2012

Haut Comité Français
pour la Défense Civile

Protéger l'avenir...

RAPPORT

Risques et menaces exceptionnels - Quelle préparation ?

Rapport d'activité 2011

2 30ANS 1 2

Sommaire

Le mot du Président d'honneur

Avoir eu l'honneur de présider le Haut Comité pour la Défense Civile pendant près de 15 ans, et avoir succédé dans cette responsabilité à son fondateur, le prestigieux et visionnaire Maurice Schumann, suffirait à marquer une vie…

30 ans de réflexion sur la défense des civils et le rôle de ces mêmes civils dans la Défense …

Sentir au quotidien l'immensité des bonnes volontés et les engagements qui en découlent, mais en même temps mesurer le peu de préparation de notre population, constater les lourdeurs, complexités, et parfois, hélas, aveuglements de notre appareil de gestion de crises invite à l'interrogation et à l'humilité.

Ces 30 années en débouchent sur 30 propositions d'ordre général ou ponctuel. Mon vœu est qu'elles soient examinées au fond, sans a priori, et avec la même ouverture d'esprit que celle qui anime le HCFDC, son nouveau Président Jean-René Lecerf, Christian Sommade et son équipe ainsi que l'ensemble de ses si nombreux membres, experts et correspondants tant publics que privés. Le Haut Comité n'est-il pas en effet un des trop rares lieux où ils se rencontrent et dialoguent sans tabous, ou enjeux directs ou immédiats ?

Remarquable, ce Rapport en témoigne, est l'intensité de leur réflexion. Tout autant leur souci de diffusion, d'information et de formation.

Soyons reconnaissants à tant de dévouement, d'inspiration et de franchise.

Puissent les années qui s'ouvrent être marquées par la prise de conscience de tous du fait que le monde dans lequel nous vivons comporte de très grands dangers, mais que les citoyens que nous sommes peuvent et doivent savoir se préparer et être prêts à les dominer.

La Défense de notre Pays repose sur nous tous … et l'assurance n'est hors de prix qu'avant l'évènement.

Paul Girod
Président d'honneur du Haut Comité Français pour la Défense Civile
Membre honoraire du Parlement

Le mot du Président

Le Haut Comité Français pour la Défense Civile édite pour la troisième fois en 10 ans un rapport. Il a cette année une signification spéciale, car le Haut comité fête ses 30 ans. Vous trouverez dans ce document un peu exceptionnel, non seulement le rapport moral sur l'année écoulée, mais aussi 30 témoignages de nos membres sur la vision qu'ils ont du Haut comité.

Mais au-delà de cela, il ne fait pas de doute que la sortie de ce rapport 2012, au démarrage d'une nouvelle mandature et au moment où le Livre blanc de la défense et de la sécurité nationale va connaître une nouvelle édition, n'est pas due au hasard.

Ce travail a un double objectif : premièrement, faire le point sur les menaces et sur les retours d'expériences des crises que nous avons vécues ces dernières années et surtout depuis 2008, date de notre précédent rapport; deuxièmement, être force de proposition sur des sujets où le plus souvent, ni la classe politique, ni les médias (hors temps de catastrophes) ne sont très prolixes.

Or, la préparation de la nation aux situations d'exception est bien l'objet que s'est fixé le Haut comité depuis la présidence de mon ami et prédécesseur Paul Girod, auquel je tiens à rendre hommage dans cette introduction, pour le travail sans relâche qu'il a, avec l'équipe permanente du Haut comité, effectué de 1998 à la fin 2011. Sans lui le Haut comité ne serait pas ce qu'il est devenu, à savoir un lieu unique d'échanges entre les élus, l'administration, mais aussi les grandes entreprises, les opérateurs d'infrastructures ou les fournisseurs d'équipements et de services qui contribuent à la sécurité de nos populations.

Si le Haut comité a pu en arriver là, c'est je crois, et j'ai pu le constater depuis le début de ma présidence, qu'il répond à un véritable besoin d'échanges tant «politiques que techniques» entre les acteurs; mais aussi parce qu'il permet de se plonger dans une approche concrète au travers des formations (sessions longues et courtes) et des entrainements et exercices qu'il organise régulièrement. Il est non seulement un lieu de réflexion mais aussi d'action, et il le sera de plus en plus dans l'avenir.

Le HCFDC ne peut agir que grâce à toute la communauté qui le soutient : gouvernement, services de l'Etat, collectivités, entreprises et experts qui concourent tous à la prévention et à la préparation de notre pays aux risques et menaces les plus graves.

J'espère que ce document sera riche d'enseignements et vous donnera des «idées concrètes». Il s'agit avant tout d'un rapport destiné à faire «bouger les lignes» et à s'interroger sans cesse sur les efforts à entreprendre pour élever notre niveau de résilience nationale. Je vous souhaite une bonne lecture.

Jean-René Lecerf
Président du Haut Comité Français pour la Défense Civile
Sénateur du Nord

RAPPORT ANNUEL

Risques et menaces exceptionnels - Quelle préparation ?

I

ETAT DES MENACES ET RISQUES MAJEURS

Introduction

Depuis son origine, le HCFDC s'est toujours attaché à analyser les dangers les plus graves menaçant nos populations. Ses recherches se sont portées particulièrement sur les menaces potentielles non encore concrétisées. C'est ainsi que sous l'impulsion de son fondateur Maurice Schumann, Etienne Copel a signalé, dès 1991, le danger représenté par des avions gros porteurs détournés par des pilotes prêts à se suicider.

L'objectif de ce chapitre n'est donc pas de faire un inventaire des grands risques et menaces auxquels sont exposées les populations françaises, mais simplement de prendre deux ou trois aspects qui ont connu des évolutions notables au cours de l'année 2011. Nous traiterons donc successivement de la menace terroriste et de son évolution, des risques naturels majeurs toujours très présents dans le cadre incertain du changement climatique, et du risque nucléaire après l'accident de Fukushima.

HCFDC 2012

Sendai, Japon, mars 2011

1 - Les menaces terroristes majeures

Le HCFDC ne s'intéresse au terrorisme que dans la mesure où celui-ci peut entraîner des conséquences graves ou catastrophiques qui seront à gérer comme tout autre accident d'origine technologique ou naturelle. Il faut en effet préciser que les mesures d'antiterrorisme et de contre terrorisme ne sont pas de son ressort, mais certaines mesures de prévention ou de sécurité peuvent l'être.

Depuis de nombreuses années, la menace terroriste qui vise le territoire français trouve pour l'essentiel sa source dans l'extrémisme islamiste. Il faut toutefois corriger cette évidence en rappelant que la Corse reste marquée par un terrorisme nationaliste, aujourd'hui de faible intensité, et que la dernière victime du terrorisme en France est un policier abattu par des membres de l'ETA en 2010.

La commémoration des attentats du 11 septembre 2011 à New-York a été l'occasion de faire le point sur les menaces terroristes majeures en ce début de la deuxième décennie du XXIème siècle.

La menace terroriste en France en 2011, la prépondérance du danger islamiste et le nouveau défi posé par les individus et groupes auto-radicalisés

La menace du terrorisme islamiste reste forte car exprimée à de nombreuses reprises par les dirigeants d'Al-Qaïda ces dernières années. Oussama Ben Laden lui-même, avant son élimination par l'armée américaine le 2 mai 2011, avait clairement inscrit la France parmi les principaux «oppresseurs de l'Islam». Ces discours sont fréquemment repris par l'émir d'Al-Qaïda au Maghreb Islamique (AQMI), Abdelmalek Droukdal qui proclamait en juillet 2010, «Sarkozy a ouvert pour lui, son peuple, et son pays les portes de l'enfer».

Ces menaces ont plusieurs fois été mises à exécution au Sahel ces dernières années : après l'enlèvement et la séquestration de quatre Français au nord du Mali par un commando d'AQMI, une tentative d'attentat au camion piégé visant l'Ambassade de France à Nouakchott a été déjouée en février 2011.

La menace contre la France s'est ainsi traduite ces dernières années par des actions à l'étranger, mais la France a jusqu'à présent «**sanctuarisé»** son territoire national depuis l'attentat du 3 décembre 1996 au métro Port-Royal. Grâce à ses services de sécurité et à une planification antiterroriste (plan Vigipirate) particulièrement efficace, ainsi qu'à un arsenal juridique préventif et répressif, la France a déjoué de nombreux projets terroristes, à divers stades de leur mise à exécution ces dernières années.

Depuis 2001, la police a interpellé en France, 914 présumés terroristes islamistes, dont 224 ont été écroués et 132 «éloignés».

Toutefois, ces succès peuvent à tout moment être remis en question, le passé récent montrant que le territoire européen reste accessible à des actions terroristes d'Al-Qaïda. Si les attentats meurtriers en Russie (35 morts en janvier 2011 à l'aéroport moscovite de Domededovo) relèvent d'une menace islamiste caucasienne spécifique, des pays plus proches ont été affectés en 2010 ou 2011, comme la tentative d'attentat suicide contre un centre commercial à Stockholm en décembre 2010.

Sept otages, dont quatre français, enlevés par AQMI au Niger, septembre 2010

Les nouvelles formes de l'activité terroriste

Les formes nouvelles et diverses que prend l'activité terroriste la rendent très difficile à juguler de manière permanente sur notre sol. Elle est d'abord représentée par des Français ou résidents Français liés à AQMI. L'arrivée en France d'un groupe envoyé ou financé par les Katiba d'AQMI présentes au Sahel reste une éventualité qui ne peut être totalement écartée. Dans ce cadre, les «volontaires» partis de France présents dans les «terres de Djihad» et susceptibles de rentrer en France représentent un danger permanent. Au Pakistan notamment, leur nombre reste important (14 identifiés en 2010).

Sans refuge comparable à l'Afghanistan d'avant l'intervention de la coalition, Al-Qaïda dispose de moins de moyens qu'auparavant lui permettant de commettre des actes «d'hyperterrorisme» équivalents au 11 septembre 2001.

Les petits groupes et les terroristes solitaires échouent souvent en raison de leur manque de compétence technique. Mais cela peut vite changer : l'avenir de l'Afghanistan est bien incertain et ce qui se passe dans certaines régions du Pakistan reste inquiétant.

Plusieurs facteurs sont au contraire susceptibles de renforcer la menace terroriste à court et moyen terme, dont :

- L'éventuel retour au pouvoir des Taliban à Kaboul après un retrait des troupes alliées dans un proche avenir pourrait renforcer la capacité d'Al-Qaïda en lui donnant à nouveau un sanctuaire qui lui permettrait de reprendre des projets de grande envergure.

- Le fait que les islamistes soient arrivés en tête aux premières élections libres en Tunisie, tout comme les premières déclarations du chef du Conseil National de Transition (CNT) sur la «Charia», désormais source de toute loi en Libye, peuvent faire craindre des basculements des révolutions du printemps arabe vers un islam plus radical avec les conséquences que cela peut avoir sur notre sécurité.

- L'hypothèse de constitution, de l'autre côté de la Méditerranée, de zones sanctuarisées pour les fondamentalistes djihadistes, comme le fut à une certaine période l'Afghanistan des Taliban, est également une réelle source d'inquiétudes.

Cet état de choses nécessitera donc une surveillance constante pour être certain que les Etats de droit nouvellement créés n'hébergent pas une menace terroriste vers l'Europe.

Par ailleurs, les groupes isolés et les individus «loose groups» et «lone wolves», représentent aujourd'hui une menace particulièrement difficile à neutraliser. Auto-radicalisés et auto-formés, ils n'ont pas ou très peu de liens avec un quelconque centre d'Al-Qaïda. Ils se nourrissent de l'idéologie ou de recettes «terroristes» diffusées par des sites internet de mouvances diverses. Leur radicalisation est souvent très difficile à détecter par les services de sécurité.

Tel a été le cas de Mohamed Merah, auteur présumé des trois tueries de Toulouse et Montauban en mars 2012, causant la mort de trois militaires français et de quatre civils, dont trois enfants, devant une école juive. Pourtant suivi depuis plusieurs années par la DCRI, du fait de deux voyages dans la zone pakistano-afghane et de sa radicalisation au sein d'un groupe idéologiste salafiste, aucun élément n'a jamais permis de penser qu'il préparait une action criminelle d'une telle ampleur.

De plus, rien n'est encore certain quant à son appartenance à un groupe terroriste, la revendication des actes par l'organisation Jund al-Khilafah liée à Al-Qaïda ayant finalement été retirée peu après sa diffusion. Cela permettrait alors de le qualifier de «**loup solitaire**» de la mouvance jihadiste, un électron libre agissant seul et sans connexion avec un quelconque mouvement terroriste.

Centre ville d' Oslo, 22 juillet 2011

Il faut également mentionner la terrible action solitaire d'Anders Breivik en Norvège au mois de juillet dernier, qui rappelle aussi que des groupes ou individus peuvent se révéler dans nos sociétés de manière brutale. Ces «loups solitaires» (comme le tueur de Liège), ou ces désaxés, sont d'autant plus dangereux qu'ils sont pratiquement indétectables par les services antiterroristes avant leur passage à l'acte.

Ainsi, **la menace terroriste demeure et mute**. Les gouvernements, les services spéciaux et la population ont compris que le terrorisme était une menace permanente et que les attentats étaient imprévisibles et pouvaient survenir n'importe où.

Les différents modes d'actions des actes de terrorisme

Les modes d'action possibles sont très variés. Dans ce cadre, il est clair que l'emploi d'explosifs (militaires, industriels ou artisanaux) demeure l'outil principal des terroristes, même si d'autres modes ne peuvent être écartés, notamment l'emploi d'armes automatiques, sans compter les aspects NRBC ou Cyber.

La mise en œuvre de plus en plus courante par les groupes terroristes islamistes de modes d'action à distance, d'attaques suicides avec utilisation de véhicules banalisés (attentat du Drakkar) ou encore d'engins explosifs improvisés selon des protocoles nouveaux au sein d'aéronefs (tentatives d'attentat du 26 décembre 2009 sur le vol Amsterdam-Detroit, imprimantes piégées en provenance du Yemen, etc.) pose un problème technique nouveau en temps de paix, dans l'hypothèse où l'intention de l'agresseur n'aurait pu être décelée à temps par les services de renseignements.

Les modes d'actions terroristes ne résultent pas nécessairement d'une planification d'objectif au sens militaire, mais relèvent souvent du traitement d'objectif d'opportunité, ce qui rend le renseignement plus difficile à recueillir en amont.

Face à ces modes d'actions, il importe de bien hiérarchiser les cibles potentielles attractives pour ne pas trop se disperser et consacrer les moyens - en particulier financiers - là où les risques sont soit les plus importants, soit les plus probables.

Certaines infrastructures sont naturellement attractives et «intéressantes» pour un mouvement terroriste recherchant un effet destructeur maximum, celles-ci étant potentiellement très «rentables» :

- Les centres nodaux de transports terrestres et aériens (gares, métro, train, aéroports, etc.) ;
- Les actions terroristes contre certains barrages, qui engendreraient des impacts considérables et dont la protection est semble-t-il, faible au regard des enjeux ;
- Les centres vitaux de certains réseaux (énergie, télécommunications, transports, services de secours), dont la neutralisation pourrait impacter tout autant la sécurité physique des personnes, que provoquer des désordres importants pour la vie sociétale et économique ;
- Les ouvrages d'art hautement symboliques (Tour Eiffel, cathédrales, etc.).

Simulation d'attentat NRBC à la Défense, Paris

Le cas particulier des actions NRBC

Si des actes terroristes de type NRBC sont sans doute moins vraisemblables à court terme, compte tenu de la faible sophistication des individus œuvrant aujourd'hui dans les groupes terroristes (c'est en tout cas, le constat que semblent faire plusieurs services de renseignements), la menace NRBC reste d'actualité pour plusieurs raisons :

• Le concept d'emploi visant à combiner l'emploi d'agents NRBC et d'explosifs classiques conduit désormais à envisager la menace NRBC-E (Nucléaire, Radiologique, Biologique, Chimique, Explosive) dans sa totalité. Deux grandes catégories NBRC-E sont alors à considérer à considérer :

- **Les agressions NRBC-E directes :** dispersion, diffusion, combinée ou non à une explosion qui peut également apporter des effets mécaniques ;

- **Les agressions NRBC-E indirectes par effet cascade** (effet domino ou collatéral) sur une installation à risque pour l'environnement : ainsi, les actions terroristes ciblées sur des installations sensibles sont susceptibles de conduire, par «effet cascade», à des accidents technologiques majeurs, notamment sur les centrales électronucléaires, les complexes pétrochimique et chimique, les laboratoires de haute sécurité microbiologique, les sites de stockage de toxiques chimiques ou de matières radioactives, pour ne citer que les principaux.

• Certains toxiques ne sont pas très difficiles à réaliser, notamment en petite quantité (Ypérite, Tabun, Sarin, etc.), d'autres sont accessibles au niveau industriel (TICs).

• L'intérêt pour les armes de destruction massive reste dans les esprits des terroristes.

• Les technologies permettant l'accès à certains types d'agents (notamment chimique et biologique) vont dans les années à venir être de plus en plus accessibles, pour des niveaux de compétences moyens et supérieurs. Les équipements et «savoirs» tels les réacteurs chimiques de faible taille, les capacités de traitement informatique, l'accès aux techniques de manipulation du vivant, peuvent faire «exploser» la prolifération B & C aux niveaux de groupes structurés, voire d'individus, d'ici à quelques années.

• L'accès aux sources radioactives industrielles ou médicales n'est pas impossible et les véhicules banalisés piégés, dont les aéronefs, ainsi que les actions à distance (LRAC, mortier léger portable, etc.) sont à prendre en compte.

• Moins connues, donc plus préoccupantes, sont les vulnérabilités de certaines installations militaires non durcies en raison de la doctrine en vigueur pendant la guerre froide : toute attaque sévère ne pouvant être qu'étatique il n'y a pas besoin de protection puisqu'il y a la dissuasion et la certitude de représailles insupportables. Le danger terroriste non pris en compte à l'époque doit impérativement l'être aujourd'hui. Le risque est celui d'une agression «hors dimensionnement» sur une installation ou équipement sensible, notamment nucléaire, pouvant entraîner des conséquences inacceptables sur l'environnement et la population.

La menace cyber

La menace «cyber» est en pleine évolution. Des attaques ciblées tant sur les infrastructures publiques que privées sont permanentes. A ce propos, le rapport du célèbre éditeur américain McAfee 2011, notamment, met en avant la récente évolution de l'augmentation des logiciels malveillants et casseurs de mots de passe, ainsi que les attaques sur les mobiles.

Hors la problématique de la cybercriminalité qui sous tend la plupart de ces attaques, on ne peut exclure la menace terroriste et notamment celle pesant sur les réseaux d'infrastructures de type SCADA (Supervisory Control And Data Acquisition). Systèmes de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures(1) et de contrôler à distance des installations techniques, ils se retrouvent dans différents contextes critiques, comme la surveillance de processus industriels, le transport de produits chimiques, les systèmes municipaux d'approvisionnement en eau, la distribution électrique, ou encore les canalisations de gaz et de pétrole. Ces éclaircissements permettent alors de mieux d'appréhender l'ampleur d'une éventuelle attaque cyber sur ces infrastructures.

La généralisation des protocoles informatiques standards pose en effet le problème de la vulnérabilité potentielle des SCADA, notamment au travers de la migration de certains de ces systèmes sous le protocole IP.

La menace cyber «terroriste» sur les infrastructures critiques (notamment réseaux de télécommunications, de transport aérien ou ferroviaire) demeure difficile à réaliser pour des réseaux traditionnels sans moyens particuliers, mais on ne peut exclure des attaques commanditées par des Etats, dont la signature reste floue et de nature «terroriste».

Enfin, Internet demeure aujourd'hui l'outil indispensable et permanent de recrutement des terroristes de la mouvance Al-Qaida. A cet égard, les phénomènes d'auto-radicalisation et de passage à l'acte, seul ou en bande «via Internet» sont particulièrement dangereux. La surveillance d'Internet est donc une mesure indispensable et permanente pour le contrôle des sites extrémistes dangereux.

Face à toutes ces menaces, l'Etat a réagi en faisant monter en puissance l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) qui a en charge la protection des sites informatiques publics, et qui établit également sous l'autorité du SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale), la doctrine de cyber sécurité.

Parallèlement à cette action des pouvoirs publics, l'industrie et les services cherchent à s'organiser pour créer une offre «nationale» en cyber-sécurité, dominée pour l'instant par des groupes américains. La volonté du gouvernement est aussi de pouvoir disposer d'une industrie nationale.

En effet, au-delà de cet effort, le secteur privé doit aussi se mobiliser pour faire de la cyber-sécurité un axe majeur de protection, ce qu'il ne fait peut-être pas encore suffisamment, au moins dans certains secteurs économiques. Il s'agit là aussi d'une culture de sécurité/sûreté à développer, mais cela implique également la mobilisation de moyens financiers et humains.

Devant ces défis grandissants, on assiste à une mobilisation croissante tant au niveau étatique qu'international. Ces propos peuvent être illustrés par plusieurs exemples, loin d'être exhaustifs.

Ainsi, au niveau européen, la Commission européenne fait désormais de la cyber sécurité une priorité, avec notamment l'ENISA(2), agence de cyber-sécurité européenne et l'exercice «cyber Europe 2010» réalisé dans ce cadre.

Les Etats-Unis ont quant à eux mis au point un plan national de cyber sécurité, ainsi qu'une stratégie internationale dans ce domaine.

Sur le plan des organisations internationales, l'OTAN a adopté un concept de cyber-défense en mars 2011. Les Nations Unies se sont également emparées du dossier, en distinguant deux principaux axes de réflexion et de négociations : l'un à caractère économique, orienté vers la cyber-criminalité, et l'autre à caractère politico-militaire orienté vers la cyber-guerre.

Cette dernière dimension, de plus en plus nette aujourd'hui, est de nature à mobiliser encore plus fortement les Etats, que toutes les autres formes de menaces apparues dans ce domaine. Il y a au demeurant fort à parier que les autorités chinoises, dont les mesures offensives qu'elles prennent sont largement soulignées, ne sont pas les seules à s'engager dans cette voie.

(1) *Elaboration et transmission à distance d'un signal porteur d'un résultat de mesure.*
(2) *European Network and Information Security Agency, créée le 10 mars 2004.*

Le cas du virus Stuxnet

Stuxnet est un ver informatique spécifique au système Microsoft Windows initialement découvert en juin 2010 par VirusBlokAda, une société de sécurité informatique basée en Biélorussie. La complexité du ver est très inhabituelle pour un malware. Il a été décrit par différents experts comme une cyber arme, conçue pour attaquer une cible industrielle déterminée. Il s'agirait d'une première dans l'histoire.

C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels, ce qui comporte un risque élevé. Il a été écrit spécifiquement pour attaquer les systèmes SCADA qui sont utilisés pour le contrôle commande de procédés industriels. Stuxnet a la capacité de reprogrammer les automates programmables industriels (API) produits par Siemens et de camoufler ses modifications. Les automates programmables Siemens sont utilisés tant par certaines centrales hydro-électriques ou nucléaires que pour la distribution d'eau potable ou les oléoducs .

Le ver a affecté 45.000 systèmes informatiques, dont 30.000 situés en Iran, y compris des PC appartenant à des employés de la centrale nucléaire de Bouchehr. Les 15.000 autres systèmes informatiques sont des ordinateurs et des centrales situés en Allemagne, en France, en Inde et en Indonésie, utilisateurs de technologies Siemens.

Flame confirme le développement de « cyber armes »

Flame est un ver informatique, surpuissant et vingt fois plus complexe que Stuxnet, capable de s'attaquer de façon très ciblée à des systèmes informatiques pour dérober des informations sensibles, en transmettant ce qui s'affiche à l'écran ou ce qui est saisi sur le clavier. Là encore ce malware cible exclusivement des ordinateurs situés au Moyen-Orient, dont, coïncidence, les PC iraniens. La complexité et les fonctionnalités du code utilisé ne peuvent être le fruit que d'un État, seul en capacité de développer de telles cyber-armes.

Cette nouvelle affaire de programme malveillant confirme que le risque d'une cyber-guerre représente une des menaces les plus inquiétantes pour l'équilibre international, comme si les grandes puissances abandonnaient le champ de bataille de la guerre conventionnelle (et réglementée par des traités internationaux) pour s'engager dans des cyber conflits, incontrôlables, qui à première vue semblent virtuels mais peuvent rapidement dégénérer, en poussant aux extrêmes les États attaqués, soit en provoquant des dommages catastrophiques, dès lors qu'ils s'attaquent comme Stuxnet aux systèmes SCADA des opérateurs d'énergie et de transport qui gèrent les grands réseaux vitaux et les infrastructures critiques.

Comment prévenir et se protéger de la menace terroriste ?

Le plan Vigipirate satisfait sa fonction première de vigilance et de protection au travers d'un dispositif complet, mais complexe. Sa lisibilité «grand public» reste grandement à améliorer, ainsi que sa compréhension pour le monde de la sécurité privée.

Le dispositif SAIV(3) (Sécurité des activités d'importance vitale) prévu par le décret de 2006 se déploie sur le territoire, impliquant plus de 250 opérateurs pour protéger plusieurs centaines de sites. Il s'agit d'un bon dispositif, mais qui au-delà de la réglementation, doit conduire au développement d'une réelle approche et culture de sécurité/sûreté auprès des opérateurs, laquelle n'est pas encore partagée au même niveau dans toutes les entreprises concernées.

Ce dispositif doit à la fois se terminer, notamment par l'instauration des PPE (plans de protection externe), à la charge des préfets, mais aussi vivre de manière permanente. Pour cela, il doit évoluer pour prendre en compte, non seulement les aspects de sécurité/sûreté des sites et réseaux, et de manière plus large, les capacités de gestion de crise et de continuité d'activités des opérateurs d'importance vitale, mais aussi de manière à assurer réellement la capacité des services de ces infrastructures à faire face à tous types de risques ou menaces.

Enfin, il faut noter que les mesures de défense active, y compris sur les sites sensibles, sont contraintes par le cadre légal du temps de paix qui réserve l'usage de la force à la seule légitime défense. Dans ces conditions, faire face à des agressions terroristes suicides, mettant en œuvre des véhicules banalisés piégés ou de petits commandos, peut se révéler délicat.

La protection passive quant à elle, présente l'intérêt d'être permanente et d'entretien réduit. Elle peut s'avérer nécessaire pour certains centres opérationnels vitaux durcis, s'ils ne sont pas redondés et dont la continuité de l'action doit être garantie en toutes circonstances et particulièrement en période de crise.

Le développement d'une culture de sécurité ou sûreté (suivant les secteurs économiques concernés) demeure essentiel, associé à un partage du renseignement, entre services de renseignements et acteurs concernés, lequel semble aujourd'hui encore être faible.

Plan Vigipirate

(3) En 2006 a été publié le décret SAIV, Sécurité des Activités d'Importance Vitale, concernant douze secteurs d'activités. Ils sont définis comme «un ensemble d'activités, essentielles et difficilement substituables ou remplaçables, concourant à un même objectif, pouvant présenter un danger grave pour la population ou visant à produire et à distribuer des biens ou des services indispensables…».

Avancées	Inquiétudes
Déploiement du dispositif SAIV auprès des 250 opérateurs pour la sécurité de centaines de PIV	Les capacités de continuité d'activité et de gestion de crises des opérateurs d'importance vitale non obligatoires dans le dispositif SAIV
Bonne législation anti-terroriste et veille sur les menaces terroristes, notamment des services de renseignements	Réforme des procédures pénales face à la menace terroriste - harmonisation et lourdeur des législations pénales européennes dans le cadre antiterroriste
Les travaux de recherche en matière NRBC ou de réduction de la menace face aux explosifs artisanaux	Faible lisibilité du plan Vigipirate par la population et les opérateurs
Réforme des groupes d'intervention (FIPN, GIGN) pour la gestion de crises multiples et création de l'UCOFI (Unité de Coordination des Forces d'Intervention)	Permanence de l'effort de sécurité face aux menaces NRBC, notamment en matière d'investissements et de formation (centre civilo-militaire) pour les acteurs de secours
Montée en puissance de l'ANSSI	Equilibre menace/défense incertain compte tenu de la rapidité d'évolution de la menace cyber
Réalisation d'une politique d'exercices au plan national	Culture de sécurité/sûreté inégale et parfois insuffisante dans le tissu économique français y compris dans les entreprises soumises à la réglementation SAIV
Prise en compte de la menace terroriste pour les centrales électronucléaires	Faiblesse du contrôle parlementaire sur les moyens et actions des services de renseignements
	Un dispositif réactif contre les agressions par voie aérienne limité par les contraintes du cadre légal de temps de paix (Code pénal, Code de l'aviation civile…)
	La vulnérabilité des barrages hydroélectriques aux actions terroristes, ainsi que certains transports de matières dangereuses

La prévention des risques technologiques

La prévention des risques industriels (4) et le contrôle des installations à risque ont connu un fort développement dans notre pays comme dans le reste de l'Europe depuis l'accident de Seveso en 1976.

De Feyzin en 1966 à AZF en 2001, la France et le monde ont connu un certain nombre d'accidents industriels majeurs. Restant toutefois peu nombreux au regard de l'activité, ces accidents ont néanmoins été à l'origine de 270 morts et 445 blessés sur les vingt dernières années en France, sans compter les coûts économiques et environnementaux.

Même si les accidents majeurs sont aujourd'hui rares, on ne peut les exclure, et ce malgré une réglementation draconienne.

Aujourd'hui sur les 450.000 activités industrielles que compte le pays, 40.000 sont soumises à autorisation d'exploitation (régime ICPE : Installations Classées pour la Protection de l'Environnement), 524 sont classées «Seveso seuil bas» et 606 «Seveso seuil haut», aux termes de la directive Seveso 2 de 1996, révisée en 2003.

Parmi les sujets de préoccupation qui influent sur l'augmentation des risques, les experts mentionnent souvent plusieurs facteurs comme la sous-traitance mal maîtrisée, le facteur humain, ou encore la méconnaissance des interactions dans les nouveaux process industriels. L'effort d'adaptation doit donc être permanent, d'autant plus qu'il s'agit d'un domaine où il ne faut jamais baisser la garde.

Intervention des pompiers sur le site d'AZF à Toulouse, 2001

En France et en Europe, la prévention des risques et la gestion des conséquences d'accidents sont basées sur les concepts suivants :

- La réduction du risque à la source quand cela est possible ;

- La maîtrise de l'urbanisation avec la réalisation des PPRT (Plans de Prévention des Risques Technologiques), prévue par le code de l'environnement aux articles L.515-15 à L.515-24 et R.515-39 à R.515-50, ainsi que le décret PPRT du 7 septembre 2005 permettant de prescrire des mesures foncières ou de renforcement du bâti ;

- La réalisation de plans d'urgence, avec :

  - **Le POI, Plan d'Opération Interne** (article R.512-29 du code de l'environnement, décret n°2005-1158 du 13 septembre 2005 et circulaire du 12 janvier 2011) à la charge de l'exploitant ;

  - **Le PPI, Plan Particulier d'Intervention** (article 15 de la loi de modernisation de la sécurité civile et décret 2005-1158 du 13 septembre 2005), à la charge de l'autorité préfectorale.

- L'information des populations, notamment par la réalisation des DICRIM (Document d'Information Communal sur les Risques Majeurs) au niveau communal et le travail des Comités Locaux d'Information et de Concertation (CLIC), dorénavant appelés Commissions de Suivi de Site (CSS).

A ces dispositions pour les sites «fixes», s'ajoute la réglementation sur le transport des matières dangereuses (TMD), soumise aux différents règlements internationaux : ADR, RID, ADN, ou encore IATA, en fonction du mode de transport (route, fer, air, mer).

Ces règlements n'ont toutefois pas empêché la survenue de 677 accidents sur les trois dernières années (2009 à 2011), dont plus de 75 % sur le vecteur routier (environ 6 millions de transports par route, contre 500.000 par fer en France chaque année). Ce chiffre reste encore limité considérant le nombre total de TMD, mais démontre néanmoins que les autres modes de transport offrent une plus grande sûreté.

(4) Remarque : ce chapitre ne traitera pas des risques nucléaire et radiologique, traités par ailleurs dans ce document.

Le dispositif de prévention des risques technologiques est relativement complet et régulièrement remis à jour, en fonction des retours d'expériences, mais il demeure complexe.

Il s'est élaboré au fil du temps et des textes, mais pose aujourd'hui encore un certain nombre de problèmes de «compréhension» entre les exploitants, les collectivités, les populations et les services de l'Etat (tel que le service des inspections des installations classées au sein des DREAL), qui réalisent un travail important sous la double tutelle préfectorale et judiciaire.

Les problèmes relevés dans la prévention sont de trois ordres :

- La difficulté de la mise en place des PPRT et leurs interfaces avec les autres plans et le fait que ceux-ci soient le plus souvent attaqués devant les juridictions administratives ;

- La difficile communication sur le risque, associée à une planification complexe rend l'acceptation et l'interface «population-collectivités-entreprises» plus ou moins difficiles suivant le niveau de gouvernance et la taille des acteurs locaux ;

- L'intégration difficile tant au plan conceptuel que pratique des mesures de sûreté (face aux risques malveillants), notamment sur les établissements classés Seveso.

Les PPRT et la difficulté de la communication du risque

Sur les 408 PPRT qui doivent être élaborés en France et qui concernent plus de 900 communes, 386 sont encore en cours d'élaboration(5). Le délai de réalisation de ces plans est en général très long, de cinq à sept ans en moyenne. Effectivement, en janvier 2012, seuls 143 étaient approuvés, soit 35% d'entre eux.

Cela est en partie dû au fait que les délais nécessaires aux industriels, bureaux d'études spécialisés et services de l'Etat pour disposer des outils informatiques ad-hoc, ainsi que le temps nécessaire aux études ont été sous-estimés. Les textes prévoyaient un délai de cinq ans pour la réalisation des PPRT, mais nous en sommes bien loin, ces plans étant plus complexes que prévu à établir.

Mais si les PPRT apportent incontestablement des progrès en matière de prise en compte du bâti existant, permettant une prise en charge financière partielle ou totale (en cas d'expropriation) au profit des propriétaires de logement, il n'en demeure pas moins que de nombreux problèmes se posent sur les études de risques et sur la relation avec les populations.

On notera :

- Les effets domino entre sites ou les liens avec les aléas naturels ne sont aujourd'hui pas pris en compte dans les études de dangers. Certaines installations de transports notamment (gares de triage, parkings routiers, etc.) ne sont pas prises en compte, le risque étant mouvant.

- Les zonages différents entre PPRT et PPI : le zonage PPRT comprend sept zones, le zonage PPI, trois. Comment expliquer que le risque «avant» et «après» accident ne soit pas le même ? Une harmonisation et une simplification des concepts et des planifications permettraient certainement une meilleure compréhension par tous les acteurs. Il ne faut pas oublier non plus que les PCS (Plans Communaux de Sauvegarde), obligatoires pour les communes concernées par un risque industriel ne sont malheureusement pas tous réalisés, les obligations n'étant pas de même nature.

- Par ailleurs, certains zonages notamment en zones industrielles pures empêchent le développement économique. Le lien entre «risques et développement économique» incluant des mesures de protection actives et passives pourrait alors être vu d'une manière plus globale et non liée à une réglementation ayant une approche partielle du problème.

Brochure d'information du PPI révisé du Havre

(5) Source : GASPAR (Base de données du ministère de l'Ecologie pour la gestion des risques technologiques).

• Le travail des comités locaux (CLIC ou CSS) gagnerait à être aidé au travers d'un fond de soutien payé au tiers par chacune des grandes parties prenantes : Etat, collectivités, industriels. Cela permettrait une formation et une «professionnalisation» de ces structures qui, aujourd'hui ne jouent pas toujours pleinement leur rôle et se voient parfois reléguées au second plan face aux associations actives de riverains qui se forment et sont de plus en plus nombreuses ces dernières années.

• Enfin, la loi exige des entreprises implantées dans les périmètres «Seveso seuil haut» de réaliser des travaux de mise en sécurité. Il existe cependant une différence majeure avec les habitants riverains soumis aux mêmes obligations. En effet, les entreprises ne peuvent bénéficier de crédit d'impôts, aucune aide ou prise en charge n'est prévue par la loi. Plus de 10.000 entreprises sont ainsi concernées, avec un coût total de travaux estimé à 1,5 milliard d'euros.

La difficulté d'intégrer la logique de sûreté dans les établissements industriels

Si la doctrine SAIV (Sécurité des Activités d'Importance Vitale) s'applique dans ce domaine comme dans les autres secteurs d'activités définis comme vitaux, tous les sites Seveso ne sont pas considérés comme des points d'importance vitaux (PIV). Il appartient au préfet de prononcer le classement de l'entreprise et du site au titre de ses pouvoirs de défense, s'il le juge utile.

Mais le problème réside dans le fait qu'il n'existe pas d'approche globale et concertée des mesures de sûreté. Ces mesures s'appliquent si le site est classé PIV et ne s'appliquent pas si le site ne l'est pas, même s'il peut présenter un danger certain en cas d'agression.

Il serait alors souhaitable que la démarche de sécurité soit commune entre prévention des risques accidentels et sûreté des installations. Le cloisonnement entre les administrations en charge, parfois au sein même des entreprises concernées est certainement un des freins majeurs à la création de bonnes pratiques communes entre sécurité et sûreté. Le développement d'une culture commune «sécurité-sûreté» apparaît aujourd'hui nécessaire et indispensable sur les sites à risques.

La future directive européenne Seveso 3

La future directive «Seveso 3», qui devrait entrer en vigueur en juin 2015 a notamment pour objectif d'intégrer dans la législation les modifications apportées par le règlement du Parlement européen et du Conseil, en date du 16 décembre 2008 relatif à la classification, à l'étiquetage et à l'emballage des substances et des mélanges, dit «règlement CLP» (Classification, Labelling, Packaging). L'objectif est d'aligner le système de classification de l'Union européenne sur le système général harmonisé des Nations Unies, afin que les mêmes dangers soient décrits de la même façon et mentionnés de manière identique dans l'étiquetage partout dans le monde.

Cette révision comporte plusieurs évolutions par rapport à la directive Seveso : une modification du champ d'application, un mécanisme nouveau de dérogation, de nouvelles obligations en matière d'information du public, des modifications (plus légères) du contenu et du rôle des études de dangers, des systèmes de gestion de la sécurité, de la politique de prévention des accidents majeurs, des plans d'urgence, et enfin des dispositions transitoires et délais de mise en œuvre pour les établissements concernés par des changements de régime.

Par ailleurs, la nouvelle directive Seveso 3 renforce encore les dispositions relatives à l'accès du public aux informations en matière de sécurité, sa participation au processus décisionnel et l'accès à la justice. L'objectif est ainsi d'aligner la directive sur les exigences de la convention d'Aarhus.

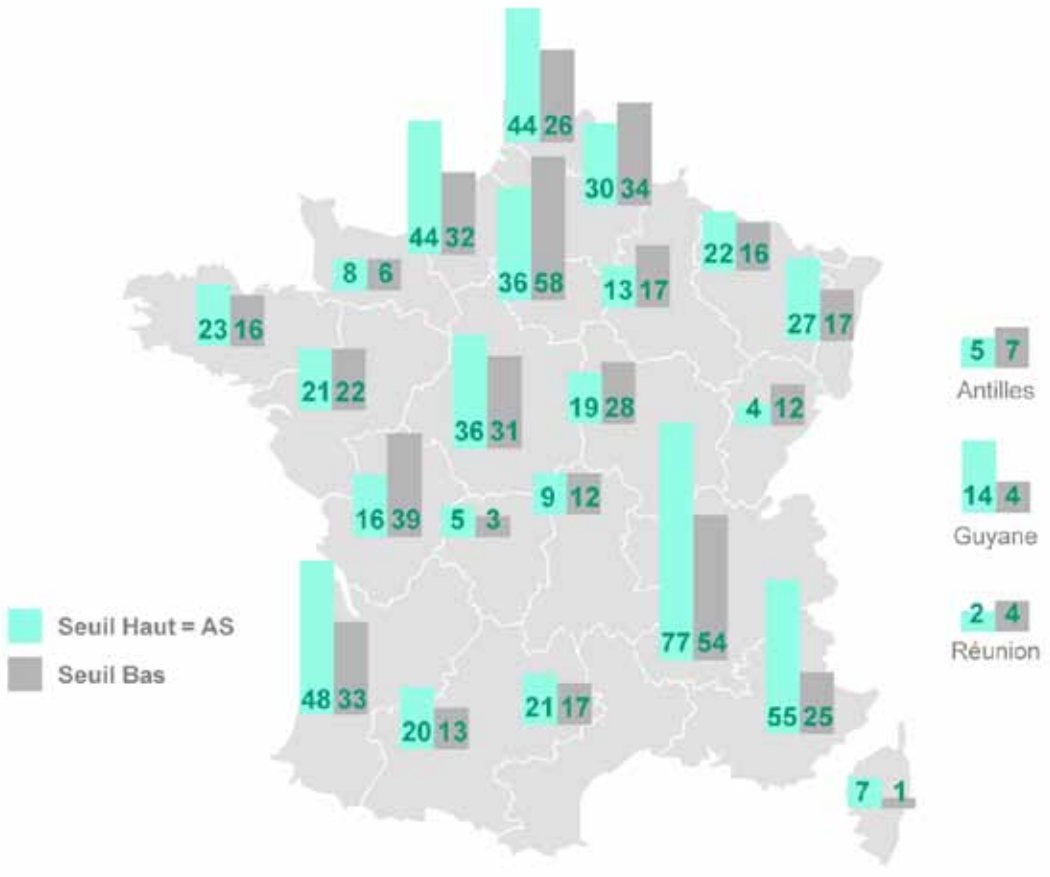
Les citoyens pourront ainsi avoir ***«un accès direct, via Internet, aux informations relatives aux installations Seveso situées à proximité de leur domicile, aux programmes de prévention des accidents et aux mesures d'urgence pour mieux réagir en cas de nécessité. Ils pourront ester en justice s'ils estiment que leurs droits n'ont pas été pris en compte lors de l'installation d'un nouveau site Seveso à proximité de leur domicile».***

La nouvelle directive comprend également des dispositions visant à améliorer la façon dont l'information est collectée, gérée, mise à disposition et partagée.

En outre, la directive maintient le principe d'une proportionnalité des obligations entre établissements «seuil haut» et «seuil bas». Certaines nouveautés sont cependant à noter, comme le renforcement de la politique de prévention des accidents majeurs, qui devra garantir un niveau de protection accru dans tous les établissements, ainsi que de nouvelles obligations d'information à destination des populations en cas d'accidents majeurs. Une autre nouveauté de la directive réside dans l'instauration d'un système de dérogations au niveau européen permettant de tenir compte des incertitudes liées à l'alignement avec le règlement CLP et des évolutions technologiques futures.

La transposition de ces nouvelles dispositions dans la réglementation française devrait conduire à des modifications substantielles de la nomenclature des installations classées, qui devra être adaptée à cette nouvelle architecture.

Repartition des sites Seveso
au 31 décembre 2010



Source : Ministère du Développement Durable

Avancées	Inquiétudes
Une doctrine cohérente de prévention des risques majeurs aboutissant à des taux faibles d'accidents industriels	Un dispositif PPRT lent à se mettre œuvre et ne répondant pas à l'ensemble des problèmes posés par la cohabitation : installations industrielles, populations, développement économique, et donc fortement contesté devant les juridictions administratives
Les efforts de réduction des risques à la source par les industriels et le dispositif Transaid pour les TMD	La non prise en compte des effets domino, des sites de transports (gares de triage, parkings poids lourds TMD, etc.) dans les PPRT
Un contrôle fréquent des installations classées	L'interaction «risques naturels – risques technologiques» dans la planification de prévention (PPRT) et de réaction (PPI)
Le développement de la directive Seveso 3	Des planifications PPRT-PPI trop éloignées l'une de l'autre pour être compréhensibles par la population
La doctrine SAIV impliquant la création de PIV sur certains sites industriels à risque	Une doctrine de sûreté trop indépendante de la doctrine de prévention des risques (tous les sites n'étant pas soumis à la réglementation SAIV) et la sûreté trop faible des véhicules transportant des TMD
Les avancées de certains bassins de risques (tel que Le Havre) qui adoptent des concepts de gestion avancée des risques sur des bases scientifiques et de coordination exemplaire entre les parties prenantes	Un soutien trop faible des structures d'information et de concertation (CLIC-CSS)

L'année 2011 a battu tous les records en terme de pertes économiques liées aux catastrophes naturelles. Le séisme japonais y a fortement contribué. Selon un rapport publié par le réassureur allemand Munich RE, 265 milliards de dollars de pertes économiques ont été enregistrées durant le seul premier semestre 2011, contre 97 milliards pour le premier semestre 2010.

Un premier semestre 2011 qui bat tous les records

Ce montant de 265 milliards de dollars dépasse celui calculé pour la totalité de l'année 2005 qui était, jusqu'alors, l'année la plus coûteuse avec plus de 220 milliards de dollars de pertes liées aux catastrophes naturelles. Ordinairement, celles-ci se répartissent plutôt sur le second semestre avec l'arrivée des ouragans dans l'Atlantique Nord et des typhons dans le nord-ouest du pacifique. Pour 2011, 355 catastrophes naturelles avaient déjà été enregistrées au premier semestre dans le monde, contre 390 en moyenne sur l'année pour les dix dernières années.

Le séisme japonais : la catastrophe la plus coûteuse de l'histoire

Le tremblement de terre et le tsunami exceptionnels survenus au Japon le 11 mars 2011 causant la mort et la disparition de 23 500 personnes, contribuent principalement à ce triste record. Selon les dernières estimations, ils auraient déjà coûté 210 milliards de dollars ; le gouvernement japonais tablant sur des dégâts estimés à 208 milliards de dollars dès le mois de mars 2011.

Ces évènements représentent la catastrophe la plus coûteuse de l'histoire de l'humanité, bien plus que l'ouragan Katrina qui avait alors entraîné des pertes de 125 milliards de dollars en 2005.

Des catastrophes météorologiques exacerbées par «La Nina»

Les catastrophes météorologiques ont été nombreuses et violentes au premier semestre 2011, notamment sous l'influence du phénomène climatique de « La Nina », qui a créé de fortes perturbations en refroidissant l'océan Pacifique tropical.

1 600 tornades ont été recensées dans le monde entre janvier et juin 2011. Des centaines de tornades, dont certaines extrêmement puissantes, ont littéralement rasé plusieurs territoires urbains, tuant plus de 500 personnes et occasionnant plus de 7 milliards de dollars de dégâts selon la société AIR Worldwide, spécialisée dans les estimations de catastrophes. Selon Munich RE, cette saison des tornades se solde par un coût estimé à environ 15 milliards de dollars.

De plus, le nord-est de l'Australie a connu des inondations exceptionnelles au début de l'année 2011 avec la crue simultanée et inédite de trois fleuves, dont le coût a été estimé à 7 milliards de dollars. Enfin, le passage du cyclone Yasi, le plus puissant dans la région depuis près d'un siècle a causé 2 milliards de dollars de pertes.

Ces pertes économiques considérables témoignent alors de la fragilité de nos sociétés qui peinent à intégrer sérieusement les risques naturels dans leurs aménagements et leur développement, malgré les efforts des Nations Unies et de l'International Strategy for Disaster Reduction (ISDR).

Inondations dans l'Etat du Queensland, Australie

Des déplacements de population considérables

En 2010, plus de 42,3 millions de personnes dans le monde ont dû tout abandonner à la suite d'un désastre naturel, selon la récente étude du Centre de surveillance des déplacements (Internal Displacement Monitoring Centre, IDMC) du Conseil Norvégien pour les Réfugiés (Norwegian Refugee Council, NRC). En 2009, 17 millions de personnes s'étaient déplacées pour échapper à un désastre, comme l'ont fait quelques 36 millions d'autres en 2008. Plus de 90 % de ces déplacements résultent de phénomènes climatiques.

Déplacements de population suite à un désastre naturel	
Année	Nombre de personnes déplacées
2010	42,3 millions
2009	17 millions
2008	36 millions

Le nombre des désastres naturels enregistré a doublé en deux décennies, passant d'environ 200 à 400 par an.

Ces mouvements massifs et les variations d'une année sur l'autre résultent en grande partie des «méga-catastrophes» les plus notables, comme les gigantesques inondations qui ont touché l'Inde en 2009, puis la Chine et le Pakistan l'année suivante, ou encore les tremblements de terre au Chili et en Haïti.

L'Asie : le continent le plus touché

Si tous les continents sont affectés par l'augmentation des catastrophes naturelles, touchant parfois de petits pays dans lesquels une proportion substantielle de la population est déplacée, c'est **l'Asie qui paye le plus lourd tribut avec 77 % des déplacements.**

En effet, l'Asie du sud et du sud-est, dont l'Inde, les Philippines, le Bangladesh et l'Indonésie, mais aussi la Chine et le Pakistan, ont connu les déplacements les plus massifs. Ainsi au Pakistan, plus de 11 millions de personnes ont dû quitter leur région après que leurs maisons et l'économie locale aient été anéanties par les inondations de juillet 2010. A la même période, une vaste zone du sud, et dans une moindre mesure, du centre et du nord de la Chine subissaient le même sort, entraînant le déplacement de plus de 15 millions de personnes. 19 % des autres déplacements concernent les Amériques et 4% l'Afrique.

L'Europe et l'Océanie restent épargnées avec quelques dizaines de milliers de déplacements pour chacun de ces continents.

Inondations en Asie

Un bilan humain exceptionnel

Séisme à Haïti, canicule en Russie, inondations au Pakistan, éruptions volcaniques en Indonésie ; les forces de la nature ont donc été particulièrement meurtrières en 2010. Avec 390 511 morts, le bilan humain des catastrophes naturelles pour l'année écoulée est le plus élevé depuis 1983.

Les catastrophes naturelles en 2010 ont fait presque six fois plus de victimes que la moyenne des catastrophes depuis 1980 : plus de 390 000 morts contre 66 000 en moyenne.

L'homme a souvent une part de responsabilité dans le bilan de ces tragédies, soulignent les experts. Le séisme de magnitude 7 qui a frappé Haïti le 12 janvier 2010 faisant plus de 316 000 morts et quelque 2 millions de sans abri, en est un parfait exemple. Ravagée par le tremblement de terre, Port-au-Prince compte presque trois fois plus d'habitants et davantage de bidonvilles qu'il y a 25 ans. Si le même séisme s'était produit en 1985, le nombre total de morts aurait probablement été d'environ 80 000.

La Russie a quant à elle connu une canicule meurtrière durant laquelle une température record de 38,2°C a été enregistrée à Moscou. La surmortalité due à cet événement a été estimée à 55 000 morts par les autorités russes.

Par ailleurs, des inondations ont fait 6 300 morts dans 59 pays entre janvier et septembre 2010, selon l'OMS. Enfin, de fortes tempêtes de neige se sont abattues sur les Etats-Unis en début d'année, tandis que la Chine et la Russie ont enregistré des chutes de neige record.

En France

L'année 2011 est encore marquée par les deux grandes catastrophes de Xynthia et de Draguignan de 2010. Le risque naturel demeure permanent sous toutes ses formes: inondations, sismicité, sècheresse, glissements de terrain, tempêtes.

On saluera cette année les travaux réalisés par le ministère de l'Ecologie et du Développement Durable dans le domaine de la prévention des risques naturels, avec notamment la révision de la carte sismique et la transposition de la directive européenne sur les inondations, ainsi que le développement des Programmes d'Actions de Prévention des Inondations (PAPI).

Cependant, on regrette toujours **le faible taux de pénétration et la lenteur à la mise en place des PPRN, DICRIM, PCS et autres plans de prévention et de préparation qui démontrent la faiblesse chronique de la plupart des collectivités territoriales à prendre en compte les législations et les efforts de préparation face aux risques exceptionnels.**

Enfin, le domaine assurantiel attire l'attention sur le projet de l'Observatoire National des Risques Naturels (ONRN) en cours de finalisation, destiné à mieux appréhender et partager les informations sur les risques par tous les acteurs concernés. Ce projet ne peut toutefois pas cacher deux problèmes : d'une part, le fait que notre régime «CatNat» n'incite pas à la prévention, de par l'uniformité de la prime, et que d'autre part, il risque, compte tenu de la montée des coûts d'indemnisation des catastrophes de se retrouver un jour «déficitaire» face à la montée des risques et aux indemnisations toujours plus importantes, constatées au plan international.

Séisme Port-au-Prince, Haïti

Avancées	Inquiétudes
Nouvelle carte sismique	Vulnérabilité de nombreuses constructions collectives aux risques sismiques, dans les régions concernées
Transposition de la directive européenne sur les inondations en droit français	Vulnérabilité des installations dangereuses au regard de la nouvelle carte sismique
Financement des initiatives PAPI	Lenteur des procédures PPRN et de la réalisation des DICRIM
Mise en place de la vigilance submersion marine	Trop lente implication de la majorité des collectivités locales sur la question des risques naturels majeurs, tant en terme de prévention que de réaction
Cartographie précise du risque de submersion sur 50 % des côtes françaises	Régime assurantiel CatNat n'incitant pas à la prévention et niveau de couverture faible au regard de l'importance des risques à venir
Création d'un observatoire des risques naturels	Manque d'interfaçage avec les collectivités locales
Création en France d'un Centre National d'Alerte aux Tsunamis (CENALT) dédié aux risques en Méditerranée et Atlantique Nord-Est	

Le 11 mars 2011, le Japon était frappé par un séisme de magnitude 9, suivi d'un tsunami destructeur d'une hauteur de 15 à 20 mètres déferlant sur les côtes de Sendai. De nombreux pays ont été touchés par ce tsunami quelques heures plus tard sur tout le Pacifique.

Quatre centrales nucléaires abritant quatorze réacteurs, les plus proches de l'épicentre, ont été exposées à l'onde du tremblement de terre.

La centrale de Fukushima-Daichi a été particulièrement endommagée par les inondations consécutives au tsunami avec l'entrée en fusion de certains de ses réacteurs et l'explosion de bâtiments enveloppes, entraînant d'importants rejets radioactifs dans l'atmosphère.

Fukushima-Daichi, où le risque «exceptionnel» n'avait pas été pris en compte

D'une catastrophe naturelle exceptionnellement violente et très meurtrière, le Japon est ainsi passé à une catastrophe technologique majeure, par effet de cascade.

Deux constats dans la catastrophe japonaise :

- Un premier sur la prise en compte du risque exceptionnel : malgré un risque historiquement connu et dont l'occurrence est supérieure au risque centennal, la centrale n'a pas été conçue, ni les procédures de sûreté envisagées, pour faire face à ce risque de submersion. Il s'agit bien là d'un défaut de conception « intellectuelle » du risque majeur. Il doit interpeller.

- Un second sur la résilience japonaise : on notera à la fois un manque évident de transparence de l'opérateur et dans une certaine mesure des autorités japonaises dans les premiers jours de la catastrophe, mais compte tenu de l'ampleur de l'évènement, on peut en imaginer, au moins pour partie, la raison. Mais c'est aussi l'excellence de comportement du peuple japonais face à une adversité majeure, grand exemple de résilience nationale.

Photo d'ensemble de la centrale avant le tsunami

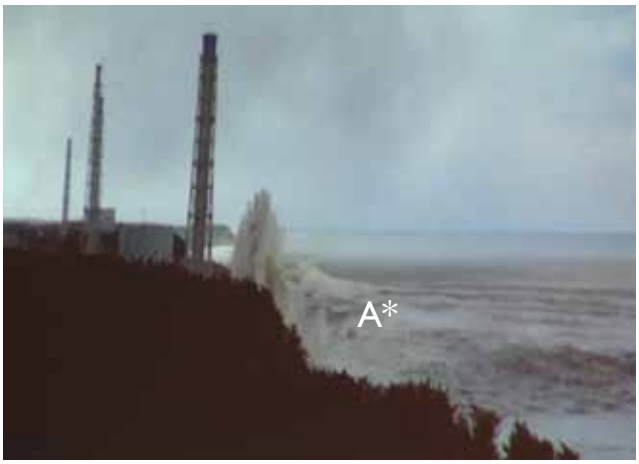


Photo de la centrale pendant le tsunami

Fukushima-Daichi, la réaction française

Par courrier en date du 23 mars 2011 le Premier Ministre a confié à l'ASN, en application de la «loi TSN(6)», la réalisation d'une **étude de la sûreté des installations nucléaires**, installation par installation, au regard de l'accident de Fukushima au Japon.

Par décision du 5 mai 2011, l'ASN a demandé aux exploitants des installations nucléaires de base concernés (AREVA, CEA, EDF, ILL) de remettre, au plus tard le 1er juin 2011, une note présentant la méthodologie retenue pour mener **l'Evaluation Complémentaire de la Sûreté (ECS)** de certaines de leurs installations au regard de l'accident de Fukushima, puis un rapport après l'été.

Les exploitants ont remis le 15 septembre 2011 un premier rapport à l'autorité sur les résultats des évaluations complémentaires de la sûreté dans les installations à examiner en 2011, que l'ASN et son appui technique, l'IRSN, ont analysé fin novembre 2011.

L'ASN souligne que les ECS constituent la première étape du processus de retour d'expérience après l'accident de Fukushima, ce processus devant se dérouler sur plusieurs années.

L'ASN a rendu public le 3 janvier 2012 son premier rapport sur les ECS (évaluations complémentaires de sûreté). Suite à celui-ci, l'ASN considère que les installations examinées présentent un niveau de sûreté suffisant pour qu'elle ne demande l'arrêt immédiat d'aucune d'entre elles.

Dans le même temps, l'ASN considère que la poursuite de leur exploitation nécessite d'augmenter dans les meilleurs délais, au-delà des marges de sûreté dont elles disposent déjà, leur robustesse face à des situations extrêmes.

Centrale nucléaire de Tricastin

Ces demandes de l'ASN portent essentiellement sur :

- La mise en place d'un «noyau dur» de dispositions matérielles et organisationnelles permettant de maîtriser les fonctions fondamentales de sûreté dans des situations extrêmes ;

- Le renforcement des référentiels de sûreté des installations nucléaires, en particulier sur les aspects séisme, inondation et risques liés aux autres activités industrielles. En particulier, l'ASN a demandé que soient examinées les conséquences de la rupture des digues du grand canal d'Alsace à proximité du site de Fessenheim, de la rupture des digues du canal de Donzère à proximité du site de Tricastin et de celle du canal de Provence à proximité du site de Cadarache ;

- L'imposition de la mise en place de dispositions renforcées visant à réduire les risques de «dénoyage» du combustible dans les piscines d'entreposage des différentes installations ;

- La mise en place progressive, à partir de cette année, de la «Force d'Action Rapide Nucléaire (FARN)» proposée par EDF, dispositif national d'urgence rassemblant des équipes spécialisées et des équipements permettant d'intervenir en moins de 24 heures sur un site accidenté ;

- La réalisation d'études de faisabilité de dispositifs supplémentaires de protection des eaux souterraines et superficielles en cas d'accident grave dans les centrales nucléaires ou les installations de La Hague.

Si les mesures ont été prises vis-à-vis de la filière, il semble que les mesures d'information du public et de gestion des situations d'urgence, notamment vis-à-vis des populations demeurent le parent pauvre de ces travaux. **Si l'ANCCLI a bien été auditionnée, les budgets des CLI sont toujours infimes au regard de la tâche d'information et de préparation des populations et des collectivités en cas d'incident majeur.**

A titre d'exemple, on estime l'investissement nécessaire aux mises en conformité à une dizaine de milliards d'euros (estimé à 2% du coût annuel de notre électricité par le ministre de l'Industrie), or le montant de la subvention pour toutes les CLI de France a été porté en 2012, à 1 million d'euros seulement.

(6) Loi du 13 juin 2006, relative à la transparence et à la sécurité nucléaire.

Fukushima-Daichi, une réaction européenne désordonnée et confuse pour les populations

Une réaction différente et non concertée des Etats européens :

• l'**Allemagne** a décidé une fermeture (annoncée comme temporaire) des sept plus vieux réacteurs (sur les 17 du pays) et un moratorium de trois mois sur l'extension de l'exploitation des centrales, puis l'abandon pur et simple de la filière ;

• l'**Italie**, pays peu nucléarisé, a approuvé un moratoire d'un an sur la construction de nouvelles centrales ;

• **le gouvernement français** a demandé un audit de sûreté et de robustesse des centrales nucléaires en activité ;

• même chose en **Espagne** où le Premier ministre a ordonné une revue des centrales nucléaires ;

• en **Slovaquie**, la construction de deux nouveaux réacteurs continue, les standards de résistances aux tremblements de terre vont cependant être relevés ;

• aux **Pays-Bas,** de nouveaux standards seront définis sur la base des évènements au Japon ;

• au **Royaume-Uni**, un rapport complet sur l'incident de Fukushima a été demandé et des mesures seront prises à la lumière de celui-ci ;

• en **Autriche**, on se félicite de n'avoir jamais adopté l'énergie nucléaire…

Commission européenne, Bruxelles

Les limites de l'action de l'UE

Face à cette catastrophe, le commissaire à l'énergie Günther Oettinger a proposé le 16 mars 2011, des stress tests des centrales nucléaires sur une base volontaire.

La Commission européenne s'est déclarée le 25 mai 2011 «très satisfaite» de l'accord obtenu la veille au sein du groupe des régulateurs européens dans le domaine de la sûreté nucléaire (ENSREG(7)) sur les tests à mener quant à la résistance des 143 réacteurs nucléaires de l'Union européenne. L'accord prévoit des tests de sûreté très poussés pour vérifier la résistance des centrales nucléaires à des catastrophes naturelles, comme les séismes et les inondations, mais aussi aux « conséquences de tout type d'accident d'origine humaine ou naturelle », comme un accident d'avion ou l'explosion d'un pétrolier, ou encore aux conséquences d'un acte terroriste.

Cependant, le commissaire a dû avaliser le principe d'une procédure de vérification pour les actions terroristes contre les centrales, dissociée des autres tests, alors qu'il refusait au départ un traitement différencié. Il s'est en effet avéré lors des discussions, que le terrorisme relève de la compétence des autorités de sécurité nationale des Etats membres, et non pas de la compétence des régulateurs regroupés dans l'ENSREG. Il a donc dû, tout comme un certain nombre d'Etats, faire marche arrière.

Le commissaire européen a également dû préciser les limites de son action. Les tests de sécurité seront menés sur une base volontaire dans les quatorze Etats membres de l'UE qui utilisent le nucléaire civil. Mais la Commission européenne n'est pas habilitée à demander l'interruption immédiate du fonctionnement d'une centrale jugée trop vulnérable. Une telle décision relève de l'Etat membre concerné qui devra tirer les conséquences d'un éventuel rapport négatif sur une de ses centrales, en toute transparence.

(7) European Nuclear Safety Regulators Group

Malgré plus de 50 ans d'EURATOM, le nucléaire est encore une affaire nationale

Alors que le traité EURATOM ratifié en 1957, est un des fondements de la construction européenne, le domaine de l'énergie nucléaire reste sous le contrôle des États membres, une directive de juin 2009 définit le cadre européen de la sûreté des installations nucléaires. Il y est précisé que **les États membres établissent et maintiennent un cadre national pour la sûreté nucléaire,** notamment par le moyen d'une autorité de réglementation indépendante (en France il s'agit de **l'Autorité de sûreté nucléaire, ASN**).

L'Union européenne donne responsabilité aux États membres et définit seulement les mesures de sûreté minimum à prendre, une posture qui sera difficile à tenir face aux populations lorsqu'un accident nucléaire touchera plusieurs pays de l'Union…

Fukushima : une nouvelle donne vis-à-vis des populations

Le sentiment anti-nucléaire s'est énormément développé à travers l'UE depuis le mois de mars, et en particulier dans les pays déjà engagés sur le chemin de l'abandon du nucléaire (Allemagne, Belgique, Italie).

La réglementation européenne, en donnant aux États membres la responsabilité des installations nucléaires sur leur territoire, a encouragé les réponses dispersées à la situation de la centrale de Fukushima. Néanmoins, s'il est normal que le choix d'utiliser, ou non, le nucléaire comme source d'énergie relève du domaine national, **la régulation et la sûreté des installations devraient être intégrées dans la gouvernance européenne**. Il est en effet légitime de se poser la question de la pertinence du choix national sur des installations dont, en cas d'accident extrême, les conséquences dépassent largement le niveau national.

Il semble aujourd'hui évident qu'une politique de communication et d'information préventive des populations doit être instaurée de manière beaucoup plus précise et approfondie en cas d'accident nucléaire de niveau 3 et au-dessus.

Or, la planification, la formation de l'ensemble de la chaîne de secours (hors spécialistes) et le niveau de jeu des exercices nucléaires nous semble, en France, et plus généralement en Europe, encore faibles face à des scénarios nucléaires majeurs : un exercice tous les trois ans et des politiques de stockage et de distribution d'iodes stables non homogènes sur le territoire national et européen. Des questions se posent également quant à la décontamination de masse, l'hébergement de longue durée, les contrôles de contamination sur les personnes et les chaînes alimentaires.

Cela se fait sans aborder concrètement les aspects de post-crise comme la décontamination des sols, les indemnités des personnes morales et physiques, ou la problématique des assurances, sur lesquels l'Etat écrit et s'exprime trop peu pour établir une confiance durable avec les populations sur sa capacité à gérer une crise nucléaire majeure.

Synthèse : le risque nucléaire après Fukushima

Avancées	Inquiétudes
Le système de gouvernance de la filière : ASN, IRSN mis en place avant l'accident	Les effets «cascades» de certains scénarios non pris en compte avant Fukushima
Rapport et recommandations de l'ASN	L'indépendance de l'ASN et de ses experts face à la filière
Le programme de robustesse mis en place par la filière nucléaire	La menace terroriste
Le renforcement du réseau de détection R	L'information des populations encore trop parcellaire, renforcement du dispositif d'alerte au-delà du périmètre de 10 km et le sous-financement des CLI et de leurs actions
La création de la Force d'Action Rapide Nucléaire à échéance de quelques années	Les mesures de gestion de crise et de secours insuffisamment calibrées pour des évènements de grande ampleur
Des exercices PPI réguliers mais n'impliquant pas toujours les populations	La gestion des pastilles d'iode auprès des populations non homogène sur le territoire
	L'insuffisance de la politique européenne sur la thématique accidentelle et post-accidentelle nucléaire
	L'insuffisance des moyens des CLI pour une préparation plus active des populations

2

LES PRINCIPAUX RETOURS D'EXPÉRIENCES DES CRISES RÉCENTES

Introduction

L'année 2011, et plus largement ces derniers mois ont été particulièrement rudes dans le domaine des catastrophes naturelles et technologiques. Ces évènements, bien que prévisibles, ont eu des impacts sensibles sur les sociétés qu'ils ont frappées, et ce à tous les niveaux. Les lourds bilans humains, économiques et environnementaux renforcent alors la réelle nécessité de préparer les populations à ces risques de plus en plus reconnus aujourd'hui.

Il semble donc important pour le HCFDC d'établir un bilan de ces crises majeures, afin de procéder à l'évaluation post-crise. En effet, la préparation ne peut venir que des enseignements tirés de précédentes expériences, en faisant ressortir les mesures positives ayant pu être relevées, tout en repérant les axes d'amélioration, afin de créer des réflexes, des procédures et des références dans un objectif de prévention des risques.

Cela correspond d'ailleurs à la méthodologie du retour d'expérience. Processus structuré, le retour d'expérience est pratiqué à l'occasion d'un accident ou d'une situation d'urgence ou lors de la constatation d'un écart par rapport à la norme ou au fonctionnement normal de l'organisation. Démarche d'analyse a posteriori de la gestion d'un événement, il constitue de fait un outil d'apprentissage.

L'objectif de ce chapitre est donc de tirer les enseignements des dernières crises à travers les principaux retours d'expérience. Nous traiterons alors successivement de la tempête Xynthia, des inondations du Var, du volcan Eyjafjöll, des chutes de neige en Ile-de-France, et enfin de la catastrophe de Fukushima.

HCFDC 2012

Côtes japonaises après le tsunami, mars 2011

1 - La tempête Xynthia

Le 28 février 2010, l'ouest et le nord-ouest de la France étaient balayés par la tempête Xynthia d'une rare violence. La conjonction de trois phénomènes naturels non exceptionnels (vents violents, dépression atmosphérique relevant le niveau de la mer et coefficient de grande marée) a provoqué une catastrophe naturelle majeure causant un bilan dramatique de 47 morts et dont le coût a été évalué à 1 milliard d'euros.

En dépit de la mobilisation des secours, les conséquences ont été accentuées par de graves défaillances, comme le relève le Rapport d'information parlementaire fait au nom de la mission commune d'information sur les conséquences de la tempête Xynthia du 7 juillet 2010.

Un système de vigilance et d'alerte insatisfaisant

Le risque d'inondation par submersion marine n'a pas été correctement évalué pour cette tempête dans la préparation à la crise. **La fiabilité du système de vigilance et d'alerte,** qualifié de « système vétuste et mal adapté aux risques d'aujourd'hui » par Monsieur Alain Perret, directeur de la sécurité civile, doit être renforcée, ainsi que sa compréhension par les autorités de sécurité civile et par la population.

La mission commune d'information sur les conséquences de la tempête Xynthia propose alors de doter le plan de gestion des risques d'inondation (PGRI) d'un volet stratégique sur le littoral en lui confiant un rôle d'évaluation de l'ensemble des mesures de gestion du risque, et d'y insérer un document retraçant l'ensemble de la chaîne d'alerte.

Concernant les systèmes d'alerte, ce même rapport évoque notamment l'intégration de **l'alerte « submersion marine »** dans les documents de planification régionaux existants, ainsi que la diffusion des messages d'alerte «submersion marine» permettant à leurs destinataires d'évaluer précisément le niveau de risque anticipé.

Enfin, la commission d'information souhaiterait mettre en place un véritable système d'avertissement destiné aux autorités et aux populations, reposant sur une prévision de hauteur d'eau qui complètera la prévision actuelle de vagues et de surcote, ainsi que sur une explication claire et concrète des effets attendus d'une rupture ou d'une surverse des ouvrages de défense des côtes et des conseils de comportements adaptés.

Nonobstant les défaillances relevées lors de cette tempête, le projet de **système d'alerte et d'information des populations (SAIP)** initié il y a une vingtaine d'années, peine à se mettre en place. Cette procédure ne devrait être opérationnelle qu'en 2013.

Une organisation des secours réactive à perfectionner

L'organisation des moyens aériens et des transmissions opérationnelles a également connu des dysfonctionnements lors de cette tempête, qu'il faut corriger, notamment dans la **coordination de plusieurs zones de défense.**

Concernant les problèmes de communication et de coordination des secours, la mission commune d'information sur les conséquences de Xynthia suggère d'établir et de structurer une coopération entre les services déconcentrés de l'Etat et les gestionnaires de réseaux et entre les opérateurs de téléphonie mobile, France Telecom et ERDF pour rétablir le plus rapidement possible les communications en cas de catastrophe naturelle.

Il est également important que les centres de secours soient implantés ou relocalisés hors des zones vulnérables.

Secours par hélicoptère après la tempête Xynthia

Une culture du risque et la préparation à la survenance des aléas naturels très insuffisantes

Par ailleurs, il est nécessaire que les communes exposées prennent les devants et organisent l'information sur les lieux et les modalités de regroupement de la population en cas de péril, la mise en place d'affichages permanents et de campagnes de communication. Il est aussi important de réaliser des **exercices périodiques de simulation** pouvant inclure des opérations d'évacuation des zones les plus menacées.

Mais c'est surtout sur le développement de **plans communaux ou intercommunaux de sauvegarde (PCS)** simples et opérationnels, établis de façon concomitante et coordonnée avec la préparation **des plans de prévention des risques (PPR),** que les communes concernées doivent mettre l'accent. De toutes les communes frappées par Xynthia, aucune n'avait réalisé de PCS. Il existe pourtant une obligation d'adoption de ces plans par les communes, dès lors que la réalisation d'un PPR lui a été prescrite. Aujourd'hui, près de dix mille communes devraient avoir adopté un PCS.

De plus, les PCS souvent vagues, ne doivent pas se résumer à des documents théoriques. Il apparaît nécessaire aujourd'hui qu'ils comportent des procédures et des mesures opérationnelles portées à connaissance de tous.

Enfin, la création d'une nouvelle catégorie de plans de prévention des risques naturels (PPRN), **les plans de prévention des risques de submersion marine (PPRS)** apparaît judicieuse, comme le suggère la mission d'information sur les conséquences de la tempête Xynthia. Ils constitueraient alors une sous-catégorie de PPR « inondation ».

A cela, le rapport d'information a répondu que les PPR étaient potentiellement un outil majeur pour la prévention des risques de submersion, étant créés afin de prendre essentiellement en compte les inondations. Les inquiétudes quant à l'impact rapide de ces plans et le financement de ces actions restent cependant d'actualité.

Une réglementation assez complète, mais peu connue ou appliquée

Dans les départements concernés, la politique d'aménagement et d'urbanisme n'a que des résultats peu satisfaisants en ce qui concerne l'application faite sur le terrain, des concepts et principes développés dans la législation et la règlementation nationales, notamment les dossiers départementaux sur les risques majeurs (DDRM), les documents d'information communale sur les mêmes risques (DICRIM), les atlas des zones inondables (AZI), ou encore les plans de prévention des risques (PPR).

Les insuffisances les plus significatives concernent :

- des aléas de référence fixés à un niveau significativement plus bas que les valeurs extrêmes enregistrées dans le passé ;

- des zonages qui sous-évaluent parfois l'intensité des aléas effectifs ;

- des documents locaux d'urbanisme souvent anciens et dépassés qui ne prennent pas en compte - ou de façon très insuffisante - la problématique des risques ;

- des autorisations d'utilisation des sols (notamment des permis de construire ou de lotir) qui, délivrées naguère dans des communes pourtant exposées au risque de submersion marine, l'ont été, sauf exception, sans contrainte ou prescription particulière ;

- La non prise en compte des effets du réchauffement climatique sur la montée des océans.

Face à ces insuffisances, la mission commune d'information propose d'interdire la délivrance d'autorisations d'urbanisme tacites dans les zones couvertes par un PPRN ou dans lesquelles un PPRN est en cours d'élaboration, mais également de les hiérarchiser. La primauté des PPRN sur les documents d'urbanisme est nécessaire afin de garantir une prise en compte réelle et effective des risques naturels.

Il faut également faire référence à la réflexion sur la mise en place d'aménagements protecteurs des populations dans les habitations individuelles ou d'infrastructures de mise en sécurité des populations. L'obligation d'information sur les risques locataires et propriétaires serait une grande avancée.

Des ouvrages de protection contre les inondations mal connus et mal entretenus

De nombreuses digues mal entretenues présentes sur le littoral ont cédé face à la tempête Xynthia, laissant pénétrer la mer à l'intérieur des terres, engendrant des dégâts majeurs aux biens et aux personnes en Vendée et en Charente-Maritime. 800 mètres de digues ont ainsi été détruits à Saint Clément des Baleines, sur les 1,4 kilomètres existants et six brèches de plus de 150 mètres ont également été relevées.

Les ouvrages de protection, dont les plus anciens datent du Moyen-Age sont souvent mal connus et recensés de façon incomplète, imparfaite et hétérogène. Ils apparaissent en décalage complet avec la réalité du terrain sur lequel les grandes propriétés se sont émiettées, conduisant à la déresponsabilisation, à de multiples incohérences et à l'inaction ou à des actions très insuffisantes.

L'article 33 de la loi du 16 septembre 1807 relative au dessèchement des marais, dispose en effet que la responsabilité de la protection contre les inondations relève des propriétaires riverains, alors que la responsabilité du maintien et du contrôle de la bonne sécurité des digues appartient au propriétaire de l'ouvrage. **Clarifier le régime de propriété** permettrait ainsi de clarifier les responsabilités.

Inondations suite à la tempête Xynthia

Le nécessaire renforcement de la politique de prévention des risques d'inondation

Il faudrait alors créer un établissement public pour conduire l'entretien de l'ensemble des ouvrages de protection contre les inondations. Sous cette même tutelle, **un plan d'action pour la réfection des ouvrages de protection contre les inondations** devra s'insérer dans les orientations plus globales d'une politique pérenne de prévention du risque d'inondation et de gestion du trait de côte.

La plus grande inquiétude ici reste celle du financement de l'entretien de ces digues, le renforcement ou la construction d'une digue coûtant un à deux millions d'euros par kilomètre. **Etablir des zones prioritaires** semble être une première solution.

Plus largement dans le domaine de la prévention des risques, il faut mentionner l'existence de la base de données de la Commission Interministérielle Catastrophes Naturelles, tenue à jour par la Caisse Centrale de Réassurance (CCR), **recensant notamment l'existence de PPR sur une commune donnée,** faisant le lien entre assurance et prévention.

L'évolution des travaux de modélisation de la CCR va permettre de mesurer l'exposition des territoires à des évènements possibles, même s'ils ne sont pas survenus.

La diffusion et le partage d'informations pertinentes par la CCR, notamment au travers de l'Observatoire National des Risques Naturels, participent également à la prévention de ces risques naturels.

Toujours dans l'objectif de prévention, le Fonds de Prévention des Risques Naturels Majeurs (FPRNM) permet le financement de mesures de prévention, de protection ou d'expropriation menées par l'Etat dans le cadre d'opérations de réduction de la vulnérabilité de territoires fortement exposés. Ce fonds a ainsi permis de financer l'expropriation de biens sinistrés ou trop fortement exposés suite à la tempête Xynthia.

Il faut enfin rappeler que ces défaillances et analyses pourront valoir pour d'autres catastrophes naturelles, telles que les inondations frappant le département du Var.

Bilan de la tempête Xynthia : 28 février 2010
47 morts
1,5 milliard d'euros
690 millions d'euros à la charge des assureurs

Source : Rapport de la mission interministérielle sur le retour d'expérience de la tempête Xynthia.

Points positifs ou de satisfaction	Points négatifs ou d'inquiétudes
Importante anticipation et mobilisation des secours	Système de vigilance et d'alerte peu fiable, notamment vers la population pour les mairies non préparées
Obligation d'information sur les risques locataires et propriétaires	Organisation inter-zonale des secours à améliorer
Réglementation sur l'aménagement et l'urbanisme assez complète mais parfois complexe	Application insatisfaisante de la réglementation sur l'aménagement et l'urbanisme
La mise en place du plan « digue »	La pérennité de l'entretien de ces ouvrages

Principaux enseignements tirés	
Points positifs ou de satisfaction	**Points négatifs ou d'inquiétudes**
Mise en place de l'alerte « submersion marine »	Insuffisance de la culture du risque au sein des populations et chez certains élus
Prise de conscience de l'importance des plans de prévention et de sécurité civile	Urgence du développement des PCS et PPR

2 - Les inondations du Var

Le 14 juin 2010, Météo France place onze départements du sud-est de la France en vigilance orange, prévoyant de fortes pluies. Le lendemain, le Var est frappé par cet «épisode méditerranéen» provoquant des perturbations allant de 150 mm à 390 mm, selon les endroits.

Montée jusqu'à quatre mètres, l'eau a entraîné de graves inondations dans certaines villes, dont celle de Draguignan. Plusieurs communes ont été dévastées, provoquant la mort de 23 personnes.

De lourdes pertes

Les inondations des 15 et 16 juin 2010 ont été provoquées par des précipitations très importantes constituant un phénomène rare par son intensité, mais pas exceptionnel. Les rivières de la zone concernée par la catastrophe de juin 2010 sont en effet bien connues pour leurs crues intenses et rapides.

Il faut en outre noter que la mort des 23 personnes, probablement surprises par la montée très soudaine et rapide des eaux, a bien souvent eu lieu en dehors de leur domicile. Ces lourdes pertes sont également liées à des **comportements inadaptés de la part des populations** ; d'où l'importance de la **préparation des citoyens** aux risques, notamment aux inondations.

Des informations en ordre dispersé

A la suite de la tempête Xynthia frappant plusieurs départements du littoral atlantique en février 2010, certaines mesures ont été prises par la préfecture du Var.

Ainsi, le schéma directeur de prévision des crues du bassin Rhône-Alpes a confié à la direction interrégionale sud-est de Météo France, le service de prévision des crues «Méditerranée Est». Celle-ci n'a toutefois pas organisé la prévision des crues sur les fleuves dans le département du Var.

Un système d'alerte médiocre

Il existe un décalage entre l'effectivité de la transmission de l'alerte aux maires et la perception de cette alerte. **Ce décalage est lié, du côté de l'émission des messages, aux limites techniques des outils de prévision et du côté de leur réception, à une culture du risque encore insuffisante** et concentrée sur le risque de feux de forêt.

La faible anticipation est sans aucun doute un facteur aggravant d'un tel phénomène météorologique et il est certain que **la procédure de l'alerte aux maires doit être revue** et raccourcie.

La question des réseaux de transmission

L'organisation des secours lors de ces inondations a été affectée par **la perte des réseaux de téléphonie fixe et mobile**, ainsi que par l'inondation de points névralgiques du dispositif public de secours.

Néanmoins, 2 450 personnes ont pu être sauvées, dont 1100 sauvetages au sol et 1 350 sauvetages aériens, 300 personnes ayant évité une mort certaine. **La réactivité du commandement face à l'indisponibilité d'organes opérationnels majeurs** a permis d'éviter des retards dans la mise en œuvre de moyens de secours nationaux et zonaux, notamment les hélicoptères.

Il faut également relever que **le bon fonctionnement des liaisons ACROPOL et ANTARES** pendant toute la crise a été un élément déterminant.

Une planification déficiente et un manque de volontarisme au plan de l'urbanisme

De nombreuses communes disposent de plans communaux de sauvegarde (PCS) utilisés lors des opérations de secours, mais qui ont été élaborés dans la perspective des feux de forêts.

En outre, **les maires méconnaissent en règle générale les atlas de zones inondables, lesquels ne sont d'ailleurs pas validés par les services de l'Etat**. Les plans de prévention des risques d'inondation prescrits depuis plus de dix ans n'ont pas abouti à cause de tergiversations sur l'aléa de référence et la prise en compte de la vulnérabilité et des enjeux dans les «zones de danger».

Les communes ont une volonté affichée de préserver la possibilité d'une urbanisation diffuse, ce qui a conduit à ne pas prescrire de plan local d'urbanisme ou à laisser traîner leur élaboration depuis plusieurs années.

Enfin, le contrôle de légalité des actes d'urbanisme est un instrument sans efficacité réelle dans une région où les conséquences en termes d'aménagement et de dommages potentiels se révèlent catastrophiques.

Une nécessaire culture du risque

Une plus grande culture du risque implique la définition d'une **stratégie d'urbanisme et d'aménagement** qui réduise les conséquences de telles catastrophes dans les zones déjà urbanisées, stratégie qui doit s'affranchir des raisonnements à court terme et être fermement contrôlée par les services de l'Etat.

Intervention de la Sécurité Civile dans le Var, juin 2010

Bilan des inondations du Var : 15 – 16 juin 2010
23 morts
44 communes sinistrées
1 milliard d'euros de dommages directs

Source : Rapport de la mission interministérielle sur le retour d'expérience des inondations survenues dans le département du Var les 15 et 16 juin 2010.

Points positifs ou de satisfaction	Points négatifs ou d'inquiétudes
2 450 personnes sauvées	Système d'alerte décalé entre l'effectivité de la transmission de l'alerte aux maires et la perception de cette alerte
Réactivité du commandement des secours	Faible anticipation du phénomène
Fonctionnement et résilience des liaisons ACROPOL et ANTARES	Perte des réseaux de téléphonie mobile et fixe
Mobilisation de l'ensemble des forces aériennes (Sécurité Civile, Gendarmerie, Armée…)	PCS mal conçus ou mal adaptés, souvent du fait de leur focalisation sur le risque feux de forêts
	Méconnaissance des atlas de zones inondables

Principaux enseignements tirés	
Points positifs ou de satisfaction	**Points négatifs ou d'inquiétudes**
Mise en place d'une stratégie d'urbanisme et d'aménagement	Culture du risque insuffisante
Révision de la procédure d'alerte aux maires	Planification de prévention déficiente au niveau des communes
Révision des réseaux de téléphonie	Manque de préparation des acteurs locaux et des populations

3 - La crise du volcan Eyjafjöll

Le 14 avril 2010, le volcan islandais Eyjafjöll au repos depuis 1823, après un réveil le 20 mars 2010, enfume l'Europe par ses colonnes de fumée allant jusqu'à 9 000 mètres de hauteur. Les nuages de cendres formés par l'éruption atteignent le ciel de Norvège dès l'après-midi, forçant Oslo à fermer son espace aérien. Dix pays européens suivront la démarche le lendemain. Le nuage de cendres entraîne alors la plus importante fermeture de l'espace aérien européen depuis la Seconde guerre mondiale.

Une crise sans précédent

Le nuage de cendres engendré par ce phénomène naturel a provoqué une crise sans précédent, au niveau du transport aérien d'abord, et par ricochet dans de nombreuses activités économiques ensuite, à travers toute l'Europe. Cette crise, qui a débuté le 14 avril 2010 avec l'éruption du volcan islandais, s'est définitivement achevée le 21 mai 2010.

Rarement des centaines de milliers personnes se seront ainsi retrouvées bloquées aux quatre coins du monde et le coût exceptionnel de cette crise dépasse probablement le milliard d'euros.

Garantir la sécurité aérienne, en ordre dispersé

Plusieurs incidents graves ont révélé les conséquences terribles que peuvent entraîner les panaches de volcans en éruption sur les avions ; moteurs abîmés, perte de toute visibilité, brouillage des communications et des instruments de bord.

En France, l'espace aérien a été fermé progressivement, du nord vers le sud, à partir du jeudi 15 avril. Le dimanche, les aérodromes de Nice et Marseille étaient à leur tour concernés, entraînant la fermeture intégrale du ciel français.

La réouverture progressive de l'espace aérien entre le 19 et le 21 avril a été orchestrée en lien avec l'ensemble des partenaires européens.

Cependant, **les préconisations de l'agence européenne de navigation aérienne Eurocontrol expliquaient que chaque Etat disposait d'une marge de manœuvre dans la juste appréciation du phénomène et les possibilités de rouvrir sous certaines conditions son espace aérien.** Chaque gouvernement a donc rouvert son ciel, selon sa propre appréciation, sans harmonisation aucune.

Assurer l'acheminement des passagers bloqués

Plusieurs dizaines de milliers de passagers ont été bloqués à l'étranger ou en France, avec parfois des conditions d'hébergement difficiles. Le Sud de la France, rapidement rendu accessible, s'est alors doté de «plate-formes d'accueil». Une logistique considérable a été mise en œuvre pour ramener à bon port tous les passagers

Les règles européennes en vigueur pour les droits des passagers ont rapidement été difficiles à appliquer. Il est dès lors indispensable de prévoir des mesures adaptées à de telles situations de sorte à éviter la multiplication des contentieux entre les voyageurs et les compagnies.

L'impact économique sur les compagnies aériennes

Le déficit d'activité aérienne qui a résulté de la propagation du nuage de cendres a été significatif, puisque l'on estime que plus de 15 000 vols desservant la France n'ont pu être assurés. Cela représente une perte de 1,7 millions de passagers, soit 1,4% du trafic annuel.

Le bilan financier de cette courte paralysie du ciel pour les transporteurs aériens français s'élève alors à 168 millions d'euros, dont 40 millions d'euros de frais d'assistance aux passagers et 11 millions d'euros consacrés aux vols supplémentaires qu'ils ont affrétés.

Conclusion

D'importants progrès sont à réaliser aux niveaux français et européen, à la lumière des difficultés mises en exergue à l'occasion de cette crise. Ils doivent être déterminants si ce type d'évènement venait à se reproduire. L'ensemble des acteurs du transport aérien, à commencer par les transporteurs eux mêmes, garants de la sécurité, doit s'attacher à rendre les vols possibles malgré les cendres volcaniques, en améliorant l'évaluation des risques.

Nuage de cendres, Volcan Eyjafjöll

Bilan du nuage de cendres islandais : 14 avril 2010 – 21 mai 2010
1,2 milliard d'euros pour les compagnies aériennes
260 millions d'euros pour la France
313 aéroports européens fermés
150 000 vols annulés dans le monde
8 millions de passagers bloqués au sol

Source : Retex public à l'Assemblée Nationale, le 8 juillet 2010.

Points positifs ou de satisfaction	Points négatifs ou d'inquiétudes
Logistique mise en œuvre pour l'acheminement des passagers	Une prévision déficiente et une information incertaine de cette alerte
Mise en place de plateformes d'accueil pour les passagers bloqués	Procédure de gestion de crise peu optimisée
Fonctionnement et résilience des liaisons ACROPOL et ANTARES	Un cas de figure non anticipé, alors qu'un historique existait
	Aucune harmonisation européenne sur la réouverture des espaces aériens
	Conditions d'hébergement des passagers difficiles

Principaux enseignements tirés	
Points positifs ou de satisfaction	**Points négatifs ou d'inquiétudes**
Prise de conscience des conséquences en cascade d'un tel évènement	Mauvaise évaluation des risques
Prise en compte de l'importance de prévoir des mesures adaptées pour la gestion de telles situations	Coût financier considérable
Développement d'une collaboration entre les partenaires européens, sous l'égide d'EUROCONTROL	Difficile coordination européenne dans la gestion de crise

4 - Ile-de-France, une crise majeure causée par…des chutes de neige

La région Ile-de-France a connu un épisode neigeux exceptionnel les mercredi 8 et jeudi 9 décembre 2010. Onze centimètres de neige ont été enregistrés à Paris ; un record depuis 1987. Au-delà de ce constat, ces chutes de neige ont provoqué des perturbations significatives dès le début d'après-midi. Des centaines de kilomètres de bouchons se forment sur les routes franciliennes, bloquant des milliers de passagers et provoquant une pagaille imprévue et difficile à résoudre.

La météo

En effet, l'évènement annoncé s'est révélé plus important que prévu, en intensité comme en durée, soulignant **les limites des prévisions de Météo France.**

De ce point de vue, le retour d'expérience milite notamment pour que Météo France donne une indication du **degré d'incertitude sur ces prévisions** et veille à la cohérence des informations fournies entre le bulletin national et les bulletins régionaux, en raison de la disparité qui a pu être observée à cette occasion.

Mais le Conseil Général de l'Environnement et du Développement Durable (CGEDD) a souligné la difficulté d'exiger de telles prestations à Météo France, celles-ci ne pouvant se faire que dans le respect des règles de la commande publique. En effet, il se trouve qu'en Ile-de-France, la direction interdépartementale des routes d'Ile-de-France (DIRIF) a contractualisé avec Météo France après appel d'offres, mais ce n'est pas le cas de toutes les directions interdépartementales des routes, et il n'est pas acquis que le même opérateur soit retenu au moment du renouvellement du marché.

RATP et OPTILE

Les réseaux métro, RER et tramway de la RATP ont été exploités de façon correcte pendant la journée du 8 décembre. En revanche, **des retards dans les prises de service ont été signalés**, de nombreux machinistes n'ayant pu rejoindre à temps les dépôts ou centres de bus.

Le réseau bus de la RATP (350 lignes pour 4.300 véhicules) s'est quant à lui progressivement arrêté sur une amplitude de trois heures à partir de 12h45, tandis que 80 % des 3.500 véhicules en service ont rejoint les centres bus, 20 % restant immobilisés sur voiries ou dans les gares routières.

Il conviendrait de définir des procédures précises avec les gestionnaires de voirie, de façon à assurer de meilleures articulations avec les collectivités locales pour **prioriser les dégagements de voie**. Il serait également utile de prévoir un équipement spécifique des véhicules dédiés à des lignes désignées comme étant prioritaires.

Le réseau OPTILE, qui regroupe 80 opérateurs en seconde couronne (4.500 véhicules), a également connu une interruption de service, du fait des entreprises selon des logiques de proximité, ou du fait des autorités préfectorales.

Il a cependant été constaté un manque de savoir-faire pour ce genre de situation, les arrêtés préfectoraux ne leur ayant pas toujours été notifiés en temps réel. Il n'existe pas non plus de **plan d'exploitation** des lignes de bus en seconde couronne pour ce type d'évènement climatique.

Perturbations sur le réseau bus RATP

Le réseau «TRANSILIEN» de la SNCF

On constate que le matériel roulant n'a pas été à l'origine de difficultés lors de l'épisode du 8 décembre. Les principales perturbations ont eu pour origine : les difficultés des agents pour rejoindre leurs prises de service du fait de l'état du réseau routier ; les dérangements d'aiguillages non munis de réchauffeurs ou dont les réchauffeurs se sont avérés défectueux ; les chutes de branches ou d'arbres sur les voies ou les caténaires en une dizaine de points. En raison de ces perturbations, la SNCF n'a pu maintenir qu'environ 70 % des trains prévus à la période de pointe du soir (17 h à 20 h).

Stricto sensu, la SNCF n'a pris aucune mesure préalable d'exploitation particulière et s'est efforcée d'effectuer le service prévu.

Il paraît alors opportun pour la SNCF de mettre au point **un schéma directeur des moyens de déneigement et de dégivrage,** et de prévoir **un service spécial lié à des fortes précipitations de neige**, plutôt que de subir de graves perturbations.

Par ailleurs, l'**information de la clientèle paraît avoir été déficiente**, voire même dans certains cas contradictoire, ce qui nécessite que la SNCF élabore là aussi un protocole de diffusion d'informations actualisées et cohérentes selon les différents vecteurs utilisés, tant vis-à-vis des passagers en gare ou dans les trains, que vis-à-vis de ceux qui s'apprêtent à utiliser ce mode de transport.

Perturbations à la SNCF, décembre 2010

Aviation civile

La perturbation du trafic aérien a été due pour l'essentiel au traitement des pistes qui, malgré la mobilisation de tous les moyens, n'a pas permis d'éviter **la suspension des opérations aériennes** tant à Orly qu'à Roissy, faute d'être en mesure de maintenir les pistes en état d'utilisation. Les deux aéroports ont disposé d'une seule piste chacun pendant une part significative du pic des chutes de neige. La fin des chutes de neige vers 18h30 a permis de rendre les pistes à l'exploitation mais avec des capacités très limitées en raison du fort enneigement des parkings et des voies de circulation des avions.

Mais, alors même que les capacités des pistes étaient restaurées, l'exploitation des compagnies aériennes et des plates-formes aéroportuaires a été perturbée par les difficultés que rencontraient les agents des compagnies et d'ADP pour rejoindre Orly et Roissy, du fait de l'indisponibilité d'une partie du réseau routier et des très fortes perturbations des transports en commun à partir du milieu de l'après-midi. De ce fait, et du fait du dépassement des temps de service de vol des équipages qui ont subi des retards, de nombreux vols n'ont pu être assurés en fin de soirée.

Le jeudi 9 décembre a alors constitué une journée de transition pour rétablir les rotations aériennes après les très fortes perturbations de la veille.

Il semble par conséquent indispensable que soit organisé le maintien de l'accessibilité des plates-formes aéroportuaires par la route, notamment celui de l'exploitation des transports en commun de manière optimum.

Par ailleurs, **l'hébergement des passagers « naufragés »** est apparu comme un réel problème. Alors, l'élaboration conjointe entre les cinq compagnies aériennes les plus importantes et les autorités publiques (préfets délégués) d'un plan d'accueil et d'hébergement des passagers (clarifiant notamment les responsabilités de chacun en la matière) apparaît comme un impératif.

Perturbations du trafic aerien à Orly

Réseau routier

Les réseaux routiers gérés par les sociétés d'autoroute, l'État (Direction des Routes d'Ile-de-France), les départements, les communes et notamment Paris sont très étroitement interdépendants. Et pourtant, ce critère d'interdépendance et de multiplicité des acteurs ne fait l'objet d'**aucun dispositif concerté et coordonné.**

Les évènements du 8 décembre ont démontré la rapidité avec laquelle un épisode neigeux peut se transformer en **crise routière majeure et rapidement en crise de sécurité civile.**

Au regard de cette crise, une interdiction de circulation des poids lourds n'aurait pu porter ses fruits que dans la mesure où elle serait intervenue vers midi dans l'ouest parisien. Or, à ce moment, le PC zonal ne disposait pas des indices lui permettant de redouter la situation de blocage.

Il faut donc que l'Etat prenne la mesure juste à temps, en coordonnant une multiplicité d'acteurs et de collectivités, ce qui passe par **le renforcement des relations entre le PC zonal de circulation, le COD zonal et les COD de préfectures,** et la formalisation des transmissions d'information des opérateurs de transports en commun.

Enfin, l'organisation coordonnée du stockage des poids lourds, avec l'identification de circuits de décision clairs apparaît comme une nécessité.

Embouteillage majeur sur le réseau routier francilien

Synthèse : Ile-de-France, une crise majeure causée par…des chutes de neige

Bilan de l'épisode neigeux en Ile de France : 8 – 9 décembre 2010
Crise routière majeure : des milliers d'automobilistes bloqués sur les routes : 400 km de bouchons en fin de journée
Perturbation du trafic aérien, arrêt du réseau bus RATP et interruption du réseau OPTILE
2 000 policiers et gendarmes déployés – 3 000 sapeurs-pompiers déployés
3 300 personnes placées dans des centres d'hébergement d'urgence

Points positifs ou de satisfaction	Points négatifs ou d'inquiétudes
Exploitation correcte des réseaux métro, RER et tramway RATP	Limites des prévisions de Météo France : incohérence entre le bulletin national et les bulletins régionaux
Bonne réactivité des services de secours	Une communication de crise inadaptée et déficiente
Bonne réactivité de certaines entreprises pour garder sur place leurs salariés (Plateau de Saclay)	Une absence d'anticipation des services de circulation routière sur Paris et la petite couronne
Capacités d'hébergement de certaines communes dotées de PCS	Des équipements neige insuffisants pour certains véhicules des services de secours (BSPP, police...)
Décisions de blocage des poids lourds et décisions d'interdiction de circulation pour certains véhicules (transports de matières dangereuses et transports scolaires)	Planification insuffisante de liquide dégivrant pour les aéronefs

Enseignements tirés	
Points positifs	**Points négatifs**
Mise au point d'un système d'aide à la décision	Absence d'indication sur le degré d'incertitude des prévisions météorologiques
Décret du 4 mars 2010 attribuant compétence au préfet de zone de défense pour prendre des mesures de régulation de la circulation sur l'ensemble de sa zone	Manque de coordination et de concertation entre les acteurs, il semblerait que la zone de défense ait été sollicitée trop tard pour la gestion de la situation – également un manque de coordination inter-zonale
Préparation d'un « plan neige » avec notamment l'identification des axes à déneiger en priorité sur l'ensemble du réseau	Manque d'information vers la population, notamment les usagers des transports collectifs (SNCF, RATP, Optile)
Hiérarchisation des zones à risque et élaboration d'un cahier de consignes en cas de crise	Conséquences en cascade d'un épisode neigeux sur le secteur aérien

Les événements du Japon avec l'accident nucléaire de Fukushima, survenant après Three Mile Island (1979), Tchernobyl (1986) et quelques autres catastrophes industrielles ou naturelles, tel que l'ouragan Katrina aux Etats-Unis, montrent une nouvelle fois la vulnérabilité des sociétés technologiquement avancées et leurs difficultés à gérer des situations non prévues.

Des questions sont à se poser quant à la prévisibilité du séisme et du tsunami associé, survenus au Japon le 11 mars 2011, provoquant la mort de 28 000 personnes et dont la facture s'élève à 208 milliards d'euros, soit environ 6% du PIB japonais. Des interrogations surgissent également quant à la gestion de la catastrophe nucléaire de Fukushima, par le gouvernement japonais comme par la société TEPCO.

La mauvaise gestion du gouvernement japonais

L'Independent Investigation Commission mise en place par la fondation **Rebuild Japan Initiative** présidée par Yoichi Funabashi, émet plusieurs critiques dans son rapport d'étude sur la gestion de la crise nucléaire, par la société TEPCO et par les autorités japonaises.

Le comité d'experts tend à démontrer **les insuffisances du gouvernement** de Monsieur Naoto Kan lors de la crise de Fukushima-Daiichi, allant même jusqu'à affirmer que ce désastre est d'origine humaine, plutôt que l'inévitable conséquence du séisme de 9.0 sur l'échelle de Richter.

Naoto Kan, Premier ministre japonais en 2011

Tout d'abord, le rapport avance comme argument que la politique de sécurité nucléaire du gouvernement a largement contribué à la catastrophe. En effet, en 2007, la Commission de sûreté nucléaire japonaise (NSC) déclarait que les mesures de sécurité au Japon étaient en parfaite concordance avec les standards internationaux et qu'ils avaient été hautement estimés. Selon la commission d'experts, le gouvernement aurait alors largement contribué à la mise en place du «mythe sécuritaire de l'industrie électronucléaire», enfermant les autorités dans un discours sécuritaire beaucoup trop idéaliste, qui ignorait jusqu'aux mises à jour technologiques.

L'agence de sûreté industrielle et nucléaire japonaise (NISA) aurait en outre refusé de prendre les mesures recommandées par la commission de régulation nucléaire américaine, pour assurer la capacité de refroidissement des réacteurs dans l'hypothèse d'une attaque terroriste ou de situations similaires. La sécurisation des sites étant potentiellement défaillante, le Japon n'était donc pas prêt à faire face à un tel désastre. Cela constitue, selon les experts, **un grave manquement.**

La commission d'enquête présidée par Koichi Kitazawa, soulève également la question de **la gestion de l'accident nucléaire par le gouvernement**. L'intervention des autorités dans les questions techniques de l'accident lui-même n'a pas été bénéfique et les experts estiment qu'il s'agissait là de temps perdu. Les dirigeants auraient dû se concentrer sur la gestion de la crise, plutôt que de se préoccuper de questions extrêmement complexes que seuls les employés de la société propriétaire du site étaient en mesure de régler.

A ce propos, les experts mentionnent l'excessive interférence des autorités japonaises dans les travaux des salariés de TEPCO gérant la crise sur le site de Fukushima-Daiichi, démontrant **la confusion des gouvernants** face à la situation.

Selon le rapport, l'action du gouvernement japonais a également oscillé entre le micro management hasardeux du Premier ministre et les mesures palliatives mal pensées, exacerbant la confusion de la situation.

Beaucoup de temps aurait été ainsi perdu, le gouvernement se focalisant en plus sur la lecture des textes et règlements administratifs, pourtant en totale inadéquation avec la nature et l'ampleur de l'accident.

En effet, la situation était telle que les autorités japonaises ont envisagé un «scénario du pire» avec l'évacuation des 35 millions d'habitants de l'agglomération de Tokyo, alors qu'elles craignaient de perdre le contrôle de la centrale. Le porte-parole du gouvernement de l'époque, Yukio Edano a même déclaré aux enquêteurs avoir pensé à la fin de Tokyo.

Yoichi Funabashi conclut toutefois que «Naoto Kan a eu ses défauts et moments d'absence, mais sa décision de se rendre en force chez TEPCO et d'insister pour que la société n'abandonne pas la centrale, a sauvé le Japon».

Les insuffisances de la société TEPCO

D'après le rapport de la fondation Rebuild Japan Initiative, **les défaillances systématiques de la société Tokyo Electric Power**, qualifiée d'irresponsable, ont largement concouru à la catastrophe nucléaire de Fukushima.

En effet, consciente des risques, la société avait alerté les pouvoirs publics sans pour autant revoir les normes de sécurité et procéder aux aménagements bâtimentaires et d'infrastructures qui s'imposaient, et qui avaient d'ailleurs été encouragés par les autorités régulatrices. La centrale de Fukushima n'était donc pas préparée à une telle catastrophe, comparable à un second Tchernobyl.

La commission souligne par ailleurs l'aberration d'avoir construit un ensemble de réacteurs nucléaires si proches les uns des autres et sur des failles sismiques. Au cœur de la crise, le directeur de la centrale, Masao Yoshida a ainsi dû gérer simultanément l'accident de trois réacteurs et l'exposition des piscines des quatre unités.

En outre, l'accident aurait été aggravé du fait que, dans la nuit du 11 mars, TEPCO était faussement convaincu que les «isolation condensers» du réacteur N°1 fonctionnaient toujours. Tout le processus de refroidissement des réacteurs et les tentatives pour faire retomber la pression interne ont alors été retardés. **Le manque d'information et le manque de préparation** ont contribué à la perte de contrôle de la centrale, tout comme l'absence de président de la compagnie, Masataka Shimizu, estime la commission d'enquête.

La considération par TEPCO de la question de **l'évacuation des employés de la centrale**, seuls à même de faire face à la crise nucléaire, a également été soulevée par les experts japonais. Dans un rapport publié fin 2011, TEPCO expliquait que seul un retrait temporaire avait été envisagé, et non une évacuation complète de toutes les personnes présentes sur le site, conduisant à l'abandon du site. La commission d'enquête reste néanmoins sceptique sur ce point, le président de la société ayant communiqué au gouvernement son intention de retrait total de la centrale nucléaire, dans la nuit du 14 au 15 mars, ce à quoi s'était fermement opposé le Premier ministre.

Enfin, les auteurs du rapport concluent qu'il ressort de l'enquête sur l'accident de Fukuhsima-Daiichi que **«même dans le pays technologiquement avancé qu'est le Japon, le gouvernement et l'exploitant TEPCO, se sont révélés être anormalement dépourvus et peu préparés pour faire face à une catastrophe nucléaire aussi complexe, et ce à presque tous les niveaux».** Se retrouver sans eau ni électricité était jusqu'alors inimaginable. Ils ajoutent enfin que ces graves manquements auront une incidence certaine sur le peuple japonais pendant des décennies.

Surveillance de la centrale par les ouvriers de la société TEPCO

Conséquences radiologiques au Japon

Suite à l'accident nucléaire, des rejets radioactifs massifs, bien que dix fois moins importants qu'à Tchernobyl ont été réalisés entre le 12 et 25 mars, mais essentiellement entre le 15 et le 17 mars.

Un mois après l'accident de Fukushima, l'IRSN a évalué l'impact radiologique sur les Japonais vivant près du site. Selon l'institut, 70 000 Japonais habitant jusqu'à 80 km de la centrale, étaient susceptibles de recevoir des doses supérieures à 10 millisieverts (mSv) la première année suivant l'accident. Cette évaluation a montré que l'impact dosimétrique sur la population non évacuée pourrait être significatif. En effet, il ressort notamment des calculs effectués par l'IRSN, que 2 200 habitants auraient pu recevoir une dose externe annuelle dépassant les 100 mSv, 3 100 des doses comprises entre 50 et 100 mSv et 290 000 de 5 à 10 mSv (8).

Des **mesures progressives d'évacuation** ont alors été prises dès le 12 mars, date à laquelle les réacteurs de la centrale ont explosé, ce qui a permis de réduire l'impact radiologique potentiel calculé.

Les autorités japonaises ont également publié un **plan d'évacuation des populations** vivant dans certaines communes situées sous les rejets intervenus les 15 et 16 mars. Cette mesure intervient notamment sur la base de la décision de principe de retenir une valeur de 20 mSv comme limite maximale admissible de la dose externe reçue du fait de ces dépôts au cours de la première année d'exposition.

Suite à l'accident survenu à la centrale nucléaire, les autorités japonaises ont ainsi largement évacué les zones touchées, limitant l'exposition au rayonnement de la population.

Population évacuée, ville de Yamagata, Japon

(8) La dose acceptée pour un travailleur du nucléaire est de 20 mSv par an, en activité normale.

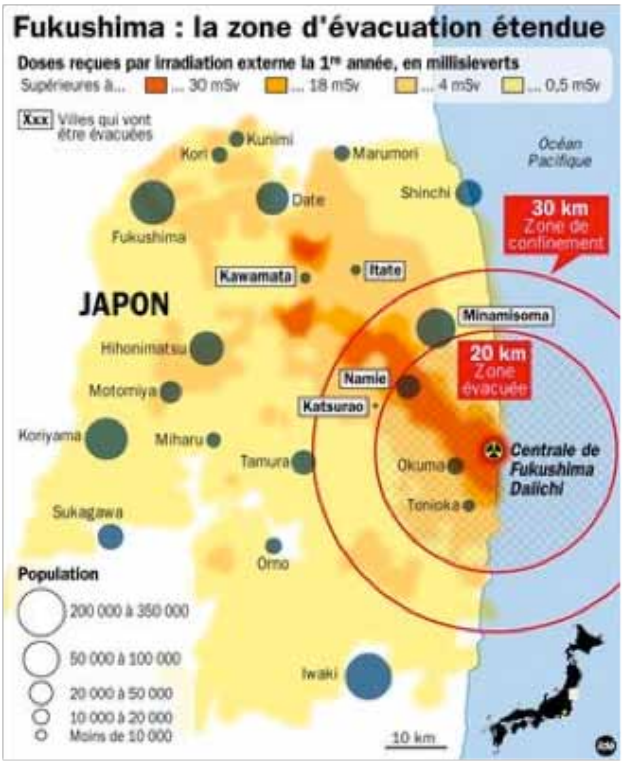
Un zonage post-accidentel a même été défini par le gouvernement japonais en avril 2011, puis réactualisé, pour assurer la protection des populations résidant dans la préfecture de Fukushima. L'accident a en effet entraîné l'exposition radiologique des hommes et de l'environnement au-delà de la zone d'évacuation :

- **une zone «interdite d'accès»** : zone de 20 km évacuée dès le début de la crise ;
- **une zone d'évacuation planifiée :** territoires au-delà des 20 km où la dose dépasserait 20 mSv pour les douze mois à venir du fait de l'exposition externe aux substances radioactives déposées dans l'environnement ;
- **une zone d'évacuation préparée :** territoires compris entre 20 et 30 km non concernés par la zone d'évacuation planifiée.

Les zones les plus contaminées par les substances radioactives sont aujourd'hui interdites d'accès et les populations y résidant ont été relogées. Au-delà de ces territoires, **des actions de décontamination et de surveillance renforcée** sont engagées.

Il est en effet important d'engager au plus tôt des actions de protection vis-à-vis des populations, en éloignant celles qui se trouvent dans les territoires les plus contaminés et qui pourraient être ainsi exposées à des doses significatives dès les premiers mois suivant la formation des dépôts.

L'IRSN a ainsi estimé que les doses potentiellement reçues au cours du premier mois par exposition externe due aux dépôts, représentent environ le tiers des doses cumulées au cours des douze mois suivants. A titre d'exemple, les estimations réalisées montrent qu'une dose dépassant 10 mSv aurait pu être reçue entre le 15 avril 2011 et le 15 avril 2012 dans la zone correspondant approximativement à la zone d'éloignement planifiée mise en place à partir du 22 avril, par les autorités japonaises.



sciences.blogs.liberation.fr

Enfin, toujours selon l'IRSN, la centrale de Fukushima-Daiichi aurait émis 6,1 millions de térabecquerels de radioactivité, soit environ 50% de la radioactivité émise à Tchernobyl en 1986. A l'échelle humaine, cette radioactivité mettra trente ans pour diminuer de 50% et ne pourra être considérée comme négligeable que d'ici quatre-vingt dix ans seulement.

Les conséquences sanitaires au Japon

La comparaison avec Tchernobyl permet de comprendre pourquoi **l'impact environnemental, mais surtout sanitaire sera très inférieur,** alors que l'accident en lui-même est plus grave, avec la destruction de trois réacteurs. Tout d'abord, l'émission de radioactivité est inférieure, puis les populations à moins de 20 km ont été évacuées avant les émissions, et enfin, l'essentiel est parti vers l'Océan Pacifique, pour s'y diluer.

Concernant l'impact environnemental, l'agence japonaise de sécurité nucléaire a toutefois indiqué le 31 mars 2011, que la radioactivité dans l'eau de mer au large de la centrale était 4 385 fois supérieure à la limite admise. La question de la réaction de l'eau de mer reste ouverte, cette expérience étant un cas de figure complètement inédit à l'échelle planétaire.

Les estimations effectuées en 2011 des doses potentiellement reçues montrent d'ailleurs que **le domaine marin aurait été le plus impacté.**

1ère phase de rejet (du 12 au 14 mars) : vers le nord de Fukushima Dai-ichi et au-dessus du Pacifique

2ème phase de rejet (du 15 au 16 mars matin) : 1er épisode de contamination terrestre au Japon

Dès la fin du mois de juin 2011, **les autorités sanitaires japonaises ont mis en place des études épidémiologiques** sur quatre groupes différents : femmes enceintes, enfants, personnes présentes à Fukushima pendant la phase de rejets de particules radioactives et personnes évacuées des zones les plus exposées. L'objectif de ces études est **d'évaluer l'état de santé des personnes exposées aux rejets radioactifs** et de détecter des pathologies, tels que les cancers, les leucémies ou encore les troubles psychologiques et thyroïdiens.

L'IRSN a pu obtenir les premiers résultats d'un bilan thyroïdien effectué chez les enfants à la fin de l'année 2011. Bien que ces résultats initiaux ne permettent pas encore de mettre en évidence l'augmentation des cancers de la thyroïde, ils démontrent que sept enfants sur dix présentent une échographie thyroïdienne normale, tandis que les autres ont développé des kystes ou des nodules.

Par ailleurs, dans le cadre des travaux menés en 2011 sur l'évaluation des rejets atmosphériques et la modélisation de leur dispersion au-dessus du Japon, l'IRSN a évalué les doses potentiellement reçues. Ainsi au cours de la phase de rejet, une dose dépassant 10 mSv aurait pu être reçue jusqu'à une quarantaine de kilomètres au sud, et **des doses dépassant 50 mSv n'auraient pu être atteintes qu'à l'intérieur d'un rayon de 20 km,** correspondant à la zone évacuée en urgence le 12 mars.

Concernant les doses de la thyroïde, des valeurs théoriques dépassant 50 mSv auraient pu être reçues jusqu'à une soixantaine de kilomètres au sud de la centrale.

A propos des travailleurs impliqués dans les opérations menées à la centrale nucléaire de Fukushima-Daiichi, les seules informations disponibles quant aux doses reçues sont celles fournies par la société TEPCO. Ainsi, le dernier bilan publié par la compagnie le 31 janvier 2012 porte sur 3 368 salariés de TEPCO et 16 226 salariés des sociétés sous-contractantes.

Il rapporte que la dose moyenne reçue entre le 11 mars et le 31 décembre 2011 par ces travailleurs est de 23,53 mSv pour les premiers, et de 9,06 mSv pour les seconds. Six employés de la société TEPCO ont également reçu une dose supérieure à 250 mSv.

A plus grande distance, les doses potentiellement reçues pendant la phase de rejet, en l'absence de protection, auraient été nettement plus faibles. Ainsi, elles auraient été en dessous de 10 mSv pour la dose efficace et de l'ordre de 0,1 mSv dans l'agglomération de Tokyo.

Les conséquences à long terme

Peu de temps après l'accident, André-Claude Lacoste, président de l'ASN déclarait à propos des rejets radioactifs, «(ils) sont d'ores et déjà importants (et il) faut donc s'attendre à ce que le Japon ait à gérer durablement les conséquences de rejets importants sur son territoire, c'est un problème que le Japon aura à traiter pendant des dizaines et des dizaines d'années.».

En effet, dès l'apparition des premières traces de contamination radioactive, la question s'est évidemment posée de l'impact à long terme de Fukushima. Les premières contaminations ont d'abord été mesurées sur du lait et des épinards à proximité de la centrale nucléaire, puis dans l'eau courante jusqu'à Tokyo, et enfin dans l'eau de mer prélevée à 100 mètres de la centrale. **La liste de produits contaminés n'a d'ailleurs cessé d'augmenter depuis le 11 mars 2011.** Selon le ministre de l'environnement japonais, Goshi Hosono, «la décontamination est le plus gros défi pour la reconstruction de Fukushima».

Une véritable fièvre de la décontamination s'est alors emparée de la région de Fukushima, alors que les rejets radioactifs de la centrale sont désormais minimes. Selon un dernier rapport de TEPCO, 0,06 million Bq/h s'échapperait encore des réacteurs, ce qui augmenterait la radioactivité à la sortie du site de 0,1 mSv par an environ.

Le plan gouvernemental japonais a prévu de diviser le territoire contaminé en deux parties. Ainsi, dans les zones où la radioactivité dépasse les 20 mSv par an, le gouvernement mène directement des opérations de décontamination, mais aucun objectif n'a été déterminé. Dans les autres zones, entre 1 et 20 mSv par an, ce sont les communes qui s'en chargent, avec pour objectif de diviser par deux la radioactivité d'ici à deux ans. Enfin, chacune de ces communes doit concevoir un **plan municipal de décontamination.**

Concernant la zone voisine de la centrale, où plus de 100.000 personnes ont été évacuées, **la question du retour** est particulièrement sensible. Personne ne peut en effet leur promettre un retour dans ces environs sinistrés. L'Agence Japonaise de l'Energie Atomique (JAEA) rappelle alors à ce propos que « à l'inverse de l'ex-URSS, le Japon ne peut se permettre d'abandonner une partie de son territoire ».

Mais malgré de nombreuses mesures prises en faveur de la décontamination, le gouvernement japonais a été contraint de reconnaître qu'il y avait peu d'espoir de reconquérir un jour les zones où la radioactivité dépasse les 50 mSv par an. Cela correspond à un territoire d'environ 250 km2 au nord-ouest du pays, depuis la centrale nucléaire.

Le chantier s'étend largement au-delà du site même de Fukushima-Daiichi, puisque ayant relevé d'importantes densités d'éléments radioactifs dans le sol sous la mer en bordure de la centrale, TEPCO a décidé de construire un gigantesque plancher au fond de l'eau, afin de fixer les particules radioactives.

Enfin, sur le sujet de l'avenir de la centrale elle-même, le Premier ministre japonais annonçait en décembre 2011, que les réacteurs de la centrale étaient stabilisés et qu'elle se trouvait en «**arrêt à froid**». Les systèmes de refroidissement en continu ont pu être rétablis et ont permis de stopper la fusion du combustible, évitant ainsi de nouvelles explosions d'hydrogène.

Cette étape a alors marqué **la fin des opérations d'urgence et le début du chantier du démantèlement** qui pourrait durer une quarantaine d'années et mobiliser des milliers de personnes. Le site est en effet condamné, quatre des six réacteurs étant endommagés. A titre comparatif, il avait été nécessaire d'attendre six ans avant de récupérer la charge d'uranium partiellement fondu à Three Mile Island.

Et dans le cas de Fukushima, la tâche sera plus compliquée. Les structures y sont en effet fragilisées, de sorte qu'**une aggravation n'est pas exclue en cas de nouveau séisme ou tsunami.**

Résilience japonaise

La commémoration du premier anniversaire de la catastrophe nucléaire de Fukushima est l'occasion de rendre hommage aux survivants du désastre et plus généralement à la résilience du peuple japonais suite à cette crise majeure.

Au regard du drame vécu par le peuple japonais, la question de la possibilité de survivre et de reconstruire suite à une catastrophe nucléaire majeure doit effectivement être évoquée. Le Japon démontre en effet son **exceptionnelle résilience** face aux assauts répétés des catastrophes naturelles et humaines.

A ce propos, Seiichiro Yonekura, professeur à l'Université de Hitotsubashi affirmait lors d'une conférence, que **toute crise constitue l'occasion de construire une société meilleure.** Au vice-maire de Tokyo, Naoki Inose de surenchérir alors, en déclarant que «les Japonais ne puisent jamais leur énergie que dans les crises».

Afin de traiter de la résilience japonaise, il est nécessaire d'évoquer **la culture du risque au Japon**. En effet, alors que le tsunami s'apprêtait à frapper les côtes orientales du pays le 11 mars 2011, plus de 90% de la population concernée s'était déjà réfugiée en lieux sûrs. Ainsi, grâce aux systèmes d'alerte rapide, aux exercices d'évacuation d'urgence et à l'accent mis sur l'information sur la réduction des risques liés aux catastrophes naturelles, des milliers d'habitants des zones sinistrées ont pu être sauvés, bien que les niveaux d'ampleur du risque de tsunami aient été sous-évalués. **Etant préparé au pire, la culture du risque du pays a donc un fort impact sur sa résilience.**

Mais comme évoqué précédemment, cela est en grande partie dû au fait que le Japon est plus exposé que n'importe quel pays aux catastrophes naturelles. Dès lors, il se prépare à les affronter, par l'éducation des populations et par l'adaptation des constructions aux risques sismiques. Les citoyens s'entraînent ainsi dès l'école à se protéger des séismes et le Japon développe l'art de bâtir antisismique.

Aux normes techniques s'ajoute donc la préparation psychologique, en apprenant dès le plus jeune âge à se comporter convenablement en cas de catastrophe, au plan humain et de manière opérationnelle.

La capacité de résilience du Japon s'illustre également par la mobilisation des forces d'autodéfense japonaises (JSDF), massive et immédiate : 50 000 militaires à J+3 et 100 000 à J+8 pour la gestion du séisme, mais également de la crise nucléaire.

Les JSDF ont ainsi mis en oeuvre des moyens du génie et la marine a déployé près d'une cinquantaine de navires pour le transport logistique et l'acheminement de vivres. Les forces aériennes quant à elles, ont engagé près de 500 aéronefs pour le redéploiement des personnels, les reconnaissances et l'évacuation des victimes de la catastrophe.

De même, la spécificité de la société japonaise joue un rôle majeur dans la résilience du pays. En effet, la cohésion du peuple japonais a été décisive dans la période qui a suivi le séisme et le tsunami. La valeur du groupe tient une place importante dans la culture japonaise et permet d'expliquer l'absence de panique des Japonais, qui préfèrent se mobiliser ensemble, supporter ensemble, plutôt que de perturber l'ensemble de la société. La force collective dont fait preuve la population japonaise entre donc dans l'étude de la résilience japonaise.

La civilisation japonaise a ainsi contribué à gérer l'après-séisme, avec notamment l'exemple significatif de la population secourant les victimes et déblayant les zones sinistrées sans attendre la police et l'armée.

La rapide reconstruction des infrastructures après l'événement illustre également la grande capacité de résilience du Japon, les autorités locales invitant même les familles à revenir, tout juste un an après le 11 mars 2011. Il en est de même avec la rapide remise en état des principaux axes de communication et de réseaux d'électricité.

Les actions françaises

Le vendredi 11 mars, au regard des premiers éléments filtrant quant à l'impact du séisme sur les réacteurs nucléaires de la centrale de Fukushima, l'IRSN active son centre technique de crise (CTC). Ce marathon durera quatre semaines, avec la présence permanente d'au moins 30 experts, de jour et 20 experts, de nuit.

Les spécialistes ont également dû relever le défi de la transparence pendant toute la durée de l'accident de Fukushima. Le tout premier rôle de l'ASN après la catastrophe a donc été d'informer les populations sur les évènements.

En effet, **l'ASN et l'IRSN ont participé à la Cellule interministérielle de crise (CIC)** chargée de définir les mesures de contrôle des personnes et des produits en provenance du Japon. Le territoire français n'étant pas atteint, il s'agissait donc de mener des actions de contrôle des produits importés d'Asie. N'ayant pas non plus de rôle technique à assumer, elle a eu une mission d'information et de gestion de crise.

Par ailleurs, dans le cadre du **dispositif de contrôle de l'impact à très longue distance des rejets radioactifs de l'accident, l'IRSN a mis en place une surveillance renforcée de la radioactivité sur l'ensemble du territoire français.** Cela s'est traduit par un renforcement de la vigilance sur les dispositifs traditionnels de l'institut, associé à un déploiement de moyens complémentaires, tant pour la surveillance de la radioactivité ambiante que la surveillance par prélèvements d'échantillons dans l'environnement.

Les observations réalisées ont permis de montrer que les régions françaises ont été touchées de façon similaire : ont été relevées des traces des principaux radionucléides rejetés dans l'air lors de l'accident. Elles ont également révélé qu'il n'y avait aucun risque environnemental ou sanitaire.

Concernant les actions matérielles organisées suite à l'accident, ont été envoyés sur le terrain, des agents de la sécurité civile, afin d'aider aux opérations de secours. La mission française avait pour objectif d'assurer **des missions de sauvetage-déblaiement** sur la zone sinistrée.

Au vu des circonstances, une mission nationale d'appui à la gestion du risque nucléaire, dépendante de la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC) a été mise en place. Les autorités françaises ont décidé d'engager des spécialistes en matière de lutte contre les risques nucléaires et radiologiques afin d'accompagner le détachement français de la sécurité civile. Leur mission principale consistait à assurer la sécurité radiologique des personnels du détachement.

Ces équipes d'intervention regroupaient pour la plupart **différents corps de la sécurité civile**, étant ainsi composées de sapeurs-sauveteurs des formations militaires de la sécurité civile (UIISC), de sapeurs pompiers de Paris et de sapeurs pompiers de différents départements, mais également d'experts de l'IRSN.

La présence de ces derniers, dont la mission était d'assister l'ambassade de France, a également permis aux différents détachements de maintenir une liaison avec le centre technique de crise de l'IRSN.

Intervention de sapeurs sauveteurs de la Sécurité Civile française dans la région de Sendaï

L'impact en France - Retex

Le 23 mars 2011, **le Premier ministre a saisi l'Autorité de sûreté nucléaire**, en application de l'article 8 de la loi du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire. Il a en effet demandé à l'ASN de réaliser **une étude de la sûreté des installations nucléaires, au regard de l'accident survenu à la centrale de Fukushima,** audit complémentaire aux démarches de sûreté mises en œuvre par les exploitants nucléaires sous le contrôle de l'autorité. Le Premier ministre souhaite une vérification «installation par installation, (afin de voir) si des améliorations sont nécessaires à la lumière des enseignements qui seront tirés de l'accident de Fukushima.». C'est l'objet des évaluations complémentaires de sûreté (ECS) demandées aux exploitants français le 5 mai 2011 par l'ASN.

Cela conduit à évaluer jusqu'à quel niveau de séisme et d'inondation les centrales françaises peuvent résister à des agressions naturelles extrêmes.

En complément des évaluations complémentaires de sûreté, l'ASN a également engagé en 2011, **une campagne d'inspections ciblées sur des thèmes en lien avec l'accident de Fukushima.** Menées sur l'ensemble des installations nucléaires jugées prioritaires, ces inspections visent à contrôler la conformité des matériels et de l'organisation de l'exploitant au regard du référentiel de sûreté existant. Les thèmes alors abordés concernent la protection contre les agressions externes, en particulier la résistance au séisme et la protection contre les inondations, la perte des alimentations électriques et des sources de refroidissement, ainsi que la gestion opérationnelle des situations d'urgence.

Ces nouvelles mesures d'évaluation de l'ASN, constituant la première étape d'un long processus de retour d'expérience, rendent bien compte de l'ampleur de l'impact de l'accident nucléaire de Fukushima. «Elles vont déboucher en France sur un renforcement de la capacité des installations à maintenir leurs fonctions fondamentales de sûreté face à des agressions nettement plus importantes que celles retenues lors de leur conception», espère Caroline Lavarenne, chargée des évaluations de sûreté.

Ainsi, un certain contrôle se développe et l'on voit se dessiner **la prise de conscience de l'importance du retour d'expérience par les dirigeants.** Le retour d'expérience complet d'une telle crise prendra néanmoins 10 ans, tant les problématiques soulevées en matière de sûreté nucléaire, de gestion de crise et d'information aux populations sont nombreuses.

Conclusion

Cette triple crise aura amené les gouvernements à prendre des mesures de prévention et à développer les contrôles des exploitants nucléaires, face à la catastrophe «imprévisible» (mais l'était-elle vraiment ?) vécue par les Japonais. L'accent est donc mis sur la prévision et la prévention d'une telle crise, ainsi que sur le développement des moyens et outils de gestion de crise et, pour la centrale de Fukushima, des travaux de remédiation qui prendront de l'ordre de 40 ans.

Contrôle des installations nucléaires par l'ASN

Synthèse : la catastrophe de Fukushima

Rappel du bilan de la catastrophe du séisme et du tsunami Japonais: 11 mars 2011
28 000 morts ou disparus
Coût évalué à 208 milliards d'euros
Soit environ 6% du PIB japonais

Bilan de la catastrophe de Fukushima
Mars 2011 : arrêt immédiat de 11 réacteurs nucléaires, sur les 55 du pays
Juin 2012 : arrêt total des 55 réacteurs du pays

Points positifs ou de satisfaction	Points négatifs ou d'inquiétudes
Forte politique de prévention et d'information des populations sur les risques sismiques	Remise en cause de la prévision et de la planification sur des effets dominos mal ou insuffisamment pris en compte (séisme, tsunami, accident nucléaire)
Qualité de résilience psychologique exceptionnelle du peuple Japonais	La remise en cause de la conformité des mesures de sécurisation des sites avec les standards internationaux
Intervention massive des forces d'auto-défense japonaises (JSDF) – 100.000 hommes mobilisés et 20.000 personnes secourues	Manquements graves en matière de pilotage et de gestion de crises inter-acteurs, notamment entre le niveau gouvernemental et TEPCO
Gestion efficace de l'évacuation des populations	Une communication très insuffisante vers le public, y compris dans la post-crise

Premiers enseignements de la catastrophe de Fukushima	
Points positifs	**Points négatifs**
Malgré une gestion de crise chaotique, la détermination du Premier ministre face à TEPCO dans la phase cruciale de la menace d'abandon du site	Des infrastructures nucléaires sous équipées en matière de sureté face aux situations d'exception
L'intervention des unités NRBC et de sapeurs-pompiers qui ont permis de refroidir les piscines de combustibles	Une préparation à la crise et une gestion de crise très en dessous des enjeux, compte tenu des risques et des conséquences potentielles
La mise en place des mesures de desserrement efficace ayant réduit les risques d'exposition des populations	Un manque de réactivité (coordination) entre les niveaux de radiations mesurés et les mesures à prendre, notamment en dehors des zones de desserrement, ainsi que la non prise d'iode sur les populations exposées (notamment enfants) dans des délais rapides
La capacité du pays à prendre en charge un démantèlement sur 40 ans	Des risques sanitaires avérés mais non encore mesurables (aucun mort aujourd'hui en conséquence des irradiations)
La réduction importante et volontaire de la consommation électrique dans la population dans les mois qui ont suivi pour permettre un redressement économique plus rapide	Une communication vers la population à revoir

Des dénominateurs communs

Grâce à ces principaux retours d'expérience, nous pouvons relever plusieurs points communs entre les différentes crises :

- Des coûts économiques et parfois humains considérables
- Un manque «d'imagination et d'analyse» sur les conséquences d'événements potentiellement possibles, notamment sur les effets «domino»
- Consécutivement, un manque de prévention et de préparation à la hauteur des enjeux qui sont souvent sous-évalués
- Une évaluation des risques parfois sous-estimée, notamment en début de crise
- Des systèmes d'alerte encore trop souvent défaillants
- Des procédures de gestion de crise encore trop peu testées, notamment dans le cadre de crises complexes impliquant de nombreux acteurs
- Des systèmes de communication de crise pas assez fiables
- Un facteur humain fragile et un entrainement (professionnalisation) encore insuffisant des gestionnaires de crises
- Le plus souvent, un retour d'expérience intégré dans la planification pour prévenir la prochaine crise de même nature, représentant donc un progrès mais qui s'étiole dans le temps.

Cela permet également de prendre en note les points forts et les points faibles communs de **la gestion des crises**

Points forts et avancées globales	Points faibles et inquiétudes
La mobilisation et la réactivité des secours aux personnes	Toujours une faiblesse et un manque de réactivité et de clarté dans l'alerte, la communication et l'information aux populations tant préventives qu'à chaud
Prise de conscience de l'importance de la préparation à la gestion de crise par les principaux acteurs	Une gestion de crise complexe à déchiffrer par le citoyen, due à une absence de communication publique par « temps calme »
Inclusion des grands opérateurs d'infrastructures dans la gestion de crise d'ampleur nationale	Lacunes dans la communication et la coordination entre acteurs et parfois une absence de professionnalisation des acteurs de gestion de crise
Développement des plans de prévention et des procédures de continuité d'activité pour les organisations importantes	Faible anticipation ou amplitude de certains phénomènes et parfois mauvaise acceptabilité du risque sur les territoires
Bonne couverture assurantielle	Des textes réglementaires, pas toujours respectés en matière de prévention, notamment sur les règles d'urbanisme
Un renfort de la prévention et de préparation dans le secteur clé et sensible du nucléaire	Toujours une faible préparation aux évènements exceptionnels au niveau social : entreprises, collectivités, familles
	Peu de prise en compte de l'historique et des antécédents dans la préparation aux crises ; toujours une faible préparation aux évènements exceptionnels au niveau social : entreprises, collectivités, familles

Centrale nucléaire de Fukushima-Daiichi après le tsunami

3

LA GESTION DE CRISE EN FRANCE

Introduction

Ce chapitre a pour objet essentiel de faire le point sur la problématique de la gestion de crise en France, dans ses dimensions stratégiques, organisationnelles et partenariales.

Il n'aborde pas en profondeur le problème des moyens et des budgets qui seraient nécessaires pour doter notre pays d'une organisation de gestion de crise et de sécurité nationale plus robuste. Il n'aborde pas non plus la question des moyens d'actions des différents acteurs, sur les différentes problématiques de gestion et de réponses aux risques par le biais de secours spécialisés ou non. Le prochain rapport annuel du HCFDC se penchera plus spécifiquement sur ces sujets.

En France, la «gestion des crises» repose sur des principes liés aux compétences de police administrative générale dévolues au maire, aux préfets de départements et de zones et au Premier ministre, amenant ces autorités à prendre les mesures nécessaires pour prévenir et faire cesser les atteintes à l'ordre public, ainsi que pour protéger les populations et les biens.

Quel ministre pour conduire la crise ?

Cette structure est complétée par une multiplicité de dispositions visant soit à attribuer une compétence de réglementation dans un domaine particulier (police spéciale), soit à régler l'organisation des services appelés à intervenir en situation de crise (services de secours, police, services sanitaires), soit encore à instituer des procédures particulières au temps de crise et utiles à ses gestionnaires (réquisitions, mesures d'urgence etc.), et ceci en dehors des situations juridiques exceptionnelles prévues dans nos textes : état d'urgence et article 16 de la Constitution.

Cette situation est formalisée au plus haut niveau de l'Etat par une circulaire du 2 janvier 2012, qui précise les conditions dans lesquelles s'exerce la gestion des crises, et ce, au delà des situations d'urgence habituellement gérées par les services compétents (police, gendarmerie, sapeurs-pompiers, SAMU), sous l'autorité d'un directeur des opérations de secours (maire ou préfet).

Si cette circulaire clarifie le rôle de la gestion interministérielle des crises, elle ne clarifie a priori pas la désignation du ministre conducteur de crise.

En fonction de la nature des crises, trois ministères sont prédéfinis comme ayant «une responsabilité particulière dans la préparation et la gestion des crises». Il s'agit du ministère de la Défense, pour les crises concernant les forces armées, du ministère des Affaires étrangères pour toutes les crises impliquant nos ressortissants en dehors du territoire national, et du ministère de l'Intérieur, dès lors que les questions de sécurité civile, d'ordre public et de continuité de la vie collective deviennent prédominantes.

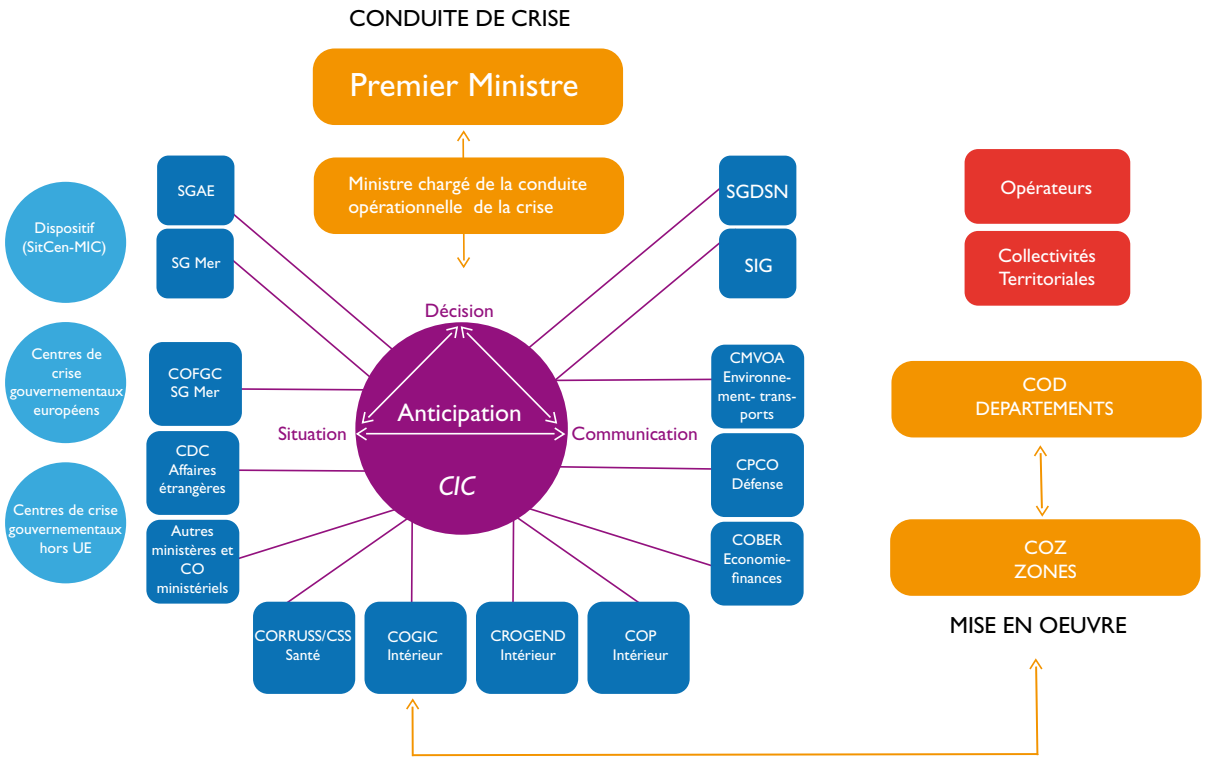


Schéma de l'organisation française de la gestion de crise

Mais la désignation du ministère n'intervient qu'après arbitrage du Premier ministre, afin d'«assurer en son nom la conduite opérationnelle de la crise». Cela soulève alors le problème d'un **éventuel flou «politique» pendant les premières minutes ou les premières heures de la crise** (surtout à cinétique rapide), même si dans les cas les plus graves, on peut penser que le ministre de l'Intérieur serait désigné pour les crises se déroulant sur le territoire national.

Nous avons néanmoins pu observer dans des crises récentes, que cette direction pouvait être confiée à d'autres ministres, comme le ministre de la Santé lors de la pandémie grippale dans sa phase initiale, le ministre de l'Ecologie lors de la crise sociale «hydrocarbure» et la crise du volcan, mais également au SGDSN lors de la crise de Fukushima, gardant la main pour le Premier ministre.

Cela pose donc **la question de l'autorité première de gestion de crise** qui, finalement, en dehors du Premier ministre n'est pas réellement définie.

Deux difficultés corollaires apparaissent alors, avec d'une part, **la fluidité des décisions et des mécanismes de gestion de crise** durant les premières minutes ou heures de la crise, et d'autre part, la problématique du «**basculement de pilotage**» entre les ministères techniques et le ministère de l'Intérieur et, dans les cas les plus graves, en cas d'empêchement du Premier ministre, et/ou du Président de la République, la question de savoir «**qui pilote ?**», et ce à tout moment.

Dans ce cadre, on pourrait imaginer de stabiliser la doctrine sur des fondamentaux solides : soit le ministre de l'Intérieur est le gestionnaire de la crise au niveau interministériel par délégation permanente, soit cette gestion de crise est assurée de manière directe au niveau du Premier ministre avec le soutien du SGDSN au moyen d'une «CIC» ad hoc 7/7 H24, et donc un centre opérationnel dédié à cette CIC, lequel n'existe pas aujourd'hui.

Le Centre Beauvau (Centre Interministériel de Crise) deviendrait alors le centre de pilotage interne du ministère de l'Intérieur, outil d'un ministère technique comme les autres, à ceci près qu'il hébergerait la synthèse des trois centres opérationnels : Sécurité Civile (COGIC), Police (COPN), et Gendarmerie (CROGEND) ; lesquels seront peut-être un jour rassemblés, comme le sont les forces armées, au sein d'un «**CPCO**(9) **Intérieur**» ? Cela gagnerait certainement en cohérence, en coût et en efficacité.

Salle de décision, Centre Intermistériel de Crise, Centre Beauvau

Le dispositif de planification

En matière de planification, la France s'est dotée d'un système complet et cohérent pour gérer tant au niveau interministériel que ministériel, la planification face à tous types de risques ou menaces.

Au plan territorial, **le dispositif ORSEC est maintenant clair, mais il n'exclut pas le travail important de mise à jour d'annexes spécialisées**, notamment au niveau départemental.

La problématique que pose le **plan Vigipirate** semble néanmoins d'actualité. Elle a été soulevée à l'occasion de l'affaire de Toulouse et de Montauban. Cinq ans de Vigipirate «rouge» ont-il donné du sens à la démarche Vigipirate pour bien expliquer ce passage en «écarlate» ?

Il y a aujourd'hui une révision des échelles à entreprendre pour permettre une bonne compréhension des situations par les populations. Les USA viennent d'ailleurs de supprimer le code couleur pour un autre système. Si nous voulons garder ce code couleur, un code orange pour les situations de menaces «non avérées», rouge pour prévenir des «attentats limités» et écarlate pour les attentats de «grande ampleur» supposés ou craints, serait probablement plus facilement compréhensible pour la population.

(9) CPCO Centre (interarmées) de planification et de conduite opérationnelle.

Au plan territorial par ailleurs, si le préfet de département est bien le gestionnaire de crise en titre, il faut reconnaître que les moyens dont il dispose ne sont pas toujours en adéquation avec ses missions, et les multiples acteurs n'ont pas toujours conscience de leurs rôles respectifs.

Six inadéquations du dispositif de gestion de crise au plan territorial

Le rapport de Paul Girod(10) sur la gestion territoriale des crises, remis en 2010 au Président de la République, souligne ainsi **six inadéquations ou faiblesses de notre dispositif de gestion de crise au plan territorial :**

1. **Une réelle complexité** créée par l'imbrication de problématiques relativement banales et de questions de principe aux tenants et aboutissants considérables, liés à l'organisation de la société et de l'Etat.

2. **Un «facteur humain» décisif** : les personnels d'Etat chargés de la crise étant souvent mal sélectionnés, insuffisamment formés et ne bénéficiant pas d'une gestion adaptée à leurs contraintes.

3. **Une politique d'exercice trop «convenue» et des retours d'expérience (RETEX) pas assez exploités** ; les RETEX étant sous-exploités, les exercices ne concourent pas assez à la préparation à la crise.

4. **Les équipements de gestion de crise dans les préfectures demeurant de qualité inégale et globalement insuffisants** : malgré l'effort de modernisation engagé dans le courant des années 1990, le bilan actuel fait ressortir une faiblesse globale de la situation des COD, même si certaines préfectures sont bien équipées.

5. **La fragilisation de l'échelon départemental de l'Etat par l'évolution de l'organisation administrative :** traditionnellement compétent pour la gestion de crise, cet échelon est marqué simultanément par les décentralisations et par le renforcement du niveau régional de l'Etat, notamment pour l'expertise sur les grands champs techniques (santé, environnement, finances, énergie...). Dans le même temps, le cœur du dispositif préfectoral de gestion de crise, le SIDPC, est réorganisé, avec des éclatements, des rattachements quelquefois hors du cabinet du préfet et une réduction des effectifs. Ces réformes, mal vécues par les personnels en sous effectif, en dépit de leur objectif de recherche de synergie, présentent des risques non négligeables(11).

6. **Le manque de clarté dans la répartition des rôles entre collectivités et opérateurs,** avec notamment de graves incompréhensions dans le rôle du maire en situation de crise.

Exemple d'une salle de crise d'un centre opérationnel de zone (COZ)

(10) Paul Girod, Membre honoraire du Parlement et Président d'honneur du HCFDC.
(11) Depuis la parution du rapport Girod, une marche arrière a été effectuée dans de nombreux départements pour revenir à une organisation où le SIDPC est rattaché plus ou moins directement au cabinet du préfet.

Paul Girod conclut alors par cette phrase, «dans ce contexte, la société française apparaît fragile face à la crise».

Si l'on se penche plus avant sur les problématiques de gestion de crise territoriale, on constate que différents domaines sont obérés de plusieurs manières.

La planification : une harmonisation souhaitable

La planification est principalement étatique et intègre des influences diverses : planification de sécurité nationale (plans pirate), planification de prévention des risques naturels et technologiques, planification de santé publique, planification de sécurité civile (ORSEC) et locale (PCS, DICRIM...). **Elle n'est pas simple d'accès pour des non spécialistes**. Or, celle-ci a aujourd'hui vocation, au moins pour partie, à être partagée avec les collectivités et les opérateurs, voire avec certaines entreprises.

Une simplification de ces planifications dans un document unique sur le territoire national de planification pour la prévention et la gestion des crises serait souhaitable pour une approche globale et «partagée» des problématiques de gestion de crise au profit de l'ensemble des acteurs, notamment non étatiques, et ce dans la perspective tant des situations de crises «planifiées» que de situations «hors cadre». Il pourrait s'agir d'un document non classifié (certaines annexes pouvant l'être au besoin), incluant une harmonisation des termes, ainsi que des principes de procédures «interministérielles».

Exemple de Totem d'évacuation, ville de Feyzin

Aider les opérateurs de terrain par des actions structurantes de niveau national tant au plan de la conception des systèmes et de leurs environnements techniques et juridiques, qu'au plan de la gestion opérationnelle

Les dossiers structurants de la gestion de crise, tels que sont l'organisation des centres opérationnels (CO), les SIC et SIG (Système d'information et de commandement/système cartographique), l'interopérabilité des systèmes, ou encore les transmissions (jusqu'au niveau local) doivent faire l'objet de **travaux au niveau national en vision «inter-acteurs».** Cela n'est pas le cas aujourd'hui, à l'exception des réseaux radios ACROPOL-ANTARES et de la main courante Synergie, lesquels ne peuvent constituer l'alpha et l'oméga des besoins en matière d'outils de gestion de crise.

L'Etat devrait proposer ou faire proposer **une chaîne de système d'information, de simulation et de communication de gestion de crise interopérable à tous les acteurs concernés : administrations territoriales, opérateurs et entreprises essentielles, et non pas uniquement à l'Etat lui-même**. On peut néanmoins comprendre que certaines informations peuvent et doivent rester confidentielles, ce que permet la technique aujourd'hui, y compris dans des systèmes partagés.

Sur le plan opérationnel, il faut s'assurer que le tamis de l'information remontante ne cache pas le détail essentiel. La mise en place de trois niveaux de synthèse entre le terrain et la CIC (niveaux départemental, zonal et national) peut faire apparaitre une situation lisse, chaque niveau globalisant l'information et donnant au décideur une information lisse. C'est pourquoi **les outils doivent permettre une granularité «sur mesure»**, et ce à tous niveaux décisionnaires.

Un autre problème évoqué par beaucoup d'acteurs, et que l'on a encore observé au Japon lors de la catastrophe de Fukushima, ou peut-être dans le cadre des attentats de Toulouse, est **la tentation du «micro management» des crises par l'échelon central**, ou le défilé ininterrompu de responsables politiques au plus près du terrain en crise, alors que les gestionnaires et les acteurs de secours sont encore en plein travail. Ces situations rendent le travail souvent plus difficile pour les gestionnaires «en charge».

Si ces visites peuvent parfois être justifiées, voire nécessaires, en fonction des circonstances, il convient de mieux former les hauts responsables administratifs et politiques à la gestion de crise, de manière à ce qu'ils prennent en compte les enjeux des comportements en temps de crise, ce qui n'est pas toujours le cas.

De plus, la formation à la gestion des situations d'urgence et de crises, à l'exception des services opérationnels, est notoirement insuffisante, notamment au niveau des administrations centrales, des collectivités et de certains opérateurs. **A titre d'exemple, il est rarissime qu'un ministre en exercice participe à un exercice national.**

Enfin, l'Etat doit aussi assurer **un environnement juridique et financier à la crise et surtout de la post-crise** en dehors des seuls aspects de libertés publiques, notamment pour permettre une facilitation de la poursuite et de la reconstruction économique et sociale des territoires touchés: adaptation du code du travail, conditions de passation des marchés etc., visant à permettre un redémarrage économique le plus rapide possible. En un mot, **le droit de la crise** doit faire l'objet de travaux plus construits au niveau national.

Le rôle du maire et des collectivités

Le rôle du maire est en France extrêmement important en matière de police générale, mais aussi en matière d'actions de prévention, de planification locale et de mise en œuvre du concept de sauvegarde. Ce concept réaffirmé par la loi sur la modernisation de la sécurité civile fixe clairement les missions du maire au regard de la protection des populations, à savoir : interdire, protéger, héberger et alimenter.

Or, de nombreux maires sous-estiment à la fois leurs rôles et leurs responsabilités, ignorant parfois leur rôle de directeur des opérations de secours et leurs responsabilités en matière de prévention et de planification des mesures de sauvegarde.

Une véritable **campagne de responsabilisation** devrait être lancée, ainsi qu'une **réelle obligation de réaliser les PCS**, car sans obligation et surtout sans contrôle, comme c'est le cas aujourd'hui, ceux-ci ne sont, soit pas réalisés, soit pas toujours très opérationnels ou appropriés pour les services.

Se pose également la question du niveau territorial de réalisation des PCS. Il n'est en effet pas toujours facile de le réaliser de manière pertinente dans les petites communes. A cette échelle, on peut penser que l'agglomération de communes serait un niveau plus adapté pour leur réalisation. Quoiqu'il en soit, le système PCS doit gagner en clarté, facilité et flexibilité de mise en œuvre. Par exemple, des applications numériques avec cartographies sur serveurs mutualisés seraient certainement un plus, permettant la flexibilité et l'évolution nécessaire, ainsi qu'une modernité d'outil permettant une mise en œuvre concrète de ces plans.

Exemple de «malette PCS», ville de Tarascon

La problématique est quasi identique pour les DICRIM (Document d'Information Communal sur les Risques Majeurs) qui sont souvent, lorsqu'ils existent (environ 2 000 à 3 000 DICRIM réalisés), des documents peu complets ou compréhensibles et faisant référence à des définitions trop souvent incomplètes ou disparates(12). Un effort important doit être mené pour permettre aux populations d'obtenir des informations fiables et professionnelles.

Enfin, le sujet des **réserves communales de sécurité civile** est toujours d'actualité. Très peu employées et témoignant finalement du faible degré d'implication des communes sur ce sujet, les collectivités se retrouvent très dépendantes, dans la catastrophe, de moyens extérieurs.

Or, les communes ayant mis en place ces réserves, soit sur une base de volontariat au sein des services (St Etienne), soit en mobilisant des jeunes dans une démarche citoyenne (La Seyne sur Mer), tirent un grand bénéfice, non seulement en cas de catastrophe, mais aussi en termes de citoyenneté partagée et de diffusion de la culture du risque et de l'autoprotection par l'effet d'entraînement et de communication.

Il faut par ailleurs poser **la problématique des communications entre services, hors Etat, en temps de crise**. La plupart des collectivités ne possèdent pas de réseaux leur permettant de rester en contact avec les préfectures si les réseaux fixes et mobiles des opérateurs sont hors service. Des initiatives intéressantes, comme en Indre et Loire, visant à la création d'un réseau radio numérique au niveau du conseil général sont encore trop rares.

Au niveau des collectivités territoriales que sont les conseils généraux et régionaux, **les dispositifs de planification et de gestion de crise sont le plus souvent réduits**. Mais même s'il semble exister un système, soit d'astreinte, soit de gestion de crise dans une collectivité sur deux en moyenne, la majorité des conseils généraux et encore moins régionaux, ne sont pas réellement, à l'exception de quelques-uns, préparés à la gestion de crise, alors qu'ils ont des responsabilités importantes tant en matière de gestion des routes, que de gestion sociale ou scolaire. Plus particulièrement, leur rôle en matière de continuité d'activité économique et de gestion post-crise est insuffisamment pris en compte.

Réserve communale de sécurité civile, ville de La Seyne sur Mer

(12) Communication aux Irisés Novembre 2011

Comme le précise le rapport Girod, «la participation des conseils généraux au traitement des crises s'inscrit dans un cadre plus complexe qu'il faut dépasser : ***les départements doivent être systématiquement associés à la préparation des crises***, *ils doivent siéger de droit au COD ; les difficultés juridiques et techniques identifiées sur ce sujet devraient être approfondies au niveau national, avec les associations de collectivités, dans la perspective d'un conventionnement global relatif au traitement de la crise, à décliner dans chaque département, cette démarche justifierait d'une disposition législative».*

Le rôle des grands opérateurs et du tissu économique

Les grands opérateurs représentent aujourd'hui les fonctions essentielles de vie, de survie et de reprise économique pour le pays. Au cœur de tout se trouvent l'énergie électrique et les hydrocarbures, et au-delà, les réseaux d'eau, les transports, le système financier, l'alimentation, les télécommunications et l'Internet. Cette liste n'est toutefois pas exhaustive car, **en fonction de la nature de la crise, chaque entreprise peut devenir «critique ou essentielle» à un certain moment.**

Par le décret de 2006, l'Etat a créé les **«secteurs d'activités d'importance vitale»**. Il a donc désigné au travers des Directives Nationales de Sécurité (DNS), environ 250 entreprises ayant le statut **d'opérateurs d'importance vitale** (OIV). Chaque OIV a pour obligation la réalisation d'un **Plan de sécurité opérateur** (PSO) aboutissant à la désignation de **Points d'importance vitaux** (PIV) (environ 1 500) et à la création d'un **Plan de protection particulier** (PPP) à la charge technique et financière de l'opérateur et d'un **Plan de protection externe** (PPE), à la charge du préfet de département où se situe le PIV.

Ce dispositif, bien conçu, mais essentiellement tourné pour protéger les sites de la menace terroriste, se met en place au sein des entreprises. Il connaît quelques difficultés d'organisation ici ou là, notamment lorsque les plans imposent des travaux de durcissement, toujours difficiles en période économique tendue, mais il se déploie et renforce considérablement la sécurité de ces infrastructures face au terrorisme et à la malveillance.

Barrage de Serre Ponçon

La question qui se pose touche **l'incompréhension qu'il existe parfois entre l'Etat et ces opérateurs sur leurs statuts et liens avec la gestion de crise et la continuité d'activité**. En effet, dans un certain nombre de crises récentes (pandémie grippale et hydrocarbures notamment), les OIV ont pensé que leur statut leur permettait de disposer de «priorités» dans la gestion de ressources rares ou de leurs interdépendances. Hélas non, la planification à froid ne «gère» pas ou très rarement les questions de priorité ou d'interdépendance, les priorités des pouvoirs publics étant avant tout l'ordre public et les secours, c'est-à-dire les métiers du ministère de l'Intérieur. Cependant, des arrangements peuvent parfois être trouvés «à chaud».

Il s'agit donc d'évoquer **l'organisation des grands opérateurs en matière de gestion de crise, de continuité d'activité et de gestion des interdépendances.** Or sur ce point, pas de texte ou d'obligation, seulement quelques bonnes pratiques ici ou là et des situations très diverses. Nous pensons que **pour les OIV, l'Etat devrait mieux cadrer, dans une refonte du système SAIV, l'approche «tous risques» prônée par le Livre blanc et le cycle complet de la crise**, en étant plus clair sur les actions à mettre en œuvre en matière de gestion de crise et de continuité d'activité pour les OIV.

Les opérateurs dits «historiques» sont le plus souvent relativement bien dotés en matière de capacité de gestion de crise et de dotation de plans de continuité d'activité (PCA), avec toutefois deux bémols :

- Les traces profondes laissées par la mauvaise gestion du rapport entre Etat et entreprises dans la pandémie H1N1, qui rend aujourd'hui la préparation des PCA plus difficile en interne ;

- Dans certaines structures, le manque d'intérêt des hautes directions générales sur ces questions, et par voie de conséquence, le manque de formation des dirigeants et des cadres de direction aux situations de crises.

Chez les opérateurs «nouveaux entrants», la situation est plus délicate car on constate **une absence de culture de «sécurité nationale»** et peu de volonté à s'intéresser à ces questions, challenge économique oblige. Il semble qu'à ce titre l'Etat devrait mieux inclure dans les contrats de «concession» ou de PPP(13), les obligations qui doivent peser en matière de gestion de crise ou de continuité d'activité.

Enfin, la question des interdépendances, point clé, n'est elle non plus, pas du tout assurée aujourd'hui. Plusieurs raisons à cela :

- La question est complexe et la modélisation des interdépendances n'est pas encore réellement possible, rendant difficile une planification opérationnelle ;

- L'Etat n'est pas véritablement intéressé à la gestion des interdépendances, hors de son rôle d'intérêt général. Son rôle se situe plus sur la priorisation et l'allocation de ressources rares au moment aigu de la crise, et s'oriente vers les problématiques régaliennes d'ordre public et de secours.

La gestion des interdépendances n'est pas du ressort de l'Etat, il n'en a ni la mission, ni le temps, ni les moyens. Celle-ci est donc bien **une organisation à mettre en œuvre par les opérateurs et pour les opérateurs eux-mêmes**, avec le double intérêt de réduire les pertes économiques et d'être en capacité de délivrer leurs services sous les meilleurs délais.

Ainsi, la problématique consiste, en temps de crise et de post-crise, à avoir les moyens d'analyser les besoins et problématiques réciproques des opérateurs, de manière à optimiser les besoins et les rétablissements en fonction des priorités décidées par l'Etat.

Or l'Etat n'a pas effectivement les moyens d'accueillir les opérateurs avec les moyens ad hoc aux différents niveaux territoriaux, ni aujourd'hui et encore moins demain avec l'ouverture à la concurrence à plus d'opérateurs. Il n'a pas non plus les moyens d'offrir de réelles capacités en matière de renseignements sur l'état des réseaux, de leur partage et de leur analyse.

Il conviendrait que **les opérateurs se groupent pour créer un centre d'analyse des interdépendances**, étude de cas que le HCFDC a proposé à ses membres, mais qui n'a pas reçu aujourd'hui, un accueil favorable des pouvoirs publics.

La continuité d'activité et le retour rapide à une situation économique normale, seuls permettent la diminution des coûts directs et indirects des crises et catastrophes. Une plus grande implication des CCI (Chambre de Commerce et d'Industrie) sur ces thèmes serait d'ailleurs souhaitable.

Les Etats-Unis l'ont d'ailleurs bien compris. Ils ont créé en 2010 le premier BEOC (Business Emergency Operation Center) en Louisiane. Près de 27 projets sont actuellement en cours de réalisation.

BEOC (Business Emergency Operation Center), Louisiane, USA

La société civile et le citoyen

Si la loi de modernisation de la sécurité civile place le citoyen en qualité de premier acteur «au cœur» du dispositif de protection des populations, la réalité est encore toute autre aujourd'hui, et ce pour plusieurs raisons.

a) La communication «grand public»

Le citoyen ne se sent pas impliqué, l'Etat s'affichant toujours dans un rôle très «protecteur» et par cette attitude et par l'environnement ainsi créé, ne pousse finalement pas le citoyen à se responsabiliser en cas de crise grave et à prévoir ses moyens d'autonomie, au moins sur une certaine période (24 à 72h), comme cela est fait aux Etats-Unis ou au Japon.

Même si le gouvernement lance un site «risques.gouv.fr» au travers du SIG (Services d'Information du Gouvernement), site fort bien fait au demeurant, ce site ne fait l'objet d'aucune communication réelle auprès du grand public, le rendant finalement assez confidentiel. Notons par ailleurs que ce site ne prend pas en compte les menaces terroristes et les comportements à suivre face à ces scénarios, notamment NRBC. Il mériterait d'être complété sur ces points.

(13) Partenariat public-privé

L'Etat a donc du mal à infléchir, dans les faits, la doctrine du citoyen «acteur de sa sécurité». Il souffre de l'ancienne tradition «dormez bien, le gué veille», doctrine très ancrée dans une partie de l'administration publique. Malheureusement aujourd'hui, par faute de moyens, l'Etat ne réalise pas de campagnes d'information pertinentes sur ces thèmes, à l'exception notable des risques sanitaires.

b) La communication et les formations de sécurité civile vers les jeunes

Les dispositifs de formation à la sécurité civile et aux gestes qui sauvent, prévus par la loi de modernisation de la sécurité civile, notamment dans le milieu scolaire, ne sont le plus souvent pas mis en œuvre par l'Education nationale, faute de moyens.
Le dispositif ne repose actuellement que sur le bénévolat et les actions directes des associations et dans certains départements, des Sapeurs-pompiers. L'éducation aux risques est ainsi très inégale aujourd'hui sur le territoire.

On note donc que **le système actuel, du plan local au plan national, ne pousse pas le citoyen à être «informé et responsable» face aux risques et menaces majeurs et face à sa propre protection**, un tournant politique majeur reste à prendre en ce sens.

c) La société civile et les associations

Les associations issues de la société civile sont également peu, et le plus souvent mal utilisées par les pouvoirs publics dans les missions de préparation.

Le professeur Lareng déclarait, devant le Conseil national de la sécurité civile, le 23 avril 2008, *«ne pas retrouver, sur le terrain, au sein même de ce grand mouvement d'espoir qu'avait créé, entre nous, le décret du 27 février, décliné par la circulaire du 12 mai 2006, une communion d'idées avec les pouvoirs publics (...). Nos bénévoles sont surpris de ne pas percevoir quelques souffles chaleureux à l'intention de ce qu'ils réalisent toujours avec beaucoup de cœur et dans une volonté loyale de changement.».*

Cette affirmation pourrait être reprise encore aujourd'hui par beaucoup de responsables associatifs du secteur des associations agréées de sécurité civile ou non, qui se plaignent souvent du **peu de dialogue entre l'Etat et leurs structures**. L'Etat considère souvent que les associations sont des «quémandeurs de subventions», alors qu'elles réalisent, à coût souvent extrêmement réduit, des tâches d'animation et de communication, parfois d'actions directes, en faveur des politiques publiques de prévention des risques et de sécurité civile, que personne d'autre ne pourrait réaliser à ces coûts.

Sur ce plan, un dialogue plus «chaleureux» et constructif serait le bienvenue car, au delà du support financier, les associations concourent et concourront encore plus à l'avenir, consécutivement à la réduction des moyens de l'Etat, à la réalisation des politiques publiques dans ce domaine, tant sur la prévention que sur l'action, en étant une interface efficace et à moindre coût entre les différents acteurs : Etat, entreprises, collectivités et population.

La diffusion de l'alerte et l'information de la population

Pourtant prévue par le Code national d'alerte(14) (CNA), l'alerte est mal connue de la population, par défaut d'informations pratiques et par manque d'affichages permanents dans les lieux publics. Il serait alors intéressant que cet affichage soit réalisé au même titre que les consignes de sécurité réglementaires.

Un projet de modification du Réseau National d'Alerte (RNA) a vu le jour en 2004(15), dans une volonté de modernisation de la sécurité civile. Cela ne signifie pas la fin de la sirène entendue chaque premier mercredi du mois à midi, mais représente une adaptation aux nouvelles technologies disponibles.

Ce dossier de l'alerte a été totalement négligé pendant plus de 10 ans et il aura fallu attendre le Livre Blanc de la Défense et de la Sécurité Nationale de 2008 pour le voir resurgir dans la doctrine au travers du concept SAIP (Système d'alerte et d'information des populations).

(14) Le décret n°2005-1269 du 12 octobre 2005 définit le Code national d'alerte. Ce dernier contient les mesures destinées à alerter et informer en toutes circonstances la population, soit d'une menace ou d'une agression, soit d'un accident, d'un sinistre ou d'une catastrophe.
(15) Loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile

Cette nécessité de modernisation a été accentuée suite aux enseignements majeurs tirés des deux grandes catastrophes naturelles survenues durant l'année 2010, la tempête Xynthia et les inondations dans le Var. La vétusté et la mauvaise adaptation des systèmes d'alerte aux risques d'aujourd'hui ont en effet été évoquées dans les chapitres traitant de ces évènements. Ce projet de modernisation repose donc sur la mise en place d'un dispositif d'alerte performant et résistant.

Le SAIP cumule alors deux fonctions :

- Une fonction d'alerte de la population d'un danger imminent ou immédiat;

- Une fonction d'information de cette population sur les consignes de sécurité à suivre et pour donner l'évolution de l'événement.

Il est basé sur des technologies multiples : le déclenchement des 5 650 sirènes (souvent anciennes) du réseau, réparties sur 3 886 communes, et d'autres moyens tels que les 500 automates d'appel et les 3 213 panneaux à messages variables urbains recensés.

Mais l'information du public est surtout prévue via les téléphones mobiles par le biais de la technologie «cell broadcast».

Il s'agit d'une technologie intéressante, mais qui pose un certain nombre de problèmes techniques tant du côté des capacités des terminaux mobiles de différentes générations, toutes ne supportant pas le cell broadcast, que du côté des opérateurs eux-mêmes, qui ne peuvent pas tous le mettre en œuvre, semble-t-il, à courte échéance ou sans financement ad hoc.

Le Livre Blanc avait prévu de «sanctuariser» une dépense de 80 millions d'euros pour ce programme. Où en sommes nous depuis ?

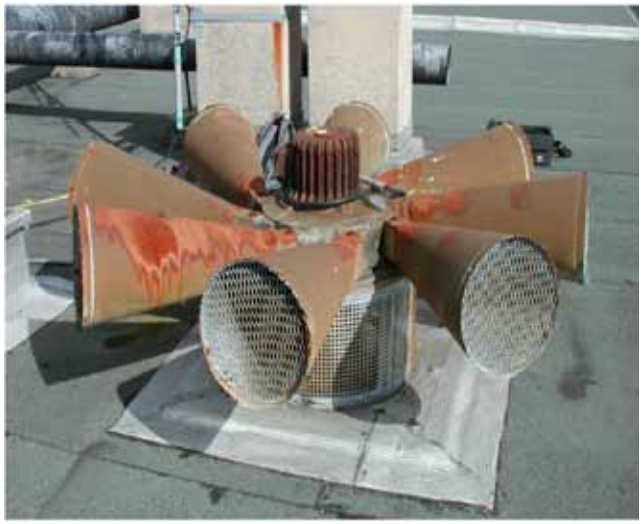
La réalisation du projet est prévue sur une durée de 7 ans (2009-2016). Les études ont été menées entre 2008 et 2012, et un premier marché de développement a été signé pour démarrer le développement du système cette année. 7,95 millions d'euros en crédits de paiement, minorés de 2,5 millions d'euros de coupe budgétaire, ont ainsi été alloués.

Cependant, des informations récentes laissent à penser que le budget total ne dépassera pas 23 millions d'euros.

Ce qui est inquiétant dans ce type de programme est la lenteur du déploiement de la programmation financière, au regard des technologies et des habitudes sociales de communication qui mutent très rapidement.

L'enjeu est de faire un programme global significatif incluant technologies, terminaux d'alerte et «communication» du système vers le grand public, enjeu qui ne semble pas vraiment pris en compte dans le programme SAIP.

Sirènes, Le Havre



Etat fréquent des sirènes de l'ancien réseau RNA

La communication de crise

Comme toujours la communication de crise est basée sur la confiance qu'a le citoyen dans son rapport avec l'autorité. Pour créer cette confiance, les ingrédients sont connus depuis plus de vingt ans : **communication avant la crise, transparence, rapidité à communiquer,** y compris avec les incertitudes de la situation, **leadership et gestion efficace de la situation.**

Si heureusement, on observe une amélioration continue dans la communication des acteurs, on ne peut en dire autant en termes de communication des acteurs politiques dans la crise. Que ce soit au moment de la pandémie grippale, de la mini-crise hivernale en Ile-de-France ou de la crise hydrocarbure, **la communication de crise «politique» a été chaotique et n'a pas fait l'objet d'une réelle «stratégie» de communication publique**, utilisant à la fois la parole de l'Etat et celle des «alliés» potentiels : organisations professionnelles, associations, relais et collectivités.

Ces erreurs nuisent à la gestion des crises présentes, mais elles laissent également une trace dans la gestion des crises futures, comme un «héritage» négatif fait de méfiance.

La parole publique doit répondre à trois impératifs : **la vérité, la simplicité et l'utilité**. Pour cela, la communication de crise, notamment face aux situations d'exception, doit s'abstenir de tout «équivoque» politique sous peine d'être rapidement disqualifiée. Cela doit en plus s'apprécier dans un contexte où les médias sont hyper réactifs, disposant de moyens d'investigation à chaud et à froid, et où tout un chacun a la possibilité de photographier, filmer et poster sur Internet en quelques minutes les évènements auxquels il assiste.

Car le phénomène nouveau est sans contexte **l'irruption des réseaux sociaux dans la crise**. Les réseaux sociaux sont à la fois des «amplificateurs» de crises et des sources pour les médias traditionnels. Mais ils sont aussi par eux-mêmes dans les catastrophes, des vecteurs de communication pour l'alerte et pour les victimes. Ils peuvent également aider les services de secours dans leurs activités de sauvetage ou de soutien aux populations.

En un mot, **la communication de crise**, comme la gestion de crise, doit être plus professionnalisée chez tous les acteurs autant publics que privés, afin de permettre une adhésion des populations. **Elle doit également s'inscrire dans une politique de prévention et de communication permanente de l'Etat vers les autres acteurs et les citoyens, et doit absolument intégrer la dimension «réseaux sociaux» avant et pendant la crise.**

En conclusion, un effort important doit encore être mené, tant sur le volet de **la professionnalisation des acteurs de la gestion et de la communication de crise, que sur celui des moyens de communication et de simulation des centres opérationnels**. Cela doit se faire au profit de tous les acteurs, Etat, collectivités et entreprises, pour permettre une gestion des crises potentiellement les plus graves (accidents nucléaires, terrorisme NRBC, crises sanitaires, séismes ou inondations majeures), ayant le moins de conséquences humaines, environnementales et économiques possibles.

Points forts et avancées globales	Points faibles et inquiétudes
Une clarification de l'organisation de l'Etat	Un système encore trop complexe pour être lisible par tous les acteurs, y compris la population
Une réforme de la planification pour une simplification et une meilleure lisibilité des mesures pour les décideurs et les acteurs concernés (plans NRBC, pandémie...)	Des outils de simulation et de gestion de crise encore trop peu aboutis pour la gestion des crises complexes
Une volonté de faire évoluer la doctrine SAIV vers une prise en compte d'une approche «tous risques» et continuité d'activité pour les opérateurs désignés	Un développement à entreprendre sur les aspects d'interdépendances et de continuité d'activité «harmonisée» pour les opérateurs essentiels
Une planification nationale et locale bien structurée tant en prévention (PPRN-T, Vigipirate) qu'en réaction (PCS, dispositif ORSEC, planification pirate…)	Une planification nationale peu lisible par le grand public (notamment Vigipirate) et une planification locale, notamment en prévention des risques et en réactivité (PCS) qui reste très lente dans sa mise en œuvre, faute de prise de conscience et de moyens des collectivités
Une prise de conscience de la nécessité de professionnaliser les gestionnaires et les communicants de crise de l'Etat, des collectivités et des grands opérateurs	Une trop faible de prise en compte des réseaux sociaux dans la gestion et la communication de crise publique
Une importante politique d'exercices au niveau national	Une communication politique souvent très maladroite, une absence des responsables politiques dans les exercices et des exercices locaux encore trop rares
Contrat opérationnel 10 000 hommes (OTIAD)	Interrogations sur le nombre de 10 000 hommes, notamment pour les évènements impliquant plus de 500 000 impliqués ou victimes (tremblement de terre, inondation majeur, bioterrorisme..) et sur le lien avec le soutien de l'OTAN
Diffusion d'alerte CNA	Alerte CNA mal connue du public et absence d'affichage informatif permanent

Page suivante : accident ferroviaire aux Etats-Unis

NDKL 570586
TILX 190750

4

TRENTE PROPOSITIONS POUR AMELIORER LA GESTION DE CRISE

Ce chapitre a pour objet d'adresser trente propositions pour améliorer et optimiser, en France, la gestion de crise publique et privée et la gestion des risques. Ces propositions se déclinent en trois niveaux: les propositions stratégiques, structurantes et d'optimisation.

En effet, la crise des finances publiques et les contraintes de la RGPP sont telles, que repenser en profondeur le dispositif semble inévitable, étant donné l'absence criante de moyens. Le temps du «faire pareil qu'avant avec un peu moins» semble révolu.

Il vaut mieux viser le «faire bien» dans une optique de gestion avec des moyens modernes et ad hoc, que de s'accrocher à des organisations dont la pertinence, faute de moyens, n'est plus avérée. Ces suggestions illustrent cette prise de position.

Les propositions ci-dessous, qui s'inscrivent dans la suite du constat fait par ce rapport, s'articulent autour des préoccupations suivantes : pallier les insuffisances anciennes dans le système français de gestion de crise (les lacunes en matière de formation, d'information et de communication) ; promouvoir les réformes de structure pour une meilleure efficacité (la question de la pertinence de la gestion de crise publique au niveau départemental) ; rechercher un plus grand partage de responsabilités entre l'Etat, les collectivités territoriales et le secteur privé pour des raisons budgétaires, mais aussi et surtout pour des raisons de doctrine ; instaurer la mutualisation de moyens et d'informations entre acteurs étatiques et non étatiques ; introduire des concepts innovants (vigilance globale, résilience territoriale…) de manière à mieux couvrir la gestion de crise ; ou encore utiliser les technologies modernes (command & control) à l'instar de ce qui est fait dans d'autres pays.

Ce chapitre a donc pour objet de «bousculer» et de proposer des actions et des améliorations à notre système de sécurité globale. L'approche n'est pas systématique dans les propositions faites ; la pertinence de chacune d'elles peut être analysée de manière individuelle ou au niveau de la notion de «bloc» proposée.

Plate-forme Deepwater Horizon, Louisiane, Etats-Unis, Avril 2010

10 blocs - 30 Propositions

1 - Les propositions stratégiques

Bloc 1 : Une véritable campagne de communication sur les risques et les comportements à destination du public

- **Proposition 1 :** Campagne de communication sur les comportements à tenir en situation de crise
- **Proposition 2 :** Education aux risques, aux menaces et à la résilience au niveau de l'Education nationale
- **Proposition 3 :** Un plan d'information «grand public» sur le «comportemental» par département avec un délégué permanent - Monsieur «risques et résilience»

Bloc 2 : Repenser la planification et la gestion des crises publiques et l'interface privée (notamment OIV) au niveau central et territorial

- **Proposition 4 :** Clarifier et renforcer la gestion de crise publique au niveau national
- **Proposition 5 :** Repenser la planification et la gestion de crise territoriale
- **Proposition 6 :** Activités d'importance vitale

Bloc 3 : Doter les acteurs de nouveaux outils de réflexions et d'analyse pour optimiser la prévention, la planification et la réponse aux crises

- **Proposition 7 :** Planification globale : coupler les plans «prévention-réaction»
- **Proposition 8 :** Analyse systématique des effets domino (ou cascade) des grands risques au niveau régional
- **Proposition 9 :** Création d'un indice de résilience territoriale

2 - Les propositions structurantes

Bloc 4 : Vigilance et planification

- **Proposition 10 :** La notion de vigilance globale
- **Proposition 11 :** Repenser Vigipirate
- **Proposition 12 :** Développer la simulation et les SI de gestion de crise mixte (SAIV-Etat)

Bloc 5 : Formation et exercices

- **Proposition 13 :** Former des élus et décideurs à la gestion de crise
- **Proposition 14 :** Evaluer les exercices par des structures indépendantes

3 - Les propositions d'optimisation

Bloc 1 - Une véritable campagne de communication et de formation sur les risques à destination du public

Proposition 1 : Campagne de communication sur les comportements à tenir en situation de crise

Cette campagne de communication devrait être menée sur une base annuelle, même si elle ne porterait tous ses fruits que sur une période de 5 à 10 ans.

Elle aurait pour objet d'**intégrer dans le réflexe des Français les bons comportements à avoir face aux risques**, comme peut l'être «Bison Futé» pour la circulation routière.

Cette campagne menée sur les grands médias TV, radio, ainsi que sur le Web mettrait en lumière une série de risques quotidiens et majeurs différents chaque année, et serait accompagnée par des relais d'acteurs : associations de sécurité civile, etc.

Le SIG serait chargé de sa conception, dans le cadre d'un travail interministériel, sur un budget dédié et significatif d'au moins 5 millions d'euros par an.

Proposition 2 : Education aux risques, aux menaces et à la résilience au niveau de l'Education nationale

La formation citoyenne aux risques et aux comportements à tenir face aux risques et aux dangers est encore balbutiante au sein de l'Education nationale. Il faut élaborer une stratégie globale de formation à ces thématiques dans les programmes du primaire et du secondaire.

La proposition consiste à établir une stratégie d'enseignements, non seulement face aux risques naturels et technologiques, qui est aujourd'hui dispensée dans certains cours de géographie ou de sciences du primaire et du secondaire, mais aussi, à travers une formation aux problématiques des risques systémiques, de leur gestion et des crises potentielles pouvant en découler. Ce type d'enseignement peut en effet entrer dans le cadre de nombreuses disciplines (économie, ingénierie, citoyenneté etc.).

Il convient de donner en parallèle les bases citoyennes des comportements à adopter dans les situations d'urgence et de danger dans un cours dédié, accompagné d'une formation aux gestes qui sauvent (PSC1), sur une base annuelle adaptée, aussi bien dans le primaire que dans les deux cycles du secondaire, ce que prévoit la loi de modernisation de la sécurité civile de 2004 mais qui n'est pas vraiment appliquée de façon homogène sur le territoire.

Il convient également de noter le travail de l'association IFFO-RME sur la sensibilisation du corps enseignant à ces problématiques encore trop peu prises en compte par le monde de l'éducation.

Proposition 3 - Un plan d'information «grand public» sur le «comportemental» par département avec un délégué permanent – «Monsieur risques et résilience»

Afin d'accompagner durablement et efficacement la campagne d'information nationale, le relais local est indispensable.

La proposition consiste en la création d'un poste «Monsieur risques et résilience» au niveau départemental, identifié par la population. Directement rattachée au Préfet, cette personne aura pour mission de faire travailler ensemble, tout au long de l'année, les différents acteurs contribuant à la prévention, à la planification et à la réponse face aux risques majeurs, mais aussi quotidiens. Elle aura auprès du préfet, les visions «population» et «prévention globale» locales, au-delà des visions particulières des différents services et administrations d'Etat ou des collectivités. Elle assurera le lien avec les associations (CLI, associations de sécurité civile, etc.), mais aussi avec les médias, en qualité de porte-parole départemental.

Documents IFFO-RME

Bloc 2 : Repenser la planification et la gestion des crises publiques et leur interface avec le secteur privé (notamment OIV) au niveau central et territorial

Proposition 4 - Clarifier et renforcer la gestion de crise publique au niveau national

4 - 1. Clarifier la notion de «ministre conducteur de crise» et le doter d'un outil ad hoc

Le ministre conducteur de crise doit être défini de manière claire, sans ambiguïté et de façon définitive, afin d'éviter confusion et basculement, mais également afin d'optimiser les outils de gestion de crise. Il convient donc de mieux définir la doctrine.

Deux choix se présentent aujourd'hui à cet effet :

- Soit confier au ministre de l'Intérieur la gestion de toutes les crises majeures ; la CIC (Cellule Interministérielle de Crise) pouvant alors se confondre avec le «CIC» (Centre Interministériel de Crise) de la place Beauvau ;
- Soit laisser au Premier ministre la coordination interministérielle et il convient alors de créer un véritable centre opérationnel pour la CIC (par exemple au SGDSN).

Dans les deux cas, la gestion des crises complexes semble difficile sans un centre de crise approprié.

4 - 2. Créer un «CPCO-I»

La chaîne de gestion de crise actuelle est encore trop éclatée et complexe. La spécificité des crises systémiques modernes réside à la fois dans la manière rapide avec laquelle elles se propagent et la grande étendue des champs concernés.

Pour y faire face, les dispositifs doivent alors être très clairs, interconnectés et multidisciplinaires, mais également capables d'interfaces en temps réel avec des données très diverses et des structures externes.

Il convient pour cela de s'appuyer sur des outils d'agrégation et de fusion de données, qui seuls permettent d'espérer gérer la complexité des crises modernes. Mais ces outils coûtent cher et ne peuvent donc pas être multipliés à l'infini.

La proposition consiste en l'agrégation dans un centre unique opérationnel, des trois centres de sécurité intérieure que sont le COGIC, le COPN et le CROGEND, auquel devrait être ajouté au moins virtuellement, le CORRUSS.

Ce nouveau centre «CPCO-I», durci et installé hors zone inondable, permettrait dans le respect des compétences des différents services, de disposer sous la direction d'un chef d'Etat-major inter-services, d'une salle de situation commune avec des outils de dernière génération, comme c'est le cas aux Etats-Unis, notamment.

Cela permettrait d'avoir une vision globale de la crise en temps quasi réel et d'anticiper grâce à des outils de simulation, les situations critiques, afin d'être «en avance» sur la crise et non «en retard» comme on le constate trop souvent.

La composante «planification nationale», aujourd'hui parent pauvre des différentes réformes récentes du ministère de l'Intérieur, pourrait en outre être intégrée par ce moyen, au sein d'une structure de planification unique, inter-services, conjointe au centre opérationnel.

CPCO du Ministère de la Défense

4 - 3. Créer une réserve «gestion de crise nationale»

Un effort sans précédent doit être conduit pour permettre de gérer les crises longues et complexes, mais les structures actuelles sont dans l'incapacité de le faire, faute de ressources humaines formées. Il convient donc de constituer des réserves compétentes à cet effet.

Un millier de réservistes spécialisés et formés à la gestion de crise (généralistes ou personnes ayant des compétences particulières dans certains domaines techniques) sont nécessaires.

Ils pourraient être recrutés à la fois au sein des réserves habituelles de sécurité nationale, mais aussi dans certaines réserves citoyennes, ou encore dans des associations ou groupements professionnels.

Cette réserve spécialisée viendrait en appui aux structures en place (préfectures de départements, de régions, de zones, CO des ministères ou des grands opérateurs, collectivités etc.) sur le long terme et sur des expertises pointues.

Proposition 5 - Repenser la planification et la gestion de crise territoriale

5 - 1. Planification et régionalisation

La gestion de crise au niveau du préfet de département semble satisfaisante à la fois pour des questions de pérennité et de connaissance fine des territoires.

Toutefois, la fonction de planification, parfois très faiblement dotée au niveau départemental (SIDPC) pose problème. Il serait semble-t-il plus judicieux de **créer un service de planification de risques et de menaces majeurs au niveau régional,** qui serait plus à même de répondre aux défis qui se présentent.

Ce **service de planification régionale de sécurité nationale (SPRSN)** permettrait de disposer d'un outil de planification plus adapté pour faire face aux différents risques et menaces majeurs et à leurs effets domino, qui dépassent l'échelon départemental.

Le préfet de département s'appuierait alors sur un COD resserré sur les services compétents de la composante dominante de la crise : ordre public (Police, Gendarmerie) ou sécurité civile (Sapeurs-pompiers, Samu), ainsi que sur les réserves de gestion de crise évoquées plus haut.

La coordination départementale de la crise est aujourd'hui assurée sous l'autorité du préfet et d'un «délégué aux risques» par un ou plusieurs cadres de préfecture désignés et formés. Les tâches effectuées auparavant par les SIDPC (commission de sécurité etc.) pourraient alors être transférées aux services directement compétents (S-P ou autres services) qui sont souvent en charge, ou participent actuellement déjà à ces démarches.

Il s'agit aussi d'un bon niveau pour les territoires de plus en plus interdépendants, les grands services de l'Etat (DREAL, ARS etc.) étant dorénavant régionalisés.

Ce nouveau niveau de planification régionale serait alors un autre acteur qui ferait jeu égal avec ceux-ci, ainsi qu'avec les grandes collectivités : métropoles et communautés urbaines.

Il incarnerait aussi l'interlocuteur de bon niveau face à un CPCO-I, évoqué précédemment en liaison et sous l'autorité des préfets de zone (préfet délégué). Ceux-ci garderaient leurs prérogatives actuelles, telles que définies dans les textes de 2010 et couvrant ces nouveaux termes de planification.

5 - 2. Un rôle accru pour les collectivités et notamment les élus municipaux

Les collectivités pensent toujours pouvoir s'appuyer sur l'Etat en temps de crise. Or, si le rôle des services de secours et de sécurité, le rôle du préfet conducteur de crise, ainsi que la solidarité nationale ne font pas de doute, il convient néanmoins de prendre en compte les crises de grande ampleur qui mettraient ces dispositifs sous tension.

Chaque maire et chaque collectivité, et ce conformément à la loi de modernisation de la sécurité civile de 2004, doivent être en mesure d'assurer leurs responsabilités en matière de sauvegarde. Or, la faiblesse de réalisation des plans communaux de sauvegarde et la faiblesse de la formation de la population aux gestes qui sauvent, démontrent qu'un effort important doit être mené envers les collectivités.

5 - 3. Le rôle des grandes collectivités

Les grandes collectivités doivent pouvoir disposer de véritables systèmes de gestion de crise : salles de gestion de crise, personnels formés, moyens de communication, représentants au sein des COD de préfectures. Elles doivent avoir, plus généralement, la capacité d'organiser les phases de post-crise, d'assurer la continuité des services de leurs collectivités, et de favoriser la continuité d'activité économique dans les zones sinistrées.

Leur rôle est déterminant pour aider et soutenir les populations et surtout se focaliser sur les problématiques de continuité d'activité au sens large, et ce dans le respect de leurs compétences.

A cette fin, il est proposé que chaque conseil général et régional mettent en place **une cellule de «gestion de crise et de continuité d'activité» couplée avec une planification ad hoc**. Une disposition législative sera nécessaire pour rendre ces dispositions obligatoires pour les collectivités.

Proposition 6 - Activités d'importance vitale

6 - 1. Repenser le décret de 2006, passer du SAIV au SCAIV

Le décret de 2006 portant création du dispositif SAIV a été très bénéfique pour la création d'une véritable culture de sécurité dans les groupes industriels reconnus opérateurs d'importance vitale (OIV) au travers des directives nationales de sécurité.

Néanmoins, ces dispositions très ciblées sur la protection face aux actes terroristes n'ont pas généré d'obligations en matière de gestion de crise et de continuité d'activité. Elles n'ont pas non plus donné de droits particuliers à cet égard pour les entreprises dont l'activité est reconnue comme essentielle.

La proposition consiste à faire évoluer la sécurité des activités d'importance vitale (SAIV) vers un système de sécurité et de continuité des activités d'importance vitale (SCAIV), lequel engloberait les trois volets au sein d'un dispositif de gestion unique : sécurité, gestion de crise et continuité d'activité.

Ce système devrait en outre clarifier les «aides ou priorités» que l'Etat donnerait à ces entreprises dans le cadre des grandes crises.

Le décret de 2006 doit donc évoluer et couvrir le champ complet de la crise, mais également être à double sens (obligation et soutien) entre les entreprises concernées et l'Etat.

La centrale nucléaire de Tricastin, dans le sud de la France.

6 - 2. Créer un centre d'analyse des interdépendances et des continuités d'activités et de services au profit des opérateurs et filières économiques nationales

L'objectif est de permettre aux opérateurs d'infrastructures essentielles d'échanger directement entre eux dès les premières heures d'une crise sur les interdépendances entre opérateurs essentiels.

La proposition est de créer un centre équipé et sécurisé où les opérateurs, alertés par une structure de veille, enverraient sous bref délai un délégué de gestion de crise en lien avec son ou ses centre(s) opérationnel(s) et avec, suivant leurs intérêts respectifs, des représentants de centres opérationnels d'Etat.

Ce centre pourrait apporter une qualification de l'événement, ainsi qu'une analyse rapide et documentée des interdépendances, des effets en cascade possibles et des solutions de reprise, de continuité d'activité ou de services mises en œuvre par ces opérateurs. Il ne s'agirait pas d'un centre de gestion de crise supplémentaire, mais d'un centre de fusion de renseignements et d'analyse au profit des opérateurs et de l'Etat en tant que besoin.

Cette proposition permettrait de gagner en efficacité et d'offrir une meilleure réactivité inter-secteurs, et ce à un moindre coût pour les opérateurs par une mutualisation de moyens.

Elle faciliterait également **le dialogue Etat - Entreprises sur la qualification de la crise** (surtout dans les crises à cinétique rapide), et permettrait une meilleure analyse des problématiques générées par celle-ci, en ce qui concerne les services essentiels (continuité d'activité).

Ce centre qui n'a pas vocation de «gestion de crise» mais seulement d'analyse, pourrait aussi bien aider les centres opérationnels de chaque entité membre, venir également en appui de la cellule économique de continuité d'activité du ministère de l'Economie ou répondre à des demandes ponctuelles de tel ou tel centre opérationnel d'Etat, voire de la CIC.

Dans la phase post-urgence, **ce centre faciliterait le dialogue multi-opérateurs et multi-secteurs,** afin de diminuer la gêne des populations et du tissu économique, et ainsi de réduire le coût et l'impact économique et humain des catastrophes et des crises. Car, indépendant des structures d'Etat ; il peut poursuivre une mission de coordination dans les phases de reconstruction.

Ce dispositif est en plein essor aux Etats-Unis où 17 centres tel que le Business Emergency Operation Centre de Louisiane, sont opérationnels ou à l'étude, l'objectif étant de doter à terme chaque Etat.

Bloc 3 : Doter les acteurs de nouveaux outils de réflexion et d'analyse pour optimiser la prévention, la planification et la réponse aux crises

Proposition 7 - Planification globale : coupler les plans «prévention - réaction»

L'analyse de nos plans de réaction de toutes natures montre souvent que la planification est réalisée sans référence au contenu des plans de prévention. Par exemple, les PPRT et les PPI sont basés sur des logiques différentes qui rendent difficilement compréhensibles les hypothèses de risques pour les populations concernées.

La proposition consiste à créer un document de synthèse entre planification de prévention et planification de réaction, le PSGS «Plan de Sécurité Global de Site», afin d'avoir une meilleure vue d'ensemble de la problématique du risque, de sa prévention et de sa réponse.

Proposition 8 - Analyse systématique des effets domino (ou «en cascade») des grands risques au niveau régional

Dans l'esprit de la création de grands services régionaux de planification de sécurité nationale, **la proposition** consiste en la création d'une nouvelle planification d'analyse des effets domino dans les grandes catastrophes au niveau régional et zonal.

L'analyse des effets «domino» ou «en cascade» en cas de risques naturels, technologiques, sanitaires, malveillants ou terroristes mérite en effet d'être faite au niveau régional ou zonal. Imaginer leur impact sectoriel permettrait de définir les contre-mesures de toute nature qu'il conviendrait de mettre en œuvre pour réduire le phénomène «surprise» d'un enchainement d'évènements sur des scénarios majeurs.

Centre de crise EDF, salle des opérations

Proposition 9 - Création d'un indice de résilience territoriale

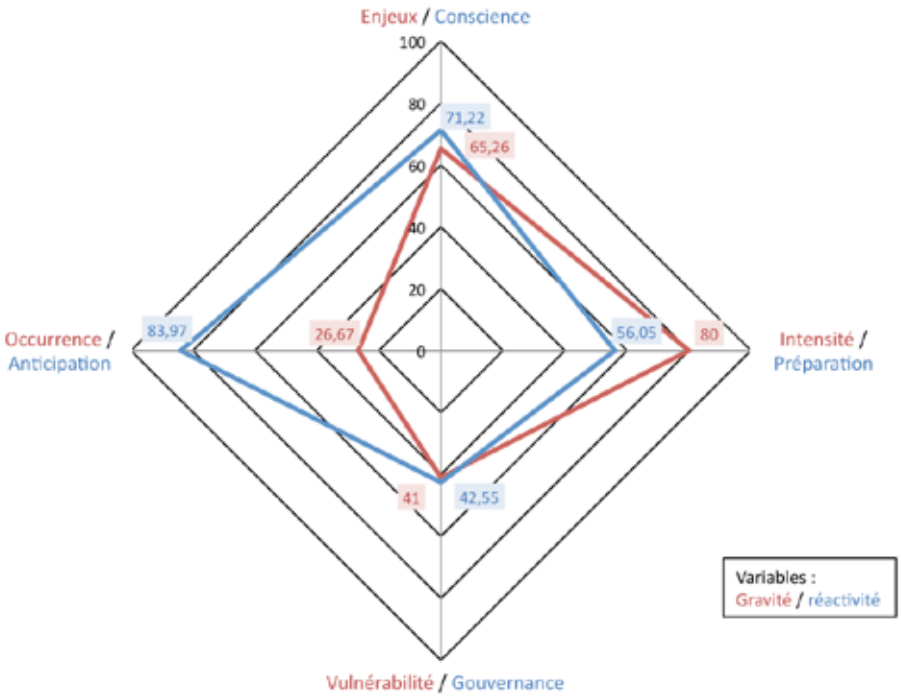
Comment évaluer la capacité d'un territoire à faire face aux risques qui le concernent ? Quelles sont les voies pour améliorer cette capacité ? Quel volet de la politique globale de sécurité est à mettre en œuvre ? Faut-il plus s'axer sur la prévention, la planification, la gouvernance ou l'éducation aux risques ?

Les études de résilience territoriale ont pour objectif de réaliser un indice évaluant la résilience d'un territoire face à certains types de risques ou face à la globalité des risques et menaces pour permettre une meilleure analyse et une meilleure gouvernance des politiques publiques et partenariales.

Cet indice que l'on nommera «indice de résilience territoriale» s'inspire du concept de résilience sociétale et évaluera l'ensemble des paramètres qui concourent à construire la résilience sociétale d'un territoire face à des aléas naturels, technologiques, voire à l'avenir face à des risques de toutes natures qui le concernent.

L'indice de résilience territoriale du HCFDC

Notes des variables de gravité et de réactivité pour le calcul de l'indice de résilience



Ces paramètres sont étudiés pour chacun des acteurs de la résilience d'un territoire et sont ceux d'une approche globale de la résilience : de la prévention à la reconstruction, en passant par la gouvernance, l'éducation et l'information, l'alerte et la vigilance, la préparation et les entraînements et exercices.

Le Haut Comité Français pour la Défense Civile en partenariat avec le Ministère de l'Ecologie, du Développement Durable, des Transports et du Logement a lancé dans ce cadre une étude expérimentale sur les risques naturels et technologiques. Son ambition est que cet indice soit vulgarisé et utilisé à terme par les acteurs concernés, afin de mieux asseoir leurs politiques de gestion et de prévention des risques majeurs.

La proposition a pour objet deux actions tirées des enseignements de cette étude :

– Mettre à disposition la méthodologie au profit des centres de planification «régionaux» qui souhaiteraient une analyse de résilience sur un plan départemental ou régional ;

– Proposer une version simplifiée de cette méthodologie au travers d'une analyse de résilience «locale» (niveau communal, communautés de communes ou métropoles) via une labellisation du type Pavillon Orange, étendue à la prévention des risques.

L'indice de résilience territoriale a pour objet d'analyser le facteur résilience d'un territoire et de guider les responsables territoriaux (Etat et Collectivités) à harmoniser les différents pans de politique publique entre prévention et réaction. L'indice se base sur des rapports entre des thématiques diverses : objectives et subjectives, tels que enjeux et conscience des risques, intensité et préparation, vulnérabilité et gouvernance, occurrence et anticipation pour exprimer les «déficits ou les surinvestissements» sur le territoire considéré. Il est basé sur une note globale composée d'une analyse par aléa étudié.

Bloc 4 : Vigilance et planification

Proposition 10 - La notion de vigilance globale

Tout le monde connaît la vigilance météorologique qui est maintenant très bien ancrée dans le quotidien des Français, y compris les concepts de vigilance «orange» et «rouge». Incluant depuis peu les risques de submersion marine et d'inondations, le système a d'ailleurs démontré sa pertinence.

La proposition vise à étendre ce concept de vigilance sur une base identique (code couleurs) et cartographie aux trois autres risques, niveaux de menaces ou incidents prévisibles que sont :

- Les risques sanitaires par région ou les risques d'épidémie ou de pandémie face à une ou plusieurs maladies infectieuses ;
- La menace terroriste (Vigipirate) ;
- Les incidents spécifiques d'infrastructures (fermetures ou interruptions majeures de services) également par lettre et code couleur (A = Aérien, F = Ferroviaire, T= Transport terrestre, R = Route, etc.).

Ces vigilances seraient présentées dans le cadre de la météorologie nationale, au quotidien, avec un pictogramme global, et ne serait commentées qu'en cas de préoccupation particulière.

Proposition 11 - Repenser Vigipirate

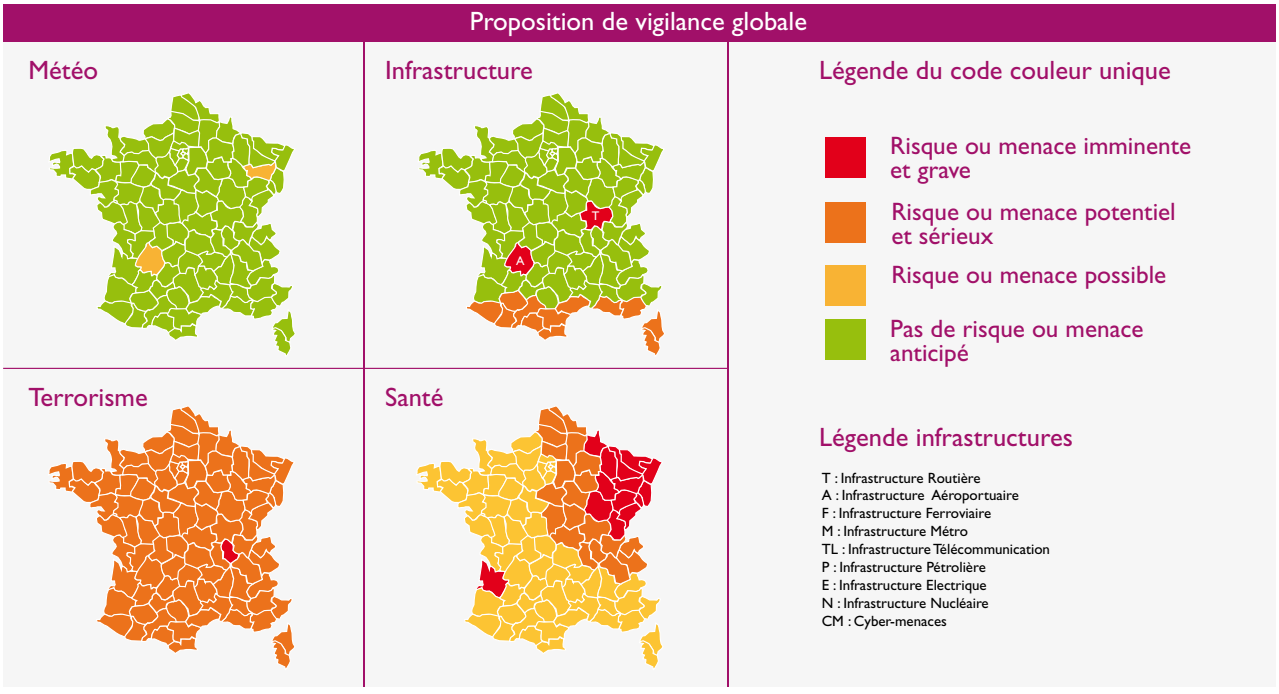
Le plan Vigipirate est aujourd'hui devenu une affaire de «spécialistes», entre postures et code couleur. Il est difficilement compréhensible tant pour la population que pour les personnes concernées «non expertes», et il faut donc le rendre à la fois plus lisible et plus automatique.

La proposition est double :

11 - 1) Réformer le code couleur sur une base plus explicite: un code orange pour les situations de menaces «non avérées», rouge pour prévenir des «attentats limités» et écarlate pour les attentats de «grande ampleur» supposés ou craints. Quoiqu'il en soit, sans renseignements avant l'attaque, le plan ne peut être mis en œuvre avec efficacité et dans ce contexte, un orange «mûr» vaut mieux que le rouge «mou» actuel.

11 - 2) Automatiser la réduction des niveaux écarlate et rouge au niveau inférieur si, six mois après le déclenchement du plan, aucun évènement ou information de menaces ne vient contredire cet abaissement. Si l'abaissement est refusé, il faut le motiver publiquement et obligatoirement, non en détail, mais dans son esprit.

Ainsi, si une menace persiste, le plan est maintenu à son niveau, sinon il baisse. La déclaration du niveau devrait d'ailleurs être faite par une autorité administrative, comme le secrétaire général de la défense et de la sécurité nationale, plutôt que par une autorité politique.



Proposition 12 - Développer la simulation et les SI de gestion de crise mixtes (SAIV-Etat)

Le parent pauvre des centres opérationnels est aujourd'hui la simulation en temps quasi-réel face aux menaces les plus sérieuses. De nombreux modèles existent face aux différents risques ou menaces : NRBC, inondation, feux de forêts, etc.

La problématique actuelle réside dans la création d'une interface commune pour la fusion de données sur des outils de visualisation, permettant de coupler les enjeux et les effets des risques ou menaces sur une cartographie opérationnelle (3D en milieu urbain) et de disposer des outils d'analyse ad hoc.

Ces systèmes existent et il convient d'en doter les centres opérationnels les plus importants. Cela représente un véritable enjeu technologique majeur pour la sécurité de nos concitoyens et pour permettre aux gestionnaires de crises d'anticiper et non de subir les évènements. Il faudra toutefois faire preuve d'une véritable volonté politique pour arriver au partage de l'information entre acteurs, seul gage d'une gestion de crise efficace.

Enfin dans le même esprit, il serait nécessaire d'établir une cartographie des enjeux croisés des grands réseaux d'infrastructures. Ces échanges de données (données de base et informations «chaudes») pourraient être faits entre opérateurs et entre opérateurs et Etat, par fusion de données sur des cartographies sécurisées et sur des réseaux eux-mêmes sécurisés.

Bloc 5 : Formation et exercices

Proposition 13 - Former des élus et décideurs à la gestion de crise

Former les maires et les élus responsables est un impératif majeur si nous voulons que ces hommes et ces femmes puissent jouer leur rôle de gestionnaire de crise au profit des populations.

Il conviendrait pour cela d'organiser une formation d'une journée pour tout nouvel élu dans l'année de sa prise de fonction. Il pourrait s'agir d'un stage d'une à deux journées pour les maires et principaux adjoints pour les villes de plus de 50 000 habitants, ou d'une e-formation pour les élus des communes de moins de 50 000 habitants.

Proposition 14 - Evaluer les exercices par des structures indépendantes

Les exercices d'Etat ou plus rarement des collectivités sont, en général, évalués par les pairs. Ainsi, le sapeur-pompier du département voisin jugera son collègue et il en sera de même dans les différentes fonctions, lorsque celles-ci sont évaluées (ce qui n'est pas toujours le cas). Ces évaluations restent par nature discrètes et n'aboutissent que rarement ou pas du tout à un Retex public ou «confidentiel», et encore moins à son exploitation (cf. le rapport du sénateur Paul Girod, sur la gestion territoriale des crises, remis en 2010 au Président de la République).

Il est proposé de faire évaluer les exercices par des personnes indépendantes, n'ayant aucun lien direct hiérarchique ou de carrière avec les personnes évaluées.

La proposition serait de constituer, soit au sein de réserves de gestionnaires de crise ou de sécurité nationale (citées plus haut), soit au sein de sociétés privées compétentes, des «task forces» d'observateurs habilités en raison de leurs compétences. Ces derniers seraient rémunérés selon un tarif fixe journalier, ce coût entrant dans le budget de l'exercice. Chaque exercice devrait disposer d'un budget propre pour être considéré comme un exercice de validation.

Exercice OMEGA, Paris 2010

Bloc 6 : Réseaux et Technologies

Proposition 15 - Appels d'urgence

Le numéro 112 ne fonctionne pas convenablement. Il conviendrait donc de fusionner entre régions, les systèmes de prise des appels d'urgence de chacune des forces de sécurité : police, gendarmerie, sapeurs-pompiers et SAMU. Cela pourrait se faire à travers une application standardisée et interopérable entre services, et des centres d'appel offrant une masse critique et des possibilités de reprise d'un autre centre, qui serait, pour une raison ou une autre, neutralisé.

Cette action aurait trois avantages : fiabiliser les services, les rendre plus résilients grâce à cette l'interopérabilité et en diminuer les coûts d'investissement et de fonctionnement par une mutualisation interservices, police et gendarmerie, sapeurs-pompiers et SAMU.

Proposition 16 - Alerte et réseaux sociaux

16 - 1. Accélérer le développement du SAIP pour disposer d'un outil d'alerte au profit des départements et des communes

Cela permettra non seulement de déclencher l'alerte grâce aux différents dispositifs : sirènes, messages variables sur les panneaux extérieurs, cell broadcasting, etc., mais aussi d'informer les personnes à travers les réseaux sociaux type Twitter (sous réserve de leur disponibilité en cas de crises majeures) notamment sur les consignes à tenir.

Il s'agira également en complément d'un certain nombre de nouvelles sirènes qui seront prochainement déployées par l'Etat, de confier la responsabilité aux collectivités de la réfection, de l'acquisition et du déploiement des terminaux d'alerte ad hoc pour les populations. Ce programme devrait être achevé dans les deux à trois ans à venir, ou alors des questions légitimes pourront se poser sur sa pertinence.

16 - 2. Mettre en place une veille sur les réseaux sociaux

Il conviendrait de mettre en place une veille des services de secours au niveau des CTA(16) sur les réseaux sociaux en cas de catastrophe, pour capter, notamment en cas de difficultés de communication, les appels (notamment via Twitter) qui ne passeraient pas, à la suite à une destruction partielle ou une saturation des réseaux de communication filaires ou mobiles. Il convient par ailleur de développer des applications sur les «Smartphones» permettant de mieux qualifier les demandes d'urgence, et d'aider aux actions réflexes sur les gestes qui sauvent.

16 - 3. Une campagne d'information significative sur l'alerte et les comportements à tenir, dès que le développement du SAIP sera achevé

Concernant l'alerte, l'utilisation des sirènes peut en effet être particulièrement vitale lors de certains événements qui impliquent des réactions adaptées, tels qu'une évacuation immédiate ou un confinement en points hauts, dans l'hypothèse d'une contamination atmosphérique ou d'une menace d'inondation, ou encore dans le cadre d'une situation d'agression majeure nécessitant d'éviter une saturation des réseaux routiers urbains et périurbains par des mouvements incontrôlés de population.

Proposition 17 - Réseaux de communication spécifiques de gestion de crise

Les réseaux gouvernementaux de communication durcis satisfont l'Etat pour ses besoins de communication de crise, ainsi que certains opérateurs d'importance vitale qui y sont abonnés. Les services de secours et de sécurité ont développé depuis de nombreuses années les réseaux radio qui sont aujourd'hui numérisés et interconnectables entre sapeurs-pompiers, policiers et gendarmes (réseau INPT(17)). Cependant, si plus de soixante-cinq SDIS ont totalement basculé sur le nouveau réseau INPT, il devient urgent que les autres départements accélèrent leur arrivée afin de garder une cohérence globale de sécurité nationale. Mais seule une petite vingtaine de SAMU est raccordée à ce réseau aujourd'hui, posant ainsi le problème de son «universalité» dans les opérations de secours.

Il serait hautement souhaitable que l'Etat accélère l'ouverture de ce réseau à tous les acteurs de secours et d'urgence qui, lors des crises sont sous l'autorité du préfet, sans oublier la création de passerelles, ou la possibilité de raccorder les associations agréées de sécurité civile, les collectivités territoriales et les niveaux opérationnels et techniques des grands opérateurs d'infrastructures essentielles.

La proposition consiste donc à étendre le ou les réseaux sur l'infrastructure partagée INPT à d'autres acteurs, sur des standards peut-être moins sécurisés, mais plus accessibles financièrement à des structures diverses. Ces réseaux doivent permettre de disposer de passerelles laissant la possibilité à chaque acteur de terrain, collectivités (notamment conseils généraux et communes), associations agréées, opérateurs d'importance vitale, de disposer de connexions ad hoc avec l'ensemble des services de secours et des autres acteurs lors de catastrophes majeures, notamment en cas de destruction ou de neutralisation des réseaux filaires ou GSM.

(16) Centre de Traitement de l'Alerte.
(17) Infrastructure Nationale Partageable des Transmissions.

Un programme d'études et de faisabilité devrait être lancé au plus vite par la puissance publique pour examiner l'interopérabilité des réseaux civils de sécurité et les réseaux de sécurité nationale, et émettre des recommandations, car sans communication durant la crise entre tous les acteurs, il n'y a pas de vraie gestion de crise possible.

Proposition 18 - Cyber sécurité/défense

La cyber sécurité/défense est une préoccupation récente et galopante pour de nombreux grands acteurs étatiques économiques et pour les citoyens, sur trois thèmes en particulier :

- Le vol de données et les risques d'espionnage ;
- Les malveillances de toute nature ;
- L'intrusion sur des systèmes de type SCADA se rapprochant d'actes de terrorisme potentiels pouvant non seulement neutraliser des systèmes entiers, mais aussi mettre en danger les populations.

Un effort d'échelle majeur doit être entrepris par l'ensemble des acteurs pour faire face à la «cyber menace» actuelle et future, car le niveau d'information est encore très faible, compte tenu de la non médiatisation des attaques et des enjeux, notamment sur les grands acteurs économiques. Même si ces derniers commencent à comprendre les enjeux et à prendre des mesures pour la sécurité et la surveillance en temps réel de leurs systèmes d'informations, un effort d'accompagnement et de sensibilisation global doit être entrepris. Mais ces menaces touchent également les PME et les opérateurs de second rang, lesquels peuvent aussi être des cibles fragiles. Or, ces PME n'ont le plus souvent ni la connaissance, ni les moyens des grandes structures pour assurer la sécurité de leurs systèmes d'information ou de commande-contrôle.

La proposition consiste alors en la création d'un CERT(18) pour les PMO-E (petits ou moyens opérateurs - entreprises) qui serait subventionné en partie par l'Etat, sous forme de crédits d'impôt, sur les cinq premières années d'abonnement et dégressifs jusqu'à 50%. Ils bénéficieraient également d'une protection ad hoc. Ce CERT/PME-O pourrait être créé avec le contrôle de l'ANSSI, sous la forme d'une structure à but non lucratif impliquant les organisations patronales (du type CGPME-MEDEF). Il ciblerait essentiellement la protection de la cyber-sécurité des petites structures innovantes et technologiques à fort potentiel et des opérateurs de second rang, mais dont l'activité est essentielle pour les communautés qu'elles desservent (petits opérateurs d'eau, de transport, etc.).

Bloc 7 : Points d'attention particuliers

Proposition 19 - Faire de la réponse NRBC une vraie priorité

La menace NRBC a été l'une des priorités du Livre Blanc de 2008. Elle constitue en termes de risques économiques, et potentiellement en vies humaines, un risque considérable. Le coût économique d'une bombe sale radiologique est ainsi estimé entre 4 et 20 milliards d'euros.

Si la menace NRBC est toujours présente dans les discours, son traitement et sa prise en compte réelle sont paradoxaux, avec un financement régulier en matière de R&D mais en «yoyo» sur le plan des acquisitions d'équipements opérationnels.

En ce domaine, la mise en place pour le monde civil d'une véritable démarche capacitaire «moyen-terme» permettrait de donner plus de visibilité aux industriels et faciliterait par conséquent les transferts technologiques issus de la R&D, en adéquation avec les besoins et les marchés futurs. Cette démarche trouverait toute sa cohérence dans le cadre de la mise en place de la filière nationale de sécurité pilotée par le SGDSN.

En effet, si les rapports décrivent toujours des actions «en cours», force est de constater que sur le terrain, les matériels vieillissent (notamment en protection individuelle des intervenants), les nouveaux dispositifs sont mis en place au compte-gouttes (tel le véhicule de détection-identification et de prélèvement VDIP déployé en deux exemplaires), les programmes s'allongent faute de financement et le centre civilo-militaire de formation NRBC peine à se mettre en place. La France commence à faire pâle figure face à certains pays.

Certes, le dispositif «Etat» reste encore cohérent, mais les experts observent une diminution très préoccupante des investissements sur les deux dernières années. On note également l'absence d'une politique claire de prévention et de réaction sur les menaces NRBC à destination des opérateurs d'infrastructures vitales, aucune recommandation étatique n'existant à l'heure actuelle.

(18) Computer Emergency Response Team.

Enfin, il convient de réfléchir de manière urgente sur les protocoles et dispositifs de décontamination des infrastructures face aux agressions de type RBC pour optimiser la gestion de crise et la reprise d'activité au cas où un événement se produisait.

Ceci est d'autant plus important que l'industrie française de défense NRBC est l'une des premières au monde mais elle doit pouvoir compter sur un minimum de projets concrets gouvernementaux et civils pour garder sa crédibilité au plan mondial.

La proposition consiste à sacraliser le montant de 80 millions d'euros/an en dépenses d'investissement NRBC «civil», proposé dans le Livre Blanc de 2008 (hors stocks stratégiques de santé), afin d'éviter de voir le système se déliter dans le temps et les capacités opérationnelles de nos primo-intervenants diminuer rapidement ; et de laisser à penser que nous sommes prêts à faire face à la menace NRBC, alors que nous ne le serions pas vraiment.

La mise en place d'une filière nationale en sécurité, adossée à une réelle démarche capacitaire pour le domaine civil, est par ailleurs indispensable.

Proposition 20 - Adopter une politique de biodéfense-biosécurité plus ambitieuse

Si notre posture en biodéfense-biosécurité est fondée sur le plan NRBC adossé pour la partie «sanitaire» sur des plans ou annexes ad-hoc (variole, pandémie grippale etc.), il convient de noter que la posture n'est aujourd'hui plus très claire, car les choix de 2001 ne sont plus ceux de 2012 et il faut donc déterminer une politique nouvelle face aux différentes menaces bio-terroristes.

En effet, seule une politique à «long terme» adoptant des options raisonnables et raisonnées, en période calme, avec les quelques laboratoires mondiaux (parfois français mais souvent américains) ayant les brevets et la maitrise de la production des vaccins ou médicaments clés face aux agents de la menace paraît efficace. Pour les agents de la menace pour lesquels il n'existe pas de solution thérapeutique et/ou prophylactique efficace, les actions de R&D doivent être soutenues et accompagnées, y compris pour les phases cruciales des essais précliniques et cliniques. En ce domaine où les cycles de développement sont long et complexes, les décisions doivent impérativement s'insérer dans le cadre d'une démarche pérenne couvrant l'ensemble du cycle de développement, partant de l'expression du besoin jusqu'à la vision capacitaire, en privilégiant notamment quand cela est possible les approches duales portant sur des thérapies NRBC et de crises sanitaires. Seule une politique structurée, long terme et guidée par des choix scientifiquement étayés permettra d'assurer notre sécurité en cas de crise grave.

La proposition vise à lancer un débat public sur ce sujet et à renouveler la pensée et l'action sur ce thème.

Bloc 8 : Sur les ouvrages sensibles ou critiques

Proposition 21 - Mieux protéger le patrimoine dans une approche «tous risques-menaces»

La protection du patrimoine en France fait l'objet d'une approche encore trop parcellaire et par silos de risques. Le patrimoine doit faire l'objet d'une protection plus construite, plus fine, basée sur une approche «tous risques» envisageant la sécurité non seulement face aux risques classiques (incendies, vols, dégâts des eaux etc.), mais aussi face aux risques et menaces exceptionnels. Le patrimoine national constitue un atout économique et culturel majeur, et qui sera encore plus essentiel pour notre pays dans le futur.

La proposition consiste à rendre obligatoire un plan global de prévention du patrimoine (PGP) pour les établissements publics ou privés, prenant en compte à la fois les aspects de prévention et de réaction face aux différents types de sinistres majeurs (inondations, risques technologiques ou menaces terroristes). Il convient également de saluer le travail de l'association «Bouclier bleu» dans ce champ d'activité.

Proposition 22 - Sûreté des zones sensibles

La sûreté des zones sensibles pose des problèmes particuliers d'intervention aux forces de l'ordre. En effet, sur une centrale nucléaire ou sur d'autres sites dit «Points d'Importance Vitale», les règles classiques d'interpellation s'imposent : les forces de sécurité ne peuvent faire usage de leurs armes qu'en cas de légitime défense. Cela signifie premièrement que la réponse devra être nécessaire et proportionnelle à l'agression, et deuxièmement que face à des personnes déterminées et armées, la réponse ne pourrait s'engager qu'une fois que les agresseurs auraient ouvert le feu.

Or, si l'on imagine des modes d'intrusions «aériens» tels que des deltaplanes sur un site très sensible, faut-il juridiquement attendre que les forces ennemies se soient regroupées et qu'elles aient placé leurs explosifs, avant de pouvoir défendre le dit site ?

La proposition consiste à classer les PIV en trois catégories et à autoriser pour la première catégorie, l'emploi en premier des armes par les forces de sécurité, à l'exemple des Zones de Défense Hautement Sensibles (ZDHS) militaires. Cela implique bien évidemment que ces sites soient durcis pour éviter toute intrusion «facile», qu'ils soient très clairement signalés, ainsi qu'une évolution de la législation.

Proposition 23 - Mieux partager le renseignement entre sphère publique et privée

Le renseignement est l'apanage de l'Etat et nos services de renseignements intérieur sont principalement tournés vers la surveillance des individus potentiellement dangereux. Les liens avec les entreprises existent et se concentrent, depuis longtemps déjà sur la sensibilisation à l'intelligence économique au plan intérieur.

Or, les entreprises disposent souvent de renseignements qui, faute de correspondants, ne sont pas ou peu exploités. De même, les services de renseignements disposent parfois d'informations qui seraient susceptibles d'intéresser les entreprises, notamment dans le cadre de la vigilance terroriste ou de l'intelligence économique.

La proposition consiste en la création d'une réunion trimestrielle «zonale» animée par la DCRI, sous l'égide du préfet délégué à la défense et à la sécurité. Elle serait réservée aux entreprises «sensibles», principalement aux OIV, aux responsables de sécurité communaux et organisations diverses participant à la sécurité et à la protection des populations, et les participants émanant de la «société civile» y seraient habilités. Cette réunion permettrait d'échanger sur le thème de la «menace», tant au plan national que local.

Proposition 24 - Sur le risque nucléaire civil : relancer et professionnaliser le travail des CLI

La France a lancé il y a de nombreuses années les CLI, lesquelles n'ont malheureusement pas apporté une pierre décisive à la préparation des populations qui ont souvent méconnu ou voulu méconnaître les risques d'un accident majeur. Poids économique des installations nucléaires dans les territoires concernés, négation de la possibilité d'un accident majeur durant des décennies et sous-financement des CLI sont autant de raisons qui font que le dialogue sur la préparation des populations tant en cas de crise que de gestion environnementale post-crise, a été tronqué. Au fil des ans, les CLI sont parfois devenues plus des tribunes anti-nucléaires que des lieux de concertation pour l'information des populations face aux risques.

Les accidents de Tchernobyl, mais surtout de Fukushima, ont montré que les populations devaient vivre avec un risque, certes d'une occurrence infime, mais que l'on ne pouvait occulter, et qu'à partir de là, ce risque infime devait, en toute transparence et en toute conscience être reconnu et les populations informées. Pour cela les CLI, dont le rôle doit être réaffirmé, doivent être mieux subventionnées par les opérateurs concernés de manière à permettre une véritable information du public sur toutes les phases potentielles de la crise et de la post-crise potentielle.

La proposition est de créer une taxe afin de financer chaque CLI à hauteur de 200 K€/an par CLI pour permettre un travail d'information et de veille efficace au profit des populations et des collectivités dans un rayon de 20 Km autour des installations nucléaires de base.

Bloc 9 : Mieux sensibiliser à la prévention et la continuité d'activité

Proposition 25 - Mieux entretenir les ouvrages de prévention

Les catastrophes comme Xynthia récemment, ainsi que les inondations du Rhône ou de la Somme il y a quelques années, montrent la difficulté de maintenir en état des ouvrages de prévention dont les maîtres d'ouvrages sont aussi nombreux que variés.

La proposition consiste à faire des conseils généraux les responsables de l'entretien de ces ouvrages si le propriétaire est défaillant, la collectivité pouvant alors se substituer au propriétaire en cas de défaut de celui-ci.

Proposition 26 - Repenser le régime CatNat en incluant une incitation forte à la prévention

Le régime CatNat est un système assurantiel très protecteur. Son défaut réside dans le fait qu'il indemnise dans (presque) tous les cas de figure, dès que l'arrêté de catastrophe naturelle a été pris et qu'il ne fait pas la part belle à la prévention. Si nous pouvons comprendre que le montant de la prime forfaitaire ne change pas grand chose à l'économie du système au niveau d'un particulier, il nous semble en revanche important qu'un signal fort soit envoyé à l'industrie et aux communes.

La proposition consiste donc à moduler le tarif assurantiel pour les industries et les communes dans une fourchette de 10 à 30 % en fonction des travaux de prévention réalisés par rapport à un risque centennal, voire millénaire pour les réductions les plus importantes, cet effort étant associé à une aide au financement avec des taux d'intérêt réduits offerts par des banques publiques.

Proposition 27 - Lancer les initiatives innovantes «continuité d'activité»

La continuité d'activité a du mal à s'imposer en France. Le grand exercice de la pandémie H1N1 a laissé un goût amer de mauvaise gestion entre grandes entreprises et Etat. Les BCM (Business Continuity Managers) ne parviennent pas toujours à s'imposer et à actualiser leurs travaux et procédures dans les entreprises. Dans les PME, la situation est encore plus critique. Peu de choses y sont faites hors obligation d'un donneur d'ordre. Or, la résilience sociétale passe impérativement par la prise en compte dans les entreprises grandes ou petites, de plans et d'exercices réguliers en matière de continuité d'activité.

La proposition consiste à ce que l'Etat soutienne, en partenariat avec le monde économique, et notamment les chambres de commerce et d'industrie, sur une base biannuelle, une «semaine de la continuité d'activité» pour aider à faire pénétrer le concept au sein du monde économique français et particulièrement vers les PME/TPE.

Il convient de saluer les travaux du Club de la Continuité d'Activité (CCA), rare structure française travaillant sur ces sujets.

Proposition 28 - Créer un titre d'identité «officiel» pour les gestionnaires de crises privés (SAIV et Activités essentielles)

Cette mesure peut paraître de second ordre mais elle nous paraît essentielle dans le cadre d'un dispositif SAIV élargi à la gestion de crise. En effet en cas de crise ou de chaos, il est extrêmement important que les autorités, notamment de police, puissent reconnaître les responsables de gestion de crise ou de continuité d'activité d'une entreprise, notamment en cas de bouclage de zone ou d'événements ayant des implications de sécurité.

La proposition consiste à créer un titre officiel de «gestionnaires de crise», sous la forme d'une carte professionnelle délivrée et administrée par le Conseil National des Activités Privées de Sécurité (CNAPS).

Bloc 10 : Mieux travailler la normalisation de sécurité et les aspects de post-crise

Proposition 29 - Etre plus présent dans la standardisation des normes de sécurité au plan international

La France est encore trop peu présente dans les forums internationaux de normalisation. Or, les normes sont tant pour les entreprises que plus généralement pour les organisations, une nouvelle forme juridique de «bonnes pratiques» que l'on ne peut ignorer. L'expertise en France est encore trop limitée et la participation aux travaux internationaux trop réduite.

La proposition consiste à créer un bureau de la normalisation de sécurité, au niveau du Premier Ministre (SGDSN) doté d'une équipe d'ingénieurs et spécialistes bilingues, ainsi que d'un budget permettant d'entrer des projets de norme, et la participation aux travaux internationaux, de manière à défendre et à soutenir les intérêts nationaux et européens. Ce bureau resterait en liaison au plan national avec les différents ministères, les partenaires industriels et les organisations professionnelles compétentes, dont l'AFNOR.

Proposition 30 - Réaliser des plans de post-crise systématiquement en regard des plans de prévention et de gestion de crise - Travailler la problématique du traitement des déchets

La planification de «post-crise» est aujourd'hui inexistante en France. Si la continuité d'activité commence à être prise en compte, la «reconstruction ou l'adaptation» après une catastrophe, la problématique de la gestion des déchets, de la gestion environnementale, ne sont pas ou très peu planifiées.

La résilience économique et sociale passe pourtant par une planification poussée destinée à optimiser la reprise économique et renforcer la cohésion sociale après une catastrophe, et surtout après la phase aigüe de la crise.

La proposition consiste en la réalisation d'un plan «Résilience territoriale» au niveau départemental, face à tous les risques majeurs naturels et technologiques visés dans le DDRM. Ce plan aurait une visée d'échéancier au mois, au trimestre et à l'année (du T0 à 5 ans). Il pourrait être préparé et mis en œuvre par les collectivités territoriales (conseils généraux), avec le soutien des structures régionales de planification (SIRDPC).

Abréviations et acronymes

ACROPOL : Automatisation des Communications Radiotéléphoniques Opérationnelles de Police
AFNOR : Association Française de Normalisation
ANSSI : Agence Nationale de Sécurité des Systèmes d'Information
ANCCLI : Association Nationale des Commissions et Comités Locales d'Information
ANTARES : Adaptation Nationale des Transmissions Aux Risques Et aux Secours
AQMI : Al Qaïda au Maghreb Islamique
ARS : Agence Régionale de Santé
ASN : Autorité de Sûreté Nucléaire
AZI : Atlas des Zones Inondables
BSPP : Brigade de Sapeurs-Pompiers de Paris
CCA : Club de la Continuité d'Activité
CCI : Chambre de Commerce et d'Industrie
CCR : Caisse Centrale de Réassurance
CENALT : Centre National d'Alerte aux Tsunamis
CERT : Computer Emergency Response Team
CGEDD : Conseil Général de l'Environnement et du Développement Durable
CIC : Cellule Interministérielle de Crise
CIC : Centre Interministériel de Crise
CLI : Commissions Locales d'Information
CLIC : Comités Locaux d'Information et de Concertation
CNA : Code National d'Alerte
CNAPS : Conseil National des Activités Privées de Sécurité
CNT : Conseil National de Transition
COD : Centre Opérationnel Départemental
COGIC : Centre Opérationnel de Gestion Interministérielle des Crises
COPN : Centre Opérationnel de la Police Nationale
CORRUSS : Centre Opérationnel de Réception et de Régulation des Urgences Sanitaires
CPCO : Centre de Planification et de Conduite Opérationnelle
CROGEND : Centre de Renseignement Opérationnel de la Gendarmerie Nationale
CSS : Commissions de Suivi de Site
CTA : Centre de Traitement de l'Alerte
CTC : Centre Technique de Crise
DCRI : Direction Centrale du Renseignement Intérieur
DDRM : Dossier Départemental sur les Risques Majeurs
DICRIM : Document d'Information Communal sur les Risques Majeurs
DGSCGC : Direction Générale de la Sécurité Civile et de la Gestion des Crises
DNS : Directives Nationales de Sécurité
DREAL : Direction Régionale de l'Environnement, de l'Aménagement et du Logement
ECS : Evaluation Complémentaire de Sûreté
ENISA : European Network and Information Security Agency
ENSREG : European Nuclear Safety Regulators Group
FARN : Force d'Action Rapide Nucléaire
FIPN : Force d'Intervention de la Police Nationale
FPRNM : Fonds de Prévention des Risques Naturels Majeurs
GIGN : Groupe d'Intervention de la Gendarmerie Nationale
ICPE : Installation Classée pour la Protection de l'Environnement
INPT : Infrastructure Nationale Partageable des Transmissions
IRSN : Institut de Radioprotection et de Sûreté Nucléaire

Abréviations et acronymes

JAEA : Agence Japonaise de l'Energie Atomique
JSDF : Japan Self-Defense Forces
NISA : Nuclear and Industrial Safety Agency
NRBC-E : Nucléaire, Radiologique, Biologique, Chimique, Explosive
NSC : Nuclear Safety Commission of Japan
OIV : Opérateurs d'Importance Vitale
ONRN : Observatoire National des Risques Naturels
OTIAD : Organisation Territoriale Interarmées de Défense
PAPI : Programme d'Actions de Prévention des Inondations
PCA : Plan de Continuité d'Activité
PCS : Plan Communal de Sauvegarde
PGP : Plan Global de Prévention
PGRI : Plan de Gestion des Risques d'Inondation
PIV : Point d'Importance Vitale
POI : Plan d'Opération Interne
PPE : Plan de Protection Externe
PPI : Plan Particulier d'Intervention
PPP : Plan de Protection Particulier
PPR : Plan de Prévention des Risques
PPRI : Plan de Prévention des Risques Inondation
PPRN : Plan de Prévention des Risques Naturels
PPRNT : Plan de Prévention des Risques Naturels et Technologiques
PPRS : Plan de Prévention des Risques de Submersion marine
PPRT : Plan de Prévention des Risques Technologiques
PSC1 : Prévention et Secours Civiques de niveau 1
PSO : Plan de Sécurité Opérateur
RGPP : Révision Générale des Politiques Publiques
RNA : Réseau National d'Alerte
SAIP : Système d'Alerte et d'Information des Populations
SAIV : Sécurité des Activités d'Importance Vitale
SCADA : Supervisory Control and Data Acquisition
SCAIV : Sécurité et Continuité des Activités d'Importance Vitale
SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale
SIDPC : Service Interministériel de Défense et Protection Civile
SIG : Service d'information du Gouvernement
TMD : Transport de Matières Dangereuses
UCOFI : Unité de Coordination des Forces d'Intervention
VDIP : Véhicule de Détection Identification et de Prélèvement
ZDHS : Zone de Défense Hautement Sensible

ANCCLI : Association Nationale des Commissions et Comités Locales d'Information

Association créée le 5 septembre 2000 et regroupant les comités et commissions locales d'information, l'ANCCLI a été constituée dans un objectif de prévention des risques, de surveillance et d'information des populations et de l'ensemble des acteurs d'un territoire où une activité nucléaire est présente.

ANTARES : Adaptation Nationale des Transmissions Aux Risques Et aux Secours

Réseau de radiocommunications numériques mis en place par l'Etat pour permettre l'interopérabilité des réseaux de communication des services publics participant aux missions de sécurité civile.

CLI : Commissions Locales d'Information

Mises en place le 15 décembre 1981 auprès des installations nucléaires de base et de toutes les structures assimilées, ces commissions ont à la fois une mission d'information et de suivi permanent de l'impact des grands équipements énergétiques.

SAIP : Système d'Alerte et d'Information des Populations

Adopté en juin 2008 dans le Livre Blanc de la Défense et de la Sécurité Nationale dans le cadre de la modernisation de l'alerte des populations, le nouveau système d'alerte, SAIP, intègre une capacité à avertir les populations de tout événement de sécurité civile : catastrophes naturelles (inondations, séisme…), technologiques (accident industriel…), outre les attentats terroristes. La vocation initiale de l'ancien système d'alerte se focalisant sur le danger aérien est donc dépassée.

SCADA : Supervisory Control and Data Acquisition

Système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques. On les retrouve dans différents contextes critiques : surveillance de processus industriels, transport de produits chimiques, systèmes municipaux d'approvisionnement en eau, distribution électrique, canalisations de gaz et de pétrole…

Remerciements

Le groupe de rédaction tient à remercier tous les contributeurs à cette étude, mais aussi tous les intervenants à nos travaux qui nous permettent de réunir l'information, de discuter les idées et d'établir les propositions qui vous sont proposées dans ce rapport annuel.

Un certain nombre d'entre eux, d'origine publique ou privée, venant du monde de l'entreprise ou associatif, ayant des postes sur Paris ou en région, actifs ou retraités, reconnaîtront certainement leurs idées, commentaires ou propositions. Il nous est impossible de tous les nommer, mais qu'ils en soient remerciés. Le Haut comité n'a d'autre but que de faire progresser la préparation de notre pays aux situations de risques et de menaces majeurs.

Le groupe de rédaction a été composé de :
M. Christophe BOUCHER, Journaliste, HCFDC
Gal (cr) COPEL Etienne, Président du collège des experts, HCFDC
M. Richard NARICH, Administrateur HCFDC
Mlle Claire SABATIER, Chargée de mission, HCFDC
M. Christian SOMMADE, Délégué général du HCFDC

CONTRIBUTIONS :

M. Alexis ARIF, Collège des experts, HCFDC
M. Christophe BOSSUET, Assistant projet NRBC, CEA
M. Franck BRACHET, Directeur général des services techniques de la Mairie de Limay
Gal (cr) Etienne COPEL, Président du collège des experts, HCFDC
M. Jean DE LA RICHERIE, Directeur grands comptes sécurité, Cassidian
M. Marian DUMITRU, Directeur exécutif, Isarss International
Mme Alexia FLEURY, OSMOS
M. Christophe FRERSON, SDIS des Bouches-du-Rhône, ATRISC
M. le sénateur Paul GIROD, Président d'honneur du HCFDC
M. Daniel LALLEMANT, Collège des experts, HCFDC
M. Patrice-Louis LAYA, Animateur du blog Pavillon Orange, Infocommune
M. le sénateur Jean-René LECERF, président du HCFDC
M. Jean-Jacques LOUGEZ, Officier de sécurité, MEDDTL
M. Laurent MONTADOR, Directeur catastrophes naturelles et fonds publics, CCR
M. Jean-François MOREAU, Ingénieur nucléaire
Mme Danielle MORONI, Chef de la mission sécurité confidentielle, RTE
M. Max MOULIN, Ingénieur consultant
M. Richard NARICH, Administrateur HCFDC
M. Laurent OLMEDO, Chef de projet recherches en sécurité globale, CEA
M. Richard OLSZEWSKI, Administrateur HCFDC
M. Jacques POINAS, Conseiller sûreté, Inspecteur général de la police nationale (er), ancien directeur de l'UCLAT
M. Claude SCHMITT, Expert NRBC, Préfecture de l'Essonne
M. Gilles TENEAU, Professeur associé ISC Paris
M. Hugues THIERY, Consultant, Links conseil
Mme Pauline TREMBLOT DE LA CROIX, Ingénieur d'affaires, OSMOS
Gal (2s) VERNOUX François, Conseiller scientifique NRBC

Les vues exposées dans cet ouvrage sont le fruit d'un travail collectif. Les contributeurs ne peuvent être engagés dans aucun aspect particulier de la rédaction. Ils se sont exprimés à titre personnel et en aucun cas au nom de la société ou de l'organisme auxquels ils appartiennent.

Graphiste : M. Gaëtan GAUTHIER

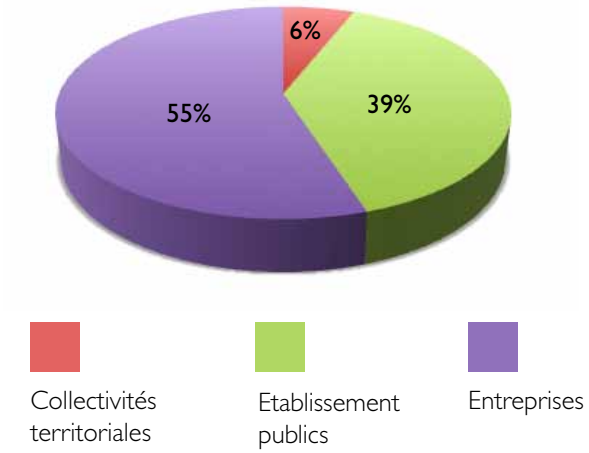
RAPPORT D'ACTIVITE 2011

Nos membres et correspondants en 2011

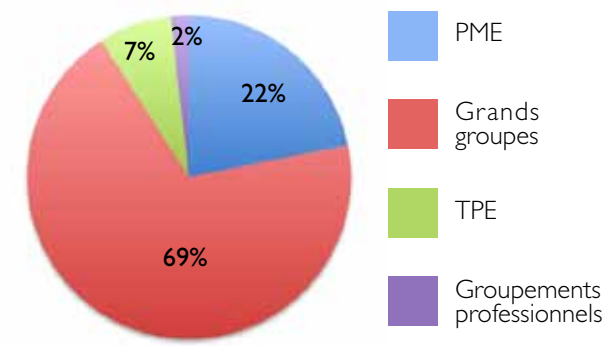
Le Haut Comité Français pour la Défense Civile, en sa qualité de plateforme d'échanges et d'information, constitue en France le premier réseau d'experts et acteurs de haut niveau sur la préparation de la nation face aux risques et menaces majeurs. Il réunit des parlementaires, les services de l'Etat compétents, les opérateurs et les entreprises, les collectivités territoriales, les associations, et est ouvert à toutes les parties prenantes.

Le HCFDC compte parmi ses membres une grande partie des sociétés du CAC 40, des PME, les services de l'Etat concernés par ces questions, des collectivités locales, des associations et de nombreux experts.

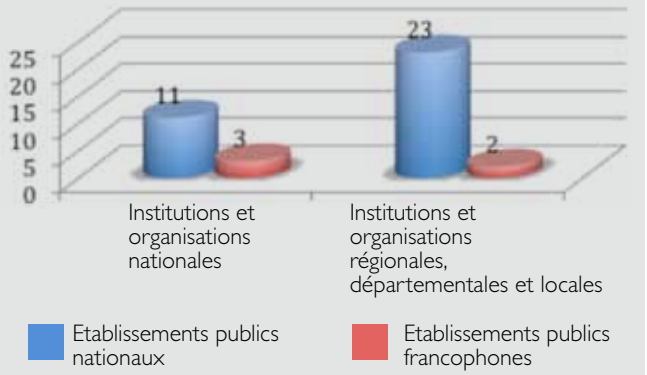
Les membres : personnes morales en 2011 (hors Etat)



Répartition des entreprises membres en 2011



Répartition du collège institutions et associations en 2011



Près de 200 référents (personnes physiques ou morales) cotisants 2010, dont :

39 industries et services
16 opérateurs d'infrastructures vitales
31 associations ou institutions ou collectivités

Soit plus de 1200 correspondants «membres»
Plus de 14000 contacts et correspondants au sein du domaine de la défense et de la sécurité.

Les collèges du HCFDC

1 - Le collège des élus et des collectivités territoriales
2 - Le collège des associations et des institutions
3 - Le collège des entreprises de défense et sécurité
4 - Le collège des opérateurs d'infrastructures critiques
5 - Le collège des entreprises industrielles et de service
6 - Le collège territorial
7 - Le collège des experts

Le collège des élus et des collectivités territoriales

Le collège des associations et des institutions

Le collège des entreprises de défense et sécurité

Le collège des opérateurs d'infrastructures critiques

Le collège des entreprises industrielles et de services

Une centaine de personnalités membres du collège des experts et du collège territorial

Bilan 2011 - Activités

EVÈNEMENTS :
5 colloques HCFDC
11 petits-déjeuners rencontres
10 Talk vidéo en direct
4 dîners «club» (membres)
Les Trophées de la Résilience Sociétale

FORMATIONS :
25 jours de formations spécialisées
Une session nationale (35 jours – 100 intervenants)

MÉDIA :
Le Blog
Web tv www.defencivTV.org

ETUDE :
Résilience territoriale

Les colloques

23 mai 2011
JOURNÉE PRÉVENTION DES RISQUES MAJEURS ET SAUVEGARDE DES POPULATIONS
En partenariat avec le Ministère de l'Intérieur, de l'Outre-Mer, des Collectivités Territoriales et de l'Immigration

30 juin 2011
Journée SECURE DAY
En partenariat avec l'institut CEA LIST
Lors de cette journée, le CEA LIST a fait connaître ses innovations et sa roadmap technologique dans le domaine de la sécurité et de la défense. Cet évènement organisé en partenariat avec le Haut Comité Français pour la Défense Civile, il a également été l'occasion de mener une réflexion sur les enjeux majeurs du futur et de dégager des perspectives, notamment au travers de discussions et tables rondes.

9 septembre 2011
ANTHRAX (Maladie du Charbon) : menaces et réponses ?
En partenariat avec Emergent Biosolutions, l'EPRUS, le CEA, la DGA Maîtrise des armements NRBC, le Ministère de l'Intérieur, NBC Sys, Paul Boyé, Bertin Technologies, Proengin

8 et 9 novembre 2011
INONDATIONS MAJEURES : quelle prévention et quelles réponses?
En partenariat avec la FFSA, la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC), Ministère de l'Intérieur, le GICAT et le Ministère de l'Ecologie (MEDDTL/DGPR)

28 novembre 2011
LE RISQUE INFECTIEUX DANS TOUS SES ETATS : Quelle gestion du risque et des crises sanitaires dans le domaine biologique?
En partenariat avec l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (EPRUS)

Les petits-déjeuners débats au restaurant du Sénat

Janvier 2011
Le modèle SAMU est-il menacé ? Urgences, réforme hospitalière et démographies médicales – quel apport des nouvelles technologies dans le secours médicalisé ?
Docteur Marc Giroud, Président de SAMU de France

Février 2011
Plan de prévention des risques et PCS : une nouvelle législation est-elle nécessaire?
M. Christian Kert, Député des Bouches du Rhône, Président de l'AFPCN

Avril 2011
Quelle organisation pour la cyber défense française?
M. Patrick Pailloux, Directeur général de l'Agence nationale de la sécurité des systèmes d'information, SGDSN

Avril 2011
Spécial Japon : Du séisme à la résilience; point sur la situation sanitaire et économique du Japon
Professeur Patrick Gourmelon, Directeur de la Radioprotection de l'Homme, IRSN et M. Michel Nesterenko, Consultant

Mai 2011
La gestion des crises en Belgique et quelle interface pour les centres de gestion de crise en Europe?
Mme Monique Bernaerts, Directrice du Service de Planification d'Urgence, Direction Générale du centre de crise belge

Juin 2011
Sécurité civile : une nouvelle organisation pour quelles missions?
Monsieur le Préfet Jean-Paul Kihl, Directeur de la Sécurité Civile, Ministère de l'Intérieur

Juillet 2011
Escherichia coli : les dispositifs français et européens de réponse sanitaire sont-ils adéquats ?
Docteur Jean-Claude Desenclos, Directeur scientifique de l'Institut de Veille Sanitaire (INVS)

Septembre 2011
Point sur les avancées du Conseil National des Activités Privées de Sécurité (CNAPS)
M. le Préfet Jean-Louis Blanchou, Délégué interministériel à la sécurité privée, Ministère de l'Interieur

Octobre 2011
L'Autorité de sûreté nucléaire : son rôle et ses actions après Fukushima
Mme Marie-Pierre Comets, Commissaire de l'Autorité de sûreté nucléaire (ASN)

Novembre 2011
Biométrie : enjeux de sécurité et de société, questions de fond et d'actualité
M. Bernard Didier, Directeur général adjoint, Directeur de la technologie et de la stratégie, Morpho

Décembre 2011
Brigade de sapeurs-pompiers de Paris: actualité et nouveaux enjeux
Général Gilles Glin, Commandant de la Brigade de Sapeurs-Pompiers de Paris (BSPP)

Talks techniques sur le web

Emission diffusée en direct sur internet à destination des acteurs de la sécurité globale (revisionnable pour nos membres).

12 janvier 2011
Cyber défense : quelle réalité ?
Avec M. Nicolas Arpagian, journaliste, rédacteur en chef, Prospective Stratégique,
M. le Vice-Amiral Michel Benedittini, Directeur général adjoint, Agence Nationale de la Sécurité des Systèmes d'Information,
Maître Etienne Drouard, Avocat, Cabinet MORGAN LEWIS,
M. Sébastien Héon, Expert SI, CASSIDIAN Systems.

21 février 2011
Les exercices de gestion de crise
Avec M. Charles-Edouard Anfray, Délégué à la gestion de cirse, Groupe Total,
Lcl Alain Chevallier, Chargé de mission exercices entrainement, Ministère de l'Intérieur/Direction de la Sécurité Civile,
M. Edouard de Pommery, Bureau des exercices majeurs, SGDSN,
M. Emmanuel Teboul, Direction des opérations et de la qualité des processus, SNCF.

15 et 22 mars 2011
Spécial japon – 1er et 2ème édition : Un regard à plus long terme... (2 émissions)
Avec M. Patrick Lagadec, Directeur de recherche, Ecole Polytechnique,
M. Eric Stemmelen, Consultant, ancien attaché de sécurité intérieure à l'Ambassade de France au Japon,
M. Laurent Vibert, Consultant en communication de crise et ancien Lcl de la BSPP,
M. Gérard Lucas, Conseiller scientifique au CEA,
M. Michel Nesterenko, Consultant PTE et spécialiste des questions énergétiques et d'infrastructures,
M. Jean-François Riffaud, Porte-parole de la Croix Rouge Française,
Mme Régine Serra, Spécialiste de l'Asie et du Japon à Sciences Po, chercheuse à l'Institut Français des Relations Internationales (IFRI).

23 mars 2011
Les outils de simulation sont-ils opérationnels pour un emploi dans la gestion des crises ?
Avec Lcl Philippe Giraud, Conseiller technique, BSPP,
M. Jean-Christophe Lambert, Business Development Simulation, CASSIDIAN,
M. Christophe Meyer, Responsable des études amont, Thales Services,
M. Patrick Samama, Président & CEO, MASA Group.

7 avril 2011
Quelles avancées pour un emploi opérationnel des drones dans le domaine de la sécurité intérieure et civile ?
Avec M. Jean Caron, en charge de la politique produit drones chez EADS-CASSIDIAN,
M. Gérard Feldzer, Expert en aéronautique, Ancien directeur du musée de l'air et de l'espace du Bourget,
M. Nicolas Guillemet, responsable commercial des activités Défense et Sécurité, Bertin,
Col. Bruno Guion de Meritens, Adjoint au Général commandant les formations militaires de la sécurité civile, Ministère de l'Intérieur.

22 juin 2011

Assurances et régimes CAT NAT : quel futur et comment financer la prévention?

Avec M. Patrick Bidan, Directeur de la souscription, Caisse Centrale de Réassurance,
M. Nicolas-Gérard Camphuis, Directeur du Centre Européen de Prévention du Risque Inondation (CEPRI)
M. Christian Kert, Député des Bouches du Rhône, Président de l'AFPN.

12 septembre 2011

Spécial 11 septembre : dix ans après. Quelle évolution dans la politique de contre terrorisme et quelle efficacité ?

Avec M. Christophe Caupenne, Consultant en sûreté, Ancien chef du groupe gestion de crise et négociation au RAID (Recherche, assistance, intervention, dissuasion), Ministère de l'Intérieur,
M. Denis Fortier, Directeur de la rédaction, AEF sécurité globale,
M. Jean Guisnel, Journaliste au «Point», Spécialiste des questions militaires et de renseignement,
M. Jacques Poinas, Conseiller sûreté, Inspecteur général de la police nationale (er), ancien directeur de l'UCLAT, Ministère de l'Intérieur.

Les presse clubs sécurité
En coopération avec AEF Sécurité Globale

aef.info

Emission diffusée en direct via notre plateforme internet à destination des acteurs de la sécurité globale, et revisionnable pour nos membres.

- Une personnalité invitée par mois
- Durée 45 mn : 30' interview - 15' questions
- Un nouveau décor - 4 interviewers

Octobre 2011

A la veille de Milipol ; le marché mondial de la sécurité : quelle place pour la France ?

Avec M. Emile Perez, Directeur de la direction de la coopération internationale (DCI), du Ministère de l'Intérieur

Novembre 2011

L'évolution des moyens techniques à la Préfecture de police

Avec M. Thierry Delville - Directeur des Services Actifs de la Police Nationale, PRÉFECTURE DE POLICE – DOSTL

Décembre 2011

Sécurité et Europe

Avec M. Luigi Rebuffi, Chief Executive Officer, Europe Organisation for Security (EOS)

Les Trophées de la résilience sociétale 2011

Les Trophées de la Résilience Sociétale ont pour objectif de récompenser tous les deux ans les meilleures actions et initiatives concourant à améliorer la résilience sociétale, la sécurité, la protection des populations et la continuité d'activité, face aux risques et menaces majeurs. Les Trophées ont été remis le 23 mai 2011 dans la salle Clémenceau du Palais du Luxembourg.

Trophée d'Honneur
M. Patrick Lagadec

Trophée de la résilience sociétale
Mayane Association
Sensibilisation des publics scolaires au risque inondation

Trophée de l'action opérationnelle
Force Aérienne de la Gendarmerie Nationale
Actions de sauvetage menées lors des inondations du Var 2010

Brigade nautique de Saint-Gilles Croix-de-Vie (DGGN)
Actions de sauvetage menées lors de la tempête Xynthia 2010

Trophée de l'Administration publique
Etat-Major de la Zone de Défense de Paris
Système d'Information Numérique Standardisé (SINUS)

Trophée de la Collectivité locale
Mairie de Notre-Dame-de-Gravenchon
Sensibilisation de la population à la sécurité / Semaine de la sécurité

Intercommunalité APTV / SMP / CCPM / Arlysère
Gestion des risques à l'échelle intercommunale

Trophée de la Citoyenneté
FNRASEC
Action permanente de soutien de la Sécurité Civile

Trophée de l'opérateur d'infrastructure critique
RATP - Mission Défense
Préparation aux menaces NRBC

Trophée Européen
EOS - European Organization for Security
Organisation en 2011 de la première table ronde Public-Privé de haut niveau sur la sécurité à l'échelon Européen

Trophée de l'Innovation technologique
Service d'Incendie et de Secours du Département des Landes
Système de localisation des incendies par surveillance vidéo

Prix Spécial du Jury
CEA (DSV et DAM)
Tickets détecteurs d'agents biologiques pathogènes

Proengin
Capteur unique de détection biologique et chimique

Statistiques 2011 de la plateforme numérique

Plateforme numérique : www.hcfdc.org
+ de 300 vidéos
+ de 100 petits-déjeuners en archives
+ de 70 colloques en archives
+ de 450 présentations
des centaines de pages
des centaines de liens
des émissions vidéo en direct plusieurs fois par mois

Fréquentation du site www.hcfdc.org : + 33% 2010 - 2011

50 000 visites uniques par an, tous sites confondus

Sur le site hcfdc.org :

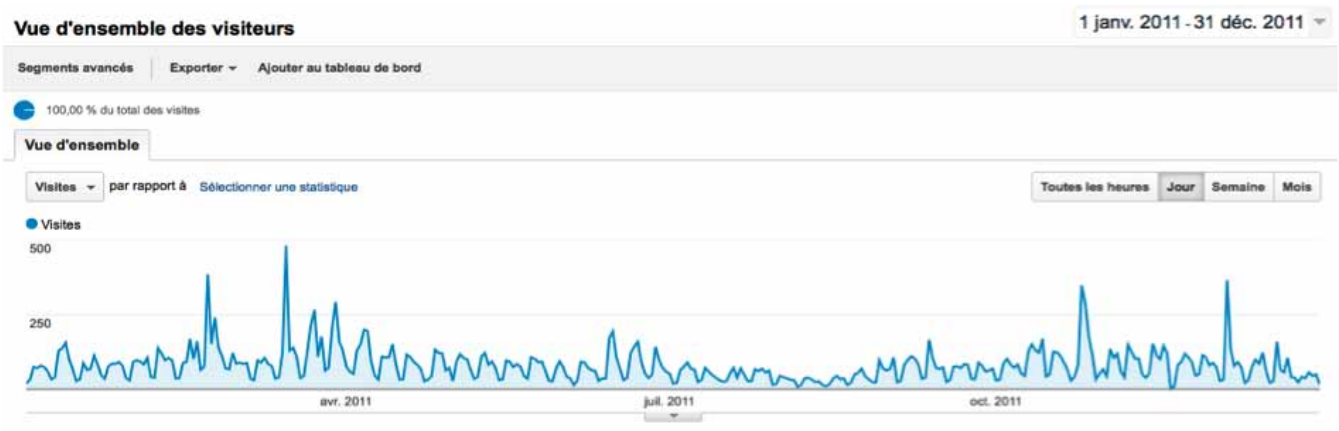
16 845 Visiteurs uniques
97 422 Pages vues
69 083 Consultations uniques

Statistiques 2011du Pavillon Orange

Sur le site pavillon.hcfdc.org :

7 278 Visiteurs uniques
17 912 Pages vues
13 619 Consultations uniques
150 villes enregistrées sur le site

Courbe de fréquentation du site hcfdc.org



Formations 2011

Formations à la sécurité globale (HCFDC Services) : «Former et rapprocher l'ensemble des acteurs de la sécurité globale dans la gestion de crises complexes».

3 sessions de formation «Gestion de crise : quelle interface public-privé ?»

3 sessions de formation «Menaces et modes opératoires d'actions terroriste» (Confidentiel – Défense)

1 session de formation «Plan de Sécurité d'Opérateur» (Réservé aux opérateurs d'importance vitale et préfectures)

1 session de formation «Gestion de crise communale»

1 session de formation «Sensibilisation aux menaces NRBC»

Session Nationale : Résilience et sécurité sociétales

Pour répondre à une demande croissante de formation permanente à haut niveau des cadres de direction en matière de sécurité globale, le Haut Comité Français pour la Défense Civile a lancé en Mars 2010 la première session nationale : «Résilience et sécurité sociétales».

L'objectif de cette session est de former, sur une base de 30 jours par an, des cadres supérieurs ou à fort potentiel, aux risques et menaces majeurs ainsi qu'aux concepts, organisations et techniques de la gestion des crises. L'objectif pédagogique est d'inculquer les meilleures pratiques en matière de sécurité et résilience au profit de tous types d'organisations : entreprises, collectivités, institutions...

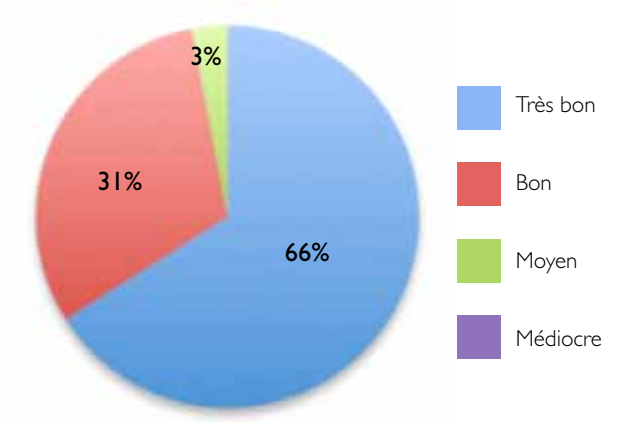
Une cinquantaine d'auditeurs ont participé à la 2ème Session nationale Résilience et sécurité sociétales du HCFDC, de janvier à décembre 2011.

Modules de la Session nationale 2011

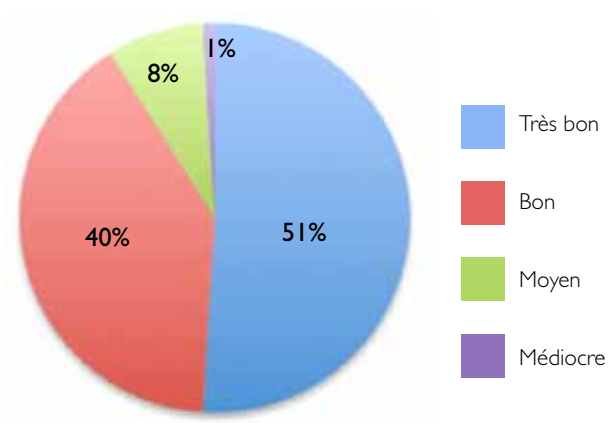
Module 1 : Introduction aux risques, menaces systématiques et à la résilience
Module 2 : Organisation de la défense et de la sécurité nationale
Module 3 : Gestion des crises
Module 4 : Modes d'action terroristes et cybercrime
Module 5 : Sécurité des activités d'importance vitale et interdépendances et continuité d'activité
Module 6 : Risques naturels majeurs, réchauffement climatique et sécurité
Module 7 : L'Europe et la sécurité globale (voyage à Bruxelles)
Module 8 : Menaces NRBC (Nucléaire, Radiologique, Biologique, Chimique) et grands risques sanitaires
Module 9 : Voyage d'études à Washington DC
Module 10 : Risques technologiques majeurs et vieillissement des infrastructures
Module 11 : Module de clôture

Indice général de satisfaction sur la Session nationale 2011

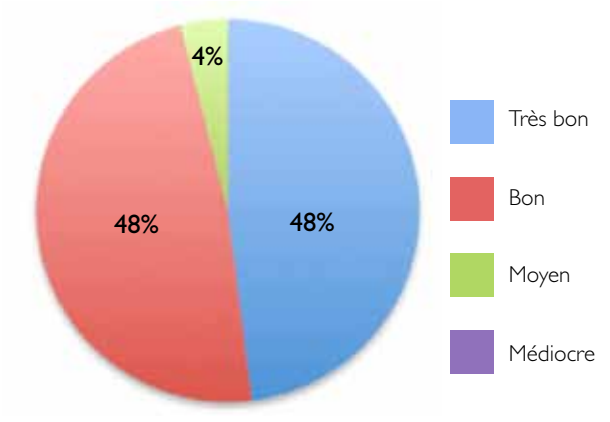
Sur l'ensemble des modules



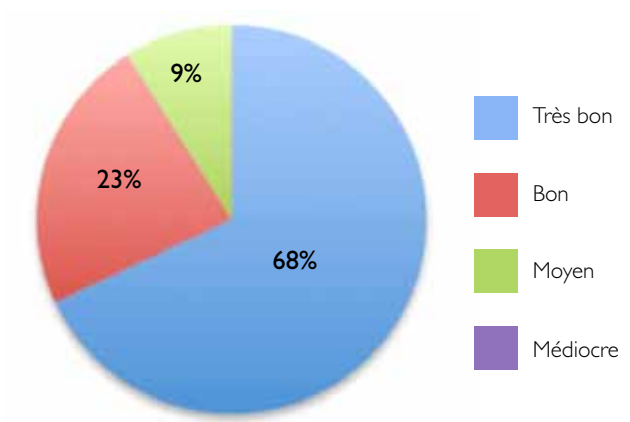
Sur l'ensemble des interventions



Sur la logistique



Sur l'ensemble des visites



PAVILLON ORANGE : www.pavillon-orange.org

Un label décerné par le HCFDC aux communes qui répondent à un certain nombre de critères en termes de sauvegarde et de protection des populations face aux risques et menaces majeures, et qui ont notamment réalisé un Plan Communal de Sauvegarde.

Les objectifs du label :

- Récompenser et valoriser toute commune ou communauté de communes qui a mené des actions concrètes en vue de renforcer la sécurité et la protection de sa population face aux risques majeurs et notamment par la mise en place d'un Plan Communal de Sauvegarde et de moyens associés.
- Motiver les communes et sensibiliser les citoyens sur les questions de protection civile et sur leur propre sécurité face aux risques majeurs.

21 villes labellisées Pavillon Orange :

Nievroz, Céreste, Nice, Tarascon, Venelles, Biganos, Guichen, Tours, Champ sur Drac, Saint-Etienne, Nancy, Neuville sur Saône, Feyzin, Albertville, Gonfreville l'Orcher, Toulon, La Seyne sur Mer, Sorgues, Mont-Dore, Dumbéa, Bourbonne les Bains.

Enrichissement du site Web en 2011 : création d'un blog PCS&Résilience, espace d'expression sur la sauvegarde des populations.

BOUCLIER ORANGE : www.bouclier-orange.org

Valoriser les démarches de prévention des risques majeurs dans les établissements d'enseignement.

Le Bouclier Orange est une distinction valorisant l'état de bonne préparation face aux risques naturels et technologiques, selon une double approche opérationnelle et culturelle.

Il s'inscrit dans l'esprit de la loi de modernisation de la sécurité civile où chacun contribue à sa propre sécurité à titre individuel ou collectif.

Soutenue par le Ministère du Développement Durable, cette initiative est conduite conjointement entre l'Institut Français des Formateurs Risques Majeurs et Protection de l'Environnement (www.iffo-rme.fr) et le Haut Comité Français pour la Défense Civile (www.hcfdc.org); avec la participation de l'Observatoire National de la Sécurité et de l'accessibilité des établissements d'enseignement (ONS).

Autoprotection du citoyen www.autoprotectionducitoyen.eu

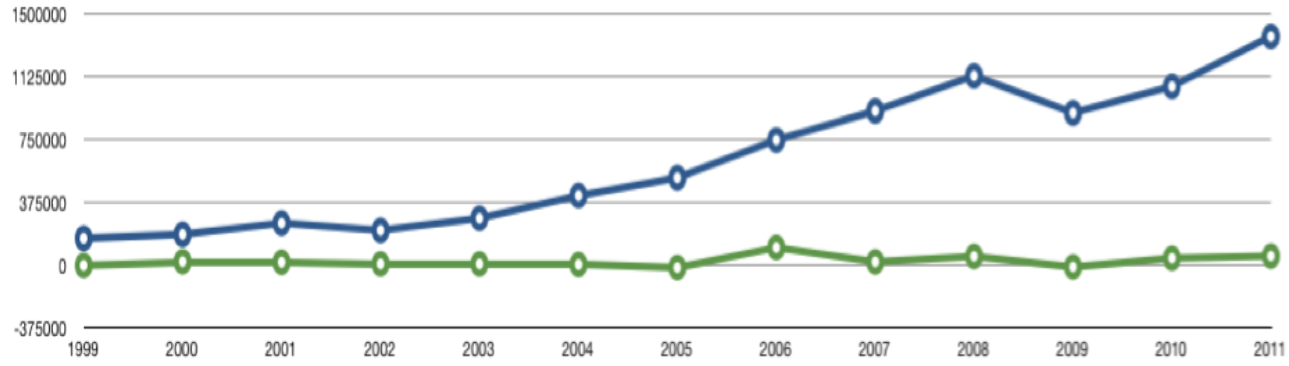
Résultat financier 2011

HCFDC Association		HCFDC Services
684 561 €	Produit d'exploitation	674 024 €
29 206 €	Produit d'exploitation	8 616 €
3 107 €	Résultat financier	2 758 €
4 363 €	Résultat exceptionnel	1 470 €
36 675 €	Résultat net	12 844 €
Résultat consolidé	49 519 €	

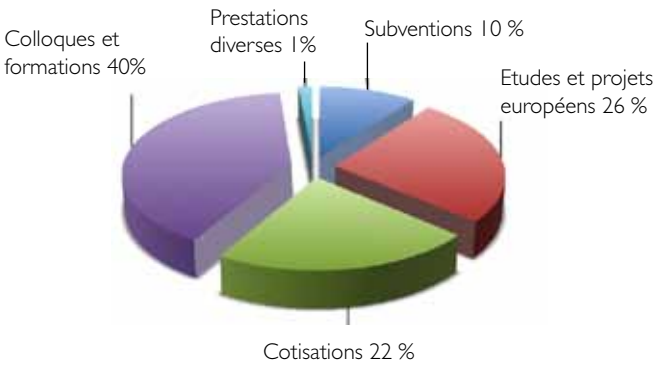
Le HCFDC reste structuré dans un ensemble à caractère non lucratif, composé de l'association loi 1901 et d'une EURL détenue à 100 % par l'association conformément aux recommandations de l'instruction 4H-5-06 du 18 décembre 2006 (Ministère des Finances).

Produit d'exploitation consolidé : 1 358 585 €

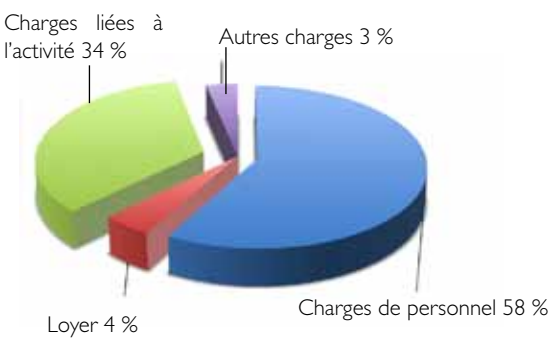
Evolution de la structure (€ d'activités)



Recettes HCFDC / HCFDC Services consolidées année 2011



Dépenses HCFDC / HCFDC Services consolidées année 2011



30 ANS

Trente témoignages de nos membres

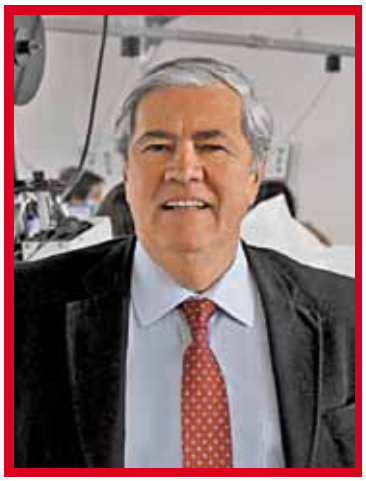
Alain BELLAICHE

Directeur pôle sécurité et continuité d'activité
Crédit Agricole SA
Collège des opérateurs d'infrastructures critiques

«Le Haut Comité Français pour la Défense Civile est une organisation qui a sa place dans le dispositif global qui concourt à la sécurité nationale. Ses formations sont utiles et de qualité, ses petits déjeuners permettent de rencontrer des intervenants de haut niveau et d'échanger en toute convivialité. Ses publications sont généralement pertinentes et au fil de l'actualité. Enfin, j'ai pu apprécier sa capacité d'intervention intra-entreprise dédiée à la gestion de crise.

Si je devais exprimer un vœu, c'est celui d'une plus grande implication de ses membres, notamment les opérateurs d'importance vitale, pour un partage d'expériences plus actif.»

Jacques BOYÉ



Président Directeur Général
Paul Boyé Technologies
Collège des entreprises de défense et de sécurité

«Pour une entreprise comme Paul Boyé Technologies, le Haut Comité apporte la vision transverse des risques et menaces et une approche globale à 360 degrés de notre environnement. Que ce soit en termes de politique, de stratégie des acteurs publics et privés, ou au niveau d'un benchmark européen voire international, les échanges : petits-déjeuners, colloques, émissions vidéo (très pratique pour les provinciaux) permettent une réelle appréciation des enjeux. Dans un environnement où l'industrie consacre maintenant une grande part de ses ressources à l'international, il est important qu'une structure comme le HCFDC fasse le lien sur les thématiques environnants nos métiers, notamment la relation avec les pouvoirs publics, et garde une dynamique sur notre marché national, c'est aujourd'hui essentiel.»

Francis BRUCKMANN

Directeur délégué à la promotion de la sécurité
Orange
Collège des opérateurs d'infrastructures critiques

«Voilà plus d'une douzaine d'années que je fréquente le Haut Comité et son équipe, ses membres, encore peu nombreux à l'époque en ce qui concerne les grandes entreprises qu'on appelle aujourd'hui les «Opérateurs d'Infrastructure Vitale». J'y ai pris de temps en temps la parole lors de colloques techniques, pour apporter ma contribution sur le vaste sujet des (télé)communications : résilience des réseaux (à l'époque, ça ne s'appelait pas encore comme ça), moyens de crise et dualité militaro-civile, alerte à la population, sécurité des technologies de voix sur IP, etc.

Au fur et à mesure du temps, le Haut comité a su dépoussiérer le concept de Défense Civile, en l'adaptant à l'évolution de notre société et à ses nouveaux concepts de continuité d'activité, interdépendance des infrastructures, dialogue constructif entre public et secteur privé.

Centré initialement sur l'organisation de colloques et de petits déjeuners, il a aussi su se recréer en profitant de l'arrivée des Nouvelles Technologies de l'Information et de la Communication, et redynamiser son auditoire grâce à internet : site web, talks vidéo, publi-reportages, lettre de la défense civile (un modèle du genre). Longue vie au Haut Comité !»

Professeur Pierre CARLI

Chef de service
SAMU de Paris – SMUR Necker
Collège des experts

«Au cours de ces dernières années, j'ai eu la possibilité de participer régulièrement aux activités du HCFDC en tant qu'expert médical SAMU-SMUR dans le domaine des risques et des crises sanitaires. Ces interventions m'ont permis d'apprécier la plateforme d'échange exceptionnelle que constitue ce haut comité. Il y a peu de lieu où le concept d'analyse et de gestion globale peut être mis en pratique.

Les crises sanitaires traversées par notre pays comme la canicule ou celles vécues récemment par d'autres pays comme le Japon, ont montré que l'approche technique devait s'intégrer dans une dimension sociétale et même politique. La planification doit répondre à la même transversalité. En mettant au contact les experts français des différents domaines impliqués qu'ils soient issus du public ou du privé, le HCFDC permet une approche décloisonnée aussi bien pour l'analyse des risques que la gestion de la crise et la résilience.»

Didier CHAMPION

Directeur de la crise
Institut de Radioprotection et de Sûreté Nucléaire
Collège des associations et des institutions

«2011, année du 25ème anniversaire de la catastrophe de Tchernobyl, pouvait laisser croire qu'avec le temps, le risque nucléaire était sous parfaite maîtrise dans le monde entier. La catastrophe de Fukushima, en mars 2011, est malheureusement venue nous rappeler que la vigilance s'imposait toujours dans ce domaine. Elle montre également que le risque est multiforme : ici, ce n'est pas tant les morts ou blessés provoqués par l'accident qui marquent les esprits, mais plutôt la rupture brutale et durable qu'il a entraîné pour des dizaines de milliers de personnes qui vivaient dans des territoires désormais contaminés par des retombées radioactives. Je tiens à saluer l'action du Haut comité français pour la défense civile qui offre un cadre propice à un échange et une réflexion collective sur la manière de faire face à de tels événements exceptionnels.»

Thierry COMBASTEIL

Responsable du pôle sûreté, alerte et gestion de crises
VEOLIA Eau
Collège des opérateurs d'infrastructures critiques

«Le Haut Comité Français pour la Défense Civile soutient les actions qui concourent à la Sécurité Nationale. C'est en fait un relais entre la société civile et l'Etat sur les questions de Sécurité Nationale. En tant qu'opérateur d'importance vitale du secteur de l'Eau, Veolia Eau adhère pleinement à la démarche du HCFDC. C'est ainsi que des collaborateurs de Veolia Eau participent aux programmes de formations du HCFDC, que ce soit pour des formations thématiques courtes mais aussi pour des sessions plus longues du type «session nationale résilience et sécurité sociétales». Les petits-déjeuners rencontres permettent régulièrement d'échanger sur des sujets variés, traités le plus souvent par des représentants publics de premier plan. Enfin la lettre de la défense civile permet de rester «au contact» des informations diverses liées aux thématiques de la Sécurité Nationale. Pour toutes ces raisons, le HCFDC est un partenaire très utile qui favorise une approche globale des sujets liés à la Résilience et à la Sécurité Sociétale»

Patrice DALLEM

Directeur de l'urgence et du secourisme
Croix-Rouge française
Collège des experts

«Il y a trente et un ans, nous nous demandions ce qui pouvait bien nous manquer pour être vraiment heureux... Un enfant bien sûr ! Sur les fonts baptismaux il fût appelé HCFDC... Après une enfance sans histoire, notre HCFDC se sera affirmé comme un adulte accompli, jovial mais au caractère trempé.

Comment se passer de lui aujourd'hui, il dort peu, est curieux, réactif, s'agite constamment, bouillonne et partage avec ses camarades et autres relations qu'il a le désir de tisser, sa passion pour la sûreté et la sécurité globales.

Il est partout, certains le lui reprochent, d'autres l'entourent et l'encouragent dans ses entreprises, et elles sont nombreuses : petits-déjeuners pour les gourmands, dîners pour les gourmets, talk-shows, films et reportages pour les fans, colloques pour les bavards, sessions de formation pour les nostalgiques de Jules Ferry, etc.

Où va ce jeune pressé, travailleur acharné, dynamique, à la fois robuste et fragile, qui ne prend jamais de vacances et qui semble toujours avoir perdu son portefeuille avec son argent à l'intérieur ? Jusqu'à un âge avancé, j'espère...»

Alain DE CHANTÉRAC

Conseiller zonal de défense et de sécurité
Agence Régionale de Santé Rhône-Alpes
Collège des associations et des institutions

«Depuis sa création, dans tous les secteurs de la défense et, aujourd'hui, de la sécurité nationale, le HCFDC répond à la nécessité d'une appropriation, par la société civile, des réponses aux enjeux de la sécurité globale que décrit le Livre Blanc (2008).
Par exemple, dès lors qu'une menace, quelque soit sa nature ou son origine (naturelle, malveillante, technologique, sociétale...), pèse sur la santé humaine, la sécurité sanitaire est étroitement interdépendante avec les autres volets de la sécurité (publique, économique, civile). Elle les accompagne à tous les stades de la réponse (veille, surveillance, alerte, intervention), suit des principes identiques (défense en profondeur, résilience, précaution, prévention..) et n'échappe pas aux choix que ses moyens ou l'urgence lui imposent (bénéfice/risque).

A la hauteur de ces enjeux, les réponses ne peuvent plus être seulement «multidisciplinaires», mais bien «interdisciplinaires» et donc «interministérielles».

Le HCFDC stimule la réflexion sur notre système de défense et de sécurité, dans toutes ses composantes (organisation, personnels, équipements, formations et entraînements) et à tous les échelons (national, zonal et départemental). Il constitue un «think tank» dans lequel chacun peut apporter et partager des expériences, grâce à des outils performants (talk show, newsletters...) dont seuls une exploitation et un suivi rationnalisés apporteront les fruits d'une amélioration continue.»

Arnaud DE LA LANCE

Chef du bureau des questions interministérielles et de sécurité
Direction Générale pour l'Armement, Ministère de la Défense
Collège des associations et des institutions

«Les thématiques de la sécurité concernent la direction générale de l'armement (DGA) sur de nombreux points : la lutte contre le terrorisme, la sécurisation de sites et des grands évènements, la gestion des catastrophes naturelles, industrielles ou provoquées, la protection des personnels, etc. La DGA est membre adhérent du HCFDC depuis plusieurs années et met à profit les évènements qu'il organise, ainsi que le réseau ainsi créé des acteurs industriels, publics et privés du secteur de la sécurité, aux niveaux national et des collectivités locales. Le partage des problématiques (analyse des risques, recherche et innovation technologiques) et le développement de synergies entre les parties prenantes, qu'anime le HCFDC, est un atout essentiel pour le développement de ce domaine.»

Jean DE LA RICHERIE

Directeur grands comptes sécurité
CASSIDIAN
Collège des entreprises de défense et de sécurité

«EADS, et plus particulièrement sa filiale CASSIDIAN sont partenaires depuis plus de 13 ans du HCFDC et nous en sommes fiers.
Si ce partenariat dure depuis si longtemps ce n'est pas sans raison. En effet, nous suivons de près depuis le début des années 2000 les nombreuses et riches initiatives du HCFDC qui a toujours su avancer au gré des évolutions de la société, et se remettre en cause pour rebondir et trouver des approches innovantes et pédagogiques pour sensibiliser l'Etat, les collectivités territoriales, les acteurs du secours voire même les industriels sur tous les risques auxquels notre société doit faire face.
Je prendrai pour exemples les nombreux et passionnants petits-déjeuners débats au Sénat, ainsi que les colloques, les Talk Vidéo aujourd'hui, mais surtout le Rapport annuel qui propose des réflexions et actions concrètes et ainsi être force de propositions et de veille permanente pour toujours mieux réagir face aux risques nouveaux de toutes natures...
Enfin, je voudrais signaler le plaisir réel que Cassidian a eu d'être le sponsor et le partenaire privilégié du lancement de l'excellente initiative qu'a été la Session nationale sur le thème «Résilience et sécurité sociétales». Cette session d'un nouveau genre est un vrai succès et un révélateur de la qualité des formations assurées par le HCFDC car elle occupe un créneau qui était jusqu'alors trop délaissé.
Après ces quelques mots je ne peux que souhaiter longue vie au HCFDC en espérant que l'Etat saura un jour reconnaître réellement le rôle et la contribution que le HCFDC a joué pour la protection de la population.»

Yvan DE MESMAEKER

Secrétaire général
European Corporate Security Association
Collège des associations et des institutions

«La European Corporate Security Association, ECSA réunit les directeurs de sécurité des institutions européennes et internationales et des grandes entreprises actives en Europe. Dans ce cadre nous avons le plaisir d'entretenir avec le Haut Comité Français pour la Défense Civile une coopération efficace, constructive et conviviale.
Sous la direction de son délégué général Christian Sommade, le Haut Comité est devenu une organisation des plus innovative et dynamique qui offre un cadre propice à l'échange d'expertises et d'expériences et qui utilise à fond les nouvelles technologies pour communiquer et former.
L'ECSA souhaite un bon anniversaire au HCFDC et se réjouit de poursuivre et même d'intensifier nos excellentes relations.»

Bernard DIDIER

Directeur Général Adjoint
Directeur Technique et de la Stratégie
Morpho (Groupe Safran)
Collège des entreprises de défense et de sécurité

«J'ai eu le plaisir d'assister régulièrement aux petits déjeuners organisés par le HCFDC, au Sénat. C'est avec grand intérêt que je prends part à ces événements qui sont pour moi des moments d'échanges et d'information privilégiés, grâce à d'excellentes interventions portant le plus souvent sur des sujets d'actualité. Si je ne devais retenir que deux mots des petits-déjeuners du Haut Comité, ils seraient sans aucun doute «qualité» et «convivialité». Le HCFDC est, à mon sens, un acteur majeur dans le monde de la sécurité entre l'Etat, l'industrie et, plus généralement, les acteurs économiques.»

Charles FABRE

Maire
Ville de Tarascon
Vice-Président de la Communauté d'Agglomération Arles Crau Camargue Montagnette
Collège des élus et collectivités territoriales

«La gestion des risques au sein de ma collectivité est une priorité dans mon engagement politique auprès de mes concitoyens et ce depuis ma prise de fonction en qualité de maire.

La plus grande responsabilité d'un maire et de se voir confier de par la loi la sécurité des personnes et des biens. Les travaux que nous menons avec le conseil municipal et les services municipaux s'inscrivent dès lors dans une approche globale des risques et une culture du risque éprouvées par notre investissement mais aussi par les crises récurrentes que nous devons gérer.

Ainsi, pour la troisième année nous avons reçu par le HCFDC le Pavillon Orange, qui au-delà de reconnaître le travail réalisé nous inscrit dans une démarche d'amélioration continue de notre organisation.»

Colonel Eric FAURE

Président
Fédération Nationale des Sapeurs-Pompiers de France
Collège des associations et des institutions

«Félicitations ! En 30 ans, le Haut comité est devenu un contributeur important dans la réflexion, l'information et la formation à la défense civile, fidèle à l'esprit de son fondateur Maurice Schumann. Jouant eux-mêmes un rôle essentiel dans la sécurité nationale, les sapeurs-pompiers de France ont à cœur de participer à ses multiples manifestations et de toujours renforcer les liens entre leur Fédération et le Haut comité.

Je saluerais particulièrement l'une de ses formations phares, à laquelle les sapeurs-pompiers apportent leur expertise : la session nationale «Résilience et sécurité sociétales», ainsi que ses initiatives - Pavillon Orange, Trophées de la résilience sociétale - qui récompensent tant les acteurs de terrain que les collectivités et les partenaires de la sécurité civile, mobilisés dans l'intérêt de la population.
J'invite enfin les services départementaux d'incendie et de secours à se joindre aux activités du Haut comité, riches par la pluralité et la diversité de ses participants, car c'est notamment par les échanges et la valorisation des actions qu'ensemble, nous faisons progresser la protection de nos concitoyens face aux crises.»

Franck GALLAND

Directeur général
Environmental Emergency & Security Services
Conseiller spécial du HCFDC pour le développement international

«Le Haut Comité est un carrefour exceptionnel d'échange de savoir-faire et de bonnes pratiques en matière de continuité d'activité et de gestion des crises hors cadre. Le dynamisme et le professionnalisme de ses équipes en ont fait un lieu unique de retour d'expérience pour les groupes industriels et les opérateurs d'infrastructures critiques de l'espace euro-méditerranéen. Charge à nous de conserver son positionnement d'excellence et de continuer à diffuser ce qui fait la raison d'être du HCFDC : accroître les capacités de résilience de nos sociétés face aux risques majeurs.»

Jean-Paul GEROUARD

Coordonnateur des mesures de défense et sécurité civile
France Télévisions
Collège des opérateurs d'infrastructures critiques

«Pertinent et moderne : le HCFDC est un très bel exemple de think-tank nourrissant et utile. La sécurité civile, la résilience, la continuité d'activité sont des sujets mouvants et évolutifs. Une mise à jour permanente est nécessaire. Le «Haut Comité» est le forum de référence sur l'analyse des risques, les avis d'experts, et les échanges de bonnes pratiques. La marque du HCFDC, c'est sa capacité à produire de vrais débats de fond, tout en restant extrêmement réactif sur les «actualités» du secteur. Cela se manifeste notamment par une utilisation habile des nouvelles technologies. Le site web est riche, et vivant. Personnellement, je me branche souvent sur les «talks vidéos» , excellent moyen pour être «brieffé» avec les meilleurs experts, sans quitter son bureau… Le HCFDC est l'endroit où l'on pose les bonnes questions au bon moment.»

Général Gilles GLIN

Commandant
Brigade de Sapeurs-Pompiers de Paris
Collège des associations et des institutions

«La brigade de sapeurs-pompiers de Paris (BSPP), unité militaire mise pour emploi à la disposition du préfet de police et plus importante structure de secours d'urgence en Europe, doit savoir anticiper les évolutions de ses missions de plus en plus nombreuses et de son environnement opérationnel de plus en plus complexe.

La population défendue, 10% de la population française, n'admettrait pas que la BSPP soit surprise et inopérante, y compris face à des évènements exceptionnels. Le HCFDC, de par la pertinence des thèmes abordés et la qualité de traitement de ceux-ci, est à même de facilité cette anticipation vitale pour notre Institution, aujourd'hui bicentenaire.»

Camille GRAND

Directeur
Fondation pour la Recherche Stratégique
Collège des associations et des institutions

«Le Haut Comité Français pour la Défense Civile s'est imposé au cours des trois dernières décennies comme un acteur majeur du débat national sur les questions de sécurité. A la croisée des mondes politique et académique et à la rencontre permanente des praticiens de la sécurité, il combine les exigences de ces milieux différents par ses actions de formation et son engagement dans le débat public. Le HCFDC a, notamment depuis le 11 septembre 2001, joué un rôle essentiel dans la meilleure prise en compte de la prévention du terrorisme et des catastrophes majeures, naturelles ou industrielles. Il a ainsi pris toute sa part dans la réflexion sur l'évolution de la défense civile et l'émergence en France du concept de résilience. Il s'agit pour la Fondation pour la recherche stratégique d'un partenaire de premier rang avec lequel nous sommes heureux de coopérer régulièrement.»

Bernard HODAC

Président directeur général
OSMOS
Président du SYNNOV, Syndicat de l'Innovation Technologique
Collège des entreprises de défense et de sécurité

«La prévision de la menace est encore peu codifiée dans la définition des risques liés aux infrastructures. Comme s'ils se suffisaient à eux-mêmes, les modèles théoriques occultent les contextes particuliers, souvent mal appréhendés, associés à leur exploitation. Pionnier de la gestion des risques liés aux ouvrages, OSMOS agit comme une entreprise consciente que la technologie qu'elle a développée possède aussi, par sa nature même, un caractère d'utilité publique.

La reconnaissance des besoins des opérateurs, des gestionnaires et des usagers nécessite d'élaborer sans délai des politiques qui seront compréhensibles, abordables et acceptables à tous les niveaux de l'exploitation des ouvrages. Pour nous, le HCFDC alimente de façon exemplaire ces champs de réflexion grâce aux savoirs partagés et à l'approche pluri-disciplinaire de ses membres. Le HCFDC est un organe précieux et nous sommes particulièrement heureux de bénéficier du point de vue original et unique qu'il permet d'acquérir et de contribuer, à notre niveau, au décloisonnement des compétences qu'il favorise.»

Christian KERT

Député des Bouches du Rhône
Assemblée Nationale
Président du **Conseil d'Orientation pour la Prévention des Risques Naturels Majeurs (COPRNM)**
Président de l'**Association Française pour la Prévention des Catastrophes Naturelles (AFPCN)**
Collège des élus et des collectivités territoriales

«Si la prise de conscience des politiques sur la problématique des risques et de leur prévention est récente elle n'en est pas moins devenue aujourd'hui, compte tenu de la succession d'évènements extrêmes, l'une de leurs priorités. Cette politique de prévention pour être efficace, doit associer de nombreux intervenants que sont bien évidemment les politiques mais aussi les autorités publiques et les représentants de ce que l'on nomme de façon un peu générique la «société civile». C'est ici que le rôle du HCFDC joue pleinement : être un relais mais aussi un «anticipateur» sur la prévention et la gestion des crises. La fragilité de nos territoires impose d'évaluer en permanence le risque dans son intensité. La qualité d'expertise du HCFDC répond à cette responsabilité essentielle. Je suis heureux d'en être l'un des acteurs.»

Patrick LAGADEC

Directeur de Recherche
Ecole Polytechnique
Collège des experts

«Dans son ouvrage, The Age of the Unthinkable, Joshua Cooper Ramo (Kissinger Associates), souligne que si Kissinger et sa génération ont eu à traiter la dissuasion, il nous revient désormais de traiter la résilience. La capacité de nos sociétés à naviguer sans se déliter dans des univers de plus en plus marqués par la surprise, la volatilité, la vulnérabilité sur des fronts mutants, le facteur granulaire. Ce tableau exige des dynamiques de questionnement, des échanges multiformes, des anticipations non conventionnelles, des préparations à la surprise, des réactivités rapides. En d'autres termes, moins des donjons préparant des plans à partir de tableaux de données stabilisés que des dynamiques d'échanges et d'invention multi-acteurs en temps réel. Le Haut Comité est de ces terrains et terreaux où s'inventent et s'expérimentent ces nouvelles aptitudes et ressorts collectifs. Un foisonnement d'échanges et d'activités qui jouent dans le même registre que les enjeux d'aujourd'hui. Et c'est bien cela l'essentiel si l'on ne veut pas subir d'Etranges Défaites.»

Jean-Marie LE GUEN

Député de Paris
Assemblée Nationale
Collège des élus et des collectivités territoriales

«Je suis très honoré de participer aux travaux du Haut comité français pour la défense civile (HCFDC). Son approche du renouvellement des politiques publiques et de l'adaptation aux nouveaux risques est l'une des plus intéressantes qui soit en France.

Je me félicite de sa capacité à être à la veille des nouvelles formes de réponse de l'action publique pour garantir la sécurité nationale et de sa recherche permanente de la transversalité dans la vision qu'il développe. La réflexion et le travail menés par le HCFDC sont essentiels pour la modernisation de la gestion des risques et des situations d'urgence dans notre pays.»

Laurent MONTADOR

Directeur Dpt catastrophes naturelles & fonds publics
Caisse Centrale de Réassurance
Collège des entreprises industrielles et de services

«Par l'organisation de colloques, déjeuners-débats, formations ou par la publication de «position papers» et dossiers spéciaux, le Haut Comité est devenu un interlocuteur privilégié de CCR - entreprise de réassurance appartenant à l'Etat - non seulement dans les domaines concernant la sécurité nationale pour la réassurance avec garantie d'Etat du risque «terrorisme», mais aussi sur les questions de résilience et gestion de crise face aux risques de nature exceptionnelle, comme les Catastrophes Naturelles par exemple, qui est le domaine historique d'intervention de CCR.
Cet acteur unique de la société civile qu'est le HCFDC a une véritable utilité publique en étant ce catalyseur d'échanges entre acteurs aussi différents.»

Laurent OLMEDO

Chef de projet recherches en sécurité globale
Commissariat à l'Energie Atomique, Direction des Applications Militaires
Collège des Associations et des institutions

«Acteur majeur de la recherche en sécurité globale, le CEA est depuis de nombreuses années, un partenaire fidèle du HCFDC. Instance de réflexion, de débats et de formation, le HCFDC est une structure originale dans sa capacité à fédérer les compétences nationales en rassemblant acteurs institutionnels, opérateurs et industriels. Sa visibilité dépasse aujourd'hui largement le périmètre national par ses nombreux contacts tant en Europe que dans les principaux pays impliqués dans les questions de sécurité sociétale.

Fort de son expertise scientifique et technique dans le domaine NRBC-E, le CEA lui apporte un soutien actif dans l'organisation des évènements en relation avec cette thématique. L'innovation est également une préoccupation forte du HCFDC, comme en témoignent les trois éditions des Trophées de la résilience sociétale auxquelles le CEA a concouru et gagné deux trophées dans le domaine de la recherche technologique.

Au plan de la formation, la session nationale «résilience et sécurité sociétale», que le CEA sponsorise, dispense un enseignement de qualité et de haut niveau dans le domaine de la sécurité et a su acquérir une place spécifique dans le paysage national.

Gageons que les 30 prochaines années verront le HCFDC poursuivre et accroître son travail d'utilité publique au profit de la collectivité et du citoyen.»

Richard OLSZEWSKI

Conseiller délégué chargé des risques
Communauté Urbaine Lille Métropole
Collège des élus et des collectivités territoriales

«Le HCFDC, tout le monde en parle, mais encore trop peu de personnes l'ont vraiment rencontré, c'est dire si son influence est plus que conséquente.
En effet, par son activité le HCFDC rayonne dans les débats nationaux et même internationaux. Loin des tabous, des doctrines stériles et des protectionnismes obsolètes, ses réflexions innovantes commencent à porter leurs fruits. Que ce soit à travers ses écrits, ses conférences, ses formations, il est devenu un des «think tanks» les plus écoutés dans le domaine de la sécurité globale.

Champions de l'efficience, les collaborateurs du HCFDC passent sans cesse du savoir-faire au faire savoir, s'appuyant sur site internet qui est devenu un véritable outil de référence.

Je souhaite que pour la prochaine décennie, nous ayons enfin la reconnaissance de toutes les autorités régaliennes qui commencent enfin à accepter ce partenariat indispensable à notre objectif final : la mise en place de la résilience territoriale.»

Bernard OUILLON

Chef de Mission Sécurité-Confidentialité
RTE
Collège des opérateurs d'infrastructures critiques

«Auditeur de l'INHESJ, Officier de Sécurité pour RTE des infrastructures critiques en relation avec les ministères concernés, après un parcours professionnel principalement orienté vers le management opérationnel dans le domaine de l'Energie, c'est avec plaisir que j'ai pris contact avec le HCFDC.

J'assure la continuité d'une collaboration commune de plusieurs années avec le HCFDC comme nouveau membre actif du collège des opérateurs d'infrastructures critiques.

Les dimensions d'informations et de débats sous forme de petits déjeuners ou de Talk-videos, permettent de prendre en compte les dimensions de partage, d'échange et de progrès sur l'événementiel dans le domaine de la sécurité sociétale. Les échanges favorisent l'écoute et la prise en compte des besoins des opérateurs par l'Etat.
Cette dynamique associée à des formations centrées sur la sécurité nationale me permet ainsi de pouvoir développer rapidement une approche des différents dossiers d'actualités.»

Anne-Laure PROUX

Conseiller Plan Communal de Sauvegarde
Association des Maires de Vendée
Collège des Associations et des institutions

«Chargée de mission à l'Association des Maires de Vendée pour accompagner les communes de Vendée à élaborer leur Plan Communal de Sauvegarde, l'adhésion au HCFDC a permis de lier des contacts avec des professionnels de la gestion de crise qui ont connaissance des enjeux des collectivités. Le blog PCS et résilience ainsi que le Pavillon Orange permettent également de promouvoir les PCS auprès des communes. Par ailleurs vous pourriez développer une labellisation adaptée pour les communes de moins de 1000 habitants qui ont mis en œuvre leur PCS avec des moyens moins importants.»

Didier SCHWARTZ

Directeur de la sûreté
SNCF
Collège des opérateurs d'infrastructures critiques

«L'expérience et le rayonnement du HCFDC constituent un atout majeur.
SNCF, de par son implication dans la vie économique du pays, est intégrée dans des démarches sûreté à tous les niveaux institutionnels. Attachée au travail en réseau, SNCF anticipe en restant acteur des réflexions et de l'élaboration des normes. Elle est attentive et se met en capacité d'écoute tout en offrant son expérience d'opérateur national.

La qualité des rencontres et la pertinence des thèmes traités par le HCFDC permettent d'avoir un suivi sur des sujets majeurs, d'échanger et de partager entre partenaires.»

Catherine TROENDLÉ

Sénatrice du Haut-Rhin
Sénat
Collège des élus et des collectivités territoriales

«Membre du HCFDC depuis 2007, j'ai trouvé auprès de cette instance un interlocuteur privilégié dans mes recherches annuelles lors de l'élaboration de mon rapport pour avis budgétaire. Les colloques et séminaires sont d'une grande qualité, d'une grande technicité.

Les collaborateurs sont eux recrutés sur des compétences pointues et leurs interventions d'une grande efficacité.

La Sécurité civile mériterait d'être davantage valorisée au niveau national ; grâce à l'implication telle que celle du HCFDC, la Sécurité civile est expertisée. Les rapports permettent d'y puiser de précieux conseils pour une évolution toujours plus performante de la Sécurité civile.»

Charles YVINEC

Directeur de la sûreté
Air France
Collège des opérateurs d'infrastructures critiques

«Air France a choisi d'être membre du Haut Comité Français pour la Défense Civile parce que cette association est devenue un contributeur incontournable dans le domaine de la sécurité. Le Haut Comité est en effet un lieu exceptionnel de rencontre entre Etat, Collectivités locales et entreprises privées et il complète en ce sens parfaitement l'action d'autres associations telles que le Club des Directeurs de l'Entreprise, plus centrées sur la seule problématique «privée». Les travaux, les formations de grande qualité dispensées par le HCFDC, notamment dans le domaine de la gestion de crise, présente un intérêt évident pour une entreprise de transport aérien, confrontée presque quotidiennement en raison de son réseau mondial, à des évènements susceptibles d'impacter son activité.»

L'équipe de permanents du HCFDC et HCFDC Services

au 1er Juin 2012

L'équipe de permanents du HCFDC et HCFDC Services au 1er Juin 2012

Christian Sommade
Délégué Général
christian.sommade@hcfdc.org
Lauriane Abriat
Adjointe au délégué général, chargée des relations membres et institutionnelles
Didier Cuisset
Chargé de mission Gestion-Administration-Comptabilité

PÔLE ÉVÈNEMENTS ET COMMUNICATION (par ordre alphabétique)

Christophe Boucher
Journaliste, responsable des publications
François Deschamps
Concepteur-Réalisateur multimedia
Gaëtan Gauthier
Graphiste
Mathilde Le Clainche
Chargée de mission Communication-Evénements
Claire Sabatier (Stagiaire)
Chargée de mission Communication-Evénements, en charge du Rapport annuel
Didier Saillant
Chargé de mission Audiovisuel

PÔLE FORMATIONS ET ÉTUDES (par ordre alphabétique)

Maïté Merlot
Chargée de mission Formations
Léo Muller
Chargé de mission Etudes
Martin Ryan (Stagiaire)
Assistant mission Formations
Véronique Vatan
Assistante, chargée de mission sur les sessions nationales et zonales

L'équipe de permanents du HCFDC et HCFDC Services au 1er Juin 2012

L'équipe du HCFDC en 2011 en stage chez notre partenaire Pegasus leadership

Notes

HAUT COMITÉ FRANÇAIS POUR LA DÉFENSE CIVILE
59, rue Galilée - 75008 Paris - France
Tél : +33 (0)1 49 52 94 28
Fax : +33 (0)1 47 20 75 27
www.hcfdc.org - contact@hcfdc.org