Rapport

Défense civile

2008

Constats et propositions pour une vision globale de la sécurité

Haut Comité Français pour la Défense Civile

Protéger l'avenir...

Actualisation du Livre Blanc HCFDC 2003

HAUT COMITÉ FRANÇAIS
POUR LA DÉFENSE CIVILE

Rapport Défense civile

2008

Constats et propositions pour une vision globale de la sécurité

Actualisation du Livre blanc HCFDC 2003

SOMMAIRE

Avant-propos

En 2003, à l'occasion de ses vingt ans d'existence, le Haut comité français pour la défense civile publiait un Livre blanc intitulé "*20 constats et 20 propositions pour la défense civile".*

Aujourd'hui, deux raisons principales poussent à remettre l'ouvrage sur le métier. D'une part, de nouvelles menaces et de nouveaux risques systémiques sont apparus. D'autre part, la France a entrepris de nombreuses actions depuis 5 ans et réexamine actuellement en profondeur la pertinence de son dispositif de défense et de sécurité au travers d'un Livre blanc qui, suivant la volonté du nouveau Président de la République, considère enfin la dimension globale de la sécurité collective de notre pays.

Près de 50 ans se sont écoulés depuis la création de notre concept de défense fondé sur les ordonnances de 1959 portant organisation générale de la défense. Cinquante années structurées autour d'une défense nationale forte, théoriquement basée sur un équilibre entre la dissuasion nucléaire et les autres formes de défense : militaire, civile et économique. Cependant, la mise en œuvre de ces dernières n'a pas toujours été à la hauteur d'un concept parfaitement bien écrit et équilibré, très en avance sur son temps. En particulier, comme l'a souvent souligné Maurice Schumann cofondateur du HCFDC, la défense civile a longtemps été sacrifiée en raison d'une doctrine prioritairement tournée vers l'armement nucléaire. Par la

suite, elle est devenue le parent pauvre budgétaire des grandes orientations de défense et de sécurité.

Il aura de même fallu attendre sept ans pour que la France tire pleinement les enseignements des attentats du 11 septembre 2001 et réexamine son dispositif de défense et de sécurité.

Il est donc logique que le Haut comité français pour la défense civile apporte aujourd'hui sa pierre à l'édifice au travers d'un rapport 2008 fondé sur une méthodologie de travail citoyenne, dont le résultat est le fruit des travaux de nombreux membres du HCFDC venus de tous horizons professionnels et le plus souvent experts des domaines traités.

Ce travail, nous l'espérons, servira non seulement à la commission du Livre blanc Défense et Sécurité sous la présidence de M. Jean-Claude Mallet, mais également à Mme Alliot-Marie, ministre de l'Intérieur, qui a annoncé la rédaction d'un Livre blanc sur la protection civile, prélude à une loi de programmation sur le sujet.

Introduction

CONSTATS, PROBLÉMATIQUE ET PROPOSITIONS

1 - Un constat partagé sur la défense militaire

• Des forces armées en perpétuelle adaptation depuis les années 1990. Le passage d'une armée de conscription, prête à affronter l'ennemi en centre Europe, à une armée de projection prête à défendre les intérêts de notre pays en Afrique, au Moyen-Orient, et parfois sur les autres continents, en recherchant le soutien de la communauté internationale.

• Une dissuasion nucléaire permanente qui assure à la France un rang de puissance nucléaire totalement indépendante, la seule en Europe.

• Un outil industriel de défense qui a suivi avec lenteur les modifications du contexte stratégique, devenant de ce fait surdimensionné. Aujourd'hui le secteur privé de la défense doit aller chercher sa survie et sa croissance à l'exportation.

• Une DGA, fleuron technique reconnu, mais encore bien lourde ; des programmes majeurs qui coûtent trop cher au pays, qui ne peut plus se payer, seul, ces programmes tant actuels que futurs.

• Une vision de défense européenne souhaitée mais trop lente à prendre pied et qui achoppe sur la réalité politique de l'Europe d'aujourd'hui.

• De nombreux engagements et des lois de programmation militaire rarement achevées (sauf la dernière), associés à un saupoudrage des crédits ont conduit à une disponibilité technique des matériels qui n'est pas à la hauteur de ce que les militaires et leurs concitoyens sont en droit d'attendre de leur armée.

• Sur le plan national, une vision de la défense non-militaire quasi inexistante et quelque peu archaïque jusqu'à l'avènement du terrorisme de masse en 2001.

2 - Élargir le concept de sécurité intérieure

La sécurité intérieure, concept apparu au début des années 1990, a été jusqu'à aujourd'hui orientée sur la problématique rémanente de l'ordre public, du terrorisme politique et/ou séparatiste, et de la menace que représente le crime organisé, le champ de la défense civile et économique étant quasiment absent.

Le ministère de l'Intérieur a traditionnellement porté son action et ses crédits sur les problématiques policières, focalisant son action « secondaire » de défense et de sécurité civiles sur la réorganisation des services de secours (principalement à la charge des collectivités) et sur le maintien d'une capacité nationale d'intervention minimum face aux catastrophes, particulièrement sur la lutte contre les feux de forêt. Or on constate une difficulté permanente d'adaptation et d'anticipation face aux nouvelles menaces : la loi de modernisation de la sécurité civile de 2004 n'indique que dans ses annexes, sous forme d'orientations (acte révélateur), les principaux aspects « novateurs » concernant la protection des populations. Le ministère de l'Économie et des Finances considérant, lui, ces sujets comme secondaires jusqu'à une période récente (2003-2004), y compris celui de l'intelligence économique.

Mais au-delà des ministères de l'Intérieur et des Finances, acteurs clés de la réflexion et de l'action, **un travail important a pourtant été accompli au plan interministériel et ministériel pour mieux préparer le pays aux situations de crise**. Le SGDN et certains

autres ministères comme la Santé, l'Équipement, l'Agriculture ou l'Écologie, ont beaucoup travaillé depuis 2001, parfois sous la pression des règlements internationaux, pour répondre à des problématiques importantes comme la pandémie grippale, la rénovation des plans de défense, ou la sécurité des activités d'importance vitale. Ces actions ont été menées dans un cadre conceptuel et organisationnel paradoxalement structuré, mais qui demeure le plus souvent complexe, sous financé, et finalement peu lisible pour les non-initiés.

Enfin, la population est largement écartée de l'information sur les dangers, sur les comportements à tenir en cas de péril, et surtout peu responsabilisée, l'État et les pouvoirs publics étant là pour assurer la sécurité et la protection de tout un chacun et en toutes circonstances, vœu pieux, posant le problème réel et crucial, si la crise prend le dessus, de la crédibilité des postures gouvernementales.

On constate donc que malgré le travail fourni, souvent de grande qualité, le citoyen voit difficilement les réalisations concrètes faute d'un « pilote dans l'avion », c'est-à-dire d'un responsable politique apte à coordonner l'effort, de crédits clairement à la hauteur des ambitions et d'une communication pertinente sur ces sujets.

3 - La problématique actuelle

La multiplicité et la prégnance des menaces et des risques tels qu'ils sont décrits dans notre premier chapitre, la mondialisation et l'interdépendance de l'économie, l'enjeu d'image lié à la cinétique rapide des crises, font qu'**un pays développé ne peut plus s'offrir le luxe ni économique, ni social, ni politique de l'impréparation aux événements exceptionnels** et du non-renforcement de la sécurité et de la prévention face aux menaces et risques les plus graves.

Or dans cette approche sur la « sécurité globale », notre pays souffre aujourd'hui de maux qui sont à la fois des faiblesses et des forces potentielles, mais qui sont ancrés culturellement au-delà de la difficulté traditionnelle de l'interministérialité ou de la gestion transverse.

• **La culture des gouvernants** français a toujours été caractérisée par un manque de volonté politique d'envisager les situations catastrophiques, au prétexte de ne pas affoler la population. Le moment n'est semble-t-il jamais propice pour l'informer : un événement politique ou social étant toujours là pour empêcher une communication sereine. Cette attitude de défiance déniant tout sens civique au citoyen, entretient la méfiance vis-à-vis des pouvoirs publics, soupçonnés au mieux d'incompétence, au pire de masquer délibérément la réalité. En fait, la vraie solution consiste à faire une communication « administrative » et non politique sur ces sujets.

• **La culture « Défense »** comprend bien les enjeux à long terme, intègre la dominante technologique, a le sens de l'organisation et de la planification qui y est associée, mais a du mal, culturellement, à s'intéresser aux problèmes de protection territoriale, moins "professionnalisant" pour les militaires que le combat haute intensité ou la dissuasion.

• **La culture « Intérieur »** plus axée sur la gestion du quotidien, intègre moins bien la composante technologique, et a du mal à se projeter et à planifier sur des problématiques complexes et le long terme, pensant que l'État, puissant, peut, au moment de l'événement, notamment au travers du corps des préfets, porté par la culture historique de la centralisation et de l'ordre public en France, assumer et gérer tout type de crise, même quand les contraintes budgétaires limitent fortement les ambitions.

• **La culture des « collectivités locales »** qui ne veulent pas assumer les risques majeurs nationaux ou transverses (technologiques, terroristes…) qui doivent, de leur point de vue, rester de la compétence étatique, mais qui, parallèlement, se rendent compte de la demande croissante de leurs administrés pour une « protection » globale.

• **La culture du secteur privé**, pour lequel la contrainte de sécurité doit être justifiée, proportionnée et limitée, surtout en termes de responsabilité civile ou pénale. Les grandes entreprises ont intégré depuis longtemps la maîtrise des risques industriels ou opérationnels mais elles ne prennent pas encore en compte, au niveau adéquat les problématiques de sûreté face au terrorisme et celles de la gestion des crises, même si des progrès importants sont en cours

dans de nombreux secteurs. Les fonctions de sécurité, de gestion de crise et de continuité d'activité sont donc le plus souvent vues sous l'angle de la protection du patrimoine de l'entreprise et de la conformité à des règles internationales ou nationales, plutôt que sous celui de l'entreprise citoyenne et sécuritaire, l'un n'étant d'ailleurs pas exclusif de l'autre.

• **La culture de la « société civile »**, enfin, aujourd'hui tout à la fois individualiste et solidaire, organisée mais très dépendante, voire interdépendante, tant au plan économique que social qui, faute d'avoir été informée et formée à « faire face », s'en remet à l'État dans les situations d'urgence et d'exception. État qui, face aux crises réellement majeures, ne pourrait aujourd'hui prendre en charge les citoyens sans que ceux-ci soient capables d'assurer, eux-mêmes, leur « autoprotection et autogestion », ce qu'ils ne sont pas à ce jour prêts à faire au sens matériel et psychologique.

4 - Nos propositions

Cependant notre pays a les moyens économiques, techniques et humains d'être beaucoup mieux préparé à faire face à des désastres majeurs qu'ils soient d'origine naturelle, terroriste, sanitaire ou technologique, il en a même le devoir.

L'approche proposée par le HCFDC passe par le lancement d'une vraie et claire politique de « défense civile ou sociétale » prise en compte au plus haut niveau de l'État et relayée médiatiquement dans le cadre d'une approche renouvelée de la défense et de la sécurité nationales.

Cette nouvelle politique de « sécurité globale » pourrait s'exprimer à l'occasion de débats autour du Livre blanc sur la sécurité et la défense, sur les réels risques et menaces qui pèsent sur notre pays et sur l'implication nécessaire de toutes les forces de la nation.

Pour lancer cette politique, il faut abolir le travail en « silo » entre les différents piliers administratifs, économiques et citoyens du pays et privilégier la mise en réseau de l'ensemble des acteurs au travers de ce nouveau concept transverse. Dans ce cadre, chacun, pourvu de cette vision globale et cohérente sur les buts recherchés, des responsabilités et des objectifs de sécurité et de protection à

atteindre, pourra apporter sa contribution pour permettre à la nation, dans le cadre européen, de « faire face ».

Le HCFDC propose d'adopter une politique de confiance dans le sens civique des citoyens en diffusant largement l'information élémentaire nécessaire à l'acquisition de réflexes conservatoires.

La politique de transparence vis-à-vis de la population, nécessaire en ce qui concerne les risques naturels ou industriels, ne doit cependant pas conduire à diffuser des informations sensibles susceptibles de faciliter les actions à caractère malveillant ou terroriste. Une attention particulière doit être portée sur ce point capital.

De même, le principe de précaution ne doit pas se réduire à un immobilisme stérile de refus systématique de tout risque, mais plutôt s'appliquer à une évaluation objective des risques induits par de nouvelles activités de manière à en maîtriser les effets de nuisance potentielle ou effective.

Le Haut comité français pour la défense civile a voulu, au travers de ce rapport actualisé et complémentaire de son Livre blanc sur la défense civile de 2003, apporter sa contribution à cette réflexion en cours, en faisant un certain nombre de constats et de propositions concrètes pour la protection de nos populations.

CHAPITRE I

Cadre géostratégique, menaces et risques

LE CADRE GÉOSTRATÉGIQUE

Ces dernières années se caractérisent au plan sécuritaire par l'irruption de ce que l'on a appelé les « nouvelles menaces ». Cette irruption s'est faite dans un contexte géostratégique plus complexe consécutivement à la fin de la guerre froide et à l'essor de la mondialisation et de la technologie.

La décennie qui a suivi la fin de la guerre froide et la chute de l'Union soviétique avait été marquée par le processus de la mondialisation et l'avènement de l'hyperpuissance américaine. Cependant, contrairement aux prédictions de Fukuyama, on n'a pas assisté à la « fin de l'histoire », mais au contraire à plusieurs phénomènes négatifs : conflits consécutifs à la décomposition du communisme (Caucase ; ex-Yougoslavie) ; dégradation de la situation en Afrique avec extension des foyers d'instabilité et apparition d'États « faillis » (Sierra Leone, Liberia, Corne de l'Afrique, etc.) ; forte tension au Proche-Orient (guerre du Golfe ; difficultés du Processus de Paix) ; poursuite et, dans certains cas, aggravation des rivalités et des tensions entre puissances asiatiques (Inde/Pakistan ; Chine/Taiwan ; Chine/Japon).

De nouveaux défis en matière de sécurité sont cependant apparus depuis, tandis que les problématiques classiques sont passées au second plan des préoccupations. Notre monde est en effet apparu soudain fragile et vulnérable non plus seulement en temps de guerre, comme cela avait été le cas dans le passé, mais aussi en temps de paix. Les attentats terroristes du 11 septembre aux États-Unis ont déclenché ce sentiment, renforcé les années suivantes par une série d'événements tels que les mégapannes électriques aux États-Unis, en Italie, en Suisse, l'épidémie de SRAS et l'épizootie de grippe aviaire qui s'ajoutent au Sida, le Tsunami qui a frappé le Sud-Est asiatique ou encore l'ouragan Katrina qui a dévasté la Nouvelle-Orléans. Ainsi, aux « menaces » est venue s'ajouter une série de « risques ».

Pourquoi ce sentiment de vulnérabilité et de fragilité est-il apparu plus intensément aujourd'hui alors que l'humanité a connu dans son histoire de nombreuses calamités comme l'épidémie de grippe espagnole au début du siècle dernier ou, plus récemment, des catastrophes technologiques comme Tchernobyl et Bhopal ?

Plusieurs explications, au demeurant complémentaires, peuvent être avancées. Tout d'abord, la guerre froide a occupé nos esprits pendant des dizaines d'années, occultant par-là même des risques que nous ne percevions que de temps en temps, alors qu'ils étaient pourtant là. Puis, la mondialisation, qui a indubitablement ses aspects positifs, a favorisé en même temps au niveau international des phénomènes négatifs comme la criminalité organisée et le terrorisme.

Nos sociétés modernes, de plus en plus complexes, et donc plus vulnérables, se trouvent en outre dans un état d'interdépendance technologique de plus en plus grand. Cette mondialisation a rendu notre planète plus petite : nous sommes maintenant conscients des catastrophes qui se produisent à l'autre bout du monde et qui, du fait de la mondialisation des échanges, peuvent avoir des conséquences économiques, financières ou de santé publique, en tout lieu et rapidement. La technologie contribue aussi à être un facteur potentiel très aggravant de l'action terroriste.

Par ailleurs, notre environnement est incontestablement en grand danger en raison de l'activité humaine. Enfin, le phénomène de migration de populations pour cause de pauvreté, de guerres ou de désastres environnementaux constitue désormais un vrai problème de sécurité.

Ces préoccupations sont-elles exagérées ? Il faut certes faire la part de l'imaginaire et aussi des intérêts qui ont parfois tendance à exagérer les dangers. Mais, ces réserves étant faites, nos sociétés doivent incontestablement s'armer pour affronter désormais ces menaces et ces risques. Il en sera de plus en plus ainsi dans le monde de demain.

L'actualité et l'acuité des problèmes classiques de sécurité se rappellent cependant en même temps de plus en plus à nous et compliquent en partie notre riposte aux nouvelles menaces. Ainsi en est-il de l'arrêt total du processus de paix et de la détérioration de la situation au Proche-Orient ; des conséquences néfastes des guerres d'Irak et d'Afghanistan ; des nouveaux foyers d'instabilité qui se créent dans le monde et qui constituent autant de niches pour le développement du terrorisme (toujours Afrique de l'Ouest et Corne de l'Afrique, mais aussi Darfour, Indonésie, etc.) ; des risques de prolifération nucléaire, biologique.

L'Europe occidentale est protégée pour l'instant. Les risques de conflits armés y sont pratiquement inexistants. Des tensions sont cependant perceptibles avec la Russie. À terme, l'Europe occidentale pourrait se trouver menacée par certains États du Proche-Orient ou d'Afrique. Si la défense civile doit incontestablement s'armer pour faire face de manière plus efficace aux nouveaux défis qui se présentent, elle ne doit donc pas pour autant faire oublier les problématiques classiques de sécurité internationale qui, un jour ou l'autre, peuvent se rappeler brutalement à nous, Français et Européens. Malgré la faible probabilité actuellement d'un conflit armé mettant en cause directement le territoire national, cette menace ne doit pas être totalement écartée.

La défense civile, prise dans le sens du code de la défense, est, aujourd'hui encore plus qu'hier, une des formes fondamentales de la sécurité de la nation aux côtés de la défense économique et militaire. Il convient de lui donner une vraie réalité, dans une approche

de sécurité globale face à l'ensemble des risques et menaces de toute nature, tant internes qu'externes, qui pèsent sur nos populations, et ce tant dans le cadre français qu'européen.

PRISE EN COMPTE AU NIVEAU EUROPÉEN

La France prend une part active au traitement de ces sujets au niveau international notamment dans le cadre des Nations unies. Mais son horizon premier demeure l'Union européenne, dimension incontournable pour assurer à notre pays une sécurité optimale.

Celle-ci, dont les traités ne prévoyaient pas à l'origine qu'elle était compétente pour s'occuper des questions de sécurité, les a prises en compte de manière progressive et empirique sous la poussée des événements et des contraintes. La tâche est cependant immense. La sécurité dans les transports et l'énergie, domaines intéressant forcément l'ensemble des pays de l'Union, a été le premier domaine dont s'est occupée la Commission européenne.

La nécessité de lutter contre le terrorisme intérieur dans les années 1975 a rapidement imposé ensuite une coordination dans ce domaine. Puis la mise en œuvre des accords de Schengen a poussé la Commission à se préoccuper de la lutte contre l'immigration clandestine et le crime organisé (création d'Europol en 1992 et du SIS -*Schengen information system*; agenda de Tampere en 1999).

Les attentats terroristes de septembre 2001 aux États-Unis puis de 2004 à Madrid et 2005 à Londres ont par ailleurs suscité de nombreuses initiatives et mesures au niveau communautaire (adoption d'une clause de solidarité; nomination d'un coordinateur antiterroriste au sein du Secrétariat du Conseil; mise en place du MIC *Monitoring Information Center*; des systèmes d'alerte rapide en cas de menaces biologiques et radiologiques notamment; création d'Eurojust, de Frontex; adoption du Programme de La Haye pour la période 2005/2011; Plan d'action de la Commission révisé tous les six mois; etc.).

La Commission européenne s'est en outre investie de plus en plus au cours des dernières années, en grande partie pour contrer la menace terroriste, dans la question de la protection des infrastructures critiques (Livre vert sur les infrastructures critiques) et de la

sécurité fonctionnelle de nos sociétés (sécurité des réseaux d'information et des transports d'énergie).

La protection civile, préoccupation présente depuis de nombreuses années à Bruxelles, a pris un peu d'ampleur. Elle est l'objet de nombreuses réflexions dans le but de la rendre plus adaptée aux nouveaux défis et plus efficace (Rapport Barnier). Son mécanisme d'entraide a été amélioré grâce à un nouvel instrument financier, mais qui demeure encore trop modeste.

Enfin, la nécessité de répondre aux défis environnementaux, aux risques naturels ou sanitaires au niveau de l'Europe ou de la planète, sujets qui sont aussi depuis longtemps suivis par la Commission, est désormais passée au premier rang de ses préoccupations.

Il a résulté de cet élargissement des compétences et des activités des instances communautaires dans le domaine de la sécurité, l'adoption au cours des dernières années d'une importante série de directives et la création d'organismes nouveaux.

La Commission européenne a également lancé un programme de recherche en matière de sécurité qui est le fruit d'une longue réflexion. Une action préparatoire pour la recherche de sécurité (PASR) a été mise en place en 2004 par la Commission européenne. Puis, un « programme européen pour la recherche de sécurité », doté de 1,5 milliard d'euros, a été adopté pour 2007/2013 dans le cadre du « 7e Programme-cadre de recherche et développement ». Enfin, l'ESRIF (*European Security Research and Innovation Forum*) a été créé en mai 2007 en vue de favoriser le dialogue public-privé dans le domaine de la recherche et de l'innovation en matière de sécurité. Cette instance remplace l'ESRAB (Comité Consultatif pour la Recherche de Sécurité).

En outre, l'Union européenne s'est dotée d'un début de doctrine en matière de sécurité. Celle-ci a pour but affiché la sécurité et la liberté du citoyen. Elle prend en compte cinq types de menaces (terrorisme, prolifération, conflits régionaux, États faillis, crime organisé) et développe une stratégie combinant une politique régionale de « bon voisinage », des programmes de coopération et une action multilatérale et, si nécessaire, des opérations de maintien de la

paix. L'idée générale est que l'Union ne peut se sentir en sécurité que « dans un monde meilleur ».

Le traité simplifié adopté au sommet de Lisbonne le 18 octobre dernier a permis de nouvelles avancées pour l'ensemble des activités qui concernent l'espace de liberté, de sécurité et de justice, c'est-à-dire le contrôle des frontières ainsi que la coopération judiciaire et policière. L'Union dispose d'une compétence partagée dans ce domaine, c'est-à-dire qu'elle peut, à l'instar des États-membres, légiférer et adopter des actes contraignants. Il en est de même pour ce qui concerne les « réseaux transeuropéens » et les « enjeux communs de sécurité en matière de santé publique ». Pour la protection civile en revanche, l'Union peut seulement mener des actions pour appuyer, coordonner et compléter l'action des États-membres. La règle de la majorité qualifiée deviendra en outre la règle générale d'ici sept ans (novembre 2014) sauf dans les cas où le traité le stipule autrement. Enfin, la clause de solidarité joue en cas d'attaque terroriste et de catastrophe naturelle ou d'origine humaine en mobilisant tous les moyens mis à la disposition par les pays-membres, y compris les moyens militaires.

Malgré ces avancées, la construction européenne en matière de sécurité reste inachevée et limitée. Elle pèsera pourtant d'un poids plus lourd dans certaines politiques nationales des pays-membres.

ÉVALUATION DES MENACES ET DES RISQUES AU NIVEAU MONDIAL ET NATIONAL

La sécurité interne étant de plus en plus liée à notre environnement extérieur, menaces et risques au niveau international ont forcément des répercussions en France. Nous sommes cependant plus sensibles à certains problèmes qu'à d'autres.

Au premier plan des préoccupations figurent incontestablement les menaces dites "sociétales", la criminalité organisée transnationale et sur un mode plus agressif, le terrorisme international. Il est suivi, en ordre d'importance décroissant par les risques sanitaires, naturels et environnementaux. Le risque technologique, lui, demeure constant.

L'accent sera mis essentiellement dans ce Livre blanc sur le terrorisme, les risques technologiques et naturels et le risque sanitaire. On verra que, dans tous ces cas, le diagnostic est le même : une situation actuelle inquiétante ; un accroissement du péril au cours des prochaines années, une évolution qui doit appeler notre vigilance.

Dans chaque cas, des mesures concrètes, parfois en complément de celles déjà proposées ou prévues au niveau gouvernemental, seront formulées dans les chapitres suivants.

1- La menace terroriste internationale

État de la menace au niveau mondial et européen

Le Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme publié en mars 2006 a fait le point sur le terrorisme mondial, son évolution et ses méthodes. Il suffira donc de rappeler ici que le 11 septembre 2001 a marqué l'avènement d'une nouvelle ère, celle de l'hyperterrorisme (actions de masse) et du « terrorisme mondialisé » et que l'Europe n'a pas été épargnée par cette vague (Madrid en mars 2004 ; Londres en juillet 2005) qui s'est étendue à une bonne partie de la planète. Depuis la publication de ce rapport, la situation s'est encore détériorée.

Les interventions américaines en Afghanistan et en Irak initiées pour contribuer à la lutte contre le terrorisme ont incontestablement

fait naître de nouveaux groupes terroristes et semblent « donner » une légitimité aux extrémistes islamistes. L'Irak est en outre devenu un véritable laboratoire d'expérimentation pour former de nouvelles générations de terroristes et pour mettre au point de nouvelles techniques d'action. Les dernières informations en provenance de ce pays ne sont pas optimistes.

Évolution et caractéristiques de la menace terroriste actuelle

Au lendemain du 11 septembre, la menace prenait les traits suivants qui demeurent aujourd'hui :

• Des effets d'agression sur le territoire touché comparables à la « guerre conventionnelle ».

• L'absence de préavis, liée à la difficulté de renseignement (difficulté d'infiltration dans les mouvements terroristes islamistes).

• L'absence de « planification » précise et perceptible, compliquant la recherche du renseignement.

• La décentralisation et l'autonomie de groupes terroristes, voire l'encouragement d'initiatives individuelles de la part d'« agents dormants », apparemment bien intégrés.

• La nature des cibles, qui peuvent être très souvent des « cibles d'opportunité » (pétrolier *Limburg*) suffisamment significatives (atteinte à un symbole) ou à « très haut rendement » avec la recherche de pertes humaines élevées.

• Les possibilités de communication moderne : Internet, téléphones mobiles et satellitaires, la puissance de l'informatique portable, les logiciels de cryptologie en accès libre etc. rendent les moyens de communication et de diffusion d'informations des terroristes difficiles à suivre et à intercepter, tant les voies de communication sont nombreuses.

• Le recrutement de jeunes gens, souvent très jeunes, rapidement endoctrinés et aptes à passer à l'acte en quelques semaines ou quelques mois rendant leur détection très difficile par les services spécialisés.

• Le mode d'action par attaque suicide de la part de terroristes fanatisés recherchant un statut de « martyr ». Ce qui prend en défaut

pratiquement la plupart des dispositifs de prévention et de défense habituels, soumis par ailleurs aux contraintes du cadre légal de temps de paix (hors régime juridique d'exception).

• La mise en œuvre de moyens banalisés comme vecteurs porteurs ou armes par destination rendant quasi impossible l'identification « hostile » par reconnaissance de forme.

• La « mémoire longue » de certains de ces mouvements, qui s'inscrit dans un esprit de revanche, voire de reconquête, faisant désormais peser une menace permanente et « intemporelle », notamment sur les sociétés occidentales.

Genèse d'un nouveau terrorisme

Les responsables gouvernementaux européens ne craignent plus d'évoquer la possibilité que les terroristes aillent désormais plus loin. En effet, selon la directrice du service de renseignement intérieur britannique : « Aujourd'hui, il s'agit surtout de bombes artisanales improvisées, mais je pense que la menace pour demain comprendra le recours à des agents chimiques, bactériologiques et radioactifs, voire à la technologie nucléaire[1]. »

Cette information était confirmée le 14 novembre 2006 par un haut fonctionnaire du Ministère des Affaires étrangères britannique[2]. Par ailleurs, le 5 septembre 2007, les autorités allemandes annonçaient l'arrestation sur leur territoire de terroristes prêts à commettre des attentats majeurs avec des modes d'action très proches de ceux utilisés pour les attentats de Londres en 2005, impliquant notamment des agents chimiques comme le peroxyde d'hydrogène[3].

Ainsi, force est de constater que des groupes de plus en plus fanatisés cherchent à acquérir des armes de destruction et/ou pour le moins de désorganisation massive (NRBC/E).

Enfin, l'apparition naturelle de maladies ou l'utilisation d'agents infectieux dans une agression malveillante ne peuvent plus être écartées. La menace biologique étant susceptible de revêtir aujourd'hui des formes très singulières, le risque est grand de ne pas pouvoir l'identifier comme une agression, du moins dans les phases initiales de l'attaque.

Les menaces provenant des armes de destruction massive

- La menace nucléaire

L'incertitude sur le sort d'un certain nombre d'armes nucléaires tactiques ex-soviétiques (dont des charges de démolition portables), révélée en son temps par le général Lebed (sept. 1997) comme sur l'état d'avancement de programmes nucléaires clandestins, ne permet plus d'écarter « a priori » une menace d'utilisation de ce type d'arme, en temps de paix, par des mouvements terroristes, surtout si ceux-ci sont soutenus par des États de manière tout aussi clandestine.

Il s'agit là d'une révolution culturelle dans la mesure où, jusqu'à présent, ce type d'action n'était envisageable que de la part d'États, et donc rendu impossible dans une logique cartésienne de dissuasion du « faible au fort ». Ce concept a cependant commencé à évoluer avec l'apparition d'États proliférants et l'adaptation du concept de dissuasion au dialogue « du fort au fou ».

La possibilité d'emploi de moyens de destruction massive par des organisations non étatiques échappant par nature au concept de dissuasion ne permet plus de faire totalement l'impasse sur cette menace, même si son occurrence est faible aujourd'hui.

- La menace radiologique

La menace radiologique est très présente. Il est d'ailleurs étonnant que des terroristes ne soient pas encore passés à l'acte « R » tant le nombre de sources radioactives contenant des isotopes nécessaires dans l'industrie (alimentaire, médicale, pétrolière, aéronautique etc.) est élevé et tant le suivi de ces sources est toujours difficile. L'AIEA recense chaque année plusieurs dizaines de sources dites « orphelines » dont certaines feraient des armes à dispersion radiologique de choix. Si la mise en œuvre de ce type d'attentat nécessite une certaine technicité, notamment dans le transport des sources, elle est accessible à des terroristes formés. Si les conséquences n'étaient pas – ce qui est probable – majeures en termes de mortalité, l'impact psychologique et de désorganisation, notamment face à plusieurs événements simultanés, serait, lui, majeur.

- La menace chimique

Les agents explosifs ont aujourd'hui encore une place de choix dans l'arsenal terroriste, notamment ceux réalisés artisanalement à partir de substances chimiques du commerce. Cependant, les agents chimiques toxiques pourraient en particulier prendre une part de plus en plus importante dans les menaces à venir. Ces craintes sont renforcées par le fait que parallèlement au développement de la mondialisation et à l'essor de l'extrémisme islamiste, le profil des terroristes a changé. Ce sont aujourd'hui de jeunes hommes et femmes souvent bien intégrés socialement dont certains ont fait des études supérieures universitaires leur permettant d'acquérir des compétences techniques et scientifiques importantes.

La guerre chimique n'est pas nouvelle, l'Union soviétique et les pays du Pacte de Varsovie, les USA avaient développé des armes NBC[4]. Mais, concernant le terrorisme chimique, l'événement de référence est l'attentat de Tokyo en 1995. L'utilisation par la secte Aum de sarin, un neurotoxique organophosphoré très toxique, dans le métro de la capitale japonaise avait alors fait 12 morts et 5 500 personnes intoxiquées, un faible résultat dû au fait d'un manque de temps dans la préparation de l'attentat mais qui démontre bien l'ampleur des pertes atteignables par ce type d'agent.

Par ailleurs, bien que longtemps focalisés sur les agents chimiques de guerre (notamment vésicants et neurotoxiques), les services spécialisés ont aujourd'hui pris conscience des menaces dues aux agents chimiques industriels, dont certains sont hautement toxiques. L'accès aux substances chimiques industrielles est beaucoup plus aisé que la fabrication ou le vol d'agents C militaires. Le seul marché communautaire compte aujourd'hui près de 100 000 substances dangereuses enregistrées dont 10 000 qui sont commercialisées en quantité supérieure à 10 tonnes par an et 20 000 comprises entre 1 et 10 tonnes par an[5].

Depuis le début de l'année 2007, des groupes terroristes en Irak mettent au point de nouvelles tactiques d'action puisque plus de dix attaques ont été réalisées à l'aide d'engins chimiques improvisés (ECI) contenant du chlore. Le chlore est une substance chimique largement utilisée dans l'industrie. Aujourd'hui, 24 pays produisent approximativement 50 millions de tonnes de chlore par an.

En Irak, il est utilisé en association avec des explosifs ou des camions chargés d'essence. Les forces américaines et irakiennes sur le terrain ont annoncé courant février la découverte d'un atelier de fabrication artisanale d'ECI au chlore dans lequel ont également été retrouvés : 5 véhicules, des mortiers, des bombes artisanales, des cuves de propane et des barils de propane et de nitroglycérine[6]. Ainsi, il semble que jusqu'ici la majeure partie des victimes résulte des effets de l'explosion. Mais des informations récentes semblent indiquer que les terroristes perfectionnent leurs systèmes de dispersion et prennent en compte les conditions météorologiques. Ainsi, on peut s'attendre à un risque de montée en puissance de ce type d'attentat et craindre, à la lumière de ces événements, que des actions de ce type soient menées en dehors du contexte irakien.

Deux autres types de scénario peuvent également être envisagés : soit des attaques directes sur des infrastructures critiques de la « chimie » (installations classées produisant ou stockant des substances chimiques, infrastructures portuaires, transport de matières dangereuses par voie terrestre ou maritime etc.), soit le détournement de substances chimiques volées pour la réalisation d'ECI à composante explosive ou non, d'engins explosifs improvisés (EEI) ou pour la contamination de réseaux d'eau.

- Les menaces biologiques

Le monde est de plus en plus confronté à des problèmes sanitaires liés à l'émergence ou à la réémergence de maladies. La mondialisation (déplacements des personnes et des marchandises), la croissance démographique, la modification des écosystèmes, le réchauffement climatique, les changements d'habitudes alimentaires, l'évolution des populations à risque, la possibilité d'utilisation d'armes biologiques conçues à l'aide des biotechnologies amplifient la menace sanitaire.

La menace biologique terroriste a été exercée aux USA avec les attaques à l'anthrax de l'automne 2001. Bien que cette affaire n'ait pas encore connu d'épisode judiciaire, il est clair que des terroristes ont utilisé un agent hautement pathogène dans une démonstration, à toute petite échelle, de ce que pourrait constituer avec le même type d'agent une attaque massive *via* un réseau de distribution de

masse (ici le courrier).

L'augmentation de la circulation des agents pathogènes accroît les risques de contamination ainsi que la probabilité d'apparition de nouveaux agents issus de combinaisons génétiques autrefois inimaginables. Le décodage du génome humain associé au développement des biotechnologies peut faire craindre une menace biologique terroriste et militaire extrêmement « dangereuse » sur le moyen et le long terme au fur et à mesure de la dissémination de ce savoir et des équipements liés aux biotechnologies.

2 - Risques et menaces technologiques et sanitaires

Parmi les risques et menaces technologiques existants et depuis la parution du Livre blanc de la défense civile de 2003, les principaux domaines qui suivent ont été retenus en raison de leur gravité.

La gravité d'un risque ou d'une menace réside dans le nombre de personnes pouvant être affectées, dans la persistance des conséquences de l'événement ainsi que dans sa médiatisation potentielle tant préaccidentelle que postaccidentelle.

- Les risques sanitaires

De nombreuses maladies ont occupé ces dernières années le devant de la scène médiatique (fièvre aphteuse, maladie de la vache folle, SRAS, peste aviaire, etc.). Les incidences sanitaires et économiques de ces maladies sont considérables. Un seul pays défaillant en matière sanitaire constitue un danger permanent pour le reste des pays du monde.

En outre, des maladies considérées comme exotiques et qui font actuellement des ravages dans des pays en développement peuvent s'installer durablement en France du fait, notamment, du réchauffement climatique, fièvre du Nil, fièvre de la vallée du Rift…

La sécurité sanitaire des aliments constitue également un enjeu important dans toutes ses composantes (biologique, chimique ou physique) et sur toute la chaîne de production.

Même si la pandémie grippale constitue aujourd'hui le risque sanitaire qui apparaît comme le plus important, d'autres maladies émer-

gentes (dont 75 % sont des zoonoses, maladies transmissibles de l'animal à l'homme) présentent des risques à prendre en considération, en renforçant notamment le système de surveillance européen et les capacités des services sanitaires et vétérinaires. Il convient d'aider les pays en développement et en transition à éliminer les maladies sur leur territoire et de les sensibiliser à la nécessité de respecter les normes internationales de gouvernance sanitaire.

C'est pourquoi, menace biologique, agroterrorisme et risques sanitaires ne peuvent être dissociés dans une approche globale à ces typologies de risques et menaces basés sur les sciences du vivant, et doivent être approchés avec un continuum de réponses commun.

- Le risque nucléaire

Il s'agit du risque le plus médiatisé et celui qui suscite le plus d'inquiétude en France. Il reste l'un des risques industriels les mieux surveillés dans notre pays. Le nombre limité de réacteurs nucléaires, l'existence d'un unique exploitant (EDF) et d'une autorité de contrôle indépendante, l'Autorité de Sûreté Nucléaire (ASN), facilitent grandement cette tâche.

Pourtant trois problèmes apparaissent progressivement qu'il convient de traiter :

• Un fort développement de la production électronucléaire en France, en Europe et dans le monde est actuellement prévu. La construction de réacteurs nucléaires permettant la production de 160 gigawatts d'ici à 2020 dans le monde[7], soit l'équivalent d'une centaine d'EPR, est envisagée. Cette prospective s'appuie sur une prolongation de la durée de vie des réacteurs nucléaires actuellement en exploitation (durée de vie initiale d'un réacteur nucléaire de 40 ans pouvant être prolongée jusqu'à 60 ans aux USA et au Japon).

• L'augmentation du nombre de réacteurs nucléaires qui résultera de cette situation provoquera mathématiquement un accroissement de la probabilité d'occurrence globale d'un accident à fiabilité constante des installations. Un devoir d'amélioration de leur sûreté est ainsi rendu nécessaire. Cette exigence est en fait une des priorités des constructeurs et des exploitants de réacteurs nucléaires.

Les organismes de contrôle doivent s'assurer que cela le restera.

• Les attentats du 11 septembre 2001 ont radicalement fait évoluer la prise en compte de la chute d'avions sur une centrale. Avant cette date, on considérait qu'elle ne pouvait résulter que d'une défaillance accidentelle de l'appareil. Ce risque était maîtrisé en dimensionnant mécaniquement l'enceinte du réacteur nucléaire à l'impact d'un avion dont la chute était considérée statistiquement probable, c'est-à-dire de manière générale en France à un appareil de l'aviation dite « générale » (avions légers d'affaires à réaction ou à turbines). La probabilité de chute d'un avion de type militaire ou commercial était considérée comme résiduelle. Depuis le 11 septembre, les exploitants et les concepteurs ont réévalué ce risque. En effet, dans le cas d'une attaque, on ne peut plus parler de probabilité, puisqu'il s'agit d'une action volontaire délibérée de la part d'un agresseur. En revanche, l'approche probabiliste peut être utilisée pour évaluer l'efficacité et les conséquences de l'attaque (probabilité pour que l'agresseur impacte à l'endroit visé, probabilité de défaillance des protections etc.). Ainsi sur les réacteurs futurs ou en construction tel l'EPR, l'approche probabiliste a été abandonnée. Dorénavant l'ensemble du trafic aérien issu de l'aviation générale, militaire et commerciale est pris en compte dans la conception et le dimensionnement des bâtiments nucléaires[8].

Il reste cependant le problème des réacteurs existants dont ni l'enceinte ni, encore moins, le bâtiment d'entreposage du combustible ne sont dimensionnés pour résister à la chute d'un avion de type militaire ou commercial.

Les déchets nucléaires à haute et moyenne activité peuvent présenter une menace dont il conviendrait d'évaluer l'ampleur, en cas d'agression terroriste. Dans l'attente que la totalité de ces stockages soient sécurisés dans des infrastructures souterraines, les dépôts en surface, relativement vulnérables aux actions terroristes terrestres ou par voie aérienne, doivent faire l'objet de sujétions particulières de sécurité.

- Le risque barrage

Le risque de rupture de barrage semble en France bien moindre que le risque nucléaire traité précédemment. Il aura fallu la publi-

cation d'un rapport confidentiel d'EDF sur l'état des barrages français[9], dévoilé par la presse en mars 2007 pour sensibiliser l'opinion publique à cette problématique. Ce risque n'est cependant pas à négliger car, bien que rare, il n'a rien d'exceptionnel. Ainsi l'accident industriel ayant fait le plus de victimes depuis 1970 est la rupture du barrage de Morvi en Inde le 11 août 1979 avec 15 000 victimes dont 5 000 morts[10], bien devant la catastrophe de Bhopal.

Il convient également de rappeler qu'une catastrophe de cette nature est survenue en France : le 2 décembre 1959, la rupture du barrage de Malpasset provoqua une vague de près de 40 mètres de haut sur la vallée, qui atteignit Fréjus en 20 minutes. Les conséquences en furent considérables : plus de 400 morts, 951 immeubles détruits, 1,5 kilomètre de routes et 2,5 kilomètres de voies ferrées arrachées avec le train qui y circulait.

Outre les conséquences directes liées à l'inondation, il faut prendre en compte l'impact qu'une rupture de barrage peut avoir sur les installations industrielles en aval (telles que des sites Seveso ou des installations nucléaires) et les effets dominos générés rendant la maîtrise de la situation beaucoup plus délicate pour les pouvoirs publics, sans oublier les conséquences sur les structures et les moyens des pouvoirs publics chargés de gérer cette situation (bâtiments publics, hôpitaux etc.).

La probabilité d'occurrence d'une telle rupture est également à réévaluer compte tenu des accidents récents liés au vieillissement d'ouvrages d'art en béton, comme l'effondrement le 1er août 2007 du pont de Minneapolis aux États-Unis, construit en 1967. De plus, il convient de constater que, compte tenu du risque existant que l'on pourrait comparer au risque nucléaire, les prescriptions réglementaires ainsi que les contrôles associés semblent beaucoup moins exigeants.

Sur le plan de la vulnérabilité aux actions terroristes, les barrages représentent des cibles potentielles à « très haut rendement », voire l'équivalent de moyen de destruction massive en cas de destruction. Ce sont donc des cibles particulièrement attractives du fait de leur absence de surveillance et de protection active. Il conviendrait d'entamer rapidement une réflexion sur la possibilité de mise en place de dispositifs de surveillance et de prévention visant à un

durcissement de ces installations. On pourrait pour cela s'inspirer de ce que font les Russes pour protéger leurs barrages du terrorisme (tchétchène) ou alors rechercher des moyens techniques de protection.

- Les risques industriels et le risque TMD (transport de matières dangereuses) et les menaces associées

Les risques industriels sont maintenant très contrôlés dans le cadre des réglementations dites Seveso II, le nombre de Seveso à seuil haut est sous le contrôle permanent des DRIRE, les accidents industriels sont toujours possibles mais le point noir qui demeure est la protection de ces sites face aux menaces terroristes, qui ne sont pas prises en compte aujourd'hui face à un niveau de menace élevé. La réglementation de 2006 sur les SAIV (secteurs d'activités d'importance vitale) apportera certainement une réponse, mais la menace est là présente encore pour plusieurs années, une forte sensibilisation de ces industries aux menaces demeure donc une priorité.

Le développement du risque lié au transport de matières dangereuses (TMD) est favorisé par le contexte actuel. On constate en effet une augmentation globale des marchandises transportées par voie terrestre de l'ordre de 2,4 % du nombre de tonnes-kilomètres entre 2005 et 2006. Cette tendance semble s'accentuer en 2007[11], or la volonté existe notamment au niveau de la société civile de développer des modes de transport permettant de réduire l'impact sur l'environnement et le risque accidentel, par exemple avec la création de la ligne Lyon-Turin.

Malgré une probabilité plus faible d'accidents ferroviaires comparés aux accidents routiers, ce développement aura deux conséquences : tout d'abord l'augmentation importante du kilométrage parcouru augmentera mathématiquement le nombre d'accidents ferroviaires, en considérant un référentiel de sûreté constant. Ensuite, l'augmentation des capacités des moyens de transport ferroviaires entraîne automatiquement une aggravation des conséquences d'un accident en cas de TMD. Il faut donc éviter que le développement de ce mode de transport, qui favorise une plus grande concentration de matières dangereuses pour un même moyen de transport, n'aboutisse à la création de « risques Seveso sur rail ».

La Loi n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages a permis le rapprochement de la réglementation liée au transport avec celle liée aux installations industrielles, en instituant une étude de dangers pour les sites de stationnement des différents moyens de transport (ferroviaire, routier, maritime). Mais la réglementation liée aux transport ferroviaires diffère encore sur un point important avec celle liée aux installations industrielles. La comptabilisation des quantités de matières transportées, et les seuils associés, sont réalisés wagon par wagon et non pour le chargement complet. Il n'existe ainsi aucune limitation des quantités de produits dangereux transportés.

Tout cela est d'autant plus préjudiciable que ces véhicules sont particulièrement sensibles à la menace terroriste (détournement, sabotage) et peuvent constituer avec les chargements les plus dangereux des armes de destruction massive pouvant facilement pénétrer le cœur des grands centres urbains.

- Les risques liés aux déchets radioactifs à haute activité

Le seul risque identifiable est celui de la dissémination suite à une agression terroriste sévère. Le principe du stockage profond étant différé et le stockage en surface vulnérable aux agressions, une solution intermédiaire parfaitement réversible pourrait être le stockage temporaire dans des structures souterraines protégées existantes et disponibles telles que les ouvrages de fortification type Maginot. Le niveau très élevé de protection passive offert par ces ouvrages permettrait d'envisager une simple télésurveillance.

- Les risques liés aux laboratoires de recherche biologique

Le risque est représenté par les laboratoires de niveau P4, qui, s'ils sont construits en surface, sont plus vulnérables aux agressions terroristes sévères. Il paraîtrait en conséquence souhaitable d'aménager à l'avenir ce type de laboratoire en infrastructure souterraine, n'offrant, d'une part, aucune cible visible et identifiable aux actions à distance, et d'autre part, se prêtant plus facilement au confinement automatique d'urgence en cas d'accident.

- Les risques sur les infrastructures de transports, les ouvrages d'art, les bâtiments culturels et les lieux de rassemblements

Les tunnels, routiers ou ferroviaires, les grands ouvrages d'art (viaducs, ponts…), les bâtiments et lieux symboliques de notre culture (tour Eiffel, musées nationaux, biens culturels, concerts…) : tous les lieux de forts rassemblements de population deviennent des cibles attractives pour des terroristes et nécessitent une vigilance et une sécurisation accrue en accord avec le seuil de menace.

- Les risques et menaces liés aux technologies de l'information

Internationalisation des échanges, rapidité des transactions, disparition des frontières et anonymat, dans un monde encore partagé en États fondés sur la territorialité et la souveraineté, favorisent l'éclosion de nouvelles menaces sociétales liées à l'utilisation déviante des technologies de l'information et de la communication (TIC). Nos sociétés sont en fait de plus en plus vulnérables en raison de l'usage intensif des moyens informatiques à tous les niveaux, par l'utilisation croissante de produits standard tant logiciels que matériels ou réseaux, par l'accroissement exponentiel du nombre des utilisateurs (1 milliard d'internautes connectés en 2007, 2 milliards d'ici à 2012 selon l'OCDE), par l'apparition permanente de nouveaux produits présentant des failles ou encore mal utilisés.

Ces attaques, aujourd'hui principalement économiques, peuvent dans le futur constituer des attaques contre des États ou des populations. Les événements survenus en Estonie en 2007, ainsi que les capacités militaires de développement d'attaques informatiques dans certains pays, la capacité de « louer » des milliers de plates-formes pour de faibles durées dans certains pays, permettent aujourd'hui de lancer des attaques potentiellement dommageables et nuisibles pouvant paralyser ou ralentir l'économie d'une nation ou d'une région.

Au-delà de la situation présente, l'adoption du protocole IP sur certains systèmes informatiques touchant aux infrastructures et réseaux d'activité d'importance vitale fait naître de nouvelles vulnérabilités qui laissent craindre que des réseaux autrefois « fermés » ne connaissent des vulnérabilités « nouvelles » inquiétantes. Vulnérabilités permettant à des terroristes compétents de causer des dommages

« mortels » à travers la prise de contrôle d'un système informatique d'un opérateur d'énergie ou de transport, d'un hôpital, d'une centrale d'énergie ou d'un opérateur de télécommunication.

3 - Les risques naturels

Nous ne mentionnerons que pour mémoire les risques liés aux incendies de forêt, tant les services de l'État et des collectivités locales ont travaillé à la prévention et à la réponse de sécurité civile depuis plusieurs années avec un effort continu. L'efficacité atteinte est aujourd'hui optimale durant les campagnes de feux de forêt réduisant ainsi, malgré des contraintes météorologiques sévères, le nombre d'hectares brûlés.

Mais les risques naturels ne se limitent pas seulement aux risques de feux de forêt : les tempêtes de 1999, les inondations de la Somme et le risque potentiel en matière de séisme sur une partie du territoire imposent la prise en compte de ces risques majeurs en termes de prévention, ce qui est fait, mais aussi en matière de préparation des réponses de sécurité civile.

Les inondations sont un risque permanent et majeur sur un certain nombre de territoires, les évolutions prévisibles en matière de changement climatique font craindre l'augmentation en fréquence et en intensité de ce type d'événements catastrophiques.

Le séisme demeure, avec le tsunami, avec lequel il pourrait être lié, un risque d'une ampleur exceptionnelle. Les normes parasismiques appliquées depuis deux décennies sur un certain nombre d'ouvrages et de bâtiments ne peuvent faire oublier qu'une majorité des habitations (pavillons, villas etc.) ne bénéficie pas de ces normes et seraient donc vulnérables, ainsi que certains ouvrages d'art anciens.

Cela impose une réflexion sur les niveaux de prévention et de préparation à ces crises consécutives de risques naturels majeurs qui semblent aujourd'hui encore faire défaut au niveau gouvernemental. Le Conseil national de sécurité civile[12] qui s'est saisi de cette thématique doit produire un document sur l'état de la réponse face à un séisme majeur. C'est certainement un champ d'investigation important en termes de réponse de défense civile, compte tenu de

la complexité et de l'ampleur des réponses de toute nature nécessaires dans une société postindustrielle.

L'adoption du nouveau dispositif ORSEC fin 2006 est une démarche globale intéressante sur la réponse aux risques, il est néanmoins nécessaire de réfléchir à son application au travers de scénarios et d'exercices très pénalisants pour valider cette nouvelle approche dans le cadre des crises complexes.

Notes du chapitre I :

1- « The international terrorist threat to the UK », Dame Eliza Manningham-Buller, general director of the security service, at Queen Mary's College, London, 9 novembre 2006.
2- « Al-Quaeda seeks nuclear material for uk attack, ministry says Robin Stringer ». *Dépêche Bloomberg*, 14 novembre 2006.
3- J. Connan. « Allemagne : les terroristes préparaient des "attentats majeurs" » - *Le Figaro*, 5 septembre 2007.
4- F. Gombeaud, « La défense NRBC : de nouveaux enjeux pour l'Armée de terre ? » - *CDES*, Objectif doctrine n.35, 2005.
5- Livre blanc – Stratégie pour la future politique dans le domaine des substances chimiques. Commission des communautés européennes. COM88, 27 février 2001.
6- « Cinquième attaque au chlore en Irak », *Le Monde*, 18 mars 2007.
7- « Quel avenir pour l'énergie nucléaire ? », *synthèse du colloque ANAJ-IHEDN – SFEN JG* du 6 octobre 2006.
8- Source EDF, *Rapport préliminaire de sûreté de Flamanville 3,* Version publique
9- Capital. fr.
10- « Catastrophes naturelles et techniques en 2006 », *SWISS RE*, 2007.
11- DGMT.
12- Le Conseil national de sécurité civile n'a été réuni qu'une fois à sa création, et une deuxième fois en janvier 2008.


Haut Comité Français
pour la Défense Civile
Protéger l'avenir...

CHAPITRE II

Urgence et gestion de crise : prévention, planification, exercices et retours d'expérience

INTRODUCTION

La gestion de crise ou gestion des situations d'urgence est la réponse opérationnelle d'un individu, d'une organisation, publique ou privée à une situation inattendue, de nature à le (la) mettre en difficulté. Une crise bien gérée implique de réfléchir à une méthodologie de travail, permettant de prendre en compte dans les meilleures conditions la situation telle qu'elle se présente, d'en comprendre les tenants et les aboutissants, d'imaginer ses conséquences, et de prendre les décisions aptes à réduire ces mêmes conséquences.

Depuis la fin de la Seconde Guerre mondiale, le monde moderne s'est organisé en optimisant ses ressources, son fonctionnement, sa production, son économie. Au-delà de son évolution naturelle, il a vu l'émergence de nouvelles vulnérabilités, de nature à mettre en danger cette organisation. Une contradiction importante naît du fait que la crise est issue de son impréparation. Il est donc primordial de réfléchir, de planifier et d'organiser simultanément la prévention et la réponse à ces crises, même si la prévention doit être privilégiée et développée.

S'agissant des crises majeures, celles qui concernent l'ensemble de l'activité du pays ou d'une région, le bon sens exige de travailler ensemble, de mettre en commun entre tous les acteurs concernés les informations « amont », les dispositifs de gestion « pendant », ainsi que les retours d'expérience « après ».

CONSTATS

Si l'expérience montre que les acteurs de la gestion de crise sont attentifs aux résultats techniques (nombre de victimes, montant des dégâts économiques et financiers, nombre de familles déplacées, d'hectares inondés etc.) le corps social, lui, exige un résultat moral : celui de faire son maximum. Ainsi, si on analyse plus finement les crises passées, on observe qu'il est plus efficace du point de vue du grand public de démontrer sa mobilisation totale, son dévouement, son engagement, que de rechercher un résultat technique parfois peu lisible.

L'acceptation par le corps social de la gestion de crise est donc un élément déterminant. Bien entendu, l'opinion, de mieux en mieux informée et instruite ne saurait se contenter d'une justification de façade. Il reste que dans un monde largement médiatisé, le résultat général dépend pour une grande partie de l'image qu'il donne.

Si l'on considère la lutte contre les grands risques majeurs qui touchent l'ensemble de l'activité nationale, il devient absolument nécessaire de mettre en place une coopération fructueuse public/privé permettant de partager les informations, les moyens et les compétences en vue d'obtenir le résultat global décrit ci-dessus.

En particulier, l'opinion n'accepte plus que l'information circule mal entre des « puissants » et que la classe dirigeante n'apparaisse pas mobilisée, que l'information donnée au public tarde, qu'un délai trop important s'écoule entre les promesses et les actes. Enfin, le maintien de la confiance, condition *sine qua non* de la bonne exécution de ces tâches, mais aussi du maintien de la cohésion nationale, implique que les équipes en charge du pilotage des crises aient une hauteur de vue et une capacité de mobilisation suffisante et immédiate pour apporter une réponse la plus adaptée possible.

L'expérience montre donc que le bon pilotage de la crise ainsi que

la bonne exploitation des retours d'expérience sont des données fondamentales à prendre en compte dans le cadre du cycle vertueux de la bonne gestion, qui nécessite cette dimension prévention, c'est-à-dire développer une culture réflexe d'anticipation, de préparation, d'information.

Ainsi s'invitent donc dans le débat les valeurs morales d'une société moderne. L'opinion n'accepte plus que ceux qui savaient et qui avaient le pouvoir de réduire les conséquences d'une crise ne fassent rien.

1 - Le devoir de prévention

L'efficacité d'un dispositif de prévention repose sur le bon exercice du devoir « moral », mais aussi « légal ». Sans ces deux aspects il existe de puissants freins qui limitent l'action et le volontarisme et donc l'efficacité globale des actions de préparation.

- Pour le secteur public

La planification d'État est en adaptation permanente (dispositif ORSEC, plans de défense, plans sanitaires…) et c'est une bonne chose ; par contre la préparation aux situations de crise tant en termes d'investissement matériel qu'humain reste à un niveau relativement bas en France en comparaison d'autres pays européens.

Sur le plan humain, la formation à la gestion de crise, à son environnement particulier (stress, urgence, enjeux…), à ses mécanismes particuliers (gestion du temps, etc.) est encore à ses balbutiements tant en termes de formation initiale que permanente. De plus, les responsables concernés ne perçoivent pas toujours culturellement la nécessité de formation « spécifique » à la gestion de crise et, de ce fait, n'allouent pas les moyens et l'autorité nécessaires à ces formations. « La crise… on la gère tous les jours… » entend-on souvent, or cela n'est pas la réalité et handicape donc fondamentalement la réponse publique.

Sur le plan matériel, la France est en retard dans l'organisation et la spécialisation de salles de gestion de crise. Au niveau central, l'État possède peu de « salles de crise » dignes de ce nom en dehors de la défense, du COGIC et des acteurs du nucléaire. Notamment les plus hautes autorités de l'État (Présidence, Premier

ministre, ministre de l'Intérieur…) n'ont pas, en dehors de la chaîne de commandement nucléaire, de salles de gestion de crise équipées pour traiter des crises de toute nature à dominante interministérielle (du type COBR britannique) incluant les outils logiciels et bases de données *ad hoc* en fonction des risques ou menaces.

Coté défense et sécurité civiles, la dernière avancée, depuis le Livre blanc du HCFDC de 2003, est l'utilisation du logiciel « Synergi », logiciel de messagerie et d'échanges qui permet d'avoir une main courante permanente de l'événement, partagée entre tous les acteurs. Néanmoins, les outils techniques de la gestion de crise : logiciels de gestion spécialisés, de simulation et d'anticipation d'événements (risques naturels, séisme, inondations, NRBC), bases de données, et réseaux dédiés et interopérables entre secteurs publics et privés et sécurisés font aujourd'hui encore majoritairement défaut. Les remarques du Livre blanc précédent sur la pauvreté de nos salles de gestion de crise au plan territorial demeurent toujours d'actualité.

Les exemples étrangers (Katrina, 11 septembre), ont démontré que sans formation à penser et piloter les « crises » sévères, voire hors cadre, et sans outils particuliers, notamment en matière de communication, de gestion de situation, la réponse de l'État est très critiquée, voire « perdue ». Les investissements de l'État dans ce domaine sont structurellement beaucoup trop bas pour permettre une capacité de réaction à la hauteur d'une grande crise majeure et de la réalité de la menace actuelle.

Les pouvoirs publics doivent disposer d'un système de commandement (PC de crise) et de transmissions offrant une résilience suffisante pour permettre d'assurer la continuité de l'action gouvernementale et des pouvoirs publics en toutes circonstances, y compris en cas de catastrophe naturelle, d'accident technologique majeur, ou d'attaque terroriste de grande ampleur.

- Pour le secteur privé

La législation sur les secteurs d'activités d'importance vitale (SAIV) va « obliger » à assez court terme les entreprises « clés » de notre économie à mettre en place, si ce n'était déjà fait, à la fois les mesures de « continuité d'activité et de gestion de crise », mais

aussi des mesures pratiques de sécurisation des sites les plus sensibles face aux menaces malveillantes.

Mais pour les autres entreprises, non assujetties à cette nouvelle législation, rien ne les oblige à appréhender les choses « globalement », même si leurs activités sans être « vitales » n'en sont pas moins « critiques », pour certains types de crise.

L'entreprise doit envisager aujourd'hui ses risques tout au long de la *supply chain* pour lui permettre de satisfaire, en temps de crise, sa continuité d'activité. Or, par exemple, une grande entreprise refusera souvent de conseiller un sous-traitant sur sa préparation au risque de pandémie ou à une inondation car sa responsabilité risquerait d'être engagée.

Le résultat est que les informations de prévention ou préparation à la crise sont limitées à ceux qui ont les moyens de mettre les spécialistes à temps plein sur ce sujet. C'est pourquoi il est du devoir de l'État, et des spécialistes du risque que sont les assureurs par exemple, de mieux informer le tissu économique, notamment les PME, à la nécessité de mieux se préparer aux situations d'urgence et à la continuité d'activité, et de les inciter à agir.

Chacun des acteurs privés ou des opérateurs pourrait être partie prenante, au travers d'un système d'incitation fiscale ou sociale (au travers de la formation). Chaque acteur économique, notamment les grandes entreprises, pourrait être invité à prendre ses responsabilités en amont et en aval de sa chaîne de valeurs (*supply chain*). Les actions de formation et de prévention viendraient réduire la responsabilité et augmenter la résilience de l'ensemble de la filière. Ainsi, une grande entreprise formant ses sous-traitants au risque pandémie verrait son risque et sa responsabilité diminuer.

Il convient donc d'identifier et trouver les moyens d'inverser, dans les faits, le mécanisme de la responsabilité, et de la renvoyer de ceux qui agissent dans l'intérêt général vers ceux qui savent, qui pourraient, mais faute d'impulsion ne font rien. Ainsi, en cas de crise grave, ceux qui savaient et ont disposé des moyens d'action et qui n'ont pas agi doivent être appelés en responsabilité.

2 - Expertise et partage d'expériences

Le besoin de préparation commun « secteurs public et privé » sur les grands risques et menaces qui pèsent sur la nation est patent. Pandémies, ruptures énergétiques, crise sociétale, terrorisme, événements climatiques exceptionnels etc. sont autant d'événements potentiels sur lesquels les informations nécessaires et pertinentes doivent impérativement être partagées en amont, pendant la crise, et en aval, entre tous les acteurs concernés.

La notion de groupe d'expertise « public-privé » pouvant intervenir tout au long du processus de planification, gestion, restauration est un concept qui devrait être développé de manière plus formelle.

- Pour le secteur public

Le dispositif ORSEC, rénové en 2006, doit, en parallèle de son appropriation par les différents acteurs du public, ce qui n'est pas encore réalisé aujourd'hui, être simultanément pris en compte par le secteur privé. Cela dans une compréhension mutuelle des dispositifs et une complémentarité naturelle ; cela impose une communication et une formation accrues de l'ensemble des acteurs, tant publics que privés, action qui est encore trop modeste aujourd'hui.

- Pour le secteur privé

La planification des situations d'urgence et de crise pour les entreprises pose le problème de la normalisation. Nous n'avons pas en France de normes *ad hoc* dans le concept des référentiels techniques habituels (ISO, CEN, AFNOR).

Les Britanniques, Japonais et Américains ont depuis plusieurs années établi ces normes. Celles-ci nous seront prochainement imposées (ou le seront dans les groupes multinationaux) *via* la nouvelle norme ISO en préparation. Un groupe de travail, sans présence française, travaille depuis plus de deux ans (Technical Committee TC 233) sous la houlette des Suédois avec une forte participation américaine, israélienne et britannique à la création de la norme internationale de gestion de crise publique et privée. On ne peut que constater l'absence totale de la France dans ce processus ISO TC 233 qui s'imposera à l'Europe et à la France, probablement avant la parution d'une norme européenne.

D'une manière générale la France est trop peu présente dans les processus de certification, tant européens qu'internationaux, en matière de sécurité.

- Les exercices et les tests

Les exercices sont un facteur essentiel de test de la capacité à gérer les situations d'urgence et les crises. Ils sont nécessaires pour évaluer l'état de préparation, pour motiver les acteurs de l'urgence, et pour optimiser dispositifs et procédures ainsi que les interfaces avec l'ensemble des chaînes opérationnelles publiques et privées.

Ils ne sont pas à confondre avec la formation et l'entraînement nécessaire à chaque entité pour se parfaire dans cette gestion à tous niveaux, or ils servent souvent à ce double usage, sans objectifs clairs.

- Les faiblesses de nos exercices :

Les exercices, publics principalement, mais pas seulement, ne sont donc pas, en règle générale, bien faits et bien conçus en France. Plusieurs raisons à cela :

• Les exercices sont trop confidentiels ou trop médiatiques, avec les excès et inconvénients que cela procure, l'objectif de l'exercice devient le seul enjeu médiatique ou il n'y a aucun enjeu.

• Les exercices ne sont pas budgétés, leur réalisme est réduit, souvent par manque de financement. Les acteurs, notamment l'administration en charge dans le secteur public, sont à la fois juge et partie. Il n'y a pas de vision extérieure critique sur l'exercice, ou alors, l'action des observateurs externes n'est pas formalisée.

• Enfin, les retours d'expérience ne sont pas analysés, souvent à cause d'un manque de ressources mais aussi parce que les acteurs ne veulent pas que des documents de RETEX puissent servir dans une future action judiciaire en cas de catastrophe.

- Les actions souhaitables :

• Une planification à long terme du type pluriannuel des exercices qui permettrait un enchaînement logique et cohérent entre des exercices locaux, zonaux, nationaux, de type différent (exercices en salle, terrain, combiné), cela pouvant aboutir sur une fréquence bisannuelle à un exercice majeur national, voire européen (du type

Topoff US, mais corrigé de ses imperfections). Pour cela une vraie planification nationale interministérielle et publique-privée reste à concevoir.

• Une ligne budgétaire « exercice » dédiée au sein de chaque administration et service pour accroître le réalisme des exercices. La possibilité d'utiliser sous contrat de confidentialité des services extérieurs d'observateurs et d'analystes.

• Un retour d'expérience formalisé au travers de protocoles types : fiche de procédure/ auto-évaluation des acteurs, synthèse et analyse serait un plus. Une action serait la réalisation d'un guide méthodologique par type d'exercice. Ces retours d'expérience devraient être désignés comme « documents protégés », dans le cadre d'une réflexion sur le statut juridique du RETEX.

RAPPEL DES PROPOSITIONS

• Augmenter la dotation budgétaire à la formation à la gestion de crise et des situations d'urgence au sein de l'État.

• Améliorer la formation des entreprises en permettant aux grandes entreprises de former et d'inciter les entreprises en amont de leur chaîne de valeur, à améliorer leur préparation et leur résilience, au travers d'un système d'incitation fiscale ou sociale.

• Augmenter significativement la dotation budgétaire à la réalisation de salles de crise « État » équipées d'outils logiciels de gestion de l'information adéquats et de moyens suffisants de communication sécurisée au niveau préfectoral, départemental, zonal et inclure dans ces réseaux sécurisés les opérateurs concernés par le décret SAIV.

• Développer et optimiser le rôle des groupes d'experts public - privé, à disposition de l'administration, en organisant ces groupes au travers de textes réglementaires précis, leur permettant effectivement de jouer un vrai rôle en cas de crise ainsi qu'un rôle de consultation sur la préparation aux crises.

• Améliorer les exercices au travers d'une planification pluriannuelle, d'une budgétisation obligatoire et d'une méthodologie d'organisation et de retours d'expérience formalisée, incluant une externalisation de l'évaluation de ces exercices et comprenant une clause de confidentialité sur les RETEX.


Haut Comité Français
pour la Défense Civile
Protéger l'avenir...

CHAPITRE III

Information et formation des populations, alerte, communication et télécommunication

INTRODUCTION

L'information et la mobilisation de la population sont un facteur clé de réussite de la gestion des situations d'urgence, tant quotidiennes qu'exceptionnelles. Les citoyens y ont une place centrale, étant les victimes de ces situations, et également les premiers acteurs de la prévention et de la réponse à celles-ci.

Les situations d'urgence ou leurs conséquences trouvent souvent leur source dans les comportements inadaptés de citoyens quand ils prennent des risques inutiles ou les ignorent, qu'ils ne savent pas les contrôler ou s'en protéger, qu'ils ne savent pas répondre à une situation de péril imminent.

L'obligation d'information des populations est inscrite dans la loi de modernisation de la sécurité civile de 2004 et, au plus près des citoyens, dans le Plan de Secours Communal (PSC). Or, en 2006, seules 600 villes sur 10 000 en zones à risques avaient développé un PSC, et seulement 15 % des villes du bassin méditerranéen l'avaient fait au printemps 2007.

La communication vis-à-vis des situations d'urgence apparaît, pour encore un trop grand nombre de décideurs publics, comme anxiogène, et le silence, rassurant.

Souvent l'autorité publique se comporte, et est vécue, comme une structure compassionnelle et providentielle, relativement toute puissante aux yeux de trop nombreux citoyens et les populations consomment au quotidien des services d'urgence, pensant que l'assistance face à toutes les situations d'urgence quotidiennes ou exceptionnelles est un dû. Or l'efficacité de la réponse aux situations d'urgence et exceptionnelles requiert des réflexes partagés entre professionnels du secours et population, car soit dans la gestion du temps, soit du fait de l'ampleur de l'événement, les citoyens doivent pouvoir compter, d'abord et avant tout, sur eux-mêmes, dans la mesure de leurs capacités.

Pour arriver à cette prise de conscience et à cet objectif, notamment dans les zones à risques naturels, technologiques ou terroristes (grands centres urbains), il convient de développer une politique d'information des populations jeunes et adultes beaucoup plus poussée qu'actuellement.

Il n'y a pas en France de sites internet publics sur les risques, menaces et comportements à tenir face aux dangers[1]. Cette situation est quasi unique en Europe ; à titre d'exemple, le Royaume-Uni a un site d'information à la préparation aux crises traduit en 17 langues.

Les données fondamentales des risques, des dangers et des comportements à tenir face à ces dangers doivent faire l'objet de plus d'attention de l'autorité politique et des pouvoirs publics.

Note :

1- Le Haut comité français pour la défense civile a développé, en 2007, avec la Croix-rouge française le site internet **www.autoprotectionducitoyen.eu**

LES CONSTATS

1 - L'alerte des populations

Le système d'alerte par sirènes est l'un des moyens les plus simples et les plus efficaces de diffusion ordonnant des actions réflexes immédiates et « conservatoires », en attendant des consignes plus détaillées et l'intervention des secours. L'efficacité du système est malheureusement remise en cause d'une part par la vétusté des équipements existants, et d'autre part par l'absence d'information du public relative à la signification du code sirène.

Ce dossier de l'alerte des populations est « en panne » depuis de très nombreuses années au sein du ministère de l'Intérieur, le dernier rapport de l'Inspection générale (rapport HIREL, daté de 2002), faisait état du délabrement du RNA (Réseau National d'Alerte) le qualifiant de réseau inadapté aux risques d'aujourd'hui et obsolète, dont la maintenance n'est plus possible.

Depuis, les vestiges du RNA subsistent, car personne ne veut signifier la « mort » du réseau et aucune politique nationale n'a été adoptée, seules quelques expérimentations sont lancées, à peu de frais, leitmotiv d'un immobilisme de 20 ans sur le dossier, pour faire durer la réflexion et cacher la misère.

2 - Les télécommunications

Lorsqu'une situation d'urgence requiert une aide extérieure ou déborde les frontières, la mobilisation de services de secours de différents horizons demande une coordination soutenue par des télécommunications performantes.

- Les réseaux de radiotélécommunication des services de sécurité et de secours

Un effort sans précédent a été lancé pour moderniser les systèmes radio de nos services de sécurité et de secours. L'adoption d'un standard unique numérique et crypté (Tetrapol) à haute qualité de services pour la Police nationale, les Services d'Incendie et de Secours et bientôt les Samu, et probablement plus tard la Gendarmerie, est une avancée énorme et à saluer.

Le rôle de l'État dans cette démarche a été et demeure fondamental comme catalyseur de programme.

Le problème maintenant se pose pour les associations agréées de sécurité civile, les collectivités locales, et les opérateurs d'activités vitales (au sens du décret SAIV), acteurs eux aussi du secours et du retour à la vie normale qui ont également un besoin de télécommunication radio avec les services de secours et de sécurité dans la gestion des catastrophes.

- Les réseaux filaires et cellulaires

Les réseaux existants, notamment filaires ou cellulaires, peuvent être détruits ou saturés du fait de l'ampleur de la crise. Il conviendrait d'inciter les opérateurs à proposer des services prioritaires permettant à des abonnés « d'urgence » d'accéder en priorité au réseau en cas de saturation de celui-ci.

L'État pourrait également offrir des accès à ses messageries classifiées et aux réseaux sécurisés aux grands opérateurs SAIV sous forme d'abonnement.

Sur le plan des communications satellitaires, on constate encore un sous-équipement chronique des services de secours qui fait craindre des situations difficiles en cas de catastrophe naturelle majeure.

LES PROPOSITIONS

1 - Une communication, sur les risques, menaces et comportements à tenir face aux dangers plus innovante et surtout plus permanente

Nombreux sont les supports et les initiatives pour la communication dans le domaine de la sécurité civile, répondant à différentes audiences et réalités. Toutefois une identité commune et populaire renforcerait la visibilité de l'organisation sociale et solidaire face aux situations d'urgence tant quotidiennes qu'exceptionnelles.

Tel que l'est « Bison futé » pour la Sécurité routière, une mascotte et une campagne de communication récurrente, sur plusieurs années, à l'instar de ce qui est fait maintenant pour la santé

(INPES), concentreraient l'information relative aux comportements à tenir face aux situations d'urgence. En situation de crise, elle pourrait, pour les pouvoirs publics, être le fil conducteur des comportements les plus pertinents à tenir par rapport à la nature de la situation de crise.

Cette « référence d'image » pourrait, sous contrôle des autorités, être reprise par les différents acteurs de la défense et de la sécurité civiles, tant publics que privés et associatifs, qui œuvrent à la prévention et à la préparation aux situations d'urgence.

2 - Une véritable politique d'information pour tous les acteurs du domaine et la population via Internet

La proposition consiste à créer un portail internet unique sur les risques, les menaces, la gestion des situations d'urgence, à l'instar de ce qui se fait dans les grands pays industrialisés. Ce portail, renvoyant éventuellement sur plusieurs sites, serait à destination tant du grand public que des entreprises, des collectivités voire de certaines parties de l'administration.

Ce portail internet pourrait être de nature « public privé » rattaché à une gestion « interministérielle » et renvoyé en fonction des différents niveaux d'information vers des sites plus spécialisés en fonction des acteurs, certains pouvant même être à accès restreint, notamment les sites des DRIRE, et les informations relatives aux études de danger qui doivent rester confidentielles.

L'usage intensif des technologies de l'information doit pouvoir permettre, à peu de frais, de réaliser efficacement un tel dispositif destiné à la fois aux spécialistes, au public et aux entreprises.

Pour le secteur privé, et notamment les grandes entreprises, une section sur les risques et les procédures de gestion de crise devraient apparaître dans les rapports sociaux permettant à l'entreprise de mentionner non seulement sa capacité à faire face mais aussi son engagement citoyen.

3 - Le brevet d'autoprotection pour mieux préparer les citoyens

L'autoprotection, c'est le comportement que chaque citoyen, famille ou communauté choisit d'adopter pour prévenir, se préparer et répondre efficacement aux situations d'urgence dont il peut être la victime.

Pour cela il convient de pouvoir se former, le projet consiste donc en la création d'un brevet d'autoprotection du citoyen visant à lui permettre de se comporter de manière sûre et saine. Le brevet aborderait les notions de stocks nécessaires pour être autonome face aux conséquences des situations d'urgence exceptionnelles, d'alerte face à des risques ou à des urgences ; la manière de porter secours aux personnes en détresse et de contribuer à compléter les capacités du système de secours et d'assistance.

Cette formation pourrait être offerte prioritairement aux jeunes dans le cadre des programmes scolaires, aux employés et ouvriers dans le cadre des activités de santé-sécurité au travail, et offerte à la population *via* les associations agréées de sécurité civile, comme cela existe pour l'enseignement du secourisme.

4 - L'alerte des populations

Aujourd'hui, le réseau d'alerte doit être repensé de manière multimodale : sirènes, SMS, alerte téléphonique, RDS (radio data system), et les médias en relais.

L'alerte par sirènes doit être conservée et le déclenchement de l'alerte doit à la fois être dans les mains de l'État et des collectivités (SP, Police-Gendarmerie), ainsi que des générateurs de risques (ce qui est parfois le cas, mais sur des réseaux distincts du réseau national actuel).

L'objectif est donc une rénovation dans laquelle l'État, qui ne peut payer aujourd'hui la totalité du réseau dans le cadre budgétaire actuel, pourrait garder la main sur l'architecture de télécommande, *via* la chaîne d'alerte (CODIS-COZ-COGIC) et ferait supporter aux utilisateurs les systèmes de réception de l'alerte et les sirènes.

FOCUS

Le domaine des technologies spatiales

Dans le domaine de la contribution des technologies spatiales à la sécurité globale, la France a développé un savoir-faire qui lui permet de jouer un rôle majeur dans la définition des services GMES. L'effort de recherche et développement mené conjointement par l'industrie, les laboratoires de recherche et le CNES a permis d'atteindre un degré de maturité suffisant pour mettre en œuvre à court terme ces services de manière opérationnelle. La France dispose également à ce jour d'une capacité d'acquisition d'images très performante.

Trois propositions constituent des facteurs clés de succès pour les années à venir :

• Assurer la pérennité et la continuité des systèmes d'observation optique existants, comme le système Spot dont le dernier satellite Spot 5 atteindra prochainement la fin de sa durée de vie nominale, avec une amélioration des performances.

• Favoriser l'utilisation opérationnelle effective de systèmes à vocation duale (Pléiades) ou à vocation défense (Hélios). Il est indispensable que des accords cadres soient définis au préalable de manière à ce que cette capacité à haute, voire très haute résolution puisse, en cas de besoin, être exploitée de manière réactive en réponse aux situations d'urgence.

• Sur la base de l'expérience acquise dans le cadre de la charte internationale ou des différents programmes européens[6], définir un modèle d'organisation opérationnelle, associant les différents acteurs clés français et européens avec un mandat, des conditions d'activation et des procédures agréés.

Le déclenchement de l'alerte pourrait utiliser à moindres frais des réseaux satellitaires existants et l'État proposerait aux collectivités et aux générateurs de risques des boîtiers de raccordement et de déclenchement des sirènes, sous forme d'abonnement couvrant à la fois l'investissement technique et le service.

Cette activité pourrait très bien être portée financièrement dans le cadre d'un partenariat public-privé, sous réserve d'obliger les communes en zones à risques et les générateurs de risques à s'abonner au système.

5 - Une labellisation « défense et sécurité civiles » des territoires

À l'image du « Pavillon bleu » pour les plages, ce label permettrait de sensibiliser et de motiver les collectivités locales afin qu'elles prennent en compte le critère « défense et sécurité civiles » dans leur politique de développement, en complément et en renforcement des directives nationales et/ou européennes obligatoires ou volontaires.

Il contribuerait positivement à une prise de conscience et à une mobilisation collective. Les collectivités locales/territoriales feraient acte de candidature et seraient évaluées selon des critères minima tels que les critères liés à l'information et la communication pour et avec les citoyens, aux compétences de prévention, de préparation et de réponse de la collectivité et des citoyens, à l'alerte et à la mobilisation de la collectivité et des citoyens en cas d'urgence, à l'organisation des acteurs locaux concernés par la gestion des situations d'urgence.

Ce pavillon serait susceptible d'être revalorisé régulièrement, tous les 5 ans, par exemple. Le Haut Comité Français pour la Défense Civile pourrait être l'organisme faîtier de cette labellisation au travers d'un comité d'experts *ad hoc* indépendant et sur des critères précisés dans une charte.

Des mises en situation pourraient être un des indicateurs de performance pour la labellisation. Elles pourraient être graduées, impliquant seulement l'administration, impliquant les autres services de

secours, ou une partie de la population exposée directement à un risque, ou bien encore l'ensemble des acteurs d'un territoire. Ces mises en situation seraient aussi une manière d'évaluer les acquis d'autoprotection.

6. - Les télécommunications des services d'urgence

Lorsqu'une situation d'urgence requiert une aide extérieure ou déborde les frontières, la mobilisation de services de secours de différents horizons demande une coordination soutenue par des télécommunications performantes.

Pour cela il faut privilégier pour l'ensemble des acteurs, publics et privés :

- Le rétablissement des télécommunications :

*- Télécommunication radio : s*ur le plan des télécommunications radio, il conviendrait d'ouvrir l'INPT (infrastructure des réseaux Antares et Acropol) aux opérateurs de services vitaux ainsi qu'aux associations de sécurité civile agréées avec leurs droits d'accès respectifs, ces acteurs acquérant directement les terminaux suivant leurs besoins.

- Télécommunication satellitaire : un projet de « Charte internationale des télécommunications d'urgence par satellite » reposant sur une plate-forme partenariale permettrait une mise à disposition, gratuite ou à prix coûtant, de télécommunications satellitaires pour les acteurs de secours en cas de catastrophe uniquement, comme cela existe déjà dans le domaine de l'observation spatiale. Ce projet requiert un signal politique fort et le leadership d'un pays.

La France pourrait jouer ce rôle auprès des Nations unies et au cours de sa prochaine présidence de l'Union européenne en juillet 2008.

RAPPEL DES PROPOSITIONS

• Une communication sur les risques, menaces et comportements à tenir face aux dangers plus innovante et surtout plus « permanente » grâce à une mascotte partagée entre tous les acteurs de la défense et de la sécurité civiles.

• Création d'un portail internet global sur les risques, les menaces ainsi que sur les mesures de préparation et les conduites à tenir face aux accidents collectifs et catastrophes.

• Un brevet d'autoprotection pour mieux préparer les citoyens à faire face aux situations d'urgence.

• Rénovation du système d'alerte par la mise en place d'une nouvelle architecture de télécommande basée sur le satellite, avec un coût réparti entre État et collectivités, et financée au travers d'un partenariat public privé (PPP).

• Une labellisation « défense et sécurité civiles » des territoires par la création d'un pavillon « orange », à l'instar du « Pavillon bleu » sur la qualité des plages, qui indiquerait, au travers de plusieurs critères, l'effort de préparation et de communication d'une collectivité et de ses citoyens face aux risques catastrophiques.

• L'ouverture de l'INPT aux acteurs de secours non étatiques : associations agréées de sécurité civile et opérateurs de services vitaux pour le partage des télécommunications radio entre tous les acteurs du secours et de la sécurité en cas de catastrophe.

• Le développement d'une charte européenne pour l'utilisation des communications satellitaires à titre gratuit dans le cadre des catastrophes.

• Le développement de services « prioritaires » pour les services de secours et autres acteurs dans le cadre des réseaux cellulaires.

CHAPITRE IV

Réponse opérationnelle face aux situations d'urgence et de catastrophe

INTRODUCTION

Depuis la publication en 2003 du Livre blanc du Haut comité, de nouveaux textes sont venus réglementer, mieux organiser et encadrer l'organisation des secours et les réponses opérationnelles face aux accidents quotidiens et collectifs. Pour mémoire, la loi de modernisation de la sécurité civile d'août 2004, les textes sur la rénovation du dispositif ORSEC en sont des exemples et représentent des avancées significatives en la matière.

On note, au quotidien, une difficulté de plus en plus grande des services à fonctionner, en raison d'une stagnation, voire d'une diminution des crédits d'investissements, notamment dans les budgets nationaux[1], alors que les risques et menaces ne diminuent en aucune façon. Il en résulte une difficulté à anticiper et à s'adapter aux nouvelles menaces, notamment NRBC, et, en termes de prévention, à l'environnement de plus en plus complexe de notre société. On note parallèlement un accroissement des budgets des services locaux[2] (SDIS), consécutif d'un accroissement des missions et des besoins finaux de restructuration liés à la démarche de départementalisation démarrée il y a plus de 10 ans maintenant.

L'enjeu actuel majeur en termes de défense et de sécurité civiles est l'intervention face à une catastrophe d'une ampleur ou d'une nature encore inconnue, pouvant relever du terrorisme ou de grands risques naturels, sanitaires ou technologiques.

Dans ce cadre, le problème de la coordination opérationnelle, technique et « budgétaire » des différents acteurs de secours en France nécessite des échelons de planification politique, technique et financière qui font aujourd'hui défaut. La LOLF ne joue pas le rôle de catalyseur de la démarche « sécurité globale », une réforme pourrait être entreprise pour une meilleure lisibilité de l'action publique. La mission actuelle de sécurité civile ne couvrant que le ministère de l'Intérieur pourrait être étendue à une mission de défense et de sécurité civiles rattachée aux principaux ministères compétents : Intérieur, Santé, Agriculture et MEDAD.

Un effort important, tant sur la planification et la complémentarité des actions nationales et locales, que sur celui de la gestion opérationnelle, doit être entrepris. Les débuts difficiles du Conseil national de sécurité civile, créé en 2004, démontrent bien la difficulté de l'échelon de conception et de coordination en dehors des risques du quotidien.

Les services de l'État, tant au plan central que déconcentré, sont en sous-effectifs notables sur ces thématiques. Enfin, les relations entre services de secours et grands opérateurs de services sont encore trop peu formalisées sur le plan technique et opérationnel, notamment sur la coordination aux différents niveaux de décision.

On note également, dans ce contexte budgétaire restreint, une difficulté de la part de l'État à créer et gérer des programmes innovants qui nécessiteraient des investissements structurants pour faire face à ces nouveaux enjeux. Le FAI (Fonds d'aide à l'investissement) va en diminuant, contrairement aux vœux du Président de la République[3].

De plus, l'État ou les collectivités n'ont pas toujours, dans ces domaines, les compétences techniques pour assurer la maîtrise d'œuvre d'actions, de programmes ou l'acquisition d'équipements techniques. On constate donc des retards ou des ratés dans certains domaines, comme l'interopérabilité, les systèmes de gestion

de l'information, la traçabilité des interventions, les outils de gestion de crise, le domaine NRBC… bref, tout ce qui peut s'avérer nécessaire demain dans des crises majeures.

Par ailleurs, certains moyens nationaux existant pour des applications strictement militaires ou scientifiques ne sont pas toujours inclus dans les plans de défense et de sécurité civiles, faute de moyens de planification suffisants ou de cofinancement des acteurs civils : comme par exemple le spatial, les systèmes d'information, ou les outils de simulation.

Face aux grands risques et aux menaces terroristes, la démarche de pilotage reste de l'initiative de l'État, celui-ci doit prendre la mesure des besoins et mettre en œuvre une politique avec des moyens correspondant à la réalité présente des niveaux de risques et menaces, qui est de notre point de vue insuffisante actuellement, notamment par rapport à nos voisins britanniques et scandinaves.

Il convient également de renforcer la politique européenne de protection civile, de sécurité sanitaire et de lutte contre le terrorisme, notamment les volets opérationnels et budgétaires de ces politiques ; la prochaine présidence française de l'Union, de juillet à décembre 2008 ainsi que les travaux dits du « groupe du futur[4] » constituent à ce titre une véritable opportunité.

Il n'en demeure pas moins que l'État ne peut, et ne doit pas tout faire ; les collectivités et les citoyens doivent également à leur niveau prendre leurs responsabilités, encore faut-il avoir une politique et un langage clairs en la matière. Des approches existent cependant, dans le domaine de la santé communautaire (« terapia comunitaria » développée par le Pr A. Barreto au Brésil et en France), dont on pourrait s'inspirer pour augmenter la résilience de la population et des communautés au niveau local.

L'entreprise pourrait également dans le cadre d'un mécénat « civique », apporter sa contribution à la réalisation de dispositifs ou de moyens de défense et de sécurité civiles. Le mécénat culturel fonctionne très bien en France pour la sauvegarde du patrimoine, pourquoi ne pas développer une forme de mécénat civique pour les entreprises, sur les thématiques de protection civile, comme cela existe aux USA ?

LES CONSTATS ET PROPOSITIONS

1 - L'organisation des secours

Les alertes lancées par la Fédération nationale des sapeurs-pompiers de France sur le système de secours à personne en France[5] et notamment sur les problèmes de terrain rencontrés dans la coordination des secours et dans la chaîne Secours à victimes – Accueil aux urgences (SAU) méritent une attention soutenue des pouvoirs publics.

Une concertation est actuellement engagée. Nous espérons qu'elle puisse aboutir à une meilleure répartition des rôles entre les besoins médicaux qui peuvent être assumés par le système de santé « normal » et un traitement plus efficace des réelles urgences permettant aux dispositifs de se concentrer sur leurs missions et surtout de dégager les marges nécessaires à la préparation aux situations catastrophiques qui est, à notre sens, insuffisante dans le cadre des risques et menaces définis au chapitre I.

Sur le plan de la coordination, il n'y a pas assez de plates-formes communes pour la gestion des appels d'urgence, voire des centres de gestion opérationnelle communs entre services (Police/Gendarmerie/Sapeurs-pompiers/SAMU) en France. Cela devrait être une priorité à la fois en matière d'économie, de qualité et de mutualisation de moyens, qui seule permettra la mise en place du 112 dans des conditions de satisfaction optimale, notamment lorsqu'un service de traduction nationale spécialisé (sur les 23 langues officielles de l'Union européenne) sera mis en place, l'État pourrait jouer dans ce cadre un rôle pour lancer un PPP sur cette thématique. Par ailleurs, il devrait inciter les départements à réaliser ces plates-formes dans le cadre d'un programme ambitieux et coordonner techniquement pour permettre une totale interopérabilité. La question du bon échelon départemental ou régional pour de telles plates-formes peut d'ailleurs se poser…

La doctrine d'organisation des secours face aux accidents collectifs est maintenant structurée au travers du dispositif ORSEC et, toujours, des plans de défense (famille des plans Pirate notamment), qui subsistent. Mais une clarification entre tous ces plans et une

harmonisation autour du dispositif ORSEC restent à concevoir pour accroître la simplicité et l'efficacité dans la mise en œuvre des mesures d'urgence et des protocoles de déclenchement de plans associés.

2 - Les secours spécialisés et l'échelon zonal

Les secours spécialisés sont liés de plus en plus à la nature des risques tels qu'ils sont ressentis aux niveaux locaux. La planification des ressources et les budgets associés sont donc logiquement liés à la réponse aux risques territoriaux inventoriés sur les SDACR (démarche sapeurs-pompiers) et sur les SROS (Schémas Interrégionaux d'Organisation Sanitaire) pour la démarche soins d'urgence.

Le problème se pose sur les grands risques à très faible occurrence (risques industriels, naturels majeurs) ou les risques liés au terrorisme, notamment NRBC. Les Conseils généraux estiment que la prise en compte de ces risques et menaces relève exclusivement du niveau national.

Or, la capacité nationale de réponse demeure « modeste » vis-à-vis de nombreuses situations graves, notamment face aux menaces NRBC. Sur ce plan, les moyens nationaux sont répartis entre de nombreux acteurs : UIISC, moyens de la gendarmerie, du CEA, du ministère de la Défense… et la mobilisation de ces moyens sur des situations réelles serait assez longue.

Il manque très clairement un niveau d'intervention zonal plus conséquent et plus proche pour la prise en compte de ce type de situation. Entre les moyens locaux, encore trop peu formés et les moyens nationaux, forcément longs à mobiliser, des moyens zonaux financés par l'État et par les collectivités de la zone (départements et régions) pourraient assurer la liaison entre le niveau local et le niveau national.

Pour animer ces moyens zonaux de renforts, « les réserves » (police, gendarmerie, sanitaires, de sécurité civile) et associations de protection civile agréées, pourraient, au niveau et sous le contrôle des EMZD (fusionnés avec les EMIZD), jouer un rôle de moyens humains de « renforts » dans les centres opérationnels lors de

crises « longues », mais aussi d'animation sur les exercices. Il faut néanmoins, pour mettre en œuvre cette politique, avoir les moyens de coordonner et de faire vivre ces réserves qui, pour certaines, n'existent que sur le papier, ou ne sont employées que sur les missions de leurs administrations de rattachement.

La problématique des renforts et de l'échelon zonal vaut également pour les risques sanitaires graves (pandémies provoquées ou non), qui nécessitent, compte tenu des impacts potentiels, des dispositifs de réponse lourds qui pourraient toucher la totalité du territoire, donc *a priori* des réponses à concevoir sans le soutien de renforts nationaux. Sur ce plan, un travail d'exercices combinant les plans zonal, régional, départemental et local, et sur une base régulière, reste à faire.

De manière générale, la notion de crise « longue », comme le serait une pandémie grippale, est encore insuffisamment travaillée par les services de sécurité et de secours, tant sur le plan de la planification de terrain que sur celui de la gestion de crise.

La contribution des forces armées au dispositif de crise (ORSEC) nécessite peut-être encore une plus grande autonomie des échelons zonaux par rapport aux autorités d'emploi nationales, pour être capable de répondre, tant au quotidien que face à l'exceptionnel, aux demandes des autorités civiles.

Le dispositif ORSEC comprend un volet « décès massifs », à la suite de l'épisode caniculaire de l'été 2003, qui nécessite une organisation à l'échelle nationale et départementale juxtaposée aux différents niveaux d'autorité publique. Cette organisation doit être créée indépendamment des structures syndicales professionnelles qui n'ont pas de vocation opérationnelle. Cette organisation en réseau devra répondre aux critères de reconnaissance officielle des associations de bénévoles intégrées aux dispositifs de défense civile.

FOCUS

Le domaine NRBC et les grands attentats urbains

Sur le domaine NRBC, il convient de retravailler les dispositifs pour optimiser la **prise en charge de très nombreuses victimes**. La nouvelle directive 700 va dans ce sens, mais un travail plus important de réorganisation et de dotation de moyens reste à entreprendre, notamment en matière d'assistance respiratoire pour les sauveteurs et d'outils de gestion de l'intervention. Le problème demeurant parfois la simple capacité de grands corps urbains à stocker en « centre ville » des matériels lourds (chaîne de décontamination, équipements spécialisés) dans un environnement où les surfaces de stockage coûtent extrêmement cher. Or dans ce type d'intervention, la rapidité est un facteur clé de la réussite opérationnelle. Des normes globales d'intervention doivent donc être édictées sur ce type d'intervention, elles entrent totalement dans la démarche capacitaire.

Des **efforts notables de R&D** sont à développer sur les concepts techniques liés à la prise en charge de très nombreuses victimes, contaminées ou non, ainsi que sur les modes de détection et de décontamination NRBC/E. L'effort sur ces points précis demeure aujourd'hui encore très limité.

La question de l'**arrêt des transports urbains** suite à des attentats multiples ou NRBC est un sujet sensible où la vision des autorités n'est pas toujours la même que celle des opérateurs de transports et peut varier d'un pays à l'autre. L'arrêt de transports en cas d'attentat est certes une précaution compréhensible pour éviter d'autres actions qui seraient en cours, mais faute de renseignements avérés, cet arrêt ne peut être que de courte durée pour des levées de doute très rapides. Car l'arrêt des transports peut à notre sens être aussi défavorable que favorable.

La réalisation d'autres actions dans une foule compacte à l'extérieur est un danger permanent et cet arrêt peut considérablement et durablement ralentir les opérations de circulation des secours en surface, sans compter les problèmes de relève des personnels de santé ou de sécurité qui habitent généralement en banlieue. Le coût avantage/efficacité d'une telle mesure doit être bien pesé tant au plan technique que politique.

La problématique de l'évacuation d'un quartier ou d'une ville doit également faire l'objet d'une planification plus poussée qu'actuellement. Les plans de circulation et les axes réservés ne sont pas suffisants pour prendre en compte l'évacuation d'un ou deux arrondissements d'une ville comme Paris, Marseille ou Lyon, il faut des outils de planification et de gestion d'une autre nature. Une réflexion est à mener dans ce sens.

Le confinement d'urgence des populations est la première mesure réflexe à prévoir en cas de menace NRBC. Pour être efficace, l'ordre de confinement doit être audible en tout lieu et bien évidement compris et suivi par les populations.

Sur le plan sanitaire, il convient de poursuivre, d'achever et d'entraîner les hôpitaux et établissements de santé à finaliser et mettre en œuvre les plans blancs élargis dans les délais les plus brefs et de poursuivre la formation des cadres de santé aux situations exceptionnelles et notamment NRBC. Il convient également de maintenir et poursuivre l'effort réalisé pour doter le pays de stocks stratégiques de santé publique.

L'effort entrepris sur la prise en compte immédiate des **troubles psychiques** des victimes et impliqués suite aux catastrophes, et pour lequel la France est particulièrement reconnue dans le monde, est à poursuivre, en augmentant notamment les effectifs et les moyens (capacité de projection) des cellules d'urgence médico-psychologiques départementales.

3 - Les renforts nationaux et l'échelon européen

Ils sont constitués en France des unités militaires de la sécurité civile, des unités de renforts des départements (colonnes), de moyens nationaux spécialisés militaires et civils (CEA, Santé, etc.).

Dans ce cadre, face à des scénarios complexes et mouvants, et du fait de la multiplicité des acteurs, il manque une réelle vision capacitaire des secours nationaux face à tous les scénarios de crise : terrorisme, prise en charge de nombreuses victimes, sauvetage déblaiement, menaces NRBC, etc.

Comme le font les Britanniques, il conviendrait, par type de scénario, de déterminer quelles sont les capacités de réponse à l'échelon départemental, zonal, national et européen et, en fonction de la nature de l'événement, de prendre en compte les niveaux de renforts et d'organisation suivant les plans les plus adaptés.

Concernant les moyens spécialisés en général, on note souvent une difficulté à renouveler, dans les budgets existants, les matériels ou les consommables pour conserver des capacités antérieurement acquises ; c'est un problème récurrent : une fois l'investissement fait, les crédits de fonctionnement ne sont pas toujours budgétés aux bons niveaux.

Sur le plan sanitaire, la création de l'EPRUS[7] est une nouveauté dont l'expérience sera riche d'enseignement. Des concepts équivalents seraient-ils possibles dans d'autres ministères pour permettre d'accroître la flexibilité, l'efficacité au moindre coût et l'ouverture dans des partenariats public-privé pour apporter des réponses nouvelles à la gestion des situations exceptionnelles, la question reste ouverte.

Une réflexion sur la logistique des grandes catastrophes et surtout sur la mutualisation des logistiques civiles et militaires (stocks, entrepôts, moyens de transport, plans de transport) face aux situations d'urgence d'ampleur (y compris au travers de partenariats public-privé) reste à penser. Les moyens logistiques actuels sont encore très éclatés et peu coordonnés entre ministères (Intérieur, Santé, Défense), des gains d'efficacité et de productivité sont certainement réalisables.

Au plan européen, l'accueil de nombreux sauveteurs, parlant une langue étrangère, ayant des besoins d'information et de commandement est un exercice peu joué[8]. Or si l'on veut développer une capacité européenne de protection civile, la nécessité de communication et d'interopérabilité entre acteurs est primordiale de manière générale. Là encore, de gros efforts restent à entreprendre et des formations particulières, ainsi que des postes d'attachés de sécurité civile dans les pays européens, restent à promouvoir.

La création d'un collège européen de défense et de protection civiles est une proposition que la France pourrait faire lors de sa présidence du Conseil de l'Union européenne.

RAPPEL DES PROPOSITIONS

• Créer une nouvelle mission transverse « défense civile » dans la LOLF, qui pourrait être scindée en trois missions, hors missions de police et de sécurité publique : protection civile, protection sanitaire et protection environnementale, rattachées aux trois ministères compétents : Intérieur, Santé et MEDAD.

• Rétablir et augmenter notablement les crédits d'État pour la défense et la sécurité civiles, notamment le FAI, pour faire face aux risques et menaces aux conséquences exceptionnelles.

• Harmoniser « plans de défense » et dispositif « ORSEC » dans une doctrine unique pour optimiser, dans cette démarche capacitaire, les différents moyens de renforts zonaux et nationaux.

• Déterminer une approche capacitaire des secours locaux, zonaux, nationaux, aptes à faire face à des scénarios « types » en matière de grands risques ou menaces NRBC, sanitaires, naturels et technologiques.

• Revoir les échelons administratifs de coordination, de planification et de financement de programmes face aux situations exceptionnelles. Régions et zones permettraient de mieux atteindre la masse critique nécessaire en termes d'équipements (salles opérationnelles et de gestion de crise, équipements spécialisés, personnels de planification, gestion des réserves etc.) pour optimiser la réponse opérationnelle.

• Lancer un programme national de plates-formes de centres d'appels 15-18-17-112 au niveau départemental, voire régional.

• Lancer en PPP[9] une plate-forme nationale d'appels de traduction 24/24-7/7 en 27 langues pour les situations d'urgence et l'implémentation effective du 112 en France.

• Retravailler les domaines d'intervention NRBC, les plans d'évacuation et les dispositions connexes, tel l'arrêt des transports dans les grands centres urbains, en s'appuyant sur des études d'impact externes à l'administration et le RETEX des événements étrangers.

→

• Poursuivre et développer l'implémentation de technologies essentielles, notamment NRBC, spatiales, d'interopérabilité et de gestion de crise pour mieux appréhender la gestion des risques et la réponse aux situations d'urgence.

• Améliorer la formation des acteurs de la gestion des situations d'urgence, notamment dans le domaine NRBC, et de la gestion de crise, y compris les réservistes.

• Poursuivre l'effort réalisé pour doter le pays de stocks stratégiques de santé publique (masques, vaccins, antidotes…)

• Réfléchir sur un meilleur partage des capacités logistiques entre ministères pour atteindre des capacités de stockage et de projection optimisées, examiner des solutions de PPP[9] sur ces problématiques.

• Mettre en place des dispositifs (réserves et exercices) aptes à recevoir et suivre des forces de protection civile étrangères qui arriveraient en France en cas de catastrophe majeure.

Notes du chapitre IV

1- Pour 2008, le budget « Sécurité civile » reste modique avec 418 millions d'euros pour la mission sécurité civile et 900 millions d'euros pour la politique transverse de sécurité civile. Budgets en baisse depuis plusieurs années consécutives à - 2,2 % pour 2008, et une baisse très importante du fonds d'aide à l'investissement (FAI) pour les SDIS sur les équipements et programmes spécialisés : en millions d'euros : 67 en 2006, 37,5 en 2007 et seulement 28 en 2008.
2- Le budget primitif des SDIS pour 2008 est évalué à 5 milliards d'euros en 2008 contre 4,2 en 2006.
3- Discours de M. le Président de la République, 114e Congrès national des sapeurs-pompiers, 28 septembre 2007.
4- Le groupe du futur rassemble l'ensemble des ministres de l'Intérieur de l'Union européenne en charge des questions de protection civile.
5- 64 % de l'activité des SDIS en France.
6- (PREVIEW, RISK-EOS, BOSS4GMES, SAFER).
7- Établissement de préparation et de réponse aux urgences sanitaires.
8- Les événements de Grèce de l'été 2007 ont montré la difficulté d'intégrer des équipes étrangères dans des dispositifs locaux non préparés.
9- Partenariat Public-Privé.

CHAPITRE V

Infrastructures vitales et continuité de l'action gouvernementale et économique

INTRODUCTION

La sécurité dans l'entreprise répond à des préoccupations multiples, comme la protection des salariés et des populations environnantes, celle de l'outil de production, des investissements, du savoir faire, ou encore des informations sensibles et stratégiques.

L'ensemble est généralement regroupé sous le vocable de la protection du patrimoine de l'entreprise, comprenant le patrimoine humain, matériel et immatériel ou informationnel. Il s'agit de prévenir et d'agir contre les actes de malveillance quels qu'ils soient. Si le périmètre de la plupart de ces domaines est encadré par un dispositif réglementaire cela n'est cependant pas systématiquement le cas.

Souvent, les opérateurs privés, conscients des risques encourus, n'ont pas attendu l'existence d'une réglementation pour prendre les mesures qui s'imposaient afin de préserver le fonctionnement de leurs activités.

Aujourd'hui, les opérateurs privés représentent une part majeure des infrastructures vitales nationales (banques et institutions finan-

cières, réseaux de télécommunications, production d'énergie, équipement et transport…).

C'est dire l'importance et la complexité de ce secteur dès lors que l'on se penche sur la problématique de protection et de continuité de l'activité en cas de crise grave.

SÉCURITÉ DES INFRASTRUCTURES D'ACTIVITÉS D'IMPORTANCE VITALE (SAIV)

1- Un nouveau rapport « État Entreprises »

La démarche nouvelle de l'État, typiquement lancée par le décret du 23 février 2006 (SAIV) et la rédaction des directives nationales de sécurité (DNS), semble être de développer une vision d'ensemble et un meilleur contrôle des mesures à mettre en place par les opérateurs.

Elle ne doit pas s'affranchir des dispositifs propres qu'ont pu initier nombre d'opérateurs, pour certains depuis longtemps et de façon aboutie, mais au contraire les intégrer.

Cependant, ceci représente une difficulté réelle qu'il convient d'appréhender avec soin car, bien que le niveau atteint par les opérateurs soit hétérogène, la maîtrise acquise par certains est conséquente, en particulier les grands groupes confrontés en France comme à l'étranger à des menaces diverses et aujourd'hui croissantes.

Il est aussi important que les limites de compétence et le rôle de chacun (opérateur, État et État-opérateur) soient clairement identifiés, sans ambiguïté et que chacun n'ait à supporter effectivement que les exigences qui relèvent de sa compétence propre.

En effet, si, pour l'État, la sécurité est un objectif en elle-même, elle représente d'abord pour l'entreprise une condition nécessaire à la bonne exécution de son activité. L'entreprise se développe dans un environnement où l'imprévisible doit être aussi réduit que possible. Les facteurs d'insécurité de tous ordres sont un frein à son activité.

Les opérateurs privés, conscients des menaces actuelles et possibles, s'engagent donc dans une action volontaire afin de créer, en amont et avec l'État, les conditions d'une véritable osmose public-privé génératrice, pour eux, d'obligations mais aussi de droits.

2 - Construire un véritable partenariat public privé élargi

La démarche entreprise afin d'améliorer la sécurité des infrastructures vitales ne doit pas se limiter aux grands opérateurs ; elle doit aussi intégrer les entreprises petites et moyennes, entités dont les échanges avec les grands groupes impliquent nécessairement une intégration de la problématique de sûreté qui passe par une approche culturelle nouvelle.

Dès lors, il apparaît qu'un des facteurs clés de succès du dispositif, qui doit être mis en place pour préserver ces secteurs d'activités des menaces identifiées aujourd'hui et de celles à venir, repose sur un partenariat étroit et constructif entre l'État et les opérateurs privés.

Il est aussi important que ce partenariat puisse générer une réelle plus-value par rapport à l'existant et ce, quel que soit le niveau de maîtrise de la sûreté atteint par les opérateurs concernés. Ainsi donc, l'ensemble de chaque secteur doit être associé à cette démarche.

En outre, l'approche territoriale est aussi déterminante : l'intégration des entreprises périphériques et locales, qu'elles soient identifiées ou non comme infrastructures vitales, fait partie intégrante de l'évaluation du risque de proximité, afin de réduire le risque d'effet « dominos ».

3 - Bien définir les rôles de chacun

D'autre part, la responsabilisation des opérateurs face à l'ensemble des menaces actuelles auxquelles s'ajoute aujourd'hui le terrorisme, nécessite le plein soutien étatique.

Ce soutien passe par la préparation des hommes, fonctionnaires de l'État et industriels, par une assistance technique dans la pré-

vention des malveillances : visibilité sur les intervenants sur les sites, les sociétés de conseil, les sous-traitants et consultants divers, et par l'échange d'informations de sécurité portant sur les menaces visant le site et son environnement géographique.

Le rôle de l'opérateur consiste bien à prendre des mesures de prévention et de gestion du risque interne : détecter, retarder un acte de malveillance ou empêcher qu'il soit commis.

Il s'agit pour l'État, à l'extérieur des infrastructures des opérateurs et dans leur environnement immédiat ou plus lointain, d'assurer la sécurité et de prévenir les malveillances.

D'une manière générale, il est nécessaire de rechercher la participation de tous à l'élaboration des mesures capables de contrer les malveillances possibles, de s'inscrire dans une logique constructive et de dépasser le cadre archaïque du rapport « décideur et exécutant », c'est-à-dire s'inscrire dans des logiques de résultats et non plus de moyens.

4 - Proposition de mesures concrètes

- Un dispositif élargi et une confidentialité « contrôlée »

La mise en place des mesures SAIV doit, d'une part, rester dans le domaine de ce qui peut être raisonnablement exigé d'une entreprise et, d'autre part, faire partie d'un dispositif plus large instaurant une coopération et une collaboration permanentes avec les pouvoirs publics. Ce dispositif devra se construire autour :

- d'une connaissance stable et permanente des responsables et des décideurs ;

- d'un mode d'information adapté permettant la prévention, ainsi que des échanges permanents ;

- d'un travail de préparation des mesures, à effectuer en commun ;

- d'une gestion de crise claire, doublée de priorités adéquates pour contourner ou alléger les restrictions éventuelles ;

- d'une démarche réaliste concernant les Plans de Sécurité Opérateur, et conservation par les acteurs ayant un strict « besoin d'en connaître ».

- Élaborer des objectifs de sécurité adaptés, guidés par une logique d'obligation de résultat

Les directives nationales de sécurité vont s'inscrire dans le périmètre de standardisation de la sécurité des infrastructures critiques internationales. Une veille des évolutions de ces normes s'avérera nécessaire afin de protéger les investissements consacrés à ce secteur.

En effet, l'effort financier et d'organisation consenti par les opérateurs nationaux vis-à-vis des réglementations, et dans un contexte d'économie mondialisée, ne doit pas se traduire par un handicap concurrentiel.

Il s'agit peut-être là encore d'une modification de l'approche culturelle où la combinaison des exigences réglementaires de l'État pourrait se décliner à l'aune des intérêts industriels et des possibilités des opérateurs.

Le décret SAIV accentue l'importance de la protection contre les agressions « externes » (protection des sites) et introduit aussi une notion nouvelle, du moins chez certains des acteurs du système économique et financier, à savoir, la vigilance vis-à-vis des personnels extérieurs à l'entreprise, prestataires ou autres, qui interviennent en son sein, sur des fonctions lui permettant d'accéder à l'ensemble des installations (prestations de gardiennage, de nettoyage, de maintenance des équipements, etc.).

La mise en œuvre de mesures pertinentes répondant à ces deux aspects de la prévention ne peut être prise en charge par les entreprises et gérée par ces dernières que s'il existe une étroite collaboration avec la puissance publique.

Les aspects juridiques et réglementaires qui concernent alors ces échanges d'information doivent aussi faire l'objet d'études précises et la législation être adaptée autant que de besoin. Il faut aussi tenir compte de l'évolution technologique des moyens de sécurité : biométrie, vidéosurveillance analogique ou numérique, interconnexion des réseaux.

La protection des bâtiments contre les menaces exogènes relève traditionnellement de la puissance publique, alors que la responsa-

bilité de chaque opérateur ne concerne véritablement que l'emprise territoriale de ses infrastructures.

Mais une bonne prévention des malveillances demande à pouvoir détecter la menace plus en amont. Il convient alors pour ces secteurs d'activités d'élaborer les processus et d'apprendre une nouvelle manière d'aborder la protection, en liaison avec l'ensemble des acteurs concernés.

RÉSILIENCE ET CONTINUITÉ DE L'ACTIVITÉ ÉCONOMIQUE

1 - Une incontournable préparation en amont

Les enjeux de la résilience et de la continuité économique consistent, en cas de crise, d'une part à maintenir une activité aussi proche de la normale que possible et d'autre part à rétablir rapidement le niveau de service et d'activité à son niveau initial.

La priorité, en matière économique et financière, doit être donnée à la gestion de la liquidité (paiements, prêts à court terme, garanties). Il est également fondamental de travailler sur la continuité des équipements des transports et de la circulation pour éviter de briser les échanges et les opérations industriels et commerciaux à flux tendus.

Au-delà de la continuité d'activités de chaque acteur, vient donc s'ajouter la notion de continuité d'ensemble. Les opérateurs participent tous d'un même système global et la résilience de leurs processus dépend de la résilience des infrastructures et des prestataires dont dépendent ces mêmes processus.

Il convient tout d'abord de rappeler que la responsabilité civile et pénale de la société et du manager est aussi engagée en matière de sécurité et de sûreté.

2 - Une formation commune et partagée des acteurs publics et privés

- Le management des entreprises doit aujourd'hui intégrer le fait que la fonction de sécurité-sûreté et le management des risques en général font partie de l'ensemble de ses missions.

- C'est ainsi que les managers doivent être au plus tôt sensibilisés et formés à ces fonctions et à la gestion de crise « classiques » et d'événements « hors norme ». Ces processus de formation devant faire l'objet de certification.

- Il leur revient d'initier et d'animer les structures qui, au sein de leurs entreprises, ont en charge ces problématiques.

- Plus en amont encore, la diffusion de « l'esprit de sûreté » et la responsabilité individuelle en cas de catastrophe doivent être intégrées dans les cursus scolaires et de formation.

- Sur le plan technique, les entreprises doivent généraliser les « bonnes pratiques » en s'appuyant sur la complémentarité et la transversalité des préparations techniques : scénarios, exercices, plans de continuité, ceci en partageant entre opérateurs et secteurs d'activité l'expérience acquise (RETEX).

- Au-delà de cela, il convient d'améliorer les liens entre acteurs étatiques et privés, entre acteurs majeurs et petites structures, et de développer une vision large de l'entreprise dans son environnement.

3 - L'État doit assurer une coordination renforcée permettant de gérer les interdépendances entre secteurs d'activités

Ce modèle nouveau de partenariat doit s'appuyer sur l'incontournable coordination par l'État des mesures nécessaires à l'organisation au sein de chaque secteur d'activités, mais aussi sur la capacité à gérer les interdépendances entre les différents secteurs. Les opérateurs participent tous d'un même système global et la résilience de leurs processus dépend de la résilience des infrastructures et des prestataires dont dépendent ces mêmes processus.

Une problématique qui n'est pas réglée dans le domaine de la continuité d'activité des entreprises appartenant aux secteurs d'activités d'importance vitale est leur compétence à assurer, par le biais de la médecine du travail, la prophylaxie ou le soin rapide de leurs collaborateurs essentiels en cas de risques sanitaires graves (pandémie grippale, attaques biologiques…).

Une réflexion dans le cadre spécifique du SAIV sur une dérogation au droit commun concernant le stockage et la distribution de produits de santé : antiviraux, médicaments… (et non l'emploi qui resterait du domaine « étatique »), au sein des entreprises, sous le contrôle de médecins et pharmaciens appartenant à la médecine du travail, est à penser pour rendre le dispositif de résilience globale plus efficace.

Enfin, une préparation commune et la réalisation effective d'exercices associant plusieurs secteurs et les acteurs étatiques constituent des facteurs clés de succès en cas d'incident grave ou de crise majeure.

Par ailleurs, dans une logique de partenariat public-privé, qui semble aujourd'hui nécessairement s'imposer, une réflexion sur les enjeux et le financement de l'ensemble de ces mesures s'avère incontournable et il faut aussi réfléchir, pour les opérateurs, à des mesures fiscales incitatives.

Ainsi les mesures demandées par l'État doivent faire l'objet d'une évaluation ou étude d'impact en termes de faisabilité et de coût associé.

4 - Le bon niveau de coordination territoriale

Dans ce cadre-là, les états-majors de zones de défense occupent une position particulière qu'il convient de souligner, permettant un niveau de coordination approprié entre les services déconcentrés de l'État et les opérateurs (nationaux ou départementaux) et plus généralement le secteur privé.

Il s'agit donc, compte tenu de cette pertinence, de renforcer leurs compétences et moyens et d'en faire des acteurs majeurs afin d'accroître leur efficacité et leur capacité de gérer le retour à « la normale », car les situations complexes appellent des approches interdisciplinaires.

RAPPEL DES PROPOSITIONS

• Partager les informations sur les menaces et les risques au travers d'un process d'information nationale et territoriale basée sur des conférences régulières organisées par le ministère de l'Intérieur et les préfectures de zone.

• Contrôler les embauches sensibles : mise à disposition de la part de l'État d'informations ciblées au travers d'un processus officialisé, respectant tout à la fois les exigences opérationnelles et les libertés publiques, lors de recrutements sensibles.

• Créer par l'État des standards et des labels pour les entreprises fournisseurs de sécurité-sûreté en matière de conseils, audit, prestataires etc. pour les opérateurs entrant dans le cadre « SAIV ».

• Créer des réseaux permanents et institutionnalisés (géographiques et/ou sectoriels) pour le soutien des entreprises à l'étranger (analyses thématiques par les services de l'État, renseignements ciblés…).

• Mettre à disposition des standards techniques ou des raccordements de moyens de communication de crise – par exemple, permettre le raccordement des PC de crise des entreprises aux réseaux Antares-Acropol (accès sélectifs) ou aux messageries de crise.

• Reconnaître par l'État le statut de collaborateur privilégié et/ou occasionnel aux responsables sécurité-sûreté des entreprises. Établir des documents officiels spécifiques permettant au porteur de faire reconnaître sa qualité en temps de crise.

• Faire participer les entreprises aux cellules de crise interministérielles locales ou nationales, lors des exercices et en cas de crise, du type de la pratique mise en place par le ministère des Affaires étrangères.


Haut Comité Français
pour la Défense Civile
Protéger l'avenir...

CHAPITRE VI

Recherche et Technologies

CONSTAT

1 - À l'échelle nationale

Plusieurs structures traitent aujourd'hui l'expression des besoins de sécurité civile et mettent en place un certain nombre de projets de R&D. Au niveau interministériel, le SGDN coordonne et met en œuvre des décisions gouvernementales, en particulier dans le cadre de comités de pilotage interministériels destinés à effectuer un pilotage (programme interministériel de R&D NRBC, par exemple) ou à faire remonter les priorités de R&D pour l'ANR et le PERS. En parallèle, certains besoins sont directement portés par les ministères qu'ils soient civils (ministères de la Santé, de l'Intérieur, de l'Agriculture…) ou de défense (EMA, DGA).

De nombreux projets de R&D sont portés par des organismes publics de recherche (CEA, INSERM, Institut Pasteur, INERIS, CNRS, ONERA, CNES, Universités…) pouvant selon le cas être en partenariat avec les industriels français du domaine, ou par des industriels eux-mêmes. À titre d'exemple, on peut citer des programmes nationaux de recherche amont tels que le programme

interministériel de R&D NRBC lancé en 2005 au CEA et piloté par le SGDN, le programme de l'ANR CSOSG depuis 2006 ainsi que des programmes de recherche technologique associant des industriels (ex. des pôles de compétitivité SYSTEM@TIC, SCS, Gestion des Risques et Vulnérabilités des Territoires…). En parallèle, la Défense lance des actions destinées à couvrir ses besoins spécifiques dans le domaine NRBC (PEA PERSEIDES, par exemple).

Toutefois, il n'y a pas en France une autorité unique de référence ayant les pouvoirs et les moyens suffisants lui permettant de conduire une réflexion sur une expression globale des besoins, leur hiérarchisation ainsi qu'une définition des performances minimales à atteindre, une analyse capacitaire et une définition des orientations à prendre pour structurer l'effort de R&D.

2 - À l'échelle européenne

Il existe également plusieurs initiatives de R&D qui ont été lancées par la Commission parmi lesquelles on peut citer le Programme européen de recherche en sécurité (PERS) lancé en 2007 (budget 1.4 milliard d'euros sur 2007-2013) qui a succédé à des actions préparatoires de recherche en sécurité (PASR) lancées sur la période 2004-2006 et qui s'appuie sur des structures de réflexion telles que l'ESRAB et maintenant l'ESRIF.

Ces initiatives mobilisent fortement la communauté scientifique et industrielle en raison des budgets envisagés et de la possibilité de valoriser des technologies de sécurité par ce moyen-là. Toutefois, ces initiatives sont extrêmement diverses et sans cohérence globale puisque les différentes directions (DG JLS, DG Recherche…) lancent en parallèle des appels à projet intégrant des aspects sécuritaires, et souvent sans concertation avec les États membres.

Par exemple, la Commission a lancé plusieurs actions de réflexion en vue de préparer une expression des besoins tels que les Livres verts sur la préparation à la menace biologique (2007), les technologies de détection (2006) ou une politique maritime de l'Union (2006).

FOCUS

Le programme interministériel de R&D NRBC

À la suite des événements du 11 septembre 2001, un groupe de travail interministériel animé par le SGDN, auquel a participé le CEA, a permis d'élaborer une première expression des axes de R&D pour répondre aux besoins, en particulier opérationnels, des acteurs de la lutte antiterroriste.

Cette analyse a débouché sur la mise en place du programme interministériel de R&D NRBC qui a été confié au CEA. Ce programme a été lancé sous l'égide du SGDN au printemps 2005, avec une gouvernance basée sur une cellule exécutive mixte CEA–DGA, un comité de pilotage interministériel incluant tous les ministères concernés (recherche, santé, transports, intérieur, défense, agriculture, MEDAD) et un conseil scientifique.

Le programme regroupe tant des actions de recherche amont que des développements finalisés en vue de disposer de briques technologiques nécessaires à la mise au point de moyens de détection de matière R/N, de toxiques chimiques, d'agents biologiques et d'explosifs, de dosimétrie opérationnelle, de réhabilitation (décontamination) ainsi que d'intervention (moyens thérapeutiques et prophylactiques). Le CEA a proposé une démarche de projet fondée sur des jalons identifiant clairement les progrès réalisés à partir de démonstrations technologiques.

Le positionnement du CEA dans la recherche NRBC se situe dans la continuité des lignes d'action déjà engagées, que ce soit dans le domaine de la lutte contre la prolifération ou de l'intervention nucléaire liée aux menaces terroristes. De plus, le programme de recherche est mené en cohérence avec les actions engagées par le ministère de la Défense au travers de la cellule exécutive CEA-DGA.

Le programme a pour objectifs principaux de développer de nouvelles méthodes sur les volets détection-intervention-réhabilitation, en mettant à profit les compétences et l'expertise de l'ensemble des pôles du CEA, et en faisant appel en tant que

de besoin aux compétences du tissu national de la recherche académique (Institut Pasteur, IRSN, CNRS, INRA…). Les moyens financiers annuels affectés au programme NRBC proviennent de la subvention du CEA au titre de la recherche duale (programme 191 de la LOLF) et permettent de mobiliser l'équivalent annuel de plus de 100 chercheurs.

Les travaux scientifiques ont permis de disposer de premières briques technologiques dans le domaine de la détection et de l'identification d'agents et d'identifier des voies de recherche les plus prometteuses. À ce titre, parmi les travaux réalisés, les points les plus marquants concernent :

• Le développement d'une balise de détection radiologique d'objets en mouvement, couplée avec une surveillance vidéo, testée sur piétons et véhicules ;

• L'obtention des premiers réactifs (anticorps, antigènes, oligonucléotides…), la mise au point de tests pour la détection de toxines et le diagnostic biologique ainsi que le développement des premiers tests de criblage d'inhibiteurs dirigés contre ces toxines et un virus ;

• La réalisation des premiers prototypes de laboratoire sur puces démontrant la faisabilité de la détection de pathogènes, fonctionnant soit sur le mode immunologique (immunopuces), soit sur le mode d'amplification de segments d'ADN (Polymerase Chain Reaction) ;

• Le développement de capteurs de détection chimique adaptés aux toxiques industriels (chlore, ammoniac, acide fluorhydrique) ou aux explosifs chimiques (TNT, TATP) ;

• La faisabilité de la décontamination biologique d'une surface par la formulation de gels spécifiquement conçus pour dégrader les agents pathogènes présents.

Les travaux actuels conduisent à l'obtention de délivrables représentatifs d'un niveau de maturité technologique de type TRL 4 (démonstration de laboratoire).
Les perspectives de transfert technologique s'appuieront nécessairement sur des travaux de développement menés hors du programme NRBC et conduisant d'une part à des

niveaux de maturité technologique supérieurs (TRL 6-7) et d'autre part à une étude de l'intégration des briques technologiques dans une vision système.

En ce qui concerne la répartition thématique du programme, la composante Biologie apparaît comme prépondérante, justifiée à la genèse du programme en 2005, par une forte expression de besoins dans ce domaine, compte tenu du retard national dans le domaine des parades disponibles vis-à-vis des agents de la menace considérés. Les évolutions scientifiques devront nécessairement prendre en compte l'évolutivité des menaces tant dans le domaine biologique (agents émergents, biotechnologies…) qu'en lien avec les événements récents (attentats de Madrid et Londres, trafic de matières nucléaires, attentats au chlore en Irak…). La force de proposition du CEA sur ces thématiques a permis d'ores et déjà d'engager en particulier une intensification des travaux liés à la menace des explosifs et du nucléaire/radiologique.

LES BESOINS

1 - Une approche globale

La Sécurité globale passe par une approche systémique et non pas par une approche analytique, d'où la nécessité de modifier nos modes de pensée et d'établir une véritable expression des besoins et des exigences. Cela impose :

- une redéfinition des risques et une hiérarchisation au regard de la vulnérabilité,
- une définition des niveaux de performance à atteindre,
- une identification des solutions technologiquement applicables ou déployables,
- une identification des manques,
- une *road map* (feuille de route) de la recherche technologique,
- une réflexion sur les logiques « système » à mettre en place tant dans le domaine de la sécurisation de grandes infrastructures que dans celui de l'intervention.

Cette expression des besoins permettrait de définir les niveaux de besoins et de capacité à concevoir aux plans local, national, et européen, à ce titre on pourra s'inspirer de la méthodologie des Livres verts de la Commission européenne.

2 - Une démarche capacitaire

La définition d'une démarche capacitaire en matière de sécurité est un élément important de la création d'un concept de sécurité globale. Cette démarche capacitaire doit reposer sur cinq piliers :

1 - La doctrine : Elle exprime comment chaque niveau d'action conçoit et entend conduire les opérations, en cohérence avec les objectifs de niveau supérieur, le contexte et les moyens dont il dispose, à un moment donné.

2 - Les équipements : C'est la réponse concrète aux besoins opérationnels, ces derniers permettant de structurer la démarche conduisant des actions de recherche aux programmes d'équipement.

3 - Les ressources humaines : Elles décrivent l'organisation et la politique de ressources humaines et les niveaux de compétences nécessaires à chaque capacité.

4 - L'entraînement et les exercices : C'est la définition des besoins en matière de formation continue, d'entraînement et d'exercices (éventuellement la création de structures dédiées, de moyens de simulation, de coopérations internationales).

5 - Le soutien : Définition de la politique de soutien, aussi bien du point de vue technique qu'organisationnel.

Cette approche capacitaire sera réellement efficace si on sait associer des opérationnels de terrain, des spécialistes des risques et menaces (ils connaissent l'état actuel et les évolutions des risques et des menaces), des experts scientifiques et techniques (ils peuvent dire l'impact d'un risque ou d'une menace sur l'individu, par exemple en biologie, et s'il existe des solutions pour prévenir, diagnostiquer, soigner…).

Il est donc nécessaire d'identifier, sur les bases définies précédemment, les thématiques prioritaires nécessitant la mise en place de

projets de R&D en y associant les performances à atteindre, les coûts et les délais, cela en partant des besoins exprimés par les utilisateurs.

3 - Les objectifs d'une initiative nationale de R&D en sécurité globale

- Créer un modèle français permettant d'inscrire le domaine de la R&D défense civile dans une démarche capacitaire cohérente face aux enjeux actuels, aussi bien au niveau national qu'européen. Le faire en partant des besoins exprimés par les utilisateurs couplés avec les technologies disponibles et/ou émergentes.

- Dans le contexte de l'approfondissement du lien défense-sécurité, définir une démarche qui soit duale entre besoins militaires et civils en favorisant en particulier les transferts de technologies (civils/militaires…) et les programmes de R&D communs.

- Mettre en place une démarche nationale dans le domaine de la standardisation. À ce titre, l'incitation à participer aux groupes européens et internationaux de normalisation est essentielle ; action qui est très insuffisante actuellement.

- Accroître l'implication de la France dans la réflexion européenne sur les politiques de sécurité, et tout particulièrement en ce qui concerne le développement des technologies associées.

- Coordonner et renforcer les différentes actions engagées et s'assurer de leur cohérence (ANR, pôles de compétitivité, CARNOT, GIS, RTRA…).

- Intensifier les différentes actions engagées au sein des guichets existants (ANR, pôles de compétitivité, CARNOT, GIS, RTRA…) et s'assurer de leur cohérence en renforçant la coordination.

4 - Les principales thématiques d'intérêt

- **Lutte contre le terrorisme NRBC et détection d'explosifs :** développement de nouvelles méthodes de détection/identification utilisables par les personnels d'intervention, les opérateurs sur site et en laboratoire dans l'objectif d'apporter des réponses fiables et rapides. Il y a là un vrai besoin opérationnel, tout particulièrement

au niveau de la levée de doute dans le domaine biologique pour les primo-intervenants ;

- **Détection d'explosifs :** développer des outils de détection d'explosifs (en traces ou en volume) applicables aux personnes (bombes humaines) et aux objets (bagages, fret) ;

- **Sécurisation d'infrastructures :** développer une vision « système de sécurité » intégrant le déploiement de capteurs, le traitement du signal, la gestion d'alerte en réponse à une expression de besoin de sécurité (par exemple, dans le cadre d'une gare ou d'un aéroport).

- **Développement de technologies de « criblage »** : technologies permettant le contrôle en continu d'objets vis-à-vis d'une menace : par exemple explosifs dans les bagages aéroportuaires, drogue ou substances illicites dans le courrier, matières radiologiques ou nucléaires dans les conteneurs… ;

- **Systèmes d'information :** développement de technologies de cryptage, de recherche d'informations complexes et en lien avec des activités illicites sur les contenus du web, de sécurisation de réseaux de données, de sécurisation de systèmes d'information (au niveau des réseaux et des infrastructures sensibles, par exemple) ;

- **Gestion de crise :** technologies de simulation (réalité virtuelle) en vue de la formation et de l'entraînement des acteurs de défense et de sécurité, modélisation de phénomènes de dispersion atmosphérique, utilisation de l'expertise des laboratoires en sciences humaines et sociales ;

- **Renforcer la veille technologique** : dans le domaine de la défense et de la sécurité en s'attachant en particulier à mettre en place une démarche ciblée dans le domaine de l'intelligence économique et stratégique afin d'identifier en particulier les technologies stratégiques au plan national ;

- **Renforcer les partenariats** nationaux et internationaux dans le domaine du renseignement et de l'intelligence économique afin d'adapter de façon proactive les technologies de défense et de sécurité aux menaces actuelles et futures.

NOS PROPOSITIONS

• Définir, peut-être, dans le cadre des missions du futur Conseil de défense et de sécurité nationale, les orientations et les priorités en R&D au regard de l'expression des besoins capacitaires dans le domaine de la défense civile. Identifier dans le cadre d'une mission LOLF les lignes budgétaires associées.

• À l'instar du programme interministériel de R&D NRBC, coordonner, au niveau « global » des besoins civilo-militaires, les programmes de recherche qui déboucheront sur le développement de briques technologiques destinées à être intégrées dans les futurs systèmes spécifiques à chaque type de défense militaire et civile, et à chaque domaine technique étudié.

• Définir et mettre en place, domaine par domaine, une stratégie de mutualisation des actions de R&D au niveau européen en définissant le périmètre des thématiques stratégiques au plan national. Formaliser et engager un programme d'action spécifique dans le domaine de l'intelligence économique et stratégique à cette fin.

• Assurer et garantir la cohérence entre les projets avec les guichets actuels : ANR, pôles de compétitivité, projets européens…

• Utiliser les compétences du domaine SHS (sciences humaines et sociales) pour initier des programmes de recherche spécifiques au domaine de la résilience des organisations afin de définir des guides de conception des nouvelles infrastructures et de management des organisations humaines dans le domaine de la sécurité.

• Engager une démarche proactive dans le domaine de la normalisation et de l'interopérabilité en créant des groupes de travail spécifiques auxquels des objectifs précis seront donnés, participer aux groupes européens (CEN) et internationaux (ISO) sur la normalisation de sécurité au niveau interministériel (et non seulement au niveau des organismes de normalisation français, peu experts du domaine).

• Promouvoir les recherches en sécurité, d'une part au travers d'appels d'offres lisibles en termes d'objectifs technico-opérationnels, et d'autre part par la mise en place d'un mécanisme incitatif de l'innovation dans ce domaine au travers de prix et d'aides ciblés.

• Évaluer la réalisation des projets engagés, notamment par l'établissement d'un rapport annuel (autorité interministérielle) faisant le lien entre les différents niveaux : nationaux, européens et internationaux (USA notamment) sur les avancées réalisées et projets à court et moyen termes.

• Déterminer les indicateurs permettant aux décideurs, aux élus et aux citoyens de mesurer l'impact des actions de R&D sur la réalisation de capacités dans le domaine de la sécurité.

Conclusion

L'effort à fournir pour parfaire la défense civile de notre pays reste encore important. Certes, bien des avancées ont été réalisées, mais de nombreux dossiers restent toujours à parfaire, en particulier sur la réforme ORSEC et sur l'**implémentation à tous les niveaux** de l'ensemble des plans de défense et de sécurité.

Au-delà, quatre dossiers majeurs ne sont pas traités ou le sont insuffisamment à nos yeux pour faire face aux grands risques et menaces auxquels il convient de se préparer :

• **L'alerte et l'information-formation de nos populations pour réagir aux situations de danger et d'exception :**

La formation dans le cadre scolaire est indispensable, elle doit être effectivement réalisée, mais elle ne suffit pas, il faut aborder le sujet au travers de sites dédiés et de campagnes d'information régulières du grand public. Le concept d'autoprotection du citoyen doit être affirmé, et le niveau communal renforcé et aidé dans le cadre d'une protection civile de proximité. La stratégie d'alerte des populations et son implémentation doivent enfin être traitées.

• Les capacités de gestion de crise de l'État et de la formation des gestionnaires de crise :

Les capacités de gestion de crise en termes d'outils techniques tant au niveau central que déconcentré sont insuffisantes pour faire face à des crises réellement majeures. Il faut que l'État se dote des outils de gestion et de simulation nécessaires et accorde plus d'importance au « facteur humain » en insistant sur les formations de gestion de crise à tous les niveaux de l'État et des collectivités décentralisées.

• L'enjeu de l'application de la réforme SAIV

La réforme sur les SAIV a donné à la France une législation très en avance dans ce domaine crucial de la résilience et de la capacité à faire face tant aux risques terroristes majeurs qu'aux problématiques de la continuité d'activité pour les services et fonctions essentielles de la société moderne.

Il faut maintenant s'assurer que cette législation sera bien comprise, appliquée rapidement par les secteurs publics et privés concernés par cette réforme. Cela demande une forte pédagogie, mais aussi certainement une certaine « publicité » sur la démarche et les objectifs au même titre que VIGIPIRATE qui est désormais bien connu du grand public, mais qui nous semble encore faire défaut sur cette avancée réellement essentielle.

Comme tout ne peut pas être entrepris simultanément, il importe que les acteurs étatiques et privés concentrent en priorité leurs efforts de sécurisation sur les infrastructures les plus à risques pour les populations en cas de destruction. Des infrastructures telles que les tunnels de TGV, les barrages, certains stocks ou transports de produits chimiques particulièrement dangereux (chlore, phosgène…) sont encore trop vulnérables à des actions terroristes simples.

• La préparation aux situations de nature NRBC

Elle est encore insuffisante, notamment sur la réponse de terrain avec de très nombreuses victimes (de 1 000 à plus de 10 000…) et dans le domaine des risques biologiques. La complexité de cette

menace impose une réflexion encore plus globale et une intégration des réponses opérationnelles entre les différents niveaux. Cette prise en compte est encore insuffisante, faute de moyens et de financement régulier.

Clarifier le vocabulaire pour clarifier les concepts

Enfin, en conclusion, il nous apparaît nécessaire de « redéfinir » l'ensemble des concepts de défense et de sécurité (global, militaire, civil et économique). L'usage de terminologies proches ou semblables sans définition précise des concepts associés dans de nombreux textes législatifs ou réglementaires a abouti à une grande confusion dans les esprits. Une clarification est désormais indispensable.


Haut Comité Français
pour la Défense Civile
Protéger l'avenir...

ANNEXE I

Contributions des membres du HCFDC

Ont collaboré directement au projet

Dr Jean-Luc ANGOT, Directeur général adjoint, Service administratif et financier OIE (Organisation mondiale de la santé animale)

Mme Delphine ARIAS-BUFFARD, Responsable affaires publiques et marketing, CEDRALIS

M. Vincent BALOUET, Expert, VINCENT BALOUET INNOVATION

M. Augustin BAULIG, Docteur en toxicologie, Officier de réserve, INERIS

M. Pierre BEAL, Directeur général, NUMTECH

M. Jean-Philippe BERILLON, Conseiller sûreté, DG - Mission permanente de sécurité, GAZ DE FRANCE

M. Éric BERNES

M. Jean-Louis BLANCHOU, Directeur de la Sûreté, Préfet AÉROPORTS DE PARIS – ADP

Mme Céline BOUHEY-KLAPISZ, Chargée de programmes européens, Service Applications et Valorisation, CNES – SIÈGE

M. Philippe BRONSART, Ingénieur sûreté nucléaire NEPSFD, AREVA NP

M. Jean-Claude CASSAGNOLE, Responsable PCA/Gestion de crise, CRÉDIT AGRICOLE SA

Méd. Gal(cr) Louis CROCQ, Consultant, Comité national de l'Urgence médico-psychologique

Dr Arnaud DEROSSI, Directeur Médical Assistance et aviation, INTERNATIONAL SOS

M. Patrick DILLENSEGER, Chargé de mission défense, Département environnement et sécurité, RATP

LA CROIX-ROUGE FRANÇAISE, Direction de l'urgence et du secourisme

Dr Pascal FAUCHER, Responsable de programme, Programme risques et humanitaires, CNES

M. Hans-Willem FLUIJT, Consultant soutien psychologique aux populations et intervenants, Direction scientifique Centre d'histoire et de prospective militaires (CHPM), Lausanne, Suisse

M. Guy FONTAINE, Chargé de mission, INEO/SUEZ

M. Karim HARDY, Chercheur Pôle cindyniques, ÉCOLE DES MINES DE PARIS

L'INSTITUT NATIONAL DES HAUTES ETUDES DE SÉCURITÉ, Département Intelligence économique et gestion de crise

M. Frédéric LAMU, Architecte DPLG

Dr Bruno LARTIGUE, SFMC

Xavier LIFFRAN

Cre div. (H) Daniel MARTIN, Expert, CYBERCRIMINSTITUT

Mme Danielle MORONI, Attachée à la mission sécurité, RTE

Cne de vaisseau (R) Max-Pierre MOULIN, État-major de la Marine, conseiller protection-défense, Ingénieur consultant,

Dr Dominique NAZAT, Expert judiciaire, CISCD

M. Laurent OLMEDO, Chef de projets, CEA-DAM

M. René-Georges QUERRY, Directeur de la sécurité, ACCOR

M. André VANTOMME, Sénateur de l'Oise, membre du groupe d'études sur la sécurité et la défense civiles, SÉNAT

M. Robert ZEITOUNI, Responsable du Pôle Sécurité et continuité

d'activité, CRÉDIT AGRICOLE SA

Ont soutenu le projet

Pr. Frédéric BAUD, Chef de service Réanimation médicale et toxicologie HÔPITAL LARIBOISIÈRE - AP-HP

Cdt Christian BOSSERELLE, Pharmacien commandant, SDIS DE LA RÉUNION

M. Loïc BOURNON, Directeur des systèmes d'information et de leur sécurité, SAGEM SECURITE

M. Jérôme CHEMITTE, MISSION RISQUES NATURELS

Maître Ludovic DE VILLÈLE, Avocat et Maître de Conférences

M. Bernard DIDIER, Directeur du développement - activité sécurité, SAGEM SECURITÉ

M. Olivier HASSID, Délégué général, CDSE

M. Patrice LEFEBVRE, Adjoint au sous-directeur DDSC / SDDC-PR, MINISTERE DE L'INTERIEUR

M. Roland NUSSBAUM, Directeur, MISSION RISQUES NATURELS, GPSA

M. Sylvan RAVINET, Consultant en sécurité de l'information

M. Jean-Marc SUCHIER, SAGEM

Ont coordonné le projet

Mme Lauriane ABRIAT, Adjointe au Délégué général, HCFDC

M. Christophe BOUCHER, Journaliste, HCFDC

Gal Étienne COPEL, Président du collège des experts, HCFDC

M. le sénateur Paul GIROD, Président du HCFDC

M. Richard NARICH, Conseiller du Président d'ALTRAN TECHNOLOGIES, ministre plénipotentiaire, Président de l'EHSA

M. Christian SOMMADE, Délégué général, HCFDC


Haut Comité Français
pour la Défense Civile
Protéger l'avenir...

ANNEXE II

Glossaire

AFNOR : Association française de normalisation
AIEA : Agence internationale de l'énergie atomique
ANR : Agence nationale pour la recherche
ASN : Autorité de sûreté nucléaire
CSOSG : Concepts systèmes et outils pour la sécurité globale
CEA : Commissariat à l'énergie atomique
CEN : Centre européen de normalisation
CO : Centre opérationnel
COBR : Cabinet Office Briefing Rooms
CODIS : Centre opérationnel départemental d'incendie et de secours
COGIC : Centre opérationnel de gestion interministérielle des crises
CNES : Centre national d'études spatiales
CNRS : Centre national de la recherche scientifique
COZ : Centre opérationnel de zone
DNS : Directives nationales de sécurité
DGA : Délégation générale à l'armement
DG JLS : Direction générale Justice Liberté Sécurité
DGMT : Direction générale de la mer et des transports
DRIRE : Directions régionales de l'industrie, de la recherche et de l'environnement

ECI : Engin chimique improvisé

EEI : Engin explosif improvisé (IED en anglais)

EMA : État-major des armées

EMIZD : État-major interarmées de la zone de défense

EMZD : État-major de la zone de défense

EPR : European Pressurized Reactor

EPRUS : Établissement de préparation et de réponse aux urgences sanitaires

ESRAB : European Security Research Advisory Board (2005-2006)

ESRIF : European Security Research Innovation Forum (2007)

FAI : Fonds d'aide à l'investissement

GIS : Geographical Information System

GMES : Global monitoring for environment and security

INERIS : Institut national de l'environnement industriel et des risques

INPES : Institut national de prévention et d'éducation pour la santé

INPT : Infrastructure nationale partagée des télécommunications

INSERM : Institut national de la santé et de la recherche médicale

IP : Internet protocol

ISO : International standards organization

LOLF : Loi organique relative aux lois de finances

MEDAD : Ministère de l'Écologie, du Développement et de l'Aménagement durables

MIC : Monitoring Information Center

NRBC/E : Nucléaire, radiologique, biologique et chimique/ explosif

OCDE : Organisation de coopération et de développement économiques

ONERA : Office national d'études et de recherches aérospatiales

ORSEC : Organisation de la réponse de sécurité civile

PC : Poste de commandement

PCS : Plan de secours communal

PERS : Programme européen de recherche en sécurité

PPP : Partenariat public privé

RETEX : Retour d'expérience

R&D : Recherche et développement

RDS : Radio data system

RNA : Réseau national d'alerte

RTRA : Réseau thématique de recherche avancée (Digiteo Labs)

SAIV : Secteur d'activités d'importance vitale

SAMU : Service d'aide médicale d'urgence

SCS : Pôle de compétitivité « Solutions communicantes sécurisées »

SDIS : Service d'incendie et de secours

SDACR : Schéma départemental d'analyse et de couverture des risques

SGDN : Secrétariat général de la défense nationale

SHS : Sciences humaines et sociales

SIS : Schengen Information System

SRAS : Syndrome respiratoire aigu sévère

SROS : Schéma régional d'organisation sanitaire

TMD : Transport de matières dangereuses

TIC : Technologies de l'information et de la communication

TRL : Technological Readiness Level - Échelle de maturité technologique allant de 1 (principes de base) à 9 (validation en conditions d'emploi) utilisée par la DGA.

UIISC : Unité d'instruction et d'intervention de la sécurité civile

VIGIPIRATE : Plan gouvernemental de vigilance, prévention et protection