Quelles attitudes développer face aux vulnérabilités dues à l'informatique ?

Daniel Naulleau[1]

Summary: Information technologies lead to incidents that create new risks for people and the Society. Our liberties to work, to be informed, to travel, to comunicate, to buy, are affected. Citizens, companies, and the Society are concerned. Complexification, interconnection and centralization explain this vulnerability.
New behaviours have to be developed, at individual or national levels. A new vulnerability is growing. The french governement has not yet organized the necessary survey about this vulnerability of the country. Educational programs should included an awareness campaign about vulnerability. A survey has to be undertaken, and at the same time a large sensibilization of the whole population. Resistances do exist preventing an evolution of this situation.

Keywords: Vulnerability, IT, liberties, complexity, survey, education, awareness

Résumé :
Les TIC créent des situations qui génèrent des risques nouveaux pour les individus, les entreprises et la Société. Nos libertés de travailler, de s'informer, de circuler, de communiquer, d'acheter sont affectées. Des phénomènes de complexification, d'interconnexion et de centralisation expliquent le développement de la vulnérabilité.
Il faut développer de nouvelles attitudes au niveau des individus mais aussi des organisations. Une nouvelle vulnérabilité nous affecte sans que nous y prenions garde. L'Etat doit lancer un diagnostic et une réflexion générale sur cette vulnérabilité. Faire évoluer l'enseignement pour sensibiliser la population est nécessaire. Malheureusement il existe des freins dans la société pour faire évoluer ces perceptions et s'atteler au travail de diagnostic et de sensibilisation.

Mots Clés : Vulnérabilité, TIC, libertés, complexification, diagnostic, formation, sensibilisation

1 Daniel Naulleau, Université P&M Curie, Paris VI, UFR Informatique, 4 Place Jussieu 75005 Paris daniel.naulleau@upmc.fr

Les vulnérabilités des TIC sont nombreuses et leurs conséquences mal maîtrisées.

Dans la première partie nous présenterons brièvement quelques accidents récents et emblématiques ; ces fragilités de la chaîne des TIC ont des impacts majeurs sur nos existences et la vie économique.

De fait, matérielles, logicielles ou humaines, ces failles contribuent à créer une société vulnérable. La deuxième partie développera ces vulnérabilités pour la société.

Mais la prise de conscience de cette dépendance de la société aux TIC n'est pas à la hauteur des risques encourus. Ces risquent restent pour les décideurs et les médias anecdotique ou de simples spéculations intellectuelles qui prêtent à sourire. Or les seules parades techniques (pare-feu, antivirus…) sont insuffisantes, les attitudes à privilégier feront l'objet de la troisième partie.

La question centrale sera alors de voir quelles attitudes adopter face aux vulnérabilités. En a-t-on étudié les conséquences pour notre société ? Qui en a vraiment conscience ? Y est-on matériellement et surtout intellectuellement préparé ?

Alors comment modifier les formations, le discours des médias, nos comportements pour bénéficier des avantages des TIC sans (trop) risquer de pâtir de leurs faiblesses.

1. La liste s'allonge

Historiquement les premiers incidents, tel l'incendie d'un ordinateur au Pentagon en 1959 à la suite de l'éclatement d'une simple lampe dans la salle voisine, n'avaient pas ou peu de conséquences sur la vie quotidienne des citoyens car les ordinateurs fonctionnaient alors "en circuit fermé". Actuellement de plus en plus d'incidents informatiques ont des impacts sur notre quotidien par le simple effet mécanique lié à la place importante prise par les TIC, mais aussi par la complexification des systèmes informatisés et leur mise en réseau.

Même mes étudiants d'informatique arrivent persuadés que les virus constituent le risque majeur. Si effectivement, apparus dans les années 80, les milliers de virus touchent les millions de PC de la planète, ils ne sont pas les seuls à fragiliser les TIC, en particulier car ces PC ne constituent qu'une petite partie de l'informatique mondiale alors que serveurs, mainframe, informatique industrielle... restent prépondérants.

D'autres fragilités ont des conséquences dont la portée peut être supérieure encore à celle des virus. Parmi de multiples exemples, j'en ai relevé certains en en soulignant les conséquences sur nos quotidiens.

Le 27 décembre 2006 un tremblement de terre a mis à mal les câbles sous-marins au sud de Taïwan[2] réduisant drastiquement le fonctionnement d'Internet et du téléphone en Asie.

En 2006 il a été beaucoup question d'accidents sur autoroute qui seraient liés à des défauts de régulateurs et limiteurs de vitesse. Ces accidents ont lancé le débat sur les dangers potentiels de l'informatisation des automobiles[3]. Les résultats des enquêtes se font toujours attendre.

La panne électronique est déroutante avec des effets improbables et illogiques ; le conducteur même le plus averti ne sait pas l'analyser et réagir en conséquence. Ainsi au

---

2 Un tremblement de terre d'une magnitude de 6,7 au large de Taiwan a endommagé la fibre optique du réseau Internet rendant les connexions impossibles avec la Chine continentale, le Japon, la Corée du Sud, l'Amérique du Nord et l'Europe. http://fr.theinquirer.net/2006/12/27/internet_coupe_par_le_tremblem.html.

3 Selon des blogs spécialisés : «*Dans les avions il y a jusqu'à 5 circuits parallèles qui contrôlent les infos par des logiciels différents, sur les voitures un seul circuit et un seul logiciel ; de plus l'ABS, l'ESP et le régulateur puisent leurs infos dans le même boîtier». «Une voiture moderne peut avoir un frein à main électrique* via *un bouton, inactif à vitesse élevée... et une boîte de vitesse séquentielle électrique, sans embrayage ; il est donc impossible de rétrograder si le régime moteur est trop élevé...».*

«Sur ma 207, le régulateur de vitesse ne veut plus fonctionner, par contre le limiteur fonctionne bien ; les feux de stop ne s'éclairaient plus à l'arrêt, par contre en roulant, il s'allument de temps en temps.»

problème technique se surajoute un problème humain, celui de la mauvaise gestion de l'incident.

Certains tracteurs agricoles n'utilisent pas moins de 19 calculateurs, sans compter leur guidage par GPS ; on imagine les difficultés pour éviter les bogues, pour gérer les interfaces et effectuer la maintenance[4].

En mars 2007, l'hôpital Jean Monnet d'Epinal annonçait qu'à son service de radiologie des patients, venus se faire soigner pour la prostate, avaient été sur-irradiés. Selon le rapport de l'IRSN [IRSN] une mauvaise compréhension du manuel en anglais du logiciel de pilotage CADPLAN, avait conduit à ce surdosage. Résultat : 24 patients traités ont des troubles radio-induits dont 4 ont décédé.

Selon le bulletin de mars 2007 du CERTA, le service d'alerte de la DCSSI, une nouvelle technique, le *Google hacking*, permet de pénétrer dans des sites web *via* Google[5]. Le même bulletin signale un virus *l'IE7.0.exe* inclus dans un pourriel qui a l'apparence d'un courriel de Microsoft (admin@microsoft.com) et qui propose une mise à jour d'Internet Explorer 7. En fait ce pourriel renvoie vers un site hébergeant un code malveillant exécutable qui s'incruste discrètement dans le PC.

2. De quels risques parlons-nous ?

Les risques sont essentiellement évalués en dollars, en ne tenant compte que des seuls aspects économiques [CLUSIF] : pertes de matériel, pertes d'exploitation, d'image de marque...

En réalité il faut aussi évaluer les risques en termes d'atteinte à nos libertés fondamentales car nos **libertés** de travailler, de s'informer, de circuler (voir le fameux logiciel SOCRATE de réservation de la SNCF [Naulleau 93]), de communiquer[6], d'acheter (e-commerce), d'être citoyens (débat sur le vote électronique [ODV])... sont de plus en plus liées à des technologies informatisées.

Certes il n'y a pas d'unité de mesure pour ces atteintes, mais elles n'en sont pas moins dangereuses pour nos démocraties. Faudrait-il faire l'impasse sur leur importance car elles ne sont pas aisément quantifiables ?

A noter que pour limiter les risques les techniques de contrôle et fichage sont systématiquement utilisées -avez-vous comptez le nombre de mots de passe que vous devez mémoriser ? La conséquence logique de l'usage sécurisé des TIC est donc le développement des techniques de contrôle (cybersurveillance, biométrie, vidéosurveillance, puces RFID, e-administration…), qui posent deux nouvelles séries de questions :

- celle du respect des libertés individuelles et publiques ;
- ET celle des nouvelles vulnérabilités qu'elles génèrent à leur tour. Les systèmes de cryptage largement utilisés à ce niveau ayant leurs propres faiblesses.

---

4 Moteur, boite de vitesse, climatisation, suspension, hydraulique, relevage...
La Lexus LS 460 de Toyota, embarque 94 micro-ordinateurs, dont 7 ne servent qu'à faire communiquer entre eux les 87 restants, par l'intermédiaire de quelque 33 kilomètres de fils électriques.

5 CERTA-DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), bulletin du 30 mars 2007 : www.ssi.gouv.fr/ ou www.certa.ssi.gouv.fr

6 Le système BlackBerry qui permet de recevoir des mails et Internet sur un téléphone portable est tombé en panne pendant 12 h aux USA, laissant la seule fonction téléphone opérationnelle la nuit du 17 au 18 avril 2007. Cette panne serait due à l'intégration d'une nouvelle brique logicielle mal testée. (IDG News Service)

Les risques concernent trois catégories :

- les individus : stress face aux pannes, aux "flux-tendus"[7], multiplication des contrôles d'identification, perversité d'une faux sentiment de sécurité[8], exclusion des analphabètes de l'informatique (société duale, technophobes, fracture sociale informatique), dégradation déjà évoquée de nos libertés, confiance aveugle dans des TIC mal maîtrisées. Si l'homme est affecté par ces incidents il faut reconnaître qu'il en est parfois la source par négligence, inattention, cybercriminalité, ou suite à une défaut d'ergonomie.

- les entreprises, les organisations : pertes financières, d'image et de crédibilité, fragilisation de l'organisation (75% des entreprises de plus de 200 employés se sentent dépendantes de l'informatique), déresponsabilisation due à l'automatisation des décisions, mauvaise maîtrise des logiciels[9], effet pervers de la virtualisation des processus de fabrication [Lasfargue 91]. Les "diagrammes de contrôle" qui représentent sur écrans la chaîne de production, les commandes de l'avion ou encore l'état du patient ne sont à ceux-ci que ce que *la carte est au territoire*.

- la Société : la concentration des moyens de production et des systèmes informatiques conduit à une plus grande dépendance technologique, à de nouveaux moyens d'espionnage, à des risques de sabotage, aux risques liés à l'accélération des prises de décision automatisée en matière économique, boursière ou militaire (guerre électronique)[10].

En résumé on observe :

- une intégration de plus en plus grande de fonctions dans des "boîtes noires " d'où une complexification du "puzzle" et de ses composants, bien difficile à maîtriser (pensez aux millions de lignes de code de Vista) ;

- une interconnexion de systèmes d'où une plus grande interdépendance des dispositifs avec des effets dominos bien connus dans les réseaux électriques -qui par ailleurs sont heureusement régulés par des ordinateurs. Même maillés les réseaux restent fragiles ;

- une concentration/centralisation des ordinateurs et des bases de données qui, par exemple sous la pression de la concurrence, va nécessairement aller de paire avec une accélération de la sélection des informations pertinentes et des prises de décisions. Il en va ainsi pour l'élaboration des ordres sur les champs de bataille où il faut travailler à la vitesse des missiles. Ainsi parmi la masse d'informations reçues sur les radars lesquelles sont à rejeter et lesquelles sont pertinentes ?

3. Une nouvelle attitude à développer

---

7 *L'Ergostressie* est une unité de mesure imaginée par Yves Lasfargue pour évaluer notre stress au travail : www.ergostressie.com.

8 Les voitures sont de plus en plus complexes techniquement mais en même temps totalement aseptisées, le conducteur ne "sent" plus rien et perd le contact avec sa voiture, ne reconnaît plus les bruit et les vibration.

9 Pour concevoir l'Airbus en France on utilise des logiciels de CAO en 3D Catia, Circé, à Hambourg c'est CADDS5 de Computervision qui est lui en 2D. Le dialogue est donc difficile : les câblages réalisés à Hambourg se sont avérés incorrects lors du montage à Toulouse, avec à la clef des retards et une facture en milliards d'euros.

10 Voir le concept du fantassin informatisé FELIN (Fantassin à Equipement et Liaisons INtégrées), ou bien des réseaux d'aide à la décision SCORPION (Synergie du COntact Renforcée par la Polyvalence et l'INfovalorisation) : www.defense.gouv.fr/dga.

Les exemples et analyses précédents dessinent une société plus fragilisée que l'on ne l'imagine généralement. Il faut tenter de trouver une réponse à cette problématique.

3.1. Evaluer

Il faut certainement commencer par analyser la situation qui se met en place sournoisement au niveau local ou national. Si la prise de conscience des dangers des virus informatique est largement répandue, la dépendance de notre société aux TIC à leurs vulnérabilités n'a jamais vraiment fait l'objet d'une évaluation (*assessment*), d'une réflexion et surtout de la mise en place de parades cohérentes et proportionnées au niveau national. La PME, le chercheur, l'administration, le citoyen dépose dans la machine son savoir faire et ses données les plus importantes, sans penser à évaluer les conséquences en cas d'incident.

En 1978 les suédois ont mené une réflexion sur la "Vulnérabilité de la Société" (rapport SARK) ; en 1987 en France un rapport sur la "Société vulnérable" est dirigé par Jean Louis Fabiani et Jacques Theys [Fabiani 87].

A ma connaissance depuis lors seules ont été réalisées, des démarches ponctuelles, limitées à une entreprise, à un secteur de l'activité humaine dans le meilleur des cas, mais rien à l'échelle du pays sur la vulnérabilité de la Société de l'information. Il faut tout de même citer les travaux de Patrick Lagadec [Lagadec], mais qui comme d'autres études ne portent pas ou peu sur les TIC, mais sur les diverses crises comme le 11 septembre, Bhopal, Seveso, l'amiante, la vache folle, l'Erika, AZF-Toulouse, le Prestige, les tempêtes de 1999… Ainsi le site la DCSSI ne mentionne aucune analyse générale ni plan d'ensemble national, mais seulement de nombreuses études sur des dispositifs particuliers de sécurisation.

Et pourtant l'Etat fait bien réaliser des plans sur les risques d'inondation (PPRI), les risques technologiques type Seveso (PPRT), les risques majeurs (PPRM), les risques sismiques, la grippe aviaire[11], mais rien sur les risques lié à la Société de l'information. Par contre des études ont été menées sur certains domaines clefs comme la gendarmerie, la continuité du fonctionnement de l'Etat en cas de crise ou la Sécurité civile (réseau ANTARES).

Un diagnostic, une réflexion nationale sur le sujet devraient se mettre en place ; il ne s'agit pas de devenir paranoïaques mais de prendre conscience de cette fragilité, de cette nouvelle vulnérabilité, qui se cache derrière les prouesses des TIC.

Cette réflexion devrait porter sur des questionnements tels que : Quelles sont les vulnérabilités les plus dangereuses pour les citoyens, les entreprises, le pays ? Quels risques acceptons-nous ? Quelles dépendances acceptons-nous ? (voir à nouveau le cas du vote électronique). Quel(s) plan(s) de sécurité faut-il concevoir au niveau national ?

Pour ce faire on peut penser à des enquêtes publiques, des enquêtes d'impact, des conférences de consensus, des débats publics sous la houlette de la Commission nationale du débat public (CNDP)[12]. Il faudrait aussi réfléchir aux effets pervers des dispositifs de protection qui peuvent donner un faux sentiment de sécurité (antivirus, frein ABS…) et faire prendre conscience de la disproportion entre certaines causes et leurs effets.

La démarche pourrait s'inspirer de méthodes utilisées pour les risques technologiques. Ainsi l'étude des dangers définit deux types de scénarios[13] :

---

11 Pour l'éducation nationale il y a des millions de masques de stockés, il est prévu de fermer les écoles et d'assurer la continuité de l'enseignement par téléenseignement ! www.grippeaviaire.gouv.fr

12 Commission Nationale du Débat public CNDP : www.debatpublic.fr

13 Repris du Site ministériel : www.prim.net/

- les scénarios dimensionnants : ces scénarios étudient les effets d'une défaillance d'une installation dans les conditions les plus défavorables (en considérant qu'aucune des sécurités mises en place ne fonctionne). Ces scénarios permettent donc d'envisager la "pire" des situations ;

- les scénarios résiduels : ces scénarios étudient les effets d'un accident en tenant compte des moyens de prévention et de protection mis en place (systèmes à sécurités dites "positives"[14]). Ces scénarios ont donc une ampleur moindre que les précédents et doivent être, si toutes les sécurités sont bien dimensionnées et entretenues, ceux que l'on observe en cas d'accident.

L'importance prise par les TIC dans notre société ne doit pas nous interdire, bien au contraire, de réfléchir aux risques. Il a fallu des années pour s'opposer aux lobbies des cigarettiers avant d'arriver à l'interdiction de fumer dans les lieux publics, près de 100 ans entre la découverte des risques de l'amiante et son interdiction, des dizaines d'années avant que des constructeurs automobiles acceptent de parler des accidents. Des lobbies informatiques existeraient-ils pour que ne soit pas posé sérieusement le problème de la fragilisation de notre société ?

3.2. Attitudes

Dans l'aviation ou la marine il est banal d'envisager les pannes et les accidents. Tout une série de parades préventives (maintenance, check lists, formation...), palliatives (procédures en mode dégradé, redondance et "vote" d'ordinateurs[15], extincteurs...) ou curatives (parachute, bateau de sauvetage, procédures de recherche SAR…) sont prévues, connues, enseignées et testées régulièrement.

Il est loin d'en être de même, malgré les efforts des responsables sécurité des services informatique (RSSI), dans la Société pour les TIC. Il existe bien des recommandations ou Codes de bonne pratique sous forme de normes[16] mais ils ne sont pas généralisés. Le commentaire de Ted Humphreys, animateur du groupe de travail de l'ISO/CEI est clair : "*le niveau de sécurité qui peut être obtenu exclusivement par des moyens techniques est limité. Le niveau de sécurité requis, établi par l'évaluation des niveaux de risque et les coûts associés aux violations de sécurité possibles, par rapport au coût de la mise en œuvre de la sécurité, devrait toujours être régi par des contrôles et des procédures de gestion appropriées. La gestion de la sécurité de l'information exige au minimum la participation de tous les employés de l'organisme, mais aussi éventuellement la participation des actionnaires, des fournisseurs, de tiers et des clients*".[17]

Autrement dit ces normes sont nécessaire mais pas suffisantes. La tendance est forte de résoudre les pannes par une couche supplémentaire de sécurité.

---

14 Les systèmes à sécurités positives se mettent en état sûr par défaut, ainsi dans les circuits de frein des trains et des camions il faut de la pression pour desserrer les freins, en cas de baisse de pression les freins sont plaqués par les ressorts. A l'inverse dans les voitures il faut exercer une pression dans les circuits pour freiner.

15 Pour l'Airbus 320, 2 calculateurs redondants gèrent les volets, 3 les spoilers,...

16 L'ISO/CEI 1779.:2005 est la norme internationale concernant la sécurité de l'information, publiée en décembre 2005 , c'est un Code de pratique pour la gestion de sécurité d'information. L'ISO/CEI 27001 définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO/CEI 17799. Pour les connaisseurs, l'ISO/CEI 17799 découle de la norme anglaise BS7799: (Wikipédia)

17 Organisation mondiale de normalisation : www.iso.org/iso/fr

La sécurité doit être pensée dès le départ, de même que les plans B à utiliser au cas où. Ainsi dans les tours de contrôle aérien on continue d'utiliser en plus des systèmes de contrôle informatisés des *strip*[18] où les données relatives aux avions sont reportées au stylo.

3.3 Sensibiliser, Eduquer

Une attitude importante est celle de la sensibilisation et de l'éducation. Il importe, selon moi, de former les utilisateurs de l'informatique **et** les informaticiens, aux conséquences des diverses pannes informatiques et aux moyens de s'en prémunir, ou d'y faire face. Leur environnement est fait d'automatismes complexes qu'ils ne maîtrisent pas vraiment (micro-ordinateur fragile, machine robotisée, logiciel mal maîtrisé, voiture informatisée...)

Beaucoup de conducteurs ont pris conscience des risques de la conduite automobile et ont de plus en plus intégré l'importance de bonnes pratiques et le rôle des ceintures et des airbags. Mais bien peu des utilisateurs de l'informatique pensent à réaliser des sauvegardes régulières, et surtout à imaginer ce qu'il faudra faire en cas d'arrêt de la machine ou de pertes de données. Pour filer la comparaison avec l'automobile il en est de même dès que la route est enneigée, on redécouvre alors la fragilité de la voiture face à la météo hivernale et l'absence de maîtrise des chaussées glissantes par le conducteur "moyen".

Il faudrait sensibiliser, éduquer, former les utilisateurs de l'informatique (c'est à dire quasiment l'ensemble de la population) à la vulnérabilité de l'outil. Pourquoi ne pas intégrer une telle réflexion dans le B2i (Brevet informatique et internet) et le C2i (Certificat informatique et internet) [19] ?

La société oublie d'éduquer ses citoyens à la panne, le réflexe inculqué est de demander de l'aide pour tous les actes de la vie quotidienne ou professionnelle au moindre incident. Cette attitude permet une complexification grandissante, sans limites, des dispositifs puisque chacun a acquis le sentiment qu'il y aura toujours un spécialiste pour réparer, sans penser qu'en attendant la réparation des conséquences, des dégâts ou même des accidents humains se seront déroulés.

Lors de la création d'une entreprise le *business plan* va prendre grand soin d'évaluer la trésorerie mais pas la dépendance à l'informatique ni les risques économiques qui en découlent.

Il s'agit de former informaticiens, techniciens, décideurs, à la panne et à ses conséquences. Former aussi le citoyen à ne pas dépendre entièrement de dispositifs fragiles. L'éducation à la panne n'est courante que chez les militaires, dans l'aviation ou la marine. L'ABS n'a pas fait baisser le taux d'accident. Le GPS n'empêche pas les naufrages ; la vigilance des marins s'étant amoindrie.

---

18 Les strips sont de petites "bandes de progression" sur lesquelles ont inscrit les informations relatives aux vols pris en charge par le contrôleur aérien. À chaque vol un strip, où sont imprimés les détails connus du vol : indicatif d'appel en radio, route, provenance, destination, type d'aéronef, niveau de vol ou altitude .Le contrôleur y porte les instructions qu'il donne à l'aéronef : changements de cap, d'altitude ou encore de vitesse, autorisations d'atterrissage ou de décollage, horaires de passage de certains points... Le strip est archivé et utilisé comme preuve. (Wikipedia)

19 C2i :www2.educnet.education.fr/sections/c2i/definition/,
B2i : www2.educnet.education.fr/formation/certification/b2i/

Conclusion

"De la société de peine à celle de la panne" dit Y. Lasfargue. Où est la culture de la panne, inconnue des ingénieurs. La panne nous est intolérable, elle est incongrue, niée. La vulnérabilité de l'informatique est claire, celle de l'informatisation l'est moins, celle de la société informatisée et du citoyen fort peu. Mais il en va de nos droits et libertés.

L'homme veut se protéger des aléas de la vie et de la nature, se sentir moins vulnérable, par des dispositifs de plus en plus sophistiqués, comme l'informatisation. Mais cette invulnérabilité est illusoire. Je pense que s'installe en fait une **Nouvelle Vulnérabilité**, plus sournoise.

Il nous faut apprendre -ou mieux ré-apprendre- à vivre avec. Et pour commencer choisir les solutions les plus simples, les moins mégalomaniaques, les moins prétentieuses… et celles qui ne sont pas liberticides. Celles qui sont intrinsèquement sûres donc à sécurité positive, en se méfiant des boîtes noires prétendument indépendantes… Mais rien n'est simple : la cryptologie protège nos échanges privés mais est aussi un outil aux mains des mafias. Les sites relais échappent à la censure mais peuvent être les refuges d'extrémistes.

Un pays, une entreprise, un simple citoyen chacun à son niveau devrait analyser sa dépendance, pour pouvoir ensuite se prémunir. L'Etat se doit de mener un diagnostic national et une réflexion sur les vulnérabilités de la Société de l'information.

Apprenons à résister à l'arrogance des TIC qui participent du développement d'une **Nouvelle Vulnérabilité**.

Traiter le problème par les deux bouts : des solutions techniques qui à la base fiabilisent les systèmes, ET des réflexions sur les crises susceptibles de se produire, réflexions comme les mène Patrick Lagadec depuis des années. Il précise dans sa propre présentation[20] ce qui vaut pour toutes les crises donc aussi celles de notre champs d'étude :*"L'enjeu est de réinventer aujourd'hui des repères intellectuels et de pilotage Il ne s'agit plus de protéger un système de quelque événement rare, connu, mesuré, d'amplitude relativement limité, et fondamentalement circonscrit. Il ne s'agit plus de «rassurer les populations» en leur garantissant que «tout est sous contrôle», mais de les faire partenaires d'un engagement collectif lucide, responsable et créatif. Il s'agit moins d'arrêter de grands plans de réponses, que de pouvoir ouvrir des questions inédites, pour penser et engager des dynamiques de réponses novatrices. Il ne s'agit plus de sous-traiter le leadership à quelque expert ou opérateur spécialisé, mais de faire preuve d'exemplarité et d'engagement personnel au plus haut niveau. Il ne s'agit plus de préparer à la sécurité en présentant des plans, des check-lists, des scripts non discutables, mais de construire des formations et des préparations à ces nouvelles lignes de faille. Cela suppose de s'être dégagé d'un effet pervers de ces crises : le refus, par anticipation, de tout questionnement ; le refus de mise à l'agenda.*

Crises après crises, nous observons que nos systèmes sont aujourd'hui en limite de pertinence. Katrina, tsunami, canicules, 11 Septembre, etc., ont clairement montré qu'il était urgent de repenser les paradigmes et principes opérationnels de la sécurité de nos systèmes."

Reste un dernier débat qui est loin d'être clos celui sur l'évolution de la vulnérabilité de l'humain dans notre Société de l'information. A-t-elle diminuée grâce aux TIC ou non ?

20 www.patricklagadec.net/fr/

Bibliographie

CLUSIF : Voir les études du CLUSIF sur la sinistralité : www.clusif.asso.fr

Fabiani Jean-Louis et Theys Jacques : *La Société vulnérable - Evaluer et maîtriser les risques*, Textes réunis et présentés par Jean-Louis Fabiani et Jacques Theys, Presses de l'Ecole Normale Supérieure, Paris, octobre 1987

IRSN : Institut de Radioprotection et de Sûreté Nucléaire : www.irsn.org

Lasfargue Yves : par ex *: Techno jolies, techno folies ? Comment réussir les changements technologiques*, Éditions d'Organisation, Paris, 1991, perso.orange.fr/yves.lasfargue/

Lagadec Patrick : Nombreux articles et ouvrages : www.patricklagadec.net/

Naulleau Daniel : *Avec Socrate, tout est possible à la SNCF*, Terminal N° 61, Paris, 1993

ODV : Citoyens et informaticiens pour un vote vérifié par l'électeur : www.ordinateurs-de-vote.org/

Mai 2007