Interconnexion

Comment **protéger** nos grands réseaux vitaux ?

Le 4 novembre 2006, l'Europe passait à côté d'une panne électrique de grande ampleur. Électricité, gaz, Internet, communications, approvisionnement, finances : nos sociétés sont menacées par l'écroulement en chaîne de réseaux vitaux. Il est temps de s'en soucier.

Patrick Lagadec est directeur de recherche à l'École polytechnique, et membre de l'Académie des technologies de France.

Erwann Michel-Kerjan est Managing Director du Center du Risk Management and Decision Processes Center à la Wharton Business School (États-Unis), et chercheur associé à l'École polytechnique.
erwannmk@Wharton.upenn.edu

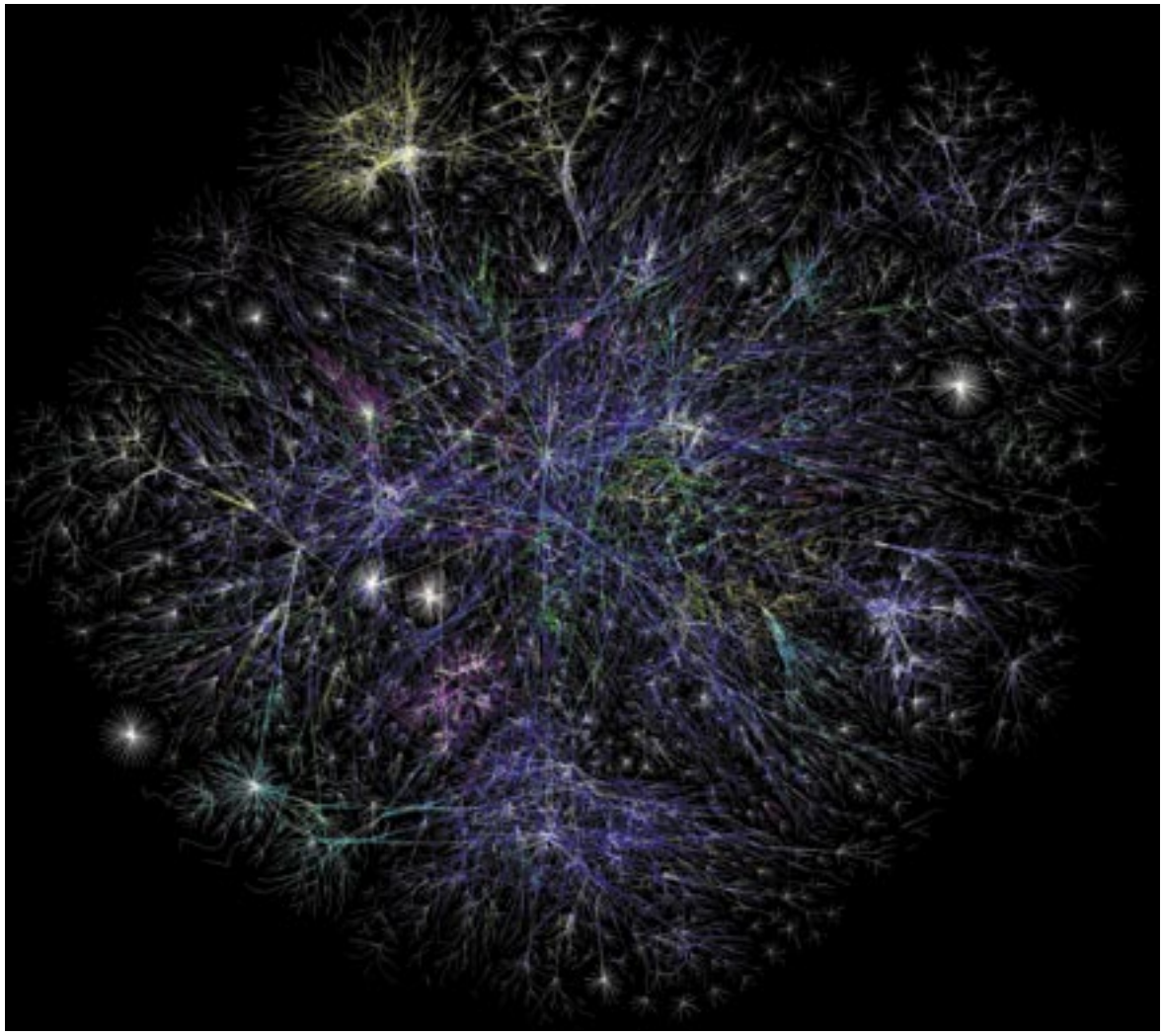
Le nouveau siècle ouvre sur des univers de vulnérabilités en rupture profonde avec ceux du passé. Les risques sont aujourd'hui globaux et interdépendants, les dynamiques de crise sortent de leur lit [1]. L'un des facteurs structurants de cette mutation est le développement des grandes « infrastructures critiques » : un ensemble enchevêtré de grands réseaux – physiques, virtuels et financiers – devenus l'armature indispensable au fonctionnement de nos sociétés. Pour mémoire, citons quelques-unes des crises majeures survenues ces dernières années.

Entre le 5 et le 8 janvier 1998, le Québec connaît une « tempête de glace » historique. Près de 3 000 kilomètres de lignes à très haute tension sont détruites. Les effets en chaîne sont inédits, avec un début d'effondrement par plaques des réseaux vitaux de Montréal et de sa région, tous dépendants de l'électricité : eau potable, transport, essence, télécommunications, banques, etc.

Le 14 août 2003, toute la façade est du continent nord-américain sombre dans le noir. Ce black-out, qui touche 50 millions de personnes, entraîne une cascade de défaillances à grande échelle – notamment des perturbations du trafic aérien jusqu'en Californie. Le mois suivant, l'Italie est à son tour plongée dans le noir. Plus près de nous, le 4 novembre 2006, à la suite d'un dysfonctionnement en Allemagne, c'est l'Europe qui passe très près du noir total. Une catastrophe évitée de peu, dont les conséquences sont encore peu évaluées.

Le 11 septembre 2001, l'attaque est opérée *via* le détournement du réseau commercial aérien, qu'il faut stopper en catastrophe pendant vingt-quatre heures sur l'ensemble du territoire américain. Une première dans l'histoire du pays ! Quelques semaines plus tard, les attaques à l'anthrax confirment ce nouveau potentiel des ris-

Interconnexion



© THE OPTE PROJECT

15 JANVIER 2005. VISUALISATION DES CONNEXIONS SUR INTERNET. La toile est devenue essentielle au fonctionnement de nos sociétés. La dépendance s'en est suivie. Quand le satellite *Galaxy IV* connut une panne le 20 mai 1998, 80 % des « pagers » aux États-Unis furent bloqués, rendant les systèmes sourds et aveugles dans de nombreux secteurs sensibles. De même, en Asie, lors de la dernière grande panne de décembre 2006.

ques associés aux réseaux : quelques lettres contaminées au départ, des systèmes de tri industriels qui pouvaient généraliser la contamination, et des centaines de millions d'envois sont devenus suspects, avec le spectre d'un blocage à grande échelle des flux postaux de nombreux pays. En 2003, l'alerte mondiale au SRAS fait trembler la ville de Toronto après avoir fait vaciller Hongkong. Voici l'alliance de la maladie émergente et du jet – les épidémies se propagent à la vitesse du transport aérien. Le H5N1 s'inscrirait sur ce même terrain de jeu, en faisant plein usage des meilleurs hubs mondiaux. Sur maints registres, ces événements ont en commun des franchissements de seuils. On peut en identifier au moins six.

La complexité : la combinaison d'un nombre incalculable d'effets dominos génère un tableau qui n'offre plus aucune prise à un traitement séquentiel des problèmes, entreprise par entreprise, pays par pays. L'interdépendance des phénomènes est le maître mot.

L'échelle : des défaillances, des destructions ou des utilisations malveillantes des réseaux peuvent affecter des continents, voire la planète. Les capacités de réaction n'ont pas encore été repensées à cette nouvelle échelle.

La vitesse : la propagation du risque ou du sinistre ne se mesure plus en mois, mais en heures, voire en minutes ou en secondes – 42 secondes dans le black-out du 14 août 2003 aux États-Unis. Et cela serait exacerbé en cas de blocage des systèmes d'information [2]. Devant de pareilles vitesses, organisations et décideurs se trouvent tétanisés.

L'ignorance : le temps et la qualité de réaction sont d'autant plus problématiques que facteurs de risques nouveaux (prion, SRAS, H5N1) et systèmes de plus en plus enchevêtrés se combinent aux réactions vite illisibles. Là encore, ignorance scientifique et managériale mènent à la paralysie.

La contagion : les chocs affectent des ensembles économiques et sociaux de plus en plus réactifs, prompts à amplifier et à généraliser toute perturbation. Les hypermarchés, par exemple, ne disposent souvent que d'une journée de stock de nourriture, et dépendent des ▷

[1] P. Lagadec et E. Michel-Kerjan, « A New Era Calls for a New Model », *International Herald Tribune* 1er novembre 2005; P. Lagadec, dans R. Dynes *et al.*, *Handbook of Disaster Research, Springer,* octobre 2006.

Interconnexion

▷ systèmes de transport ; nombre d'activités ne peuvent opérer sans électricité ; la plupart ne sauraient fonctionner en mode dégradé, notamment sans informatique.

Les coûts : au-delà des montants de pertes, qui se chiffrent désormais en dizaines de milliards d'euros, voire davantage, la stabilité même des grands réseaux financiers est aujourd'hui en jeu. Parmi les vingt catastrophes les plus coûteuses pour l'assurance entre 1970 et 2005, dix sont survenues depuis 2001, ce qui oblige aujourd'hui le secteur de l'assurance à de profondes transformations.

Effet paralysant

Si l'on ne prend pas la mesure de ces sauts, on court le risque de se fracasser à nouveau sur les réalités qui sont désormais les nôtres. Ce fut le fiasco de Katrina.

La Nouvelle-Orléans (29 août 2005) : le monde, sidéré, a regardé des jours durant une ville américaine installée dans le chaos. On ne sut pas comment réagir devant cette combinaison nouvelle : ouragan, montée des eaux, destruction des digues, accidents industriels, pulvérisation des instances publiques, violences urbaines. Près de 90 % des réseaux vitaux locaux ont été détruits en moins de trois heures. La perte d'énergie électrique a bloqué le fonctionnement de tous les autres réseaux ; celle des moyens de communication a paralysé les dispositifs d'intervention, également bloqués par le manque de carburant, la perte du réseau de transport et les problèmes aigus de sécurité. L'ouragan a aussi détruit une grande partie des installations gazières et pétrolières du golfe du Mexique, avec des impacts durables à des milliers de kilomètres de là, sur les marchés énergétiques mondiaux ; New York était à deux jours de la panne de carburant… Katrina oblige tous les acteurs – et pas qu'américains – à reprendre le dossier des vulnérabilités à l'âge des événements dits « hors cadres » et des grands réseaux, devenus effectivement « vitaux ».

C'est aux États-Unis que le mouvement fut lancé par une initiative du président Clinton. La Commission présidentielle sur la protection des infrastructures critiques fut mise en place en 1996, pour étudier ces *« infrastructures d'importance nationale, dont la défaillance ou la destruction pourrait avoir un effet paralysant sur la défense ou l'économie des États-Unis »*. Parmi celles-ci : télécommunications, systèmes de production et de transport d'énergie électrique, stockage et transport du gaz et des carburants, système bancaire et financier, transport, approvisionnement en eau, secours et sécurité publique, et services essentiels à la continuité du gouvernement. Nombre d'entreprises, d'experts, et des gouvernements locaux, des États et du niveau fédéral travaillèrent de concert pendant quinze mois – et il ne faut pas sous-estimer cette mobilisation sur un sujet alors non répertorié et inquiétant.

Après Katrina, près de 90 % des réseaux vitaux ont été détruits en moins de trois heures

Le rapport final clarifia les enjeux nouveaux : *« La prolifération et l'intégration rapides des systèmes de télécommunication et des systèmes informatiques ont lié les infrastructures les unes aux autres pour parvenir à un réseau complexe d'interdépendances. Ces liens ont créé de nouvelles dimensions de vulnérabilités qui, quand elles sont combinées avec une constellation inédite de menaces, induisent des risques sans précédent pour la sécurité nationale. […] »* [3].

Le choc majeur survint avec les attaques terroristes du 11 septembre 2001. On créa alors le Department of Homeland Security (DHS), un superministère de l'Intérieur – doté d'une direction pour les infrastructures critiques. Quatre ans plus tard, Katrina démontra que l'on était bien loin du but.

En Europe, dix ans après les États-Unis (novembre 2005), et bien timidement, la Commission prit acte

[2] G. I. Rochlin, *Future IT Disasters, A Speculative Exploration, Communication, US/EU Crisis Management Conference*, 6-10 août 2003 ; G. I. Rochlin, *Trapped in the Net – The Unanticipated Consequences of Computerization*, Princeton University Press, 1998.

[3] President's Commission on Critical Infrastructure Protection, « Critical Foundations, Protecting America's Infrastructures », Washington D.C., 1998.

* La **résilience** caractérise les systèmes qui gèrent avec succès la complexité des situaions imprévues où les routines sont habituellement en échec.

1998

© ROBERT LABERGE/AFP PHOTO

CANADA. Après une tempête historique, 3 millions de personnes sont privées d'électricité.

2001

© JIM RUYMEN/REUTERS

ÉTATS-UNIS. Le 11 septembre, le réseau aérien est bloqué pendant vingt-quatre heures.

2001

© AFP PHOTO EPA KEYSTONE/FABRICE COFFRINI

SUISSE. Un bureau électoral quelques jours après l'alerte à l'anthrax.

de cette nouvelle donne, avec la publication d'une note de 28 pages. Intitulée *Livre vert : un programme européen de protection des infrastructures critiques* [4], cette note tente de cerner quelques principes pour dessiner la compétence européenne sur les infrastructures critiques.

Pour l'heure, et malgré une réelle prise de conscience, la réflexion en est encore à un stade très embryonnaire. Les rapports les plus récents confessent le plus souvent qu'ils visent avant tout à « poser les problèmes » [5].

Nouveaux chantiers

Certes, tous reconnaissent un besoin d'ajustement dans les secteurs clés : une sécurité aiguisée pour une meilleure prévention ; des efforts spécifiques pour accroître la résilience* à tous les niveaux. Mais il faut se garder des faux-semblants : il ne suffit pas de repérer quelques « points sensibles » à enfouir sous le béton et à protéger par quelque brigade militaire. Les logiques « Maginot » sont d'un autre âge. Modestement, à partir de notre expérience de terrain, nous proposons cinq nouveaux chantiers.

1. Construire une nouvelle grammaire des risques. Les nouveaux risques sont d'abord marqués par l'inédit, la surprise, la vitesse, la contagion en temps réel. En prévention, l'attention doit privilégier ce qui se passe aux marges, hors des écrans radars habituels. Grande leçon de Katrina : il faut aussi mettre les conditions de sortie de crise dans le champ de la prévention, et non comme étape ultime de la démarche de sécurité. Prévention, pilotage de crise, cicatrisation postcrise sont à prendre ensemble, dimensions indissociables de la nouvelle stratégie de sécurité. Qui n'a pas acquis pareilles grammaires sera instantanément dépassé par les risques et les crises désormais à l'ordre du jour.

2. Conduire une réflexion avec un grand nombre d'acteurs. On signalera sur ce point l'initiative « Seeds of Disaster, Roots of Response » qui fut lancée aux États-Unis dans le sillage d'un travail commandité fin 2001 par les trois présidents des académies américaines des sciences, d'engineering et de médecine, et qui vient de s'achever fin 2006 [6]. Objectif : confronter regards, analyses, modes d'action, pour créer une dynamique commune, transsectorielle. Dans ce but, au-delà du premier cercle fondateur, on fit travailler ensemble de grands centres universitaires, des think-tanks des milieux industriels et financiers et des instances gouvernementales. Ce travail a permis de reposer la question du « partenariat public-privé », toujours au cœur des discours, mais très loin de la réalité. Des contraintes majeures viennent singulièrement freiner ces partenariats, notamment, d'un côté, la concurrence exacerbée entre opérateurs et, de l'autre, du côté public, une culture des risques et des crises qui n'est pas encore en phase avec les enjeux tels qu'ils apparaissent aujourd'hui ainsi que des expertises et des budgets souvent limités. Au-delà, les risques devenant globaux, aucune entreprise, aucun pays ne peut plus prétendre les maîtriser seul. L'intégration du facteur « hors de nos frontières », ne sera pas sans poser des problèmes de gouvernance fondamentaux [7]..

3. Se préparer aux « cinquantièmes rugissants ». Plusieurs crises récentes ont montré que le problème n'est pas tant le choc initial de la catastrophe que la constatation par le plus grand nombre qu'il n'y a plus de pilotage, que les responsables ont une guerre de retard. Les dirigeants (dont les formations se concentrent encore trop sur le pilotage d'organisations en univers calme) risquent la paralysie, le discrédit immédiat, la mise en cause judiciaire. Très concrètement, plutôt que de multiplier les exercices techniques, l'urgence est d'organiser des exercices de pilotage sur scénario de haute surprise avec les présidents d'entreprise et les cabinets ▷

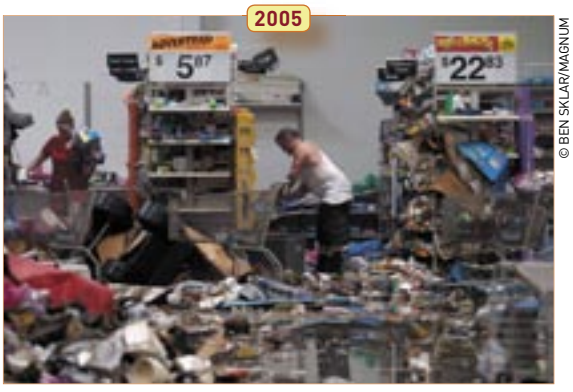
[4] Commission des communautés européennes, *Livre vert : un programme européen de protection des infrastructures critiques*, Bruxelles, 2005.
[5] « Managing and Reducing Social Vulneratilities from Coupled Critical Infrastructures », « White Paper of the International Risk Governance Council », Genève, oct. 2006.
[6] *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism.* The National Academies Press, Washington, DC, 2002.
[7] P. Auerswald *et al., Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability,* Cambridge University Press, 2006.

© RAY STUBBLEBIRE/REUTERS

ÉTATS-UNIS. Le 14 août, un black-out affecte 50 millions de personnes sur la côte est.

© XIN HUA/XIN HUAN PHOTO/CORBIS

CHINE. Le 22 avril, l'alerte au SRAS mobilise des employés du réseau ferroviaire.



© BEN SKLAR/MAGNUM

ÉTATS-UNIS. Après le passage de Katrina, le 29 août, chaos dans les centres urbains du Mississippi.

Interconnexion

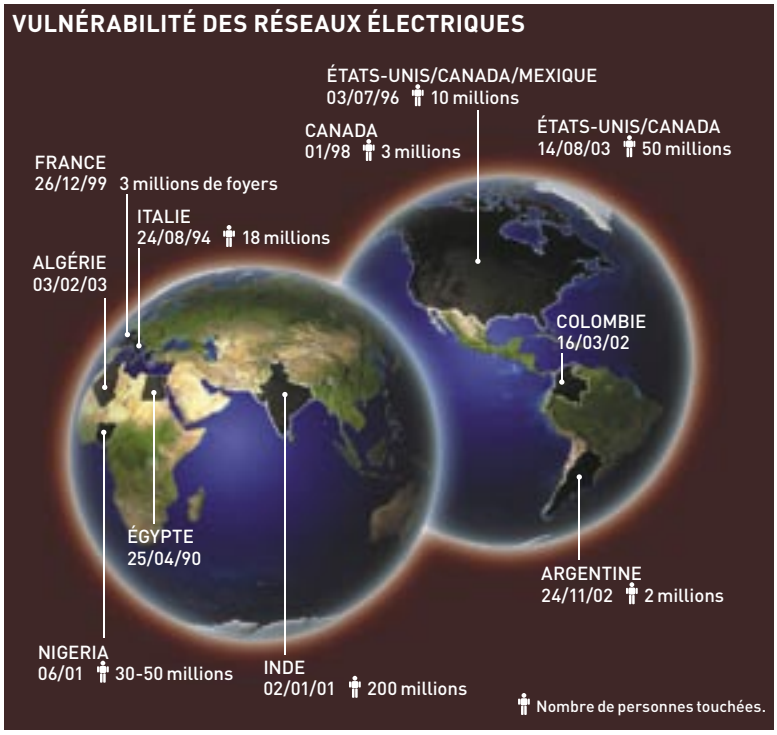


ILLUSTRATION : WWW.GREGCIRADE.COM

LES GRANDES PANNES ÉLECTRIQUES sont largement distribuées dans le monde. Celle du 4 novembre 2006, qui a touché l'Europe, n'est pas représentée.

▷ ministériels les plus essentiels d'un pays. En France, précisément, un Comité national des secteurs d'activité d'importance vitale, qui réunit notamment quinze présidents de grands réseaux, a été institué [8]. Il pourrait utilement travailler sur pareilles simulations. Et l'initiative devrait être immédiatement prolongée à l'échelle internationale, puis en direction de la société civile – qui sera au cœur des réponses en cas de crise sérieuse.

4. Tirer les leçons de tout événement hors cadre. À la suite de la crise de l'anthrax en 2001, le président de La Poste décida de lancer un retour d'expérience international, pour rassembler tous les enseignements de l'épisode – dix mois plus tard, vingt-cinq pays (Europe et États-Unis) se retrouvèrent à Paris pour partager constats et propositions, et créer une plat-forme commune d'alerte et de partage d'information [9].

Dans la même logique, à la suite des événements de 1998, au Québec, EDF envoya une équipe à Montréal pour recueillir les grands enseignements tirés par son homologue HydroQuébec. Et ces leçons furent directement utiles lors des grandes tempêtes de 1999 : on sut instantanément que l'on était sur des enjeux dépassant largement la seule question d'une panne électrique, que la réponse devait d'emblée être pensée et organisée à l'échelle mondiale, que la durée – plusieurs semaines parfois – serait une dimension capitale [10]. De même, plus récemment, la Direction du contrôle des risques d'EDF a organisé deux retours d'expérience : à Toronto sur la question du SRAS [11], à La Nouvelle-Orléans sur la gestion de l'ouragan Katrina [12] ; dans les deux cas pour mieux définir le niveau de réponse exigé si l'entreprise était confrontée à des turbulences non conventionnelles, type H5Nl.

5. Constituer des « forces de réflexion rapide ». En cas de situation hors cadre, l'essentiel est d'apporter aux décideurs quelques repères, ancrages, idées d'initiatives – créatrices de dynamiques positives. Nous proposons la création, auprès de tout dispositif de crise de grande entreprise ou institution (nationale ou internationale), de « forces de réflexion rapides ». Ces équipes réduites, composées d'acteurs de cultures diverses, sont préparées à réagir sur quatre fronts principaux : de quoi s'agit-il ? Quels sont les pièges majeurs ? Quelles sont les nouvelles cartes d'acteurs ? Quelles sont les quelques initiatives à prendre pour redonner au système une dynamique positive ? Pour l'heure, une première entreprise est entrée dans cette logique d'innovation : EDF – qui a déjà testé le dispositif en 2006 sur deux exercices (pandémie et accident nucléaire). Il reste à la développer dans de très nombreuses entités, privées et publiques, nationales et internationales.

Pour avancer sur ce dossier difficile, des pans entiers de recherche sont largement ouverts, dans un grand nombre de disciplines (science et technologie, économie et finance, gestion et administration publique, etc). Et des formations nouvelles sont à considérer d'urgence, à commencer pour les futurs dirigeants. ■

P.L et E.M.-K.

POUR EN SAVOIR PLUS

▷ Philip Auerswald *et al., Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, Sept. 2006.
Certains chapitres sont en ligne sur : www.seedsofdisaster.com

▷ Olivier Godard *et al., Traité des nouveaux risques. Précaution, Crise, Assurance*, Folio actuel, Gallimard, 2002.

▷ Patrick Lagadec et Xavier Guilhou, *La Fin du risque zéro*, Eyrolles Société-Les Echos Éditions, 2002.

[8] Arrêté du Premier ministre, 27 octobre 2006, dans le cadre du dispositif mis en place par le secrétariat général de la Défense nationale.

[9] P. Lagadec, dans « Anthrax and Beyond », *Journal of Contingencies and Crisis Management*, U. Rosenthal (dir.), *Special Issue, 11, n° 3*, 2003.

[10] M. Brugidou, *et al., Tempête sur le réseau – L'engagement des électriciens(nes) en 1999*, L'Harmattan, 2002.

[11] www.patricklagadec.net/fr/pdf/EDF_Pandemie_Grippe_Toronto.pdf

[12] www.patricklagadec.net/fr/pdf/EDF_Katrina_Rex_Faits_marquants.pdf