « la probabilité qu'un événement E occasionne des pertes d'un montant L_1 sur une période de temps donnée est p_1 » (figure 1 ci-dessous).

Cela constitue l'approche « traditionnelle » utilisée par les gestionnaires de risques.

Un premier élément d'incertitude doit être considéré lorsqu'il n'est pas véritablement possible de déterminer la probabilité (*p1* ou *p2 ?*), le niveau de pertes (L_1 ou L_2 ?) ou, bien sur, les deux à la fois : laquelle des deux courbes de niveau de risques est pertinente (C_1 ou C_2 sur la figure 1) ? Les politiques de gestion de risques et le type d'investissements humains et financiers peuvent alors grandement varier. Aussi, les probabilités d'atteinte sérieuse n'ont-elles, dans ce cas, pas vraiment de fondements statistiques. Le plus souvent, cette probabilité est incertaine. Le risque existe bien, mais il est impossible de fournir une distribution de probabilités sérieuse. Nous sommes dans une situation que les économistes qualifient d'*incertitude radicale*[19] ou d'*ignorance*.

---

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). L'espérance des pertes égale $2p(1-p)(2L) + p^2(2L)$, soit $2Lp[2-p] > 2Lp$.

Pour une analyse de cette question, voir aussi H. Kunreuther et G. Heal (2002), « Interdependent Security: The Case of Identical Agents », Working paper, The Wharton School, Center for Risk Management, Philadelphie.

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

[19] 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. Dans ce dernier cas, on parle d'*incertitude radicale*.

Pour beaucoup des nouveaux risques discutés dans cet article, nous faisons face à ces situations d'incertitude radicale. Quelle est la probabilité qu'une tempête plus puissante encore que celles de 1999 se produise cette année en France ? Quelle est la probabilité qu'un groupuscule malveillant déverse un virus dans le circuit d'alimentation en eau d'une grande capitale européenne dans les six mois à venir ? Quelle probabilité aurions-nous pu, avant le 11 septembre 2001, attribuer à un scénario dans lequel on détournerait simultanément trois avions de lignes privées pour les faire s'écraser de la manière que l'on connaît ? Certainement « zéro », au sens statistique du terme.

Ainsi, vouloir proposer des études de risques fondées sur des distributions de probabilités paraît un argument peu convainquant pour traiter ces questions. Le faire est simplement se tromper d'outil.

Quelle démarche adopter alors ? A défaut de quantifier le risque par une distribution de probabilités, on peut, dans un premier temps, caractériser des scénarios particulièrement sévères et impliquant pour l'entreprise ou l'organisation considérée. Il est alors plus aisé de comprendre les impacts éventuels de tels scénarios et de tester le degré de préparation à faire face aux vulnérabilités qui émergent. Une telle démarche est en particulier utilisée pour des scénarios susceptibles, s'ils se réalisaient, de conduire à la faillite de la compagnie (au-delà d'un plafond L_{max} ; rectangle d'incertitude F dans la figure 1). Ecarter un scénario sous prétexte qu'il paraît aberrant (et donc associé à une probabilité infime), ne saurait ici être pertinent dans la définition de la stratégie de l'entreprise, car il est bien connu que l'« on ne meurt jamais qu'une fois »[20].

[20] Voir H. Kunreuther et G. Heal (2002), « A Firm Can Only Bankrupt Once. Risk Management Strategies in an Uncertain World », article présenté lors de la conférence *Organizational Encouters with Risk* organisée par la London School of Economics.

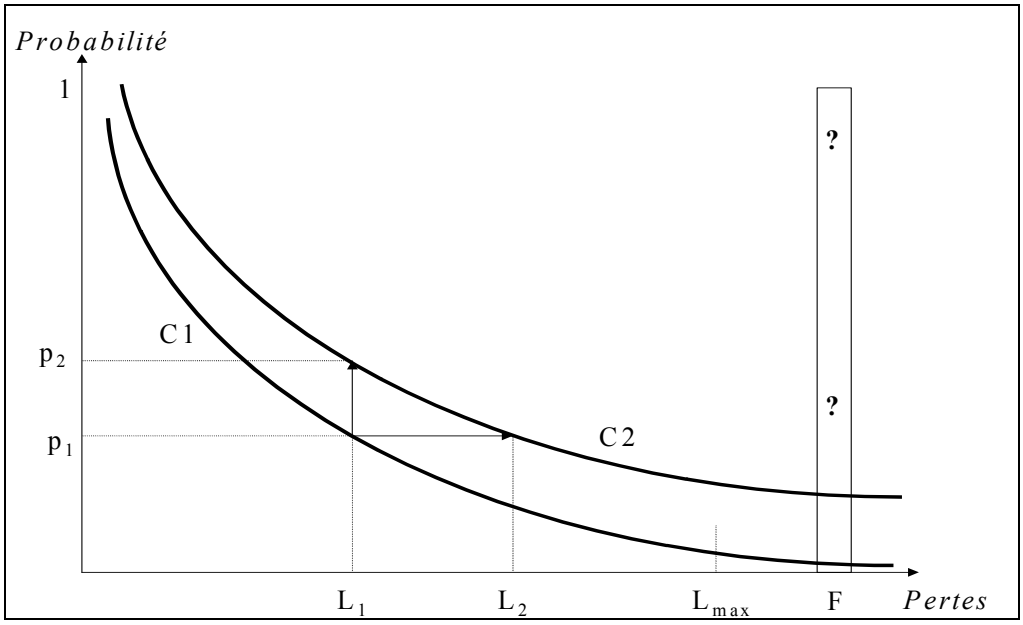

Figure 1. Incertitude et incertitude radicale.

4. Quelques pistes à étudier.

4.1. Au cœur de la crise : gérer en temps réel

Un élément est trop souvent absent des travaux théoriques portant sur la gestion des risques majeurs et des crises : le stress des décideurs. La gestion en temps réel de tels sinistres est particulièrement stressante pour celles et ceux qui doivent la piloter. Ce fait constitue un élément fondamental pour expliquer, en partie du moins, une possible déstabilisation des équipes dirigeantes qui doivent affronter ce type de situations. Cette déstabilisation peut, suivant les cas, se traduire de différentes manières ; pour n'en citer que quelques unes : prise de décisions qui apparaîtront, *ex post*, tout à fait irrationnelles ; non-dits permanents ; effet de réseaux[21] ; absence totale de communication ; refus de ses responsabilités ; refus de l'événement en lui-même (« ce n'est rien, ça passera bien ») ; sentiment d'invisibilité ou au contraire de profond désarroi.

Or, en période de crise, les décideurs seront jugés, précisément, sur leurs capacités à gérer, quasiment en temps réel, un sinistre en propagation qui touche simultanément tout un ensemble de réseaux. Dans de telles circonstances, la question centrale ne sera plus alors

[21] On ne fait confiance qu'aux personnes du même département, de la même formation, de la même écoles, du même niveau hiérarchique, …etc.

seulement de remettre en état de fonctionnement une portion de son réseau, mais bien de jongler avec tous les systèmes dont peut dépendre ou faire dépendre le bon fonctionnement de celui-ci. Le nombre d'interlocuteurs à considérer sera multiplié en conséquence et la demande de remettre en état l'ensemble du réseau dans un délai très court d'autant plus pesante. Il sera demandé aux dirigeants d'assumer leurs responsabilités, de prendre des décisions cruciales alors même qu'ils ne disposent que de très peu d'éléments –vérifiables– sur lesquels ils peuvent s'appuyer. Ils devront aussi faire face aux différents médias – qui pourront être tentés de prendre immédiatement le parti des sinistrés – dont l'action peut être décisive en temps de crise. Ces univers sont des univers de stress profond.

Une telle capacité de réaction ne s'improvise pas –bien que l'argument de type « si cela arrive, on saura bien faire face »– soit souvent de mise. Les spécialistes travaillant sur cette problématique des risques émergents, tout comme les personnes et les institutions (au sens large) qui y ont été confrontées, savent que gérer ce type de sinistres est un art difficile, qui nécessite de s'y être préparé.

Les entreprises et les organisations non préparées devront expérimenter en pleine crise : devant apprendre à gérer des sinistres inédits, elles courent de manière certaine au fiasco, pouvant entraîner avec elles celles qui ne s'y étaient préparées que de manière superficielle ou inadaptée[22].

4.2. Une nécessité urgente d'apprentissage

Et il est possible d'apprendre sur ces risques. Des éléments de réponse importants peuvent être assimilés lors de retour d'expérience sur certains grands événements déstabilisant[23]. Ces retours d'expérience sur les grands épisodes d'atteinte des réseaux doivent devenir systématiques. Ils doivent être conduits non plus seulement en interne par chacune des entreprises touchées (lorsque de telles interrogations *ex post* peuvent être mises à l'ordre du jour : trop souvent la politique interne s'inscrit plutôt sur le thème « AZF, connais pas ! »), mais avec l'ensemble de la communauté, acteurs internes et externes. Ils devraient alors constituer une base solide pour appréhender, comprendre, et solutionner ces situations complexes : 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.

[22]Pour une analyse de plusieurs cas de crises aux Etats-Unis, voir notamment *Harvard Business Review on Crisis Management* (1996) ; Cambridge, MA: Harvard University Press.
[23] Voir P. Lagadec (2000), *Ruptures* créatrices. Paris : Editions d'Organisation.

Un exemple. Après la tempête de verglas au Canada, une mission a été mise sur pied avec certains dirigeants d'EDF pour rencontrer leurs homologues québécois qui avaient du gérer cette crise. Bien sur, il ne s'agissait pas de préparer l'entreprise française à faire face à une telle tempête de verglas, mais bien de comprendre les principales difficultés à traiter efficacement de telles catastrophes ; en d'autres termes, se préparer à affronter l'imprévisible.
EDF a pu ainsi ramener les éléments clés qui furent très largement appliqués pour gérer les conséquences des tempêtes de décembre 1999. Nous pouvons en citer ici quelques-uns qui furent, et c'est là l'essentiel, intégrés dès le début de la gestion des tempêtes comme éléments fondamentaux à respecter :

- reconnaissance officielle et en interne de l'ampleur du sinistre ;
- élaboration d'une stratégie de gestion du sinistre à l'échelle nationale ;
- coopération internationale immédiate ;
- reprise de contact avec les retraités pour qu'ils apportent leur savoir-faire ;
- interaction avec les médias locaux et nationaux ;
- information donnée publiquement quant aux progressions effectuées sur le terrain par les équipes ;
- implication auprès des populations civiles (privées de courant en pleine période de fêtes de fin d'année).

Ce type de stratégie dans la gestion d'un sinistre de l'ampleur des tempêtes que nous avons connues témoigne d'un apprentissage des équipes dirigeantes, d'une volonté de comprendre –avant qu'ils ne se réalisent– des phénomènes inédits qui sortent des scénarios d'école, mais surtout, d'une politique interne affirmée de mettre en place une stratégie globale à une échelle comparable aux risques encourus.
De l'avis de tous, EDF a donc bien géré la crise. D'autres entreprises de réseaux, sans doute moins préparées, n'ont pas eu la même chance.

4.3. Anticiper sur les vulnérabilités à venir

Néanmoins, devrons-nous toujours attendre qu'un nombre « suffisant » de catastrophes soient survenues pour entamer des démarches d'apprentissage collectif sur ces questions ?
A cet égard, nous pouvons souligner ici l'initiative américaine mise en place par le Président Clinton en 1997. La création d'une commission spéciale, la *President's Commission on Critical Infrastruture Protection,* qui s'inscrit dans une volonté affirmée de développer une politique de protection des infrastructures constituant le support de vie du pays. L'objectif

premier de cette commission était de déterminer les principales vulnérabilités auxquels les grands réseaux d'infrastructures américains pourraient être confrontés à l'avenir.
Il s'agissait donc bien d'une initiative de réflexion prospective.
Le rapport intitulé *Critical Foundation: Protecting Americans' Infrastructures,* publié en 1997 s'inscrit dans cette voie[24]. Il ne s'agit pas ici de reprendre ce rapport final d'un travail de quinze mois regroupant, sur l'ensemble du pays, des équipes de spécialistes des secteurs public et privé. Ce qui importe plus est l'existence même d'une telle initiative.
Ces travaux mirent notamment en avant une dépendance aux réseaux croissante, qui constitue la source de nouvelles vulnérabilités sur lesquelles la Commission présidentielle américaine a focalisé son attention : menaces d'origine naturelle d'une part, menaces intentionnelles pour paralyser un secteur d'activité déterminé de l'autre.
Or, comme la plupart de ces grands réseaux sont possédés et opérés par le secteur privé, il convient de définir des responsabilités partagées entre ce secteur et le secteur public, de manière à assurer la continuité de l'activité économique. Comme le soulignait déjà Robert Marsh, président de la Commission, « la seule voie véritablement efficace pour cela est la mise en place de réels partenariats entre les propriétaires de réseaux, leurs opérateurs et les organes gouvernementaux. Seuls des systèmes prenant appui sur les capacités et la connaissance des deux secteurs pourront permettre de mieux mesurer nos vulnérabilités, et de les diminuer significativement ».[25]

A ce jour, et à ma connaissance, cette étude –effectuée en collaboration avec les acteurs privés et qui s'inscrivait par anticipation et souci de prospective– demeure unique au monde. Suite aux événements du 11 septembre 2001, ces travaux prennent une importance plus capitale encore.

5. Conclusion

La plupart des cas et des scénarios de risques émergents étudiés à ce jour par les équipes les plus avancées sur ces sujets au niveau national et international présentent, au-delà de ce qui a été discuté plus haut, une caractéristique commune tout à fait fondamentale. Qu'il s'agisse de catastrophe naturelle d'une ampleur nouvelle ou d'acte de malveillance à grande échelle,

[24] Les informations sur la Commission et le rapport sont disponibles sur www.pccip.gov.
[25] La création en 1999 du *Critical Infrastructure Assurance Office*, qui a notamment pour mission l'étude des scénarios pouvant conduire à l'atteinte des grands réseaux vitaux américains, constitue une première réponse ciblée ; ce bureau est doté d'un budget de fonctionnement annuel de 5 millions de dollars.

l'événement n'apparaîtra pas progressivement : il ne laissera pas aux organisations le temps nécessaire pour changer de vitesse de fonctionnement. Le facteur temps est déterminant car il engendre une profonde déstabilisation, à laquelle s'ajoute un changement radical dans le rythme de gestion et dans l'échelle des enjeux mis en cause. A l'image de la foudre qui s'abat, les nouvelles vulnérabilités se concrétisent ponctuellement, soudainement. En quelques jours seulement, toute l'organisation peut être profondément déstabilisée, ses dirigeants mis en cause, quand ce n'est pas tout un pan d'activités. Les séquelles de telles expériences perdurent souvent très longtemps au sein des organisations qui ont eu à les gérer alors qu'elles n'y étaient pas préparées ; les pertes humaines et financières pouvant être catastrophiques.

Sur un plan plus académique, ces sujets sont difficiles à appréhender car, d'une part, ils se situent à la croisée de plusieurs disciplines et, de l'autre, parce que les approches théoriques traditionnelles de modélisation mathématique s'appliquent assez mal.

Néanmoins, nous avons montré tout au long de cet article qu'il est possible d'apprendre sur ces sujets. Dans certains pays anglo-saxons, ils sont intégrés, depuis plus de 20 ans parfois, au cœur de la formation continue et initiale des décideurs et des futurs dirigeants. Or, en France, les formations d'enseignement supérieur dispensées sur ces questions demeurent encore exceptionnelles. Le thème retenu pour le seizième congrès de la Conférence des Grandes Ecoles qui s'est tenu en octobre 2002 était, précisément, « Systèmes et risques : Quelles nouvelles approches pédagogiques pour les Grandes Ecoles ? ».
Un premier pas, assurément.