

Sommaire

Avant-propos	5
Introduction	7
Première partie	
Le terrorisme mondial : une menace stratégique	13
Chapitre 1	
Un discours efficace, une volonté de maîtrise de l'espace, des structures évolutives	15
Une vision du monde simpliste et complexe à la fois	15
Une volonté de maîtrise de l'espace	18
Des structures difficilement saisissables	20
Chapitre 2	
Le terrorisme mondial renouvelle ses recrues, adapte ses méthodes et signe son mode opératoire	25
Des terroristes plus difficiles à repérer	25
Une gestion efficace des flux d'information, de financement et de déplacements	29
Des modes opératoires classiques et pourtant reconnaissables entre tous	31
Chapitre 3	
Des perspectives préoccupantes pour la France	33
La France est un objectif particulier au sein de l'Europe, cible du terrorisme	33
Les facteurs d'une menace aggravée pour la France et pour l'Europe	35
Deuxième partie	
Le dispositif français de lutte contre le terrorisme doit continuer à s'adapter	39
Chapitre 1	
Prévenir le risque : surveiller, détecter, neutraliser	45
Renforcer les capacités des services de renseignement et de sécurité	46
Conforter notre dispositif pénal et adapter notre système pénitentiaire à la menace terroriste	53
Neutraliser les flux dangereux de personnes, de biens, de capitaux et d'idées	56

Protéger le territoire des intrusions et neutraliser les terroristes à l'étranger par l'action des armées	61
Renforcer la coopération internationale	63
Chapitre 2	
Améliorer nos dispositifs	69
Protéger la population	69
Protéger l'intégrité du pays	76
Chapitre 3	
Renforcer nos capacités de gestion de crise	79
Parfaire nos capacités opérationnelles	79
La mise en place d'une doctrine de communication publique	86
Chapitre 4	
Renforcer nos capacités de réparation et de sanction	91
Réparer les dommages infligés aux victimes	91
Poursuivre les suspects : l'approfondissement de la coopération judiciaire internationale	93
Sanctionner les coupables	94
Troisième partie	
Mener une action de fond contre le terrorisme en gagnant les batailles du quotidien, de la technologie et des idées	97
Chapitre 1	
Gagner la bataille du quotidien : favoriser la détection précoce des activités terroristes par la vigilance et le renseignement humain	99
Les agents des services publics : une vigilance essentielle	100
La responsabilité des acteurs sociaux et le rôle du citoyen	102
Chapitre 2	
Gagner la bataille technologique	109
L'objectif : toujours précéder la progression de la menace	109
La méthode : une collaboration entre l'État et les entreprises, qui privilégie la dimension européenne	113
Chapitre 3	
Gagner la bataille des idées	117
En France, conforter l'adhésion de la population et isoler les terroristes	117
Lutter contre le terrorisme au niveau mondial	122
Conclusion	127
Annexes	129

Avant-propos

Avec le Livre blanc sur la sécurité intérieure face au terrorisme, notre pays se dote pour la première fois d'une véritable doctrine pour faire face à un fléau auquel il a été confronté plusieurs fois au cours de son histoire.

Bien entendu nous n'avons jamais cessé de nous adapter pour protéger notre territoire et nos concitoyens. Aujourd'hui nos forces de sécurité et de renseignement sont formées pour anticiper et lutter contre le risque terroriste. Pourquoi alors avons-nous voulu aller plus loin et formuler une véritable stratégie de sécurité ?

- D'abord parce que la menace sur notre pays n'a jamais été aussi forte : depuis les attentats de Madrid et de Londres nous savons qu'elle vise tout particulièrement l'Europe. La France n'est donc pas à l'abri. Pour assurer la sécurité des Français il est devenu impératif de mieux connaître cette menace.

- Ensuite parce que c'est une menace stratégique, qui vise nos intérêts sur l'ensemble de la planète, comme l'ont démontré les attentats de Karachi qui ont fait onze victimes françaises en mai 2002.

- Enfin nous avons besoin d'une véritable stratégie parce que la menace terroriste n'a cessé de changer. Elle exige, si nous voulons garder toujours un temps d'avance sur les groupes terroristes, que nous adaptions en permanence nos outils et notre dispositif. Nous avons commencé à le faire à travers la création des pôles régionaux de lutte contre l'islamisme radical et l'adoption de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Mais nous avons besoin d'une stratégie d'adaptation à long terme, à l'image de ce qui avait été fait en 1994 avec le Livre blanc sur la défense.

L'objectif de ce travail est triple.

- Il s'agit en premier lieu de mieux connaître le fonctionnement des groupes terroristes. Nous savons qu'ils s'appuient dans les pays européens sur de véritables chaînes opérationnelles allant des prédicateurs extrémistes aux filières qui envoient des jeunes gens vers les camps d'entraînement terroriste et les terres de combat, jusqu'aux organisateurs

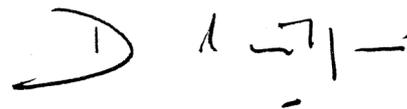
des attentats et aux poseurs de bombes. Seule une connaissance approfondie des réseaux, des relais et des outils de ces groupes peut nous permettre de protéger nos concitoyens.

- L'objectif du Livre blanc est ensuite de définir une stratégie de riposte et de lutte adaptée à la menace. Cette stratégie doit prendre en compte les nouveaux outils technologiques et les moyens de communication modernes utilisés par les groupes terroristes. Elle permettra également d'ouvrir de nouvelles pistes d'action en matière de coopération internationale. C'est indispensable pour lutter contre des groupes qui sont reliés par des ramifications mouvantes et pour appréhender les circuits de financement sur lesquels ils s'appuient. Nous avons déjà construit des partenariats bilatéraux efficaces. Nous devons maintenant développer les échanges multilatéraux.

- Enfin le Livre blanc a pour objectif de mieux informer nos concitoyens sur un risque qui les inquiète et sur les moyens que nous mettons en œuvre pour les protéger. Face à une menace qui cherche à diviser nos sociétés, notre combat doit être le combat de tous. Il doit s'appuyer sur une conviction partagée sur la gravité de la menace et l'importance des règles qui doivent encadrer la lutte antiterroriste.

Car dans le combat contre le terrorisme, notre meilleure arme ce sont nos principes démocratiques. La tolérance, le respect des libertés publiques, le respect des identités que notre pays a toujours su défendre font notre force. Renoncer à ces valeurs, ce serait faire le jeu des terroristes. Céder à la tentation de l'exception, ce serait commencer à perdre la bataille. Alors soyons fidèles à nos valeurs : elles sont notre meilleur atout dans notre combat contre le terrorisme.

Dominique de Villepin
Premier ministre



Introduction

Pour lutter efficacement contre le terrorisme, nous devons d'abord être capables de le nommer, de le définir.

« Tout acte qui vise à tuer ou à blesser grièvement des civils ou des non-combattants, et qui, du fait de sa nature ou du contexte dans lequel il est commis, doit avoir pour effet d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à agir ou à renoncer à agir d'une façon quelconque ¹ ».

Telle est la définition du terrorisme proposée par le secrétaire général des Nations unies à l'occasion du sommet de l'assemblée générale célébrant le soixantième anniversaire de l'organisation en septembre 2005. Même si cette définition ne fait pas encore l'objet d'un consensus international, la France l'a acceptée d'emblée. Elle correspond à une forme de violence dont notre pays est familier depuis près de deux siècles.

Menaces passées, actuelles et futures

Acteur engagé de la vie internationale, notre pays a été, au cours de la seconde moitié du XX^e siècle, la cible de nombreux attentats. Nous avons connu le terrorisme lié à des questions de politique intérieure, qu'il s'agisse des attentats commis dans le contexte de la guerre d'Algérie ou du terrorisme lié à des revendications idéologiques ou régionalistes.

Mais nous avons également subi une forme de violence terroriste liée à des crises extérieures, lorsque, pour la première fois, des groupes terroristes palestiniens se sont attaqués aux intérêts de leurs adversaires en effaçant les limites géographiques. En France, mais aussi en Italie (attentat de l'aéroport de Rome), en Autriche (attaque du siège de l'OPEP), en Ouganda (prise d'otages d'Entebbe) et ailleurs on a assisté progressivement à la « globalisation » d'une cause par l'action terroriste.

(1) « *Dans une liberté plus grande* », Rapport du secrétaire général des Nations unies, mars 2005, p. 67.

D'autres mouvances ont peu à peu adopté ce mode d'action. L'Armée secrète arménienne pour la libération de l'Arménie (ASALA), fondée en 1975 à Beyrouth, en est un exemple. Jusqu'à son démantèlement en 1984, elle a commis plus de trente-cinq attentats en France, montrant qu'il n'était pas besoin d'être désigné comme l'ennemi principal d'un mouvement pour en être la victime.

Pendant les années 1960 et 1970, la terreur a aussi été portée par des mouvements violents issus de l'extrême gauche et de la mouvance autonome. Une poignée d'entre eux, comme Action directe, ont poursuivi leurs actions jusque dans les années 1980, avant d'être progressivement mis hors d'état de nuire.

Les attentats majeurs les plus récents dont la France a été victime sur son territoire remontent à 1995 et 1996 : attentats dans les stations parisiennes de métro ou de RER Saint-Michel, Maison-Blanche et Port-Royal. Bien que liés aux luttes internes à l'Algérie, ces attentats préfiguraient d'une certaine manière le terrorisme islamiste. Ils furent l'œuvre de terroristes qui s'appuyaient sur des cellules préalablement implantées sur le territoire et qui basculaient du soutien logistique aux groupes armés actifs en Algérie vers l'action opérationnelle contre un État occidental. Cette dimension alors nouvelle était annonciatrice des menaces qui pèsent aujourd'hui sur notre pays.

Le terrorisme d'inspiration régionaliste n'a pas épargné la France. Les mouvements indépendantistes corse, basque et breton recourent à la violence. Cette forme de terrorisme n'est pas propre à la France. En Espagne et au Royaume-Uni, l'ETA et l'IRA ont mené, pendant plus de trois décennies, un combat intense contre les gouvernements au nom de l'indépendance basque et de l'unité irlandaise. Le terrorisme régionaliste n'a pas disparu. Il est allé dans un passé proche jusqu'à l'assassinat d'un représentant de la République. Il doit continuer à faire l'objet d'une attention soutenue des pouvoirs publics, dans le cadre d'une action de longue haleine.

Mais le terrorisme auquel nous sommes confrontés aujourd'hui est l'héritier des attentats du 11 septembre 2001 aux États-Unis, qui ont fait près de 3 000 victimes. C'est à cette menace que nous devons être préparés, si nous voulons protéger nos concitoyens.

Un phénomène de plus en plus meurtrier

La capacité de nuisance des mouvements terroristes dépend en partie des moyens de destruction auxquels ils peuvent avoir accès. L'arme blanche des Assassins¹, les armes à feu ou les machines infernales des anarchistes de la fin du XIX^e siècle ne permettaient guère que des meurtres ciblés ou des tueries faisant au pis quelques dizaines de victimes.

(1) Secte ismaélienne sévissant en Perse, puis en Syrie, de la fin du X^e au XIII^e siècle et qui s'en prenait aux élites dirigeantes.

Dans la deuxième moitié du XX^e siècle, l'accès aux moyens modernes de transport, transformés à la fois en objectifs et en moyens de l'action terroriste, ainsi que la mise sur le marché de substances explosives puissantes, ont rendu possible le passage à des prises d'otages et à des massacres d'une ampleur inédite. Le 19 avril 1995, un attentat commis par deux individus isolés à Oklahoma City, aux États-Unis, a tué 168 personnes et en a blessé 600 autres.

La synthèse d'agents chimiques tels que des neurotoxiques puissants, ainsi que l'acquisition de savoir-faire et de technologies biologiques sont désormais à la portée de certains groupes ou d'individus. La preuve en a été donnée lors des attaques au gaz Sarin perpétrées par la secte Aoum dans le métro de Tokyo en mars 1995, ou avec l'envoi d'enveloppes contenant des spores de bacille du charbon à l'automne 2001 aux États-Unis. Ces attentats, qui n'ont causé que quelques morts, ont révélé les difficultés auxquelles se heurtait la perpétration d'attentats de masse avec ces modes opératoires.

Depuis vingt-cinq ans, le nombre des victimes causées par les attentats terroristes a franchi plusieurs seuils. Avant 1983, l'attentat terroriste le plus sanglant avait causé la mort de 85 personnes (attentat perpétré dans la gare de Bologne, en Italie, en 1980). Le seuil de la centaine de victimes a été franchi pour la première fois en 1983, avec le double attentat à Beyrouth, au Liban, contre les forces militaires américaines et françaises (299 morts au total). Jusqu'en 2001, l'attentat le plus meurtrier avait tué 329 personnes (destruction d'un avion d'Air India au-dessus de la mer d'Irlande en 1985). Le seuil du millier de victimes a été largement dépassé avec l'attaque d'Al Qaïda aux États-Unis le 11 septembre 2001.

Même si on constate une diminution après septembre 2001, l'unité de compte des attentats les plus meurtriers est passée, en une génération, des dizaines aux centaines puis aux milliers de victimes.

L'examen du passé et des menaces « classiques » qui pèsent sur notre pays permet de déterminer les caractéristiques – cumulatives – du type de terrorisme susceptible de présenter, en France, une menace autre que circonstancielle. Il se manifeste par des actions violentes, préparées clandestinement. Il est l'œuvre de groupes non étatiques, ce qui amoindrit sa prévisibilité. Il est le fait d'individus idéologiquement motivés, arrimés à une cause internationale dont la rhétorique s'inscrit dans la durée. L'un de ses buts est de tuer un nombre aussi élevé que possible de Français ou de ressortissants étrangers sur le sol français, même si son cadre d'analyse ne s'arrête par principe ni aux frontières de la France ni à la nature civile des victimes. Dans sa logique, tous les coups sont permis. Il cherche à obtenir un effet psychologique majeur sur les pouvoirs publics et sur l'opinion.

La hausse potentielle du niveau de destruction recherché par les terroristes constitue la première justification d'un réexamen par la France de son dispositif de lutte antiterroriste.

L'émergence du « terrorisme mondial »

La deuxième raison qui justifie l'élaboration de ce Livre blanc est l'apparition, à la charnière du siècle dernier, d'une forme de terrorisme d'un genre nouveau.

Depuis la seconde moitié des années 1990, la mondialisation a entraîné, dans toutes les sociétés, une transformation sans précédent. L'opinion publique mondiale a désormais accès aux mêmes images, souvent en temps réel. Les distances sont abolies et les répercussions des différentes crises régionales sont de plus en plus fortes. Les pays du Proche et du Moyen-Orient sont particulièrement touchés par cette instabilité. L'héritage de l'Histoire, les blocages politiques qui perdurent dans de nombreux pays, les enjeux liés aux ressources pétrolières en ont fait une région fragile. Le désarroi des populations, confrontées à des difficultés sociales et économiques considérables a constitué un terreau privilégié pour les groupes terroristes : ils ont instrumentalisé leur sentiment d'injustice en le retournant contre l'Occident, principal responsable selon eux, de la situation de la région. Ils ont également instrumentalisé le message de l'islam pour imposer une lecture rigoriste et violente de la religion musulmane.

La sphère terroriste a ainsi connu une mutation d'une nature et d'une ampleur comparables à celle des bouleversements provoqués par la mondialisation. Cette mutation a débouché sur l'émergence d'un terrorisme d'inspiration islamiste radicale et d'envergure planétaire, qui s'attaque indistinctement aux pays occidentaux et aux nations arabes ou plus largement musulmanes avec des moyens de destruction jusqu'alors inédits.

Incarné par Al Qaïda, ce terrorisme d'un genre nouveau s'est dès l'origine fixé un champ mondial. Depuis 1998, il a frappé dans une vingtaine de pays, au rythme moyen de trois ou quatre attentats majeurs par an¹. Il a révélé sa capacité d'action en Europe à deux reprises, à Madrid en mars 2004 et à Londres en juillet 2005. Il se distingue par son aptitude à emprunter à la mondialisation les outils qui ont assuré le succès de celle-ci. Il parvient à opérer l'alchimie entre préoccupations intimes des individus et grandes perspectives transnationales, affiche sa prédilection pour les réseaux inter-individuels, recourt aux moyens électroniques, accorde la plus grande priorité à la médiatisation et démontre une capacité permanente d'évolution, voire d'anticipation. Décrite sur le plan des principes, la mondialisation se trouve ainsi simultanément acceptée, intégrée, exploitée dans ce qu'elle a de plus efficace sur le plan opérationnel.

Nous sommes entrés dans l'ère de ce que nous dénommerons le « terrorisme mondial ». Celui-ci relève d'un registre différent du terrorisme régionaliste ou du terrorisme commandité par un État. S'il n'échappe pas à la règle qui veut que tout mouvement terroriste ne mobilise qu'une minorité d'activistes, il entend à lui seul assumer un héritage historique et s'appuyer sur un socle géopolitique. Il cherche à afficher des

(1) Sans compter les attentats perpétrés dans les zones de guerre.

ambitions, apporter des innovations, développer des moyens pour obtenir des résultats qui le porteraient d'emblée au niveau d'un adversaire planétaire et générationnel, capable d'infliger des dommages et d'exercer sur la vie de nos sociétés une influence sans commune mesure avec les objectifs, somme toute limités, des autres formes de terrorisme.

Ancrée dans une génération encore jeune, la menace présentée par le terrorisme mondial devrait être durable. Elle a acquis une dimension stratégique. La France est l'une de ses cibles. Plusieurs de nos ressortissants en ont été victimes à l'étranger.

Nous devons analyser cette menace pour bien la mesurer, déterminer les adaptations à apporter à notre système de lutte antiterroriste pour la contrer, et établir une stratégie de long terme pour la résorber. Nous devons éviter le piège de la « guerre des civilisations » que nous tend le terrorisme mondial d'inspiration islamiste et refuser l'amalgame entre islam et terrorisme vers lequel il voudrait nous entraîner.

C'est ce refus de l'amalgame que manifeste la France lorsqu'elle encourage l'organisation de l'islam en France, notamment à travers le Conseil français du culte musulman, lorsqu'elle milite de manière continue sur le plan international pour un meilleur dialogue entre les peuples, en particulier vis-à-vis de nos voisins du Sud et du monde musulman, et lorsqu'elle se bat contre toutes formes de message de haine. Cette politique est d'autant mieux reçue que la plupart des musulmans de France vivent dans le respect des valeurs républicaines de tolérance et de laïcité et condamnent l'instrumentalisation par les courants extrémistes du message de l'islam.

Le Livre blanc a l'ambition de formuler la doctrine de la France en matière de lutte contre le terrorisme. Cette doctrine doit être connue de tous. Car nous ne combattons efficacement le terrorisme qu'avec l'adhésion de l'ensemble de nos concitoyens. Nous ne le combattons efficacement qu'en développant la coopération internationale.



Première partie

Le terrorisme mondial : une menace stratégique



Le terrorisme mondial tire une partie de sa force de l'efficacité de son discours. Il innove par une volonté de maîtrise de l'espace. Il adapte ses structures et ses procédures, renouvelle ses recrues et sait tirer profit des moyens de communication que lui offre la mondialisation. Incarné aujourd'hui par le terrorisme islamiste, il constitue pour la France une menace stratégique.

Chapitre 1

Un discours efficace, une volonté de maîtrise de l'espace, des structures évolutives

Une vision du monde simpliste et complexe à la fois

La simplicité apparente, et affichée, de la vision du monde proposée par le terrorisme mondial d'inspiration islamiste fournit une référence commune à un ensemble qui, à première vue, semble disparate.

Une vision du monde qui permet de délivrer un message simple et puissant

Le terrorisme islamiste puise son inspiration idéologique dans le salafisme ¹. Fondé sur le rejet des innovations sociales ou politiques, ce courant de pensée est hostile par nature au système démocratique. Sa référence est le souvenir, en partie fantasmé, d'un « âge d'or » de l'islam ori-

(1) De *Salafs*, les Anciens, qui désignent les premiers compagnons du prophète Mahomet.

ginel. Il rejette le monde tel qu'il est devenu. Il se présente comme une alternative à la mondialisation. Il propose le retour aux pratiques du califat initial¹ fondées sur une interprétation rigoriste du Coran.

Ce souhait de retour aux origines cache cependant un mouvement qui prône en réalité une « renaissance » de l'islam. Sous cet angle, le salafisme apparaît aussi comme le véhicule d'une interprétation négative de l'Histoire, douloureusement vécue comme une injustice, celle du déclin d'une civilisation « humiliée » par les invasions successives, physiques, économiques et culturelles de « l'Occident chrétien », du temps des croisades à nos jours.

L'islam « agressé », menacé dans sa survie et sur son propre sol, n'aurait pas d'autre choix que de se défendre par la violence la plus extrême. Pour le terrorisme mondial d'inspiration islamiste, cette « guerre des civilisations » serait entrée dans une phase aiguë qu'il assimile au « jihad », dévoyant ainsi cet élément central de la religion musulmane. Tel est le message d'une redoutable simplicité qu'il délivre inlassablement.

Jihad et Jihadisme

On a coutume, en Europe, de traduire jihad par « guerre sainte ». Étymologiquement, jihad signifie « effort vers un but déterminé », c'est-à-dire, d'une part, celui de défendre ou de propager l'islam et, d'autre part, celui que fait le croyant pour se conformer aux règles du Coran. On retrouve cette référence dans divers versets du Coran, sous des formes différentes : répandre l'islam par la persuasion, combattre pour repousser une attaque contre l'islam, etc. L'islam se posant comme un universalisme, sa propagation est un devoir pour la communauté musulmane, que tous les courants de l'islam admettent.

De même qu'on distingue l'islam de son exploitation politique (« l'islamisme »), il faut différencier la notion religieuse de jihad du « jihadisme », qui en est le dévoiement par l'action violente. Au cours des dernières années, le jihad a souvent été assimilé, à tort, au terrorisme. Cet amalgame a fait le jeu des terroristes eux-mêmes.

Après l'Afghanistan dans les années 1980, c'est en Algérie que le jihadisme a pris sa forme la plus aiguë au début des années 1990, lorsque le Groupe islamique armé (GIA) a commencé à s'en prendre aux Européens, en Europe ou en Algérie, ainsi qu'à des musulmans jugés trop influencés par la culture occidentale.

(1) Le mot désigne à la fois l'autorité du calife successeur du prophète Mahomet sur l'ensemble de la communauté musulmane et les territoires placés sous son contrôle.

Une stratégie plus complexe qu'il n'y paraît

Les promoteurs du terrorisme mondial d'inspiration islamiste ont pour objectif le plus immédiat de « guérir » le peuple musulman du complexe d'infériorité qui serait né du rapport colonial. Ils entendent pour cela saper la croyance des « opprimés » en la suprématie des « oppresseurs » en dévoilant la vulnérabilité de ces derniers. Tel était le but des attentats du 11 septembre 2001 à New York et à Washington.

Une fois le rapport de forces symbolique perturbé, il s'agit ensuite d'entraver, en profondeur et dans la durée, le fonctionnement des sociétés occidentales, en fragilisant leurs sources d'énergie (pétrole, gaz) et en plaçant sous la menace leurs moyens de déplacement (urbains et internationaux).

L'étape suivante est de provoquer une rupture, y compris par la séparation physique, entre l'Occident et les musulmans en incitant au départ les ressortissants occidentaux présents en terre musulmane (résidents, militaires, touristes) ou en s'en prenant aux lieux de « métissage » que sont les sites touristiques et les réseaux de transport en commun des grandes agglomérations européennes.

Pour aboutir à la cassure escomptée, c'est la lassitude des gouvernements et des opinions du monde occidental qui est recherchée.

Le terrorisme mondial d'inspiration islamiste parvient également à recycler des causes autres que religieuses, dont le flambeau s'était éteint faute de combattants. Il s'emploie ainsi à occuper autant que possible l'espace laissé vacant par l'effondrement des idéaux communistes, révolutionnaires ou tiers-mondistes. Il investit le créneau des luttes anti-impérialistes que nul ne lui conteste sérieusement aujourd'hui. Il cherche ainsi à s'inscrire dans la continuité des guerres anticoloniales. Dans ce mouvement de rejet de l'Occident et de lutte contre les grandes puissances économiques, on ne peut exclure qu'il tente un jour un rapprochement avec les mouvances alter-mondialistes les plus radicales.

Le discours tactique du proche et du lointain

Le déclenchement de la deuxième guerre d'Irak en 2003 a permis au terrorisme islamiste de retrouver le terrain concret des luttes nationales et identitaires et de renouer à travers elles le pacte qui avait si bien fonctionné en Afghanistan contre l'occupant soviétique.

L'intervention militaire en Irak a suscité une triple convergence qui a consolidé l'emprise de la mouvance terroriste : une convergence idéologique entre « jihadisme » transnational et nationalisme arabe, une convergence opérationnelle entre terroristes et services de sécurité baassistes, une convergence géographique enfin, en offrant à Al Qaïda une présence au cœur du monde arabe, alors que ce mouvement avait jusque-là

combattu à ses marges, en Afghanistan, en Bosnie, en Tchétchénie et en Afrique.

Le discours terroriste puise dans cette alliance un souffle nouveau, concrétisé par la possibilité tactique de rejouer sur les deux tableaux des ennemis « proche » et « lointain ». Le proche, ce sont les régimes locaux « apostats », accusés d'avoir rompu avec leur identité religieuse ; le lointain, ce sont les « protecteurs » occidentaux. Tirant profit de cette nouvelle assise, la mouvance terroriste peut même feindre une approche pragmatique des événements, en proposant par exemple des trêves comme Oussama Ben Laden l'a fait à deux reprises, en 2004 et en 2006.

Du large ratissage que lui permet son discours, la mouvance terroriste tire trois bénéfices principaux.

Le premier est une attractivité qui dépasse le noyau dur de son audience originelle et lui permet de séduire une part des Occidentaux convertis. Le phénomène demeure marginal. Mais il est d'une grande puissance symbolique. Il dénote une capacité à surmonter les barrières ethniques et culturelles au nom d'une fraternité universelle.

Le deuxième bénéfice est de dissimuler les divergences internes à la mouvance. Celles-ci sont pourtant bien réelles. Elles portent sur la caractérisation de l'ennemi, et notamment sur l'existence éventuelle d'une hiérarchie tactique entre pays occidentaux, qui conduirait à s'en prendre d'abord aux membres de la coalition formée en 2003 lors de la deuxième guerre d'Irak, au nom du caractère prépondérant désormais attribué à cette terre naturelle de combat.

Le troisième bénéfice est de concilier terrorisme politique et terrorisme idéologique. C'est le plus « prometteur » à long terme, car il offre la possibilité d'additionner les capacités de mobilisation propres à l'une et à l'autre des deux formes de terrorisme. Le terrorisme politique est utilitaire. Il choisit des objectifs concrets, localisés et revendiqués. Il utilise la violence comme un levier tactique. Le terrorisme idéologique exprime quant à lui un refus existentiel du monde. Il dénie toute possibilité de dialogue ou de dissuasion. Il n'a d'autre fin que lui-même. Son potentiel de nuisance est donc en principe illimité.

Une volonté de maîtrise de l'espace

La mouvance Al Qaïda répand un discours englobant. Elle affiche aussi une volonté de maîtrise de l'espace. Cet espace aujourd'hui en expansion se décompose en plusieurs zones, aux fonctions précisément définies, mais dont les frontières ne cessent d'évoluer : on y trouve les sanctuaires, les terres de combat, les zones de transit et les zones d'opérations.

Les sanctuaires

Le terrorisme a besoin de « sanctuaires » pour les refuges qu'ils offrent, les possibilités de formation qu'ils hébergent, et, éventuellement, l'organisation des trafics qui assurent une source de financement. Après avoir dû quitter en 2001 l'asile à ciel ouvert que leur fournissait alors l'Afghanistan¹, les terroristes d'Al Qaïda se sont mis en quête d'abris alternatifs.

Faute d'États disposés à les accueillir, ils se sont installés, précisément, là où toute présence des États a disparu. Ils ont donc élu domicile dans les zones désertiques ou montagneuses, vides d'autorité ou de contrôle, qui parsèment l'arc de crise courant du Maghreb à l'Asie du Sud-Est. Ces espaces recouvrent les zones tribales à la frontière entre le Pakistan et l'Afghanistan, les confins du Cachemire, ceux de l'Iran. Là se maintient ce qui subsiste d'Al Qaïda *stricto sensu*. Plus loin, ils incluent certains camps de réfugiés au Liban, les régions tribales du Yémen, ainsi que la Somalie. Au-delà encore s'étend le Sahel, devenu zone de ravitaillement et de repli pour certains groupuscules, alors qu'aux antipodes certaines îles excentrées des archipels philippin et indonésien jouent le même rôle.

La protection offerte par ces repaires est efficace. Tout porte à croire que la recherche de nouveaux sanctuaires se poursuit.

Les terres de combat

Le deuxième type d'espace est celui des « terres de jihad », lieux de combat frontal contre l'ennemi, où les terroristes acquièrent légitimité, expérience et relations.

La Bosnie a constitué au cours de la première partie des années 1990 l'un de ces lieux de combat. L'Afghanistan, la Tchétchénie et le nord du Caucase le sont demeurés à des degrés divers. Mais c'est aujourd'hui l'Irak qui constitue le centre de gravité de ces « terres de jihad ». Créant un abcès de fixation au cœur des mondes arabe et musulman, l'intervention militaire menée en 2003 a exacerbé la radicalisation, en fournissant une sorte de validation des discours les plus simplistes du terrorisme islamiste. Celui-ci y a trouvé un exemple de tentative d'imposition des valeurs de la démocratie par la voie militaire et de la collusion supposée entre chiites et « croisés ».

Est ainsi à l'œuvre en Irak une dynamique favorisant l'ancrage et la diffusion du terrorisme. Affluent dans ce pays des milliers de volontaires en provenance de l'ensemble du monde arabe, et, dans une moindre proportion, du continent européen. Ces volontaires ont vocation, après avoir acquis une expérience précieuse, à retourner dans leur pays d'origine. Le phénomène n'a pas pris, jusqu'ici, la même dimension qu'autrefois en Afghanistan, faute de véritable sanctuaire limitrophe. Mais il bénéficie à plein de la caisse de résonance que lui fournit la mondialisation de l'information.

(1) Qui succédait lui-même au Soudan, dont Oussama Ben Laden est parti en 1996.

Les zones de transit et de soutien, à mi-chemin entre sanctuaires et terres de combat

Le terrorisme mondial d'inspiration islamiste y organise les filières d'acheminement des personnes, des fonds et des armes. Ces zones de transit et de soutien revêtent une importance cardinale pour la mouvance. Cela explique qu'elles soient relativement épargnées par la violence. Aujourd'hui, leur centre de gravité se situe aux abords de l'Irak, soit qu'elles constituent des portes d'entrée privilégiées vers ce pays, soit qu'elles assurent des couloirs de communication commodes avec l'Afghanistan, voire le nord du Caucase.

Les zones d'opérations où le terrorisme mondial d'inspiration islamiste est à l'œuvre

Depuis 2001, l'essentiel des zones d'opérations se concentre dans l'aire musulmane car les terroristes vont souvent au plus simple. Dans l'immense majorité des cas ils passent à l'acte où ils le peuvent, quand ils le peuvent et comme ils le peuvent. Le plus souvent, cette équation fournit un résultat élémentaire : les terroristes agissent chez eux, dans leur propre pays, où sont généralement présents des objectifs occidentaux représentatifs de la « collaboration » de leurs autorités avec « l'occupant ».

Du Sahel à l'archipel indonésien, de plus en plus rares sont les pays épargnés par la tache d'huile qui s'étend au rythme moyen d'un attentat majeur tous les trimestres (hors de l'Irak, où le rythme est quotidien). Les objectifs se situent aussi bien dans les grandes métropoles (Riyad, Jakarta, Casablanca, Istanbul, Karachi, Amman...) que dans les centres touristiques (Djerba, Bali, Mombasa, Taba, Sharm el Cheikh...).

L'Europe fait partie depuis mars 2004 des zones d'opérations. Là comme ailleurs, les terroristes passent à l'acte chez eux, là où ils sont nés, là où ils résident de longue date.

Des structures difficilement saisissables

La nébuleuse du terrorisme mondial d'inspiration islamiste est un assemblage d'entités et d'individus, organisés sur un mode horizontal et plus ou moins connectés entre eux.

La trame de départ de la mouvance était différente et relativement simple. Elle était verticale avec, au sommet, l'organisation Al Qaïda

et, à la base, plusieurs centaines de moudjahiddin, d'extraction et d'affiliation diverses, passés par l'Afghanistan ou par d'autres zones de combat.

À l'origine, Al Qaïda est une structure conspirative, au recrutement restreint plutôt bourgeois, issue de la conjonction de wahhabites du Golfe arabo-persique et de jihadistes égyptiens. Dirigée depuis 1998 par le binôme formé par Oussama Ben Laden et Ayman Al Zawahiri, elle a, en trois moments clés, fait basculer le monde dans la nouvelle forme de terrorisme que nous connaissons en 2006.

L'accueil de milliers de moudjahiddin venus du monde entier pour combattre les Soviétiques en Afghanistan (pour la première génération, de 1979 à 1989), puis pour rejoindre les Taliban (pour la deuxième génération, de 1996 à 2001) a constitué une première étape. En fournissant ce moule originel, Al Qaïda a conquis la « légitimité » qui l'autorise à prêter son nom au terrorisme mondial d'inspiration islamiste dans son ensemble et à s'en faire le porte-parole exclusif dans la sphère des médias ¹.

Le deuxième moment clé est bien sûr celui des attentats du 11 septembre 2001, dont les résultats stupéfiants auront permis au terrorisme de faire basculer à lui seul le cours de l'Histoire. C'est en effet la chute des tours du *World Trade Center* qui a tout à la fois haussé au niveau stratégique une menace alors portée par à peine quelques centaines d'individus et conduit les États-Unis à s'engager dans la « guerre contre le terrorisme ».

C'est enfin Al Qaïda qui a organisé, après l'intervention en Afghanistan, en 2001, l'exfiltration et la dissémination des terroristes aux quatre coins de la planète.

Le modèle d'origine a cependant connu de profondes modifications depuis 2001.

Le noyau initial d'Al Qaïda a perdu, avec l'exil forcé hors de son sanctuaire afghan, un nombre significatif de ses cadres dirigeants, ainsi que sa capacité à exercer le rôle de centre unique de commandement. Quant aux combattants de base, ils ont été contraints de se disperser parmi les militants locaux. Ils contribuent à dessiner un paysage de plus en plus composite, sans précédent connu à l'échelle planétaire. Le modèle qui permet le mieux d'en rendre compte est celui du réseau internet : les terroristes forment une vaste toile interconnectée, où la neutralisation d'une partie a peu d'effet sur le fonctionnement du tout.

Le réseau se décompose en trois niveaux, dont la particularité n'est pas d'être superposés pour former une pyramide, mais d'être plutôt placés côte à côte. On peut parler à bon escient à leur propos d'un réseau de réseaux aux frontières poreuses.

(1) Son séjour en Afghanistan de 1996 à 2001 a également permis à Oussama Ben Laden de coaliser des individus et des groupes dispersés dans le monde en renforçant son ascendant, notamment financier, sur eux.

Le premier niveau : l'organisation Al Qaïda

Bien que partiellement démantelée, Al Qaïda continue, non sans difficultés réelles, de tenter de planifier des attaques depuis ses repaires situés en Afghanistan et au Pakistan. Son influence directe se concentre en 2006 sur l'axe reliant l'Afghanistan à l'Irak, à la péninsule arabique et à la corne de l'Afrique. Subsiste néanmoins sa volonté, voire sa capacité, à frapper en tout point du globe.

C'est en tout cas ce noyau qui conserve la responsabilité de donner une cohérence médiatique et idéologique à l'ensemble de la mouvance, à travers les nombreuses interventions audiovisuelles (une quarantaine depuis 2001) d'Oussama Ben Laden et d'Ayman Al Zawahiri, sans compter leurs communiqués de presse.

Le deuxième niveau : les entités terroristes qui disposent d'un enracinement territorial

Les relations de ces entités avec le groupe d'origine d'Al Qaïda sont très variables. Elles vont de la « filialisation » jusqu'à la simple imitation, en passant par le partenariat. La liste des organisations est longue, mais c'est en Irak et en Arabie saoudite que le rattachement au « centre » s'affiche le plus volontiers.

Malgré les spécificités du mouvement irakien, le modèle de la « succursale régionale » a essaimé dans la région du golfe arabo-persique ; l'Organisation d'Al Qaïda pour le jihad dans la péninsule arabique a ainsi pour objectif de regrouper les cellules actives en Arabie saoudite et aux alentours. Elle cohabite encore avec d'autres organisations, aux formats les plus hétérogènes : Osbat al Ansar dans le Sud-Liban, Al Ittihad Al Islami en Somalie, les « groupes islamiques combattants » des différents pays du Maghreb (au Maroc, en Tunisie ou en Libye), le Groupe salafiste pour la prédication et le combat (GSPC) en Algérie ou la Jamaa Islamiyya en Asie du Sud-Est.

Le dernier niveau de la mouvance : les individus, regroupés ou non en cellules

Au sein de la mouvance, les individus sont investis de responsabilités d'inégale ampleur.

Au premier rang figurent les « gradés ». Ils disposent de carnets d'adresses, nourris par les rencontres dans les terres de combat, les camps d'entraînement ou les prisons. Cela leur permet de devenir des « facilitateurs », plaques tournantes des filières de soutien aux réseaux nationaux auxquels ils fournissent leurs services : faux papiers, argent, hébergement, aide pour passer les frontières...

D'autres membres de la mouvance peuvent être qualifiés « d'experts ». Leur travail consiste à mettre un savoir-faire spécialisé (en explosifs, en confection de faux documents, en finances, en informatique) au service d'une cellule, d'une filière ou d'un réseau, voire de l'ensemble de la nébuleuse.

La cellule s'organise en général autour d'une personnalité se distinguant par son passé ou son charisme personnel. Elle constitue la particule élémentaire de la galaxie terroriste, agrégeant un nombre limité d'individus autour d'un noyau dur comptant, en règle générale, de cinq à quinze personnes. En variant sa composition au gré de ses missions, elle peut remplir un rôle de radicalisation idéologique, un rôle logistique ou un rôle opérationnel, et passer facilement de l'un à l'autre.

Quel que soit l'environnement, et même dans un contexte de guérilla comme en Irak en 2006, la cellule constitue l'unité de base autour de laquelle s'organise la lutte. Pour comprendre le fonctionnement d'une cellule, il faut déterminer son degré d'autonomie par rapport à ses semblables et à d'éventuels donneurs d'ordres extérieurs. L'observation des grands attentats attribués à Al Qaïda a permis de dégager une grille d'analyse générale, reposant sur la « théorie des trois cercles ».

La « théorie des trois cercles »

Cette théorie range les attaques perpétrées par la mouvance Al Qaïda en trois catégories : l'attaque terroriste décidée et exécutée par Al Qaïda stricto sensu agissant seule (le premier cercle) ; l'attaque planifiée par Al Qaïda et réalisée avec des éléments extérieurs (le deuxième cercle) ; l'attaque décidée et réalisée par des éléments extérieurs, qui se réclament de la mouvance Al Qaïda (le troisième cercle).

D'après ces critères, l'attentat de Madrid de mars 2004 entretrait probablement dans la troisième catégorie, ceux de Londres en juillet 2005 peut-être dans la deuxième et ceux du 11 septembre 2001 évidemment dans la première.

Le dernier cas de figure possible est l'individu, influencé par la mouvance mais décidant seul, ou presque, de son acte, de ses modalités et de son exécution.

C'est encore largement une hypothèse d'école en 2006. Mais l'exemple de l'assassinat de Théo Van Gogh¹ en novembre 2004 à Amsterdam donne à penser que cette éventualité n'est plus irréaliste.

(1) Metteur en scène néerlandais ayant fait référence de manière critique à l'islam et à certains groupes religieux islamistes radicaux dans ses œuvres.



Le terrorisme mondial renouvelle ses recrues, adapte ses méthodes et signe son mode opératoire

Des terroristes plus difficiles à repérer

Le recours à la violence et l'engagement dans des activités terroristes resteront toujours l'œuvre de minorités marginales. Le terrorisme mondial d'inspiration islamiste n'échappe pas à la règle. Il est ultra minoritaire, y compris au sein des communautés musulmanes elles-mêmes.

Il représente cependant une menace accrue et plus difficile à prévenir que par le passé, en raison de la diversification de ses méthodes et de ses cibles de recrutement.

Une minorité aux profils variés

Bien que la réalité se laisse difficilement réduire à des stéréotypes, c'est inévitablement chez les musulmans que les filières terroristes islamistes cherchent en premier lieu à recruter. Le profil majoritaire à ce jour concerne de jeunes hommes musulmans, de moins de 40 ans. Les femmes ne représentent que de rares exceptions.

Mais les origines, les parcours et les personnalités des terroristes présentent une variété inattendue qui exclut tout ciment commun, tout déterminisme simpliste dans les facteurs de l'engagement. Le déclassement ou la misère économique, sociale et culturelle peuvent jouer un rôle. Mais il n'est certainement pas aussi décisif qu'on le proclame parfois.

Ce qui transparaît chez les individus est un sentiment mêlé de frustration et d'injustice. Frustration face à ce qui est ressenti comme une perte d'identité frappant la communauté musulmane. Injustice dont seraient systématiquement victimes les musulmans dans le monde.

Le caractère cosmopolite et socialement diversifié des membres de la mouvance terroriste mondiale témoigne de la réalité et de l'enracinement d'une sorte de rage fédératrice et collective qu'il serait gravement erroné de tenir pour passagère.

La succession de trois générations

Au moins trois générations constituent le noyau dur du terrorisme mondial :

- les vétérans de la première guerre d'Afghanistan, dont beaucoup ont été neutralisés ou se sont retirés ;
- les militants formés dans les camps d'entraînement afghans à l'époque des Taliban ;
- les nouvelles recrues dont l'engagement se place sous la bannière de la « génération Irak », et chez lesquelles on constate plus fréquemment une propension à l'acte kamikaze.

Ces trois strates de recrutement coexistent au sein des réseaux actuels. La première, même décimée, fournit les figures historiques, la deuxième l'encadrement actif, la troisième les fantassins.

Les deux premiers groupes demeurent dangereux. Ils s'apparentent aujourd'hui à la catégorie des révolutionnaires professionnels, vieux routiers des zones de combat, rompus à la clandestinité, auréolés de leurs faits de gloire, de leur statut de combattant formé dans les camps, de leurs séjours en prison, ou, pour une minorité, de leur savoir théologique. Ils sont à ces divers titres plus ou moins répertoriés et localisés, en dépit de leurs multiples identités. Certains font l'objet d'une mise à l'index internationale sur des listes publiées sous l'autorité du Conseil de sécurité des Nations unies qui impliquent le gel de leurs avoirs ou des interdictions de séjour et de transit.

Au total, ils constituent un ensemble fermé de quelques milliers d'individus, dont une partie significative a déjà en 2006 été mise hors d'état de nuire ou a fait le choix de se retirer d'elle-même. Une part des survivants n'en demeure pas moins active. Elle use de son prestige et de son expérience pour rallier à la cause les jeunes recrues de la troisième génération.

Une procédure de ralliement bien rôdée

Le recruteur s'appuie sur les liens de proximité que créent la région, la tribu, le clan, la famille ou le voisinage (au sein de quartiers, de mosquées, de clubs de sport ou de prisons) pour faire jouer les ressorts traditionnels de l'embrigadement. De ce point de vue, la mobilisation relève de mécanismes plus politiques ou psychologiques que religieux.

En pays musulman seront invoqués les idéaux de pureté et de désintéressement, auxquels la jeunesse est particulièrement sensible, pour la dresser contre « l'occupant » ou contre un pouvoir corrompu.

En milieu occidental, seront plutôt exploitées les vulnérabilités dont souffrent les générations successivement issues de l'immigration, y compris celles qui viennent de pays non musulmans (Caraïbes). L'objectif est de canaliser vers le renouveau religieux et la révolte le mal-être qui existe dans certaines grandes agglomérations.

Les « born again »

Le phénomène de la « re-naissance » musulmane constitue une des réponses possibles au besoin de recherche identitaire qu'éprouvent certaines personnes parmi les plus vulnérables de notre société, souvent jeunes, issues de l'immigration ou de quartiers défavorisés, au parcours familial ou professionnel heurté.

Cherchant à résoudre leurs problèmes personnels, elles se tournent vers l'islamisme radical, qui offre une « solution » idéologique simpliste et totalisante. Vécue sur le mode sectaire ou sur celui de la radicalisation politique, en opposition avec le milieu familial et social environnant, cette conversion se distingue nettement du retour aux valeurs religieuses de l'islam héritées de la tradition familiale et culturelle.

Pris en main par un recruteur charismatique et endurci par l'influence d'un groupe restreint de pairs, le « born again » retrouve des repères, l'estime de lui-même et le respect de son entourage.

Le chemin vers la violence terroriste n'est heureusement pas automatique. Mais l'étape de la « re-naissance » peut dans certains cas y préparer les individus les plus influençables lorsque des circonstances politiques accèdent à leurs yeux la thèse d'un islam agressé et humilié.

L'exploitation des failles psychologiques des recrues potentielles est toujours puissamment aidée, en pratique, par la dynamique de groupe restreint qu'engendre la cellule. Celle-ci offre en effet un cadre recréant une forme de lien social entre des êtres qui en manquent. Elle exerce surtout sur eux une pression entre pairs propice à verrouiller l'engagement initial au cas où celui-ci viendrait à vaciller. C'est aussi en son sein

que s'opère l'idéologisation, c'est-à-dire le basculement des motivations personnelles, d'ordre social ou familial, vers un engagement politico-religieux à finalité collective.

Ces méthodes sont d'autant plus efficaces que le milieu dans lequel elles opèrent est fermé. Cela explique leur succès en milieu carcéral.

On constate enfin que, même si le passage à l'acte résulte toujours, en dernière instance, d'une décision individuelle mûrie solitairement, il est quasiment toujours exécuté dans un cadre collectif, surtout s'il s'accompagne du suicide de ses auteurs.

Une troisième vague plus problématique que les précédentes

La description du mode de ralliement des nouveaux terroristes permet de comprendre que la troisième vague pose des problèmes différents de ceux que soulèvent les deux premières.

Si l'on fait exception des « retours d'Irak », inscrits dans la même veine, identifiable, que celles des anciens d'Afghanistan ou de Bosnie, la caractéristique principale des nouvelles recrues est d'être particulièrement difficiles à repérer.

Les nouvelles recrues peuvent donner l'apparence d'une intégration réussie. Elles ne se font remarquer ni par une ferveur religieuse ou un militantisme particuliers ni par des démêlés antérieurs avec les services de police. Elles ne se démarquent en rien, ou si peu, du lot commun de la jeunesse, dont elles reflètent l'hétérogénéité des origines sociales et des niveaux d'éducation. Cette discrétion recherchée contribue à élargir considérablement le nombre des milieux potentiellement à risque, ce qui est d'autant plus problématique que le processus de radicalisation s'est accéléré.

Cette description correspond au portrait des terroristes qui ont frappé Madrid en mars 2004 et Londres en juillet 2005.

* * *

La menace présentée par le terrorisme mondial d'inspiration islamiste devrait être durable. Pourtant catalysé depuis 2003 par le rayonnement du foyer irakien, ce terrorisme ne s'est pas transformé en mouvement de masse. Mais il n'éprouvera aucun mal à renouveler ses effectifs, même s'il continue à être soumis à des pertes sévères.

Une gestion efficace des flux d'information, de financement et de déplacements

Les promoteurs du terrorisme mondial d'inspiration islamiste s'accrochent, bien qu'ils s'en défendent, de la société moderne. Ils en exploitent en tout cas systématiquement les opportunités.

La mondialisation se traduit notamment par la multiplication et l'accélération des flux d'information ou d'argent. Les terroristes saisissent toutes les possibilités offertes par ces échanges, très difficilement contrôlables, pour dissimuler leurs activités clandestines ou, à l'inverse, pour valoriser leurs faits d'armes en tirant parti de toutes les ressources de la médiatisation.

La flexibilité et la légèreté des structures des réseaux terroristes permettent à ceux-ci d'épouser les évolutions induites par la mondialisation plus facilement que les États chargés de les combattre.

L'usage par les terroristes des moyens de communication

Le réseau internet, outil du terrorisme moderne

Le « web » est le modèle qui figure le mieux l'activité du terrorisme mondial. Il est non seulement en totale adéquation avec la structure de la mouvance terroriste. Mais il est surtout devenu pour elle un vecteur à tout faire. Elle s'y sent chez elle.

Le réseau internet permet à un individu ou à un groupe, même minuscule ou clandestin, de s'adresser instantanément et ouvertement au monde entier. Il permet tout aussi bien de se mettre en rapport, pareillement immédiat mais discret, avec un nombre restreint de partenaires sélectionnés. Les caractéristiques propres du réseau sur lequel transitent des flux incomensurables de données offrent de bonnes conditions d'anonymat.

Pour leurs besoins de propagande, de recrutement, de formation à distance ou de transmission de messages, les terroristes utilisent toutes les ressources d'internet, des espaces ouverts aux espaces protégés. Les services les plus récents fournis par le réseau peuvent même les aider à améliorer leurs capacités de repérage des cibles potentielles, grâce aux données de toutes sortes, y compris géographiques, voire d'imagerie satellitaire, qui s'y trouvent en accès libre.

Le résultat de cet usage intensif d'internet est la création d'un espace virtuel, dont la portée dépasse le cadre du terrorisme. La communauté d'internautes sympathisants ainsi fédérée peut nourrir l'illusion d'une *oumma*¹ réunifiée, sans frontières ni nationalités, unie contre un

(1) Communauté des croyants.

ennemi commun. Certains estiment même que le terrorisme mondial d'inspiration islamiste cherche à créer un « califat virtuel ».

Le détournement de la télévision à des fins de propagande

Reçue dans tous les milieux et regardée à tous les âges, la télévision par satellite est un autre moyen privilégié de propagande.

Dans la rhétorique du terrorisme islamiste, l'Occident fait de l'image et du son les vecteurs d'intrusion de ses valeurs dans chaque foyer musulman. Cependant, force est de constater que les terroristes et, plus largement, certains groupes extrémistes religieux musulmans, utilisent aujourd'hui la télévision pour servir leurs fins. Celle-ci renvoie ainsi aux spectateurs les images d'otages implorant avant leur décapitation ou d'attentats-suicide, ponctuées par les appels lancinants d'Oussama Ben Laden et d'Ayman Al Zawahiri. L'objectif des terroristes est d'envoyer des messages de mobilisation à ceux dont ils se réclament et de démoraliser l'adversaire.

Si les grands médias transnationaux du monde arabo-musulman font généralement preuve du professionnalisme nécessaire pour éviter l'instrumentalisation, tel n'est pas le cas de toutes les chaînes satellitaires.

Le téléphone portable est lui aussi adapté à la structure très éclatée des réseaux terroristes

Les facultés de repérage sur les réseaux de téléphonie mobile sont plus importantes qu'auparavant. Mais les possibilités qu'offrent ces réseaux sont trop tentantes et les moyens d'y préserver l'anonymat encore suffisamment efficaces pour que leur utilisation soit évitée par les terroristes, soit à des fins opérationnelles soit, plus prosaïquement, à des fins personnelles.

Les flux de financement du terrorisme

Le financement du terrorisme se pose en termes aigus sur les « terres de jihad ». Dans ces zones, le combat paramilitaire et ce qu'il implique (achat d'armes et de munitions, acheminement et soutien des combattants, voire de leurs familles) coûtent effectivement très cher. Autant que les matériels nécessaires aux attentats, c'est le recours à des « terroristes à plein temps » qui entraîne des coûts importants. Il implique un financement structuré, qui s'alimente à deux sources principales. La première est la captation d'une fraction de la rente pétrolière, notamment dans le golfe arabo-persique. La seconde provient des réseaux de collecte établis dans les pays occidentaux. Certains imams détournent une partie de la *zakat*, contribution versée à la mosquée par les croyants.

La sécurité des transferts est assurée par la diversité des canaux, qui s'inscrivent le plus souvent possible en dehors des circuits bancaires afin de faire échec aux mesures de surveillance et d'alerte des mouvements de fonds internationaux.

Les envois par mandat postal, fractionnés, sont utilisés. Les ONG caritatives islamiques ont longtemps constitué un vecteur prépondérant, avant que leurs activités ne soient soumises dans notre pays à un contrôle accru, depuis 2002. Mais d'autres moyens tout aussi discrets subsistent. C'est le cas des vecteurs traditionnels les plus archaïques, qui n'ont rien perdu de leur efficacité. Les courriers humains sont ainsi largement utilisés, ainsi que le canal de la *hawala*¹. Enfin, des formes monétaires modernes sont apparues, qui permettent des transferts de fonds anonymes².

En Europe, les besoins locaux sont bien moindres, en raison d'activités opérationnelles encore rares et peu coûteuses. La question des flux de financement du terrorisme s'y pose donc en des termes différents. Le coût d'exécution des attentats perpétrés à Madrid en mars 2004 ou à Londres en juillet 2005 est évalué entre 15 000 et 20 000 euros. Les cellules peuvent se contenter de recourir à la délinquance, voire à la petite délinquance, pour assurer leur financement.

Les déplacements de personnes

Les mouvements de personnes demeurent indispensables dans certains cas, tels que l'acheminement des volontaires vers les « terres de jihad », le séjour ponctuel d'un spécialiste ou la transmission de messages ou d'argent par courrier humain. Ils nécessitent alors la confection de faux documents d'identité et de voyage, assurée par quelques experts, dont l'activité est vitale pour la sphère terroriste.

L'un des traits les plus inquiétants de l'évolution récente tient précisément à ce que ces déplacements – dangereux, car repérables – deviennent de moins en moins nécessaires en raison des possibilités généralisées, y compris en Europe, de recrutements locaux et de services fournis par internet.

Des modes opératoires classiques et pourtant reconnaissables entre tous

Le terrorisme mondial confère à ses opérations, où qu'elles se produisent, une marque immédiatement reconnaissable, voulant accréditer

(1) Système informel de transfert international de fonds utilisé dans le monde musulman. Il fonctionne par compensation entre correspondants.

(2) C'est le cas des cartes magnétiques prépayées, dites *Cash U Cards*, utilisées dans les pays arabes et au Royaume-Uni. Moins sécurisées que les cartes de crédit, elles sont anonymes et ne nécessitent aucune ouverture de compte. Elles permettent de transférer des fonds ou d'effectuer des achats en ligne sans l'intermédiaire d'une banque.

l'idée d'une entreprise globale capable de frapper à tout moment et en tout lieu (*cf.* annexe 1).

À l'exception des attentats du 11 septembre 2001, on doit constater que les promoteurs du terrorisme mondial ont cherché le plus souvent à aller au plus simple. Ils se sont contentés jusqu'ici de généraliser l'usage de l'explosif et de l'attentat suicide. Leur « marque de fabrique » n'est donc pas révélée par la nature des attentats.

Leur originalité se situe plutôt dans les modalités d'exercice. Celles-ci se caractérisent en premier lieu par la simultanéité des explosions sur un ou plusieurs sites (treize charges dans quatre trains à Madrid en mars 2004 ; attaques simultanées de trois rames de métro et d'un bus à Londres en juillet 2005 ; explosions de plusieurs centaines de charges de faible puissance au Bangladesh en 2005). Ce sont aussi le choix de cibles dites « molles », c'est-à-dire non directement protégées et de nature civile, ainsi que la volonté de causer le maximum de pertes humaines. C'est enfin la gestion du temps, caractérisée à l'origine par l'effet de surprise des échéances, longtemps déconnectées de tout calendrier politique, et par la répétition lancinante des attaques dans la durée.

La marque de fabrique apposée sur les attentats causés par le terrorisme mondial depuis 2001 a toutefois connu une certaine évolution, sous l'effet du processus « d'irakisation » du mouvement. En Irak même, le développement d'une guérilla à l'ancienne, qui a rapidement atteint une très grande échelle, a favorisé le retour aux assassinats ciblés et aux prises d'otages. Les attentats-suicide se sont multipliés. Par contagion, ces procédés ont commencé à se répandre hors d'Irak pour gagner d'abord l'Arabie saoudite, puis l'Afghanistan, le Maghreb et même l'Europe.

Les attaques menées en Europe ont été, semble-t-il, rattachées à des échéances politiques (élections législatives en Espagne en 2004 ; sommet du G8 au Royaume-Uni en 2005). Certains y ont décelé la volonté de peser directement sur la vie politique des États. Il peut tout simplement s'agir de la recherche d'un impact médiatique et symbolique maximal. En dépit de leur succès, les attentats commis en Europe ont été aussi caractérisés par le relatif amateurisme de recrues locales formées sur le tas et probablement autofinancées.

Au début de l'année 2006, notre continent a donc expérimenté tous les procédés, sinon utilisables, du moins utilisés jusqu'alors par le terrorisme mondial : attentats aveugles et simultanés, assassinat ciblé, franchissement de la barrière du suicide.

Le terrorisme mondial continue de privilégier l'importance du nombre instantané de victimes sur toute autre considération. Ce choix demeure guidé par la volonté d'adresser un message d'hostilité frontale au monde que les cibles retenues symbolisent. Mais quelle que soit l'efficacité de ce mode opératoire, sa répétition apparaît à long terme en contradiction avec l'exigence de nouveauté et de surenchère à laquelle se sont soumis les terroristes.

Des perspectives préoccupantes pour la France

La France est un objectif particulier au sein de l'Europe, cible du terrorisme

Le terrorisme mondial d'inspiration islamiste n'épargne pas la France

La France mène une politique extérieure équilibrée, qui prône le respect du droit et le multilatéralisme et qui est à l'écoute des pays les plus défavorisés. En aucun cas cette politique n'est dirigée contre un État. En dépit de cela, notre pays fait l'objet d'attaques de la part des inspirateurs du terrorisme mondial.

Le réquisitoire est toujours construit autour des mêmes griefs : passé présenté comme particulièrement lourd (des croisades jusqu'à la colonisation) ; présence militaire sur des terres musulmanes (par exemple à Djibouti) ; soutien affirmé aux régimes « apostats », spécialement au Maghreb ; laïcité affichée de l'État républicain ; prétention à organiser l'islam selon un modèle national (avec la création en 2003 du Conseil français du culte musulman) ; détermination des juges et des services français à neutraliser préventivement les terroristes et leurs complices.

Deux griefs supplémentaires sont venus s'ajouter, dans la période la plus récente. Il s'agit de la loi du 15 mars 2004 sur les signes religieux à l'école¹, démonstration de notre attachement sans faille à la laïcité, et de la participation des forces françaises aux opérations menées en Afghanistan.

La France est directement visée, de manière réitérée, par les diverses déclarations de guerre proférées par les porte-parole du terrorisme mondial d'inspiration islamiste.

Dès 1998, année de la création d'Al Qaïda dans sa forme historique, Oussama Ben Laden avait ainsi inscrit les implantations militaires françaises à Djibouti parmi les 23 objectifs de l'organisation. Par la suite, la visite en France, en avril 2001, du commandant Massoud, ennemi déclaré des Taliban², avait amené le chef d'Al Qaïda à tenir des propos virulents contre notre pays, dénoncé comme son deuxième adversaire après les États-Unis.

Depuis le 11 septembre 2001, pas moins de neuf communiqués ont allongé la liste des appels à nous punir. Parmi les principaux, on peut citer celui d'Ayman Al Zawahiri en date du 24 février 2004 et celui publié le 18 mai 2005 par Abou Moussab Al Zarkaoui, chef d'Al Qaïda en Irak, dénonçant tous deux la loi prohibant les signes religieux à l'école. Plus préoccupantes encore sont les déclarations de « l'émir » du Groupe salafiste pour la prédication et le combat (GSPC) qui, durant l'été 2005, a qualifié la France « d'ennemi n° 1 », confirmant l'hostilité ouverte des extrémistes maghrébins à l'égard de l'ex-puissance coloniale.

L'attentat de Karachi, le 8 mai 2002, contre les ingénieurs de DCN³, l'attaque contre le pétrolier Limburg, le 6 octobre 2002, et l'enlèvement des otages français en Irak dès 2004 ont confirmé que notre pays ne faisait pas l'objet d'un « traitement particulier » et qu'il n'était pas préservé des agressions. En outre, les nombreuses tentatives déjouées sur le sol national depuis 1998, à Strasbourg ou dans la région parisienne⁴, montrent que certains groupes ont déjà formé le projet de s'en prendre directement à la France par des attentats de grande ampleur (*cf.* annexe 2).

(1) La loi n° 2004-228 du 15 mars 2004 encadre, en application du principe de laïcité, le port de signes ou de tenues manifestant une appartenance religieuse dans les écoles, collèges et lycées publics. Son application est circonscrite aux écoles publiques de l'enseignement primaire et secondaire.

(2) Et assassiné le 9 septembre 2001 par des proches d'Oussama Ben Laden, deux jours avant les attentats perpétrés aux États-Unis.

(3) L'ancienne direction des constructions navales.

(4) Par exemple, et entre autres : 5 octobre 2001, démantèlement d'une cellule islamiste algérienne soupçonnée de préparer un attentat à l'occasion du match de football France-Algérie du 6 octobre 2001 ; 16 décembre 2002, démantèlement à La Courneuve d'une cellule soupçonnée de préparer des attaques non conventionnelles (à l'aide de produits chimiques) ; 26 septembre 2005, opération de police menée en France contre une cellule d'anciens membres du GIA soupçonnés de préparer des attentats contre le siège de la DST (Direction de la surveillance du territoire), l'aéroport d'Orly et le métro parisien.

L'Europe, cible du terrorisme

Plus proche et plus accessible que les États-Unis depuis le Moyen-Orient, l'Europe offre une alternative à quiconque envisage de s'en prendre à « l'ennemi lointain ». Elle comporte un vaste éventail de cibles spectaculaires, pour certaines liées aux États-Unis ou à Israël, de nature à assurer un retentissement planétaire aux attaques dont elles seraient l'objet. Enfin, l'Europe compte un nombre important de musulmans qui la mettent en prise directe avec les zones de crise.

L'espace Schengen ¹ auquel appartient notre pays se caractérise par l'existence d'une frontière extérieure unique où sont effectués les contrôles d'entrée, selon des procédures identiques et à partir d'un fichier recensant les personnes indésirables. Il se caractérise aussi par la suppression des contrôles aux frontières intérieures. Sa mise en place a constitué une étape importante dans le processus de construction européenne. Elle doit être consolidée car, si cet espace n'est pas facile à pénétrer, la libre circulation des personnes en son sein peut faciliter l'organisation et les déplacements des filières installées en Europe.

Les causes du basculement du continent européen dans la catégorie des zones opérationnelles sont à rechercher dans divers facteurs aggravants de la menace, récemment apparus.

Les facteurs d'une menace aggravée pour la France et pour l'Europe

Le premier des facteurs d'aggravation est le développement d'une génération de « révoltés à domicile », de nationalité française ou non, musulmans de longue date ou récemment convertis.

Si les islamistes partis de France pour combattre en Irak en revenaient ou si certains des milliers de combattants maghrébins qui s'y sont rendus en faisaient autant, un deuxième facteur d'aggravation de la menace prendrait corps immédiatement. De tels terroristes, auréolés de prestige, pourraient représenter une force d'attraction pour de nombreux jeunes de la même génération. Ces nouveaux « gradés » pourraient devenir l'âme de nouveaux réseaux, auxquels ils apporteraient en outre des compétences en matière de terrorisme urbain.

(1) Du nom de deux conventions, signées en 1985 et 1990 dans cette ville du Luxembourg par cinq pays dont la France. Cette coopération a été intégrée de plein droit dans les politiques communautaires depuis l'entrée en vigueur du traité d'Amsterdam en 1999. Elle regroupe aujourd'hui les quinze membres historiques de l'Union, avec des régimes spéciaux pour le Danemark et le Royaume-Uni, et a été élargie, selon des modalités particulières, aux pays non-membres que sont la Norvège, l'Islande et la Suisse.

Le troisième facteur d'aggravation est le mouvement de « transnationalisation » du terrorisme des groupes algériens, libyens, marocains et tunisiens. Aiguillonnées par certains terroristes à la pointe du combat en Irak, fortes désormais d'un sentiment d'appartenance à une cause fédératrice, les cellules de soutien, notamment au GSPC, qu'abritent la France et ses voisins pourraient être tentées de suivre la voie, tracée il y a dix ans par celles affiliées au GIA, et basculer de l'appui logistique au combat en Algérie à des actions violentes dirigées contre la France.

Un dernier facteur aggravant de la menace tient à sa discrétion et à sa décentralisation croissantes. L'accès par l'intermédiaire du réseau internet à toutes sortes de compétences ou, dans un registre différent, la radicalisation en milieu carcéral, dispensent les apprentis terroristes de toute intégration à un mouvement fondamentaliste et de tout déplacement vers des écoles coraniques (comme les *madrassas* pakistanaises ¹⁾ ou vers des camps d'entraînement moins nombreux et plus lointains. Les contacts avec les vétérans peuvent ainsi se nouer de manière plus discrète.

La gestation de la menace comporte désormais une part quasiment silencieuse, plus difficilement détectable par les services de renseignement et de sécurité.

L'évolution récente du terrorisme mondial dans le sens d'une plus grande atomisation devrait impliquer normalement une moindre sophistication des actions. Il reste à déterminer si cette tendance restera longtemps exclusive d'un mouvement inverse vers des modes opératoires plus spectaculaires ou plus meurtriers.

Car on ne peut exclure une autre mutation qui conduirait au terrorisme nucléaire, radiologique, biologique ou chimique. Nul interdit moral ne s'y oppose du point de vue des terroristes. Ceux-ci ont en effet suffisamment démontré qu'aucune horreur ne les rebutait et qu'ils ne négligeraient *a priori* aucun mode opératoire pour peu qu'il réponde à leurs critères d'efficacité. Il ne fait aucun doute, d'ailleurs, que certains d'entre eux ont déjà réfléchi à l'utilisation de telles armes et qu'ils ont songé à s'en procurer. Oussama Ben Laden a ainsi fait mention, à plusieurs reprises, du besoin de l'islam de se doter d'armes nucléaires ou chimiques ²⁾. Plusieurs théologiens extrémistes ont légitimé dans leurs écrits l'utilisation d'armes de destruction massive contre des civils occidentaux. Les opérations menées en Afghanistan par la coalition ont en outre permis d'établir qu'Al Qaïda avait mené, avant 2001, des recherches assez avancées dans les domaines biologique et chimique, avec le concours d'experts de bon niveau. Plusieurs terroristes interpellés en France depuis 2001 s'étaient engagés dans des projets terroristes comportant un volet non conventionnel rudimentaire.

(1) Certaines de ces écoles ont été repérées comme des centres de formation du terrorisme mondial d'inspiration islamiste.

(2) Ses propos pouvaient laisser penser néanmoins qu'il se référait davantage à l'ensemble des peuples musulmans qu'à sa propre organisation.

Plusieurs obstacles se dressent encore en travers de la volonté de commettre un attentat d'une telle nature. Il faut tout d'abord disposer d'un niveau minimal de connaissances scientifiques ou techniques. Il demeure encore le plus souvent ardu de se procurer les matières, les composants ou les matériels nécessaires. Les manipulations sont souvent complexes et dangereuses. Un attentat perpétré à l'aide de moyens non conventionnels ne peut réussir que dans des conditions d'exécution bien précises. Il comporte donc un certain risque d'échec. La perte du sanctuaire afghan a aussi privé les terroristes de la capacité de développer des projets non conventionnels d'envergure. Ce sont probablement ces complications qui ont conduit Al Qaïda à adopter, sauf en de rares occasions, un processus opératoire plus rustique, associant des techniques éprouvées (recours systématique à l'explosif) avec un mode original d'utilisation (simultanéité massive dans des lieux ouverts au public).

Mais d'autres facteurs font craindre le recours à des formes de terrorisme utilisant des armes non conventionnelles. Le besoin de nouveauté dans la manipulation de la terreur en est un. La diffusion grandissante des technologies, des équipements et des savoir-faire nécessaires au terrorisme chimique et surtout biologique en est un autre. Elle permet en effet de franchir certains obstacles techniques. Le recrutement d'individus bien intégrés dans les sociétés européennes et disposant de formations en chimie et en biologie peut permettre la mise en œuvre de savoir-faire faisant appel à des produits chimiques hautement toxiques, facilement disponibles dans le commerce et l'industrie, ou à des protocoles de fabrication et d'emploi accessibles dans le domaine biologique.



Deuxième partie

**Le dispositif
français de lutte
contre
le terrorisme
doit continuer
à s'adapter**



La menace représentée par le terrorisme mondial est susceptible de se concrétiser par des types d'attentats très divers que notre pays doit être en mesure de contrer. Pour se préparer à faire face à toute éventualité, il convient d'éprouver notre dispositif de lutte à l'aune d'un nombre limité de scénarios mettant en évidence les principales mesures destinées à prévenir les actes de terrorisme et à y répondre s'ils n'ont pu être évités.

Sept scénarios pour tester notre dispositif de lutte antiterroriste

Les scénarios décrits ci-dessous ne sont pas des instruments de prédiction de l'avenir. Plusieurs d'entre eux sont aujourd'hui peu probables en raison de leur degré de complexité. Pris dans leur ensemble, ils permettent néanmoins de dessiner le contour des politiques que nous devons mener pour lutter efficacement contre le terrorisme dans toutes ses manifestations.

Campagne d'attentats à l'explosif

Un groupe terroriste tente de conduire une campagne d'attentats répétés étalée sur plusieurs mois sous forme d'explosions dans des lieux accueillant du public (métro, bus, aéroports, écoles...).

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- la capacité à identifier et à neutraliser au plus vite les auteurs des attentats ;*
- la capacité de l'ensemble des services judiciaires, de renseignement et de sécurité à mener durablement une activité intense ;*
- la capacité à maintenir la vigilance de la population et des services de l'État en faisant fonctionner le pays au rythme des mesures contraignantes du niveau rouge voire écarlate du plan VIGIPIRATE¹ pendant plusieurs mois ;*
- l'application dans la durée de mesures drastiques et cohérentes de sécurité à l'ensemble des grandes infrastructures recevant du public.*

Attentats multiples simultanés

Une organisation terroriste cherche à provoquer dans des établissements recevant du public des explosions simultanées en recourant notamment à des attentats-suicide. Les cibles retenues sont, par exemple, de grands centres commerciaux.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- l'action en amont des services de renseignement ;*

(1) Voir p. 70.

- les mesures de vigilance, de prévention et de protection prises dans le cadre du plan VIGIPIRATE ;
- la sécurisation interne, à un niveau élevé, d'un grand nombre d'établissements recevant du public ;
- la diffusion rapide de l'alerte ;
- le déclenchement simultané de plusieurs plans de secours aux victimes ;
- le renforcement des mesures de sécurité des matières premières correspondant aux explosifs utilisés (accès, traçabilité) pour éviter une seconde vague d'attentats.

Attentats diversifiés transfrontaliers

Trois équipes de terroristes tentent d'opérer simultanément dans plusieurs pays voisins. La première équipe a pour objectif de s'emparer d'un cargo appareillant d'un pays proche afin de provoquer un sinistre dans le terminal pétrolier de l'un de nos ports. La deuxième fomenté un attentat destiné à semer la confusion au voisinage immédiat d'une centrale nucléaire située près de la frontière. La troisième tente de s'attaquer aux systèmes informatiques pour désorganiser les réseaux de secours.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- les procédures opérationnelles entre la France et ses voisins, y compris en matière de communication publique ;
- les mesures de prévention du cyberterrorisme ;
- les mesures de neutralisation et de réaction prévues dans les plans d'intervention spécialisés (PIRANET, PIRATE-MER, PIRATOME...)¹.

Attentat radiologique

Un terroriste tente de faire exploser une « bombe sale » (engin composé d'un explosif et de matières radioactives) dans un réseau souterrain de transport public.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- les mesures nationales et la coopération internationale en matière de contrôle des sources radioactives ;
- la capacité de détection précoce d'explosifs et de substances nocives ;
- la communication publique ;
- la décontamination des lieux pollués par les matières radioactives dispersées ;
- les mesures de neutralisation et de réaction prévues dans le plan PIRATOME.

(1) Voir p. 70.

Attentat chimique

Un groupe terroriste tente de répandre un neurotoxique puissant d'origine industrielle dans une grande gare à une heure d'affluence, avec pour objectif de provoquer un très grand nombre de victimes.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- la capacité de détection précoce de l'acquisition et de la transformation de produits précurseurs de composés neurotoxiques ;*
- les mesures de protection du plan VIGIPIRATE et les actions de mise en alerte et de neutralisation préventive du plan spécialisé d'intervention PIRATOX ;*
- la capacité d'identification immédiate du gaz neurotoxique et d'intervention rapide des services de sécurité et de secours en atmosphère potentiellement contaminée ;*
- la communication publique ;*
- la décontamination des lieux pollués par le gaz neurotoxique.*

Attaque biologique infectieuse

Un groupe terroriste tente d'acquérir un agent infectieux très contagieux et provoquant une mortalité importante. Il souhaite le répandre dans plusieurs endroits pour déclencher une épidémie susceptible de durer plusieurs mois.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- la détection précoce de l'épidémie par l'identification de signes cliniques diffus et le rapprochement d'analyses de plusieurs laboratoires ;*
- l'élaboration de procédures visant à confiner les foyers infectieux, à traiter les malades et à continuer à faire fonctionner les services économiques et sociaux dans la durée ;*
- la fabrication et la distribution de traitements prophylactiques et thérapeutiques ;*
- la communication publique ;*
- l'application d'une réglementation contraignante de situation d'urgence en matière de santé publique, limitant les mouvements et les activités de la population ;*
- les mesures de neutralisation et de réaction prévues dans le plan BIOTOX.*

Tentative de détournement d'une arme nucléaire

Un groupe terroriste tente d'acheminer une arme nucléaire depuis l'étranger vers un centre urbain en vue de provoquer une explosion.

Les aspects les plus sollicités de notre dispositif de lutte contre le terrorisme seraient :

- l'action internationale contre la prolifération des armes nucléaires ;*
- la capacité de détecter l'acheminement de l'arme et de mettre en œuvre une opération d'interception durant son transit ;*
- la capacité de neutralisation rapide de l'arme ;*
- les mesures de réaction prévues dans le plan PIRATOME ;*

- la capacité d'évacuation de la population ;
 - si le groupe terroriste parvenait à ses fins, la capacité de traitement des victimes à court terme et dans la durée, le maintien de capacités de communication en mode fortement dégradé, la réhabilitation des zones affectées.
-

Les scénarios évoqués ci-dessus ne sauraient être exhaustifs. D'autres menaces, susceptibles d'être mises à exécution, sont prises en compte par le dispositif national de lutte contre le terrorisme.

Pour parer à toutes les attaques envisageables, notre dispositif doit continuer à s'adapter. Nous devons avoir pour objectifs de prévenir les risques et les menaces par la surveillance, la détection et la neutralisation des terroristes potentiels, de réduire nos vulnérabilités, de renforcer nos capacités de gestion de crise terroriste et d'affirmer nos capacités de réparation et de sanction.

Chapitre 1

Prévenir le risque : surveiller, détecter, neutraliser

La mission de prévention est essentielle dans la lutte contre le terrorisme. Les moyens de détection des individus les plus dangereux, de neutralisation de ceux qui envisagent de passer à l'acte et de surveillance des milieux à risque existent dans notre pays. Cela est d'autant plus efficace que le système pénal français – et c'est sa force – n'établit pas de frontière étanche entre prévention et répression.

Cette mission de prévention mobilise chaque jour nos services de renseignement, nos forces de sécurité intérieure chargées de contrôler les personnes et les biens qui entrent, sortent et transitent sur notre territoire, nos magistrats antiterroristes, nos forces armées et notre diplomatie.

Le dispositif de prévention contre le terrorisme en place dans notre pays est solide et il a prouvé son efficacité. Mais l'évolution de la menace terroriste, caractérisée par le développement du terrorisme mondial, doit nous conduire à poursuivre l'adaptation de ce dispositif. Cet impératif a constitué un axe directeur de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme.

Renforcer les capacités des services de renseignement et de sécurité

Renforcer les capacités de repérage

L'efficacité de l'activité des services de renseignement et de sécurité, de police ou de gendarmerie réside dans la capacité de ces services à anticiper l'action violente et à analyser l'ensemble des mécanismes qui concourent au développement du phénomène terroriste pour mieux le contrer. Cela justifie l'amélioration de nos capacités de surveillance des communications électroniques, la facilitation de l'accès des services de renseignement et de sécurité à certains fichiers administratifs et une meilleure identification des voyageurs dangereux.

Améliorer la surveillance des communications électroniques

Comme on l'a vu, les acteurs du terrorisme mondial sont familiers du réseau internet, car celui-ci leur offre une bonne discrétion.

1) Par les normes techniques qui le régissent, le réseau internet est propice à la furtivité, la notion d'« identifiant »¹ y étant souvent virtuelle et temporaire.

2) Un individu peut multiplier les identifiants. Il peut ainsi disposer d'un très grand nombre d'adresses électroniques fournies soit par son opérateur internet soit par des fournisseurs de services mondiaux qui permettent, sans aucun contrôle d'identité, la création d'adresses de messagerie. Ces mêmes fournisseurs de services offrent aussi la possibilité, sans plus de contrôle, de créer des sites internet.

3) Les fournisseurs d'accès à internet sont nombreux. Certains sont moins sensibles aux préoccupations de sécurité que les opérateurs téléphoniques traditionnels.

4) Les services offerts se multiplient. Au début des années 2000, le courrier électronique et les forums² étaient les vecteurs prépondérants. En 2006, ceux-ci ne sont plus que des modes de transmission parmi d'autres : on peut communiquer par *chat*³, utiliser les systèmes de messagerie instantanée, créer des systèmes semi-privés de communication, se transmettre des fichiers, même très volumineux, en *peer to peer*⁴, télépho-

(1) Un « identifiant » est le nom que se choisit l'utilisateur ou qui lui est attribué pour s'identifier sur internet.

(2) Sites de discussion thématiques.

(3) « Discussion relayée par internet » (en anglais, *internet relay chat*), un *chat* permet de communiquer de manière instantanée avec d'autres personnes.

(4) *P2P*, c'est-à-dire directement d'ordinateur à ordinateur, sans que les données transitent par un système centralisé.

ner sans emprunter les réseaux habituels de téléphonie ¹, chiffrer les échanges grâce aux logiciels du commerce offrant cette possibilité et même discuter très facilement en vidéoconférence.

5) Les modes d'accès à internet se diversifient : à l'origine on y accédait par le téléphone fixe de son domicile. Aujourd'hui, on y accède aussi par le câble, par les réseaux de téléphonie mobile ou par satellite. Les points d'accès eux-mêmes se multiplient : on peut « naviguer » sur internet, et donc consulter sa messagerie à distance, dans les cybercafés, ou dans la plupart des lieux publics équipés d'une connexion *wifi* ², parfois en accès libre. Ces modes de connexion se développent sur les réseaux physiques et sur les nœuds de communication : on en trouve dans les hôtels, les gares, les aéroports, les stations services des autoroutes...

Le réseau internet comporte deux volets. L'un est ouvert. Il donne un accès libre à l'information à travers les sites web, certains *chats*, certains *forums*, certains *blogs* ³, dès lors que l'on se connecte aux bonnes adresses. L'autre est fermé. Il comporte notamment les messageries électroniques traditionnelles, les messageries instantanées, les comptes de téléphonie. L'accès à l'information est souvent protégé par des identifiants et des mots de passe.

La création, par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, d'une procédure de réquisition administrative des données de connexions auprès des opérateurs, sous le contrôle d'une autorité indépendante, permet aux services spécialisés d'agir plus efficacement et plus rapidement aux fins de prévention des actes de terrorisme. Le dispositif est activable 24 heures sur 24 en cas d'urgence.

Les services de renseignement doivent pouvoir identifier et sélectionner les informations dignes d'intérêt dans la masse de celles disponibles sur le volet ouvert d'internet. Ils doivent aussi pouvoir accéder, sous certaines conditions, à celles qui circulent sur le volet fermé.

Une adaptation de la loi du 10 juillet 1991 réglementant les interceptions de sécurité sera sans doute nécessaire, ne serait-ce que pour permettre de cibler, non plus seulement un numéro de téléphone prédéterminé, mais un individu, avec toute la palette des moyens de communication et des services qu'il utilise.

Nous devons en outre nous impliquer plus fortement dans l'entreprise de définition des normes auxquelles doit répondre internet. Pour cela, nous devons mener une politique d'influence plus déterminée dans les instances de régulation du réseau, tant sous l'angle de son développement opérationnel ⁴ que sous celui de la recherche plus fonda-

(1) Grâce par exemple à des logiciels disponibles en téléchargement gratuit, et pour l'utilisation desquels rien d'autre n'est exigé qu'un identifiant et un mot de passe.

(2) C'est-à-dire par réseau sans fil local.

(3) Un blog est un site internet sur lequel une ou plusieurs personnes peuvent s'exprimer, le plus souvent sous la forme d'un « journal de bord » (weBLOG).

(4) Au niveau de l'IETF, l'*Internet Engineering Task Force*.

mentale ¹, notamment afin de peser en faveur de choix techniques et juridiques permettant de limiter l'anonymat des échanges.

Autoriser l'accès des services de renseignement et de sécurité à certains fichiers administratifs « de droit commun »

La discrétion accrue des terroristes et leurs capacités de communication ou de déplacement dans un anonymat relatif sont des obstacles à l'action préventive efficace des services spécialisés. Ceux-ci doivent tenir compte de l'évolution du profil des nouvelles recrues. Ces dernières sont souvent soit inconnues au préalable des services de police, soit connues pour un passé délinquant de droit commun qui ne permet pas de préjuger d'un basculement vers le radicalisme islamiste.

Or, l'identification d'un terroriste avant tout passage à l'acte peut dépendre de la vérification d'un simple renseignement opérationnel, souvent dans l'urgence.

Jusqu'en 2006, les services de renseignement n'avaient pas légalement accès aux fichiers administratifs courants ², à l'inverse de la plupart de leurs homologues étrangers. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme leur a donné accès aux données personnelles contenues dans ces fichiers, gérés par le ministère de l'Intérieur, afin qu'ils soient en mesure de procéder aux vérifications qui s'imposent dans les délais opérationnels utiles.

Toutes les interrogations effectuées par les services de police sont conservées et placées sous le contrôle de la Commission nationale de l'informatique et des libertés (CNIL). Elles ne concernent que des données personnelles non sensibles, comme l'état civil ou l'adresse. L'accès éventuel à des données plus sensibles, comme celles contenues dans les fichiers bancaires, fiscaux ou sociaux, n'est possible que dans le cadre d'une procédure judiciaire.

Mieux identifier les voyageurs dangereux

Pour les services de police chargés de la lutte antiterroriste, il est déterminant d'avoir accès à des informations sur les voyageurs se rendant de manière régulière ou prolongée dans les pays connus pour abriter des lieux de radicalisation, ainsi que sur les déplacements des individus déjà repérés.

Le Fichier national transfrontière (FNT) répond dans son principe à cet objectif. Son mode d'alimentation est toutefois devenu inefficace et obsolète. Les fiches d'embarquement et de débarquement remplies par les passagers concernés sont purement déclaratives et ne peuvent faire l'objet d'un contrôle systématique. En outre, la saisie manuelle des fiches

(1) Ce travail de recherche revient à l'IRTF, l'*Internet Research Task Force*.

(2) Fichiers des cartes d'identité et des passeports ; fichiers des visas et des titres de séjour ; fichiers des cartes grises et des permis de conduire.

est devenue un travail gigantesque avec la croissance des flux du transport aérien. Elle monopolise indûment des agents requis pour effectuer des contrôles de sûreté et des contrôles aux frontières. En autorisant l'alimentation automatique du FNT à partir de la lecture optique des documents de voyage et des visas au moment du contrôle transfrontalier, la loi du 23 janvier 2006 a ouvert le chantier de la modernisation rapide de ce fichier.

Les fichiers des compagnies aériennes sont eux aussi une source d'information utile à la lutte antiterroriste. Il en existe deux types : les fichiers commerciaux de réservation¹ et les fichiers de contrôle des départs². Tous deux comportent des données nominatives relatives aux voyageurs ainsi que des informations sur les vols empruntés.

L'accès aux données de réservation, de contrôle des départs et de contrôle transfrontalier avant le vol permet aux services chargés de la lutte contre le terrorisme de procéder à des vérifications parfois plusieurs jours avant le déplacement. L'efficacité du traitement de l'information antiterroriste implique que ces données soient rapprochées entre elles et, dans certains cas, conservées dans un fichier unique. Dans tous les cas, elles doivent faire l'objet d'un « croisement » avec le fichier des personnes recherchées.

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a prévu que le régime relatif au transport aérien puisse être étendu aux déplacements internationaux maritimes et ferroviaires dès lors qu'une frontière extérieure de l'Union européenne est franchie.

Assurer la coordination des services de renseignement et de sécurité en matière de lutte contre le terrorisme

Pour être la plus efficace possible, l'action des différents services spécialisés dans la lutte antiterroriste nécessite une étroite coordination.

Depuis les attentats du 11 septembre 2001 aux États-Unis, un mouvement de restructuration des instances de coordination du renseignement a été mené chez nos principaux partenaires. Les États-Unis ont créé la fonction de « directeur national du renseignement³ » auprès du prési-

(1) Ces fichiers dits « PNR » (*Passenger Name Records*) comprennent un nombre variable de données collectées par les compagnies pour leurs besoins commerciaux. Si l'Organisation internationale de l'aviation civile a émis des recommandations, ils ne font pas l'objet d'une standardisation. En fonction de la destination, les compagnies aériennes sont tenues de transmettre aux services de police les données qu'elles détiennent.

(2) Ces fichiers dits « APIS » (*Advanced Passenger Information System*) font l'objet d'une standardisation internationale. Les compagnies aériennes sont tenues de recueillir un nombre défini de données auprès de leurs passagers, de les contrôler et de les transmettre aux autorités chargées du contrôle transfrontalier du pays de destination avant le départ de l'appareil.

(3) L'*Intelligence Reform and Terrorism Prevention Act* de 2004 a par ailleurs placé auprès de ce *Director of National Intelligence* une nouvelle structure de coordination qui lui est directement rattachée : le centre national du contre-terrorisme, *National Counterterrorism Center* (NCTC).

dent américain. Au Royaume-Uni, les autorités ont mis en place en 2003 une nouvelle structure inter-services d'analyse du terrorisme, le JTAC (*Joint Terrorism Analysis Center*). Fonctionnant 24 heures sur 24, cet organisme, qui regroupe des agents de onze ministères et agences, a pour fonction de centraliser, d'analyser et d'évaluer l'ensemble des renseignements relatifs au terrorisme international, aussi bien sur le territoire britannique qu'à l'étranger. La création du JTAC a permis de rapprocher le niveau opérationnel (l'action quotidienne des services sur le terrain) et l'échelon stratégique, représenté par le JIC (*Joint Intelligence Committee*) dirigé par le conseiller pour la sécurité du Premier ministre.

En France, les décisions majeures en matière de la lutte antiterroriste sont prises dans plusieurs enceintes de haut niveau. Présidé par le président de la République, le Conseil de sécurité intérieure (CSI) définit les orientations de la politique menée dans le domaine de la sécurité intérieure et fixe ses priorités¹. Le Premier ministre réunit les ministres concernés par la lutte antiterroriste pour coordonner leur action et fixer les orientations. Il préside le Comité interministériel du renseignement (CIR)². Ce comité conduit par ailleurs des travaux dans des formations techniques. Le ministre de l'Intérieur réunit le Comité interministériel de lutte antiterroriste (CILAT) afin de coordonner l'action engagée sur le plan interministériel. Le directeur du cabinet du Premier ministre relaie l'impulsion donnée par le Premier ministre en présidant des réunions régulières des hauts responsables des questions de sécurité³.

Au niveau opérationnel, l'Unité de coordination de la lutte antiterroriste (UCLAT), créée en 1984 au sein du ministère de l'Intérieur, assure la coordination de l'ensemble des services chargés de la lutte contre le terrorisme, en faisant au quotidien l'analyse et la synthèse des informations relatives au terrorisme. Elle travaille en relation étroite avec la DST, la DCRG, la gendarmerie nationale, la DGSE et la Direction générale des douanes. Elle veille au partage des informations opérationnelles pertinentes par l'ensemble des autorités et des services concernés par la lutte antiterroriste, y compris les magistrats antiterroristes et l'administration pénitentiaire.

(1) Selon le décret n° 2002-890 du 15 mai 2002 relatif au Conseil de sécurité intérieure. Le CSI réunit le Premier ministre, les ministres concernés et le secrétaire général de la défense nationale. Le secrétaire général du CSI est nommé par le président de la République et il est placé auprès de lui.

(2) Selon le décret n° 89-258 du 20 avril 1989, le CIR est chargé d'assurer l'orientation et la coordination des activités des services qui concourent au renseignement. Son secrétariat est assuré par le Secrétariat général de la défense nationale (SGDN), service qui relève directement du Premier ministre.

(3) Les « réunions renseignement » présidées par le directeur du cabinet du Premier ministre comprennent des représentants de l'état-major particulier du président de la République, du Conseil de sécurité intérieure, les directeurs de cabinet des ministres de l'Intérieur, de la Défense, des Affaires étrangères, le secrétaire général de la défense nationale, ainsi que les directeurs des principaux services de renseignement (DGSE, DST, DRM).

Les acteurs spécialisés de la lutte antiterroriste sur le territoire national

*L' **autorité judiciaire** comprend un parquet, un pôle d'instruction et des formations de jugement spécialisées dans le jugement des crimes terroristes. Toutes les affaires sont regroupées à Paris.*

*Au **ministère de l'Intérieur**, la plupart des services spécialement chargés de la lutte antiterroriste sont rattachés à la Direction générale de la police nationale (DGPN). La Direction de la surveillance du territoire (DST), outre ses missions classiques de contre-espionnage, concourt directement à la prévention et à la répression des activités terroristes grâce à ses attributions de police judiciaire et administrative. La Direction centrale des renseignements généraux (DCRG) a pour tâche de surveiller les groupes à risque. La Direction centrale de la police judiciaire (DCPJ) conduit de nombreuses enquêtes à travers sa Division nationale antiterroriste (DNAT). Dans le domaine de la délinquance financière, un de ses offices centraux spécialisés peut être co-saisi.*

L'Unité de coordination de la lutte antiterroriste (UCLAT) centralise les informations fournies par l'ensemble des services opérationnels, qu'ils relèvent du ministère de l'Intérieur, du ministère de la Défense, ou du ministère de l'Économie, des Finances et de l'Industrie. Cette unité assure également des échanges d'informations réguliers avec l'autorité judiciaire. Le RAID (Recherche, assistance, intervention et dissuasion), unité d'intervention de la police nationale, est à la disposition permanente de la DGPN en cas de crise. La Police aux frontières (PAF) veille aux entrées et sorties suspectes du territoire. À Paris, la préfecture de police dispose de cellules spécialisées de police administrative ou judiciaire. La gendarmerie nationale, rattachée pour emploi au ministre de l'Intérieur, participe à la lutte antiterroriste à travers sa couverture très étendue du territoire national.

*Au **ministère de la Défense**, la Direction générale de la sécurité extérieure (DGSE) joue un rôle essentiel en fournissant des renseignements recueillis hors du territoire national. La Direction du renseignement militaire (DRM) dispose de capacités de détection (notamment en matière d'imagerie spatiale) et d'analyse. Au titre de ses attributions militaires, notamment en opérations extérieures, la gendarmerie nationale joue aussi un rôle important. Par ailleurs, au sein de son groupement de sécurité et d'intervention (GSIGN), elle tient en permanence le GIGN disponible pour l'action antiterroriste. La Direction de la protection et de la sécurité de la défense (DPSD) assure enfin la protection contre le terrorisme des personnels et des établissements du secteur de la défense au sens large (État et industrie).*

Le ministère de l'Économie, des Finances et de l'Industrie dispose de plusieurs services associés à la lutte antiterroriste. La Direction nationale du renseignement et des enquêtes douanières (DNRED) recueille, analyse et diffuse des renseignements douaniers relatifs au financement du terrorisme. La cellule TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins) recueille des informations qu'elle enrichit en les confrontant à celles dont disposent d'autres ministères, pour les transmettre ensuite à la justice. La cellule FINATER (enceinte créée en octobre 2001 pour préparer et relayer les orientations ministérielles en matière de lutte contre le financement du terrorisme) intervient notamment pour geler les avoirs financiers des terroristes.

Coopérer avec nos partenaires étrangers

La coopération internationale dans le domaine du renseignement est d'abord traditionnellement une relation bilatérale de service à service. C'est dans ce cadre que transitent les informations les plus nombreuses et les plus opérationnelles. Cependant, il est apparu nécessaire d'élargir à un cadre multilatéral les coopérations, compte tenu des convergences d'intérêts ou de risques avec nos partenaires.

Dans l'Union européenne, a été créée, au lendemain des attentats de Madrid de mars 2004, une cellule d'analyse de la menace terroriste au sein du « Centre de situation » (SITCEN) placé sous l'autorité du secrétaire général du conseil, haut représentant pour la Politique étrangère et de sécurité commune (PESC). Ce centre de situation, auquel la France contribue de manière active, produit une évaluation de la menace, fondée sur les sources que lui fournissent les services de renseignement, les militaires, les diplomates et les services de police. Le SITCEN peut également apporter des contributions utiles sur des points opérationnels, tels que les destinations, les motifs et les circuits de déplacements de terroristes, afin de sensibiliser l'ensemble des États membres et de les aider à prendre chacun les mesures adéquates. L'expérience montre que les États de l'Union ont une perception de la menace très inégale et qu'un rapprochement des points de vue est très opportun.

La conservation des données de connexion relatives au téléphone fixe et mobile et à internet joue un rôle clé dans la lutte contre le terrorisme. C'est elle qui a permis, notamment dans le cas des attentats de Madrid en mars 2004, de remonter la filière terroriste. Les données de connexion concernent l'identification, la localisation et l'heure des appels, à l'exclusion du contenu des communications. La France a, dès 2001, pris la décision de prescrire aux opérateurs de communications électroniques de les conserver pendant un an. L'adoption de la directive européenne sur la conservation des données de connexion, qui prévoit une durée minimale de six mois de conservation, constituera une avancée très importante. Elle va permettre une coopération renforcée entre les États membres pour l'identification des terroristes.

Les chefs des services de sécurité intérieure de plusieurs pays européens se réunissent dans le cadre du **club de Berne** ¹, structure informelle d'échange d'informations dans des domaines tels que le contre-espionnage, la criminalité organisée et le terrorisme. Après les attentats du 11 septembre 2001 et sur recommandation de l'Union européenne, le club de Berne a créé un Groupe antiterroriste (GAT) qui réunit les responsables des unités de lutte antiterroriste. Celui-ci réalise des évaluations de la menace terroriste et des études thématiques portant par exemple sur les filières de faux documents et sur la menace NRBC ².

Au **niveau multilatéral**, ce sont essentiellement au sein du G8 ³ et de l'Organisation du traité de l'Atlantique nord (OTAN) que se font les échanges sur les analyses de la menace. Au sein du G8, le groupe dit des « praticiens » procède à des évaluations de la menace. Dans le cadre de l'OTAN, un comité spécial élabore des documents analytiques sur la menace terroriste qui pourrait affecter l'Alliance.

Conforter notre dispositif pénal et adapter notre système pénitentiaire à la menace terroriste

Conforter un dispositif pénal efficace

Pour être efficace, un dispositif judiciaire de lutte contre le terrorisme doit combiner un volet préventif, dont l'objet est d'empêcher les terroristes de passer à l'action, et un volet répressif, destiné à punir les auteurs d'attentats, leurs organisateurs et leurs complices.

Le système français obéit à cette logique. Mais son originalité et sa force résident dans le fait que la frontière entre prévention et répression n'est pas étanche.

Sur le plan des principes, notre pays a fait le choix de bâtir un dispositif pénal original pour prévenir et réprimer le terrorisme. L'élément central en est la loi du 9 septembre 1986, adoptée après la vague d'attentats perpétrés en 1985 et 1986. Il ne s'agit pas d'un droit d'exception. C'est un régime pénal spécialisé et adapté à la nature particulière du terrorisme. La lutte contre le terrorisme n'est d'ailleurs pas la seule à faire l'objet d'un droit spécialisé. C'est aussi notamment le cas de la criminalité organisée.

(1) Structure créée en 1968 qui regroupe les chefs des services de sécurité intérieure de dix-neuf pays européens.

(2) Nucléaire, radiologique, biologique et chimique.

(3) Le G8 est une instance multilatérale informelle qui regroupe huit États : l'Allemagne, le Canada, les États-Unis, la France, l'Italie, le Japon, le Royaume-Uni et la Russie. La France en a proposé la création au sommet de Rambouillet en 1975. Cela a conduit à la formation du G7 l'année suivante, ouvert à la Russie en 1998.

Dans notre droit, l'acte de terrorisme se définit tout d'abord par la combinaison d'un crime ou d'un délit de droit commun avec « *une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* » (article 421-1 du Code pénal). Le lien du crime ou du délit de droit commun avec le terrorisme entraîne la mise en œuvre d'un dispositif pénal comportant notamment l'alourdissement des peines encourues et un allongement de la durée de prescription de droit commun (portée à trente ans pour les crimes et à vingt ans pour les délits).

Notre régime pénal antiterroriste a trois spécificités.

La première est l'existence d'une infraction spécifique qui permet non seulement de réprimer les structures d'appui des auteurs des attentats ou de leurs complices, mais aussi de prévenir les attentats en cours de préparation. Érigée en délit spécifique par la loi du 22 juillet 1996, elle est sans conteste la pierre angulaire du système. Elle permet à la justice d'intervenir avant même la perpétration de l'attentat. C'est grâce à elle que peuvent être démantelées les cellules logistiques et les structures périphériques gravitant autour des réseaux. La caractérisation de cette infraction nécessite un échange entre magistrats et services de renseignement. L'échange est d'autant plus aisé que la DST est à la fois un service de renseignement intérieur chargé de la prévention des activités mettant en cause la sécurité du pays et un service de police judiciaire conduisant les enquêtes sensibles contre le terrorisme international. Cette nature mixte permet d'utiliser dans des procédures judiciaires des éléments recueillis lors de l'activité de renseignement, alors qu'en sens inverse, les informations recueillies dans le cadre de procédures judiciaires sont utiles pour orienter le travail de police administrative.

La deuxième spécificité du système français est de tenir compte de la gravité des actes de terrorisme dans la définition des règles de procédure, plus souples que pour les infractions de droit commun. La durée de la garde à vue peut atteindre 96 heures, contre 48 heures en droit commun, et l'intervention de l'avocat est reportée à la 72^{ème} heure de garde à vue. En cas de risque imminent d'attentat ou de nécessité liée à la coopération internationale, la loi du 23 janvier 2006 relative à la lutte contre le terrorisme autorise désormais sa prolongation jusqu'à six jours. Les moyens d'investigation sont eux aussi plus étendus : il est possible, sous certaines conditions, d'effectuer des saisies et des perquisitions de nuit ; les opérations d'infiltration et de « sonorisation » de véhicules et d'appartements sont permises. Enfin, les risques graves encourus justifient une protection particulière des témoins et même des enquêteurs. Les témoins peuvent ainsi être auditionnés de manière anonyme. L'anonymat des enquêteurs peut, dans certaines conditions, être préservé.

La spécialisation des magistrats chargés de la lutte antiterroriste est la troisième spécificité du régime pénal de lutte contre le terrorisme. Elle se manifeste par la centralisation des poursuites, de l'instruction et du jugement des affaires à Paris. Sept magistrats du parquet et sept juges d'instruction ont en charge les dossiers en matière terroriste. Le jugement des délits est confié au tribunal de grande instance de Paris, tandis que celui des cri-

mes est de la compétence d'une cour d'assises uniquement composée de magistrats professionnels, contrairement aux cours d'assises de droit commun, dont le jury est populaire. Cette spécialisation des magistrats a permis de développer au fil du temps une véritable culture de la lutte antiterroriste : l'évolution des réseaux est mieux maîtrisée ; des liens de confiance fondés sur la durée ont pu être construits avec les services de sécurité et les magistrats étrangers.

Au total, le système judiciaire français de lutte contre le terrorisme, régulièrement adapté depuis 1986 ¹, donne satisfaction. Il ne nécessite pas de réforme d'ampleur.

Un traitement carcéral à adapter

La prison est devenue un lieu de prosélytisme dangereux. Si l'on n'y prend garde, elle produira à terme un réservoir d'activistes radicalisés disponibles pour mener des actions terroristes. Le recensement des incidents permet de déterminer une cartographie nationale du prosélytisme en milieu carcéral : dans certaines régions, dont la région parisienne, la montée en puissance du phénomène est réelle.

Diverses mesures de court terme sont envisageables pour freiner l'essor du prosélytisme. Une modification des dispositions du Code pénal concernant la vie en prison devrait régler une partie des problèmes. Il est nécessaire aussi de prêter une attention soutenue au recrutement des aumôniers musulmans dans les établissements pénitentiaires.

Le phénomène doit également recevoir un traitement structurel et de long terme. La centralisation de l'application des peines au tribunal de grande instance de Paris, telle que le prévoit la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, facilitera la conduite d'une politique rationnelle de suivi des détenus condamnés pour une infraction terroriste, quel que soit le lieu de détention, mais aussi de résidence du condamné. Cette politique pourra s'appuyer sur l'établissement d'un fichier national informatisé des personnes condamnées pour une infraction terroriste.

(1) En particulier par les lois du 22 juillet 1996, du 15 novembre 2001, du 9 septembre 2002, du 18 mars 2003 et du 9 mars 2004, et tout dernièrement par la loi du 23 janvier 2006.

Neutraliser les flux dangereux de personnes, de biens, de capitaux et d'idées

Contrôler les flux de personnes dangereuses

L'entrée et le séjour en France des personnes suspectées de liens avec des activités terroristes

Si l'on excepte le cas particulier des ressortissants des États membres de l'Union européenne, l'entrée et le séjour en France des étrangers sont soumis à un régime d'autorisation administrative.

1) La possibilité d'entrer sur le territoire national est normalement soumise¹ à l'octroi d'un visa par les autorités consulaires.

Qu'ils soient saisis d'une demande de visa de long séjour, pour lesquels notre pays conserve toute sa compétence, ou de visa pour un séjour de moins de trois mois, pour lesquels le régime de délivrance est commun aux pays signataires de l'accord de Schengen, les chefs de postes consulaires possèdent la faculté légale de refuser l'octroi du titre demandé en cas de lien avec une activité terroriste. La convention d'application de l'accord de Schengen prévoit la possibilité de rejeter des demandes de visa de court séjour pour un tel motif, qui justifie l'inscription des intéressés au fichier du « système d'information Schengen » (fichier SIS).

2) Le visa en bonne et due forme ne confère pas, contrairement à l'opinion communément répandue, un sésame pour entrer sans condition sur le territoire national.

Le visa permet certes de quitter son pays à destination de la France. Mais l'admission sur le territoire peut encore être refusée par la police de l'air et des frontières, pour le motif d'ordre public tiré du lien avec des activités terroristes. L'accès peut être refusé non seulement à un ressortissant étranger muni d'un visa régulier d'entrée, mais aussi à un étranger disposant d'une carte de séjour.

De manière générale, dans l'enchaînement visa, entrée, séjour, la prise en compte d'une menace pour l'ordre public, liée notamment à un risque de nature terroriste, peut être opposée à tous les stades : au niveau de la demande de visa, à celui de l'admission sur le territoire, à celui de l'instruction d'une demande de titre de séjour, même pour l'étranger qui pourrait y prétendre de plein droit².

3) Le lien avec des activités terroristes, qui constitue un obstacle légal à l'entrée et au séjour sur le territoire, constitue symétriquement

(1) Sauf accord réciproque exonérant les ressortissants de certains pays de cette formalité.

(2) En application des articles L. 314-11 et 12 du Code de l'entrée et du séjour des étrangers et du droit d'asile.

un motif légal de départ forcé. Un « *comportement lié à des activités à caractère terroriste* » justifie ainsi l'expulsion d'un ressortissant étranger, quelle que soit la densité de ses liens avec notre pays ¹.

Les « *actes de provocation explicite et délibérée à la discrimination, à la haine ou à la violence* » permettent également de prendre une mesure d'expulsion. C'est sur ce fondement que le ministre de l'Intérieur a prononcé l'expulsion d'une dizaine d'imams fondamentalistes au cours des années 2004 et 2005.

L'identification des personnes : la question de la biométrie

Disposer des moyens de faire obstacle à l'entrée ou au séjour d'individus dangereux est nécessaire. Avoir la possibilité d'éloigner certains d'entre eux du territoire national ne l'est pas moins. Mais l'impact de ces mesures sur les libertés publiques, notamment celle d'aller et venir, n'est pas anodin. Il est donc indispensable d'avoir la certitude que les mesures coercitives s'appliquent aux bons individus, sans risque d'erreur. Cette certitude sera d'autant plus solide que l'identification ne souffrira aucune contestation.

La falsification ou l'usurpation d'identité constituent des défis importants. Elles fragilisent la fiabilité des registres d'état civil, des titres d'identité et des passeports. Le recours à la biométrie contribuera à limiter la fraude en offrant un nombre restreint d'identifiants à vocation universelle.

La biométrie fait appel à différentes techniques telles que la reconnaissance faciale, celle de l'iris de l'œil, des empreintes digitales ou de la paume de la main, l'analyse spectrale de la voix ou la comparaison des empreintes génétiques.

L'intérêt des données biométriques réside dans le fait qu'elles sont uniques et indissociables d'un individu donné. La biométrie autorise ainsi l'authentification d'une personne lorsqu'elle est présente en établissant un lien quasiment infalsifiable entre l'individu et ses documents d'identité. Elle permet également de l'identifier par comparaison de ses données biométriques avec celles contenues dans une base de données.

Plusieurs pays voisins se sont déjà engagés dans des programmes de recours à la biométrie digitale ² non seulement dans les titres de voyage, mais aussi dans les titres d'identité. C'est le cas de la Belgique, de l'Espagne, de l'Italie ou du Royaume-Uni. Dans notre pays, il a d'ores et déjà été décidé de délivrer des visas biométriques. La sécurisation des passeports et des titres d'identité par la biométrie digitale revêt un caractère prioritaire. Elle devra s'effectuer dans un cadre juridique équilibré, prenant en compte la protection des libertés individuelles et les exigences de la lutte contre le terrorisme.

(1) C'est ce qui résulte des termes mêmes de l'article L. 521-3 du Code de l'entrée et du séjour des étrangers et du droit d'asile.

(2) Il s'agit de la forme de biométrie qui recourt aux empreintes digitales et à celles de la paume de la main.

Tarir les flux de capitaux qui contribuent au financement du terrorisme

Renforcer notre dispositif juridique de lutte contre le financement du terrorisme

Financer le terrorisme constitue une infraction pénale, prévue et réprimée par l'article 421-2-2 du Code pénal. Il est donc juridiquement possible de remonter les filières et de sanctionner, le cas échéant, les soutiens financiers du réseau. La saisine conjointe, dans ce type d'affaires, du pôle financier et du pôle antiterroriste du tribunal de grande instance de Paris donne entière satisfaction aux yeux des praticiens.

L'efficacité de la prévention est plus incertaine.

L'information circule correctement entre les différents intervenants : magistrats, services de renseignement, cellule TRACFIN¹ du ministère de l'Économie, des Finances et de l'Industrie, chargée de suivre les financements occultes dans notre pays. Il serait toutefois souhaitable de donner une assise juridique plus solide aux échanges de TRACFIN avec les services de police et de renseignement intervenant dans la lutte contre le blanchiment et le financement du terrorisme.

Une grande opacité règne sur l'utilisation des fonds récoltés par certaines associations culturelles et caritatives. Plusieurs options sont envisageables pour dissiper les doutes que cette absence de transparence peut susciter.

On peut tout d'abord envisager qu'au-delà d'un certain seuil d'activité, les associations soient soumises à l'obligation de recourir à un commissaire aux comptes pour certifier la régularité des mouvements de leurs fonds, ou à un renforcement de l'obligation de dépôt de leurs comptes auprès des greffes des tribunaux de grande instance. Ces obligations, peu contraignantes et conformes à un but d'intérêt général, n'entraveraient pas l'exercice de la liberté d'association garantie par la loi de 1901. Un renforcement du régime de contrôle de la collecte de fonds sur la voie publique pourrait utilement relayer l'instauration d'une telle obligation déclarative.

Enfin, la procédure de gel des avoirs financiers des personnes ou des organismes en lien avec une entreprise terroriste, récemment réformée par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, devrait permettre de neutraliser les avoirs suspects, en conférant au ministre de l'Économie, des Finances et de l'Industrie un pouvoir qui porte aussi sur les fonds des ressortissants de l'Union européenne.

Bâtir une coopération internationale efficace

Dès 1999 a été adoptée, dans le cadre des Nations unies et à l'initiative de la France, la convention pour la répression du financement du terrorisme. Ce texte préfigurerait nombre des dispositions reprises ensuite

(1) Pour une définition, voir l'encadré page 52.

par les résolutions 1267 et 1373 du Conseil de sécurité de l'ONU, et en comporte d'autres, qui sont d'une grande aide dans la lutte contre le financement du terrorisme, comme les mesures d'extradition et d'entraide judiciaire, les mesures préventives à prendre par les institutions financières et la levée du secret bancaire.

À la suite des attentats du 11 septembre 2001, différents instruments juridiques internationaux ont été adoptés. Leur objet est de geler les ressources financières des individus et des organisations auteurs ou complices d'attentats terroristes. Les principaux instruments sont la résolution 1267 du Conseil de sécurité de l'ONU, qui confie le soin à un comité d'établir et d'actualiser une « liste noire » nominative, et la résolution 1373 qui a posé le principe d'une obligation générale du gel des avoirs liés au terrorisme. Le dispositif a été créé à l'origine pour lutter contre les protecteurs Taliban d'Al Qaïda. Les listes comportent aujourd'hui plus de 350 noms d'individus et d'entités.

Sur le fondement de la résolution 1373, l'Union européenne a bâti en décembre 2001 sa propre liste¹, qui comprend notamment des organisations terroristes européennes (organisations liées à ETA, groupes nord-irlandais, grecs et italiens) ou extérieures à notre continent (Mouvement du jihad islamique palestinien, PKK, Sentier lumineux ou OMPI irannienne), ainsi que les individus liés à ces groupes. Le dispositif est néanmoins incomplet dans la mesure où les gels d'avoirs prescrits à l'échelle européenne ne visent que les non-résidents.

Le Groupe d'action financière sur le blanchiment de capitaux (GAFI), créé lors du sommet du G7 à Paris en 1989, a placé au cœur de son action la lutte contre le financement du terrorisme. Actuellement composé de trente-trois membres, le GAFI sert de « laboratoire d'idées » notamment dans la lutte contre le microfinancement international d'activités illicites. Il propose d'élever le niveau de sécurité des virements internationaux, en contraignant les établissements financiers à recueillir l'identité de l'émetteur du virement, afin que l'État où réside son bénéficiaire puisse facilement retrouver la trace de l'échange. Dans ce domaine, l'Union européenne poursuit l'objectif d'étendre le dispositif à tous les virements, quel que soit leur montant². Notre pays doit soutenir l'adoption, sous l'égide plus large des Nations unies, d'une panoplie d'instruments s'inspirant des logiques à l'œuvre au sein du GAFI.

(1) Positions communes 2001/930 et 931/PESC du 27 décembre 2001, prises dans le cadre de la politique étrangère et de sécurité commune et règlement 2580/2001 du Conseil de l'Union, pris sur le fondement des articles 60, 301 et 308 du traité instituant la communauté européenne. Pris ensemble, ces trois instruments à la valeur juridique contraignante pour les États-membres constituent le mécanisme dit de la *Clearing house*.

(2) Elle a déjà obtenu en 2005 que le seuil de déclenchement des vigilances soit abaissé de 3 000 \$ à 1 000 \$.

Neutraliser les flux d'idées porteuses de haine, de violence ou appelant au terrorisme

Notre régime juridique comporte des dispositions permettant de combattre la propagation d'idées extrémistes.

La loi du 10 janvier 1936 ¹ prévoit la possibilité pour le président de la République de dissoudre par décret pris en conseil des ministres les **associations** ou les « groupements de fait » provoquant à la discrimination, à la haine ou à la violence envers une personne ou un groupe de personnes en raison de leur origine ou de leur appartenance (ou de leur non-appartenance) à une ethnie, une nation, une race ou une religion déterminée. Les groupements se livrant « *sur le territoire français, ou à partir de ce territoire à des agissements en vue de provoquer des actes de terrorisme en France ou à l'étranger* » tombent également sous le coup de cette législation.

Contre les groupements, des outils adaptés existent donc. L'engagement des poursuites pénales apparaît plus délicat lorsqu'il s'agit de réprimer des actes délictueux de même nature imputables à des individus agissant isolément.

La provocation directe par des **individus** à des actes de terrorisme et l'apologie de ces actes sont punies de cinq ans d'emprisonnement et de 45 000 euros d'amende. En théorie, le régime pénal apparaît donc particulièrement dissuasif. Cette infraction figure cependant non pas dans le Code pénal mais dans la loi du 29 juillet 1881 sur la liberté de la presse. C'est donc le régime juridique particulier prévu par cette loi qui s'applique à la poursuite des faits délictueux : la prescription est abrégée à trois mois ; il est interdit de procéder à des saisies et à l'arrestation préventive de la personne en cause ; le recours aux procédures rapides de traitement de la délinquance (comparution immédiate, par exemple) est impossible. Au surplus, il faut que les faits soient publics ², ce qui exclut du champ de l'infraction le prosélytisme d'individu à individu pratiqué à des fins de passage à l'action violente. Enfin, la répression échappe à la compétence nationale en matière de terrorisme dont dispose la juridiction parisienne ³.

Le droit en vigueur paraît donc ici peu adapté. Deux voies sont possibles pour l'améliorer.

La première consiste à sortir du champ d'application de la loi sur la presse le délit de provocation ou d'apologie du terrorisme pour l'intégrer directement dans le Code pénal. Cette solution ne serait pas inédite. Tel a ainsi été le sort du délit de provocation à la consommation ou au trafic de stupéfiants. Cette option permettrait en outre, en faisant tomber la

(1) Sur les groupes de combat et les milices privées.

(2) L'article 24 de la loi du 29 juillet 1881 exige en effet que les propos aient été proférés dans un lieu public, réel ou virtuel (on songe ici à l'ajout sur les moyens de communication électronique opéré par le II de l'article 2 de la loi n° 2004-575 du 21 juin 2004).

(3) Pour une description du régime pénal contre le terrorisme, voir page 53.

condition de publicité de l'infraction, d'élargir facilement son champ au prosélytisme qui a pour but ou pour effet le passage à l'acte violent¹.

La seconde option consisterait, tout en laissant inchangé le champ d'application de la loi de 1881, à reprendre l'infraction dans le Code pénal. Les faits délictueux pourraient alors être poursuivis sur l'un ou l'autre des deux fondements.

Protéger le territoire des intrusions et neutraliser les terroristes à l'étranger par l'action des armées

« La défense a pour objet d'assurer en tout temps, en toutes circonstances et contre toutes les formes d'agression, la sécurité et l'intégrité du territoire, ainsi que la vie de la population »².

Fortes de ce mandat, les armées contribuent à la prévention du terrorisme en accomplissant deux missions principales, pour lesquelles elles engagent en permanence 35 000 militaires³ : d'une part protéger et contrôler dans la profondeur les espaces nationaux et ceux où la France a des intérêts, d'autre part mener des opérations extérieures visant notamment à neutraliser la menace terroriste avant qu'elle n'atteigne notre pays.

Les forces armées protègent et contrôlent en profondeur les espaces nationaux et ceux où la France a des intérêts

1) Une centaine de radars fixes surveillent et contrôlent en permanence les dix mille aéronefs qui survolent quotidiennement le territoire national. Des radars mobiles « tactiques » complètent le dispositif chaque fois qu'une manifestation particulière l'exige.

En cas de comportement suspect d'un aéronef ou de troubles à bord d'un avion, des avions de combat ou des hélicoptères armés sont en mesure d'intervenir dans des délais très brefs, au plus haut stade de vigilance.

Afin d'optimiser encore sa capacité à défendre son territoire contre toute intrusion aérienne, en détectant la menace avant qu'elle ne pénètre dans son espace aérien, la France devra poursuivre sa politique de mise en place d'accords bilatéraux de sécurité aérienne. Des accords ont déjà été conclus avec la Belgique, l'Espagne et la Suisse. Il faut les compléter par des conventions avec l'Allemagne, l'Italie, le Luxembourg, le

(1) Ce qui réglerait au surplus une partie du problème du prosélytisme carcéral.

(2) Article L. 1111-1 du Code de la défense.

(3) Sont décrits ailleurs dans le Livre blanc la participation des forces armées au plan VIGIPIRATE et le travail mené par la gendarmerie nationale sous la direction du ministère de l'Intérieur.

Royaume-Uni, sans oublier le Brésil et le Surinam, pays voisins du département de la Guyane où se trouve le centre spatial installé à Kourou.

2) Le trafic maritime sur les façades métropolitaines comme dans les zones maritimes des départements et territoires d'outre-mer et dans les zones où nous avons des intérêts économiques ¹ est surveillé par des moyens civils et militaires. En métropole, la surveillance se fait notamment à l'aide du réseau SPATIONAV ², construit autour des sémaphores littoraux et de leurs radars. Ce réseau bénéficie aussi des renseignements fournis par l'Organisation maritime internationale (OMI), par les marines de nos alliés, ainsi que par les navires de la marine nationale en mission sur les différents océans. Tout comportement naval suspect peut faire l'objet d'une intervention à bref délai du moyen de combat le plus adapté : bâtiment de surface, sous-marin, commandos, avion ou hélicoptère.

Ce dispositif de sauvegarde pourrait utilement être promu et mis en commun au sein de l'Union européenne.

Les forces armées contribuent à la prévention contre le terrorisme en engageant leurs moyens à l'extérieur du territoire national

À l'extérieur de nos frontières, nos services de renseignement, nos forces armées et notre outil diplomatique concourent à identifier et à prévenir les menaces le plus tôt possible.

Comme cela est affirmé dans le rapport annexé à la loi de programmation militaire 2003-2008, la possibilité d'une action préemptive ³ pourrait être envisagée, dès lors qu'une situation de menace explicite et avérée serait reconnue. Le recours à une telle action s'inscrirait dans le cadre de l'article 51 de la charte des Nations unies, c'est-à-dire en situation de légitime défense.

De manière plus générale, la participation des forces armées, aux côtés des acteurs civils, nationaux et internationaux, aux opérations de restauration de la paix et de stabilisation contribue à la suppression des refuges des terroristes par la stabilisation des zones en crise. En 2006, la France contribue activement, sur le plan civil et militaire, à de telles missions dans des territoires ayant abrité ou abritant des terroristes, comme les Balkans, l'Afghanistan, ou la zone sahélienne. Pour toutes ces actions, les armées reçoivent le soutien de la Direction du renseignement militaire (DRM) qui, grâce à ses satellites et à ses moyens d'écoute, évalue, en liaison avec les

(1) Cela comprend la zone économique exclusive (ZEE), qui s'étend à 370 km environ des côtes françaises, y compris au large de nos collectivités d'outre-mer.

(2) Pour « Surveillance des espaces sous juridiction nationale et des approches maritimes ».

(3) On entend communément par action **préemptive** une action contre une menace imminente tandis qu'une action **préventive** s'exécute contre une menace qui ne serait que potentielle.

autres services de renseignement, français ou étrangers, la menace pesant sur nos forces.

Parallèlement aux efforts de prévention au sens large, les forces armées participent à la lutte contre le terrorisme en attaquant celui-ci dans ses bastions. Ainsi, au lendemain des attentats du 11 septembre 2001, la France s'est immédiatement engagée dans les opérations de lutte contre le terrorisme en Afghanistan et dans l'Océan indien, conduites sous commandement américain. La résolution 1368, adoptée dès le 12 septembre 2001 par le Conseil de sécurité, constate que de telles opérations s'inscrivent dans le cadre du droit à la légitime défense reconnu par la charte des Nations unies. Notre dispositif, baptisé HÉRACLÈS, a comporté des forces aériennes ¹, des forces maritimes ² et des forces terrestres, régulières et spéciales.

Le recours préventif à des mesures coercitives, y compris par l'emploi de la force armée, pourrait être également envisagé. Il devrait être autorisé par le Conseil de sécurité agissant dans le cadre du chapitre VII de la charte des Nations unies ³.

Renforcer la coopération internationale

Une caractéristique du terrorisme mondial est de ne pas connaître de limite territoriale. Lutter seul contre une mouvance qui méconnaît les frontières serait voué à l'échec.

La France n'a pas attendu les attentats du 11 septembre 2001 pour rechercher une réponse internationale concertée et coordonnée à la menace du terrorisme. Face à l'essor du terrorisme mondial, la coopération internationale s'est étendue et intensifiée. Outre la prévention des attentats, elle a pour objet principal de réduire les vulnérabilités de nos sociétés.

Prévenir la menace

La protection du territoire national relève de la compétence des États. Mais la coopération internationale est indispensable pour permettre à ceux-ci d'exercer cette compétence dans un contexte marqué par l'accroissement des échanges financiers, économiques et humains.

(1) Qui menaient des missions de reconnaissance, de ravitaillement, de transport et de combat, y compris des opérations aériennes offensives, conduites par l'armée de l'air et l'aviation navale en appui direct des forces terrestres américaines dans l'opération Anaconda, au printemps 2002.

(2) Groupe aéronaval sur zone pendant plus de sept mois autour du porte avions nucléaire Charles-de-Gaulle.

(3) En application du chapitre VII de la charte des Nations unies, le Conseil de sécurité peut décider des mesures à caractère obligatoire pour maintenir ou rétablir la paix et la sécurité internationale.

1) Les **Nations unies** offrent un cadre universel pour mobiliser sur le plan politique l'ensemble des États dans la lutte contre le terrorisme. Celle-ci est souvent perçue comme une préoccupation des pays du Nord. Pourtant, le terrorisme mondial avait fait, début 2006, plus de victimes dans les pays du Sud que dans les pays du Nord.

Les Nations unies offrent aussi un cadre universel pour édicter des normes juridiquement contraignantes. L'action des Nations unies dans ce domaine comporte deux volets : d'une part les treize conventions conclues sous l'égide de l'organisation ou de ses agences entre les années 1960 et 2005 ; d'autre part les résolutions du Conseil de sécurité prises en application du chapitre VII de la charte.

Les treize conventions antiterroristes de l'ONU

Treize conventions antiterroristes de l'ONU ont été négociées entre 1963 et 2005. Elles définissent des infractions pénales que les États membres doivent intégrer dans leur droit interne et des règles de compétence, d'extradition et d'entraide judiciaire applicables à ces infractions, selon le principe « extraditer ou juger ».

Ces conventions sont encore imparfaitement appliquées : beaucoup d'États ne les ont toujours pas signées ; d'autres États qui les ont signées ne les ont cependant toujours pas mises en œuvre.

La France est déjà partie à douze conventions et a engagé les procédures de ratification concernant la convention internationale pour la répression des actes de terrorisme nucléaire.

- *Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs (1963).*
- *Convention pour la répression de la capture illicite d'aéronefs (1970).*
- *Convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile (1971).*
- *Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale (1988).*
- *Convention sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale, y compris les agents diplomatiques (1973).*
- *Convention internationale contre la prise d'otages (1979).*
- *Convention sur la protection physique des matières nucléaires (1980).*
- *Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime (1988).*

- *Protocole à la convention susmentionnée pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental (1988).*
 - *Convention sur le marquage des explosifs plastiques aux fins de détection (1991).*
 - *Convention internationale pour la répression des attentats terroristes à l'explosif (1997).*
 - *Convention internationale pour la répression du financement du terrorisme (1999).*
 - *Convention internationale pour la répression des actes de terrorisme nucléaire (2005).*
-

Le Conseil de sécurité des Nations unies a qualifié à plusieurs reprises le terrorisme international de « menace à la paix et à la sécurité internationale », ce qui l'a conduit à imposer aux États de prendre des mesures obligatoires en application du chapitre VII de la charte. Il a ainsi prononcé des sanctions contre la Libye, le Soudan ou l'Afghanistan, trois États accusés d'avoir mené ou commandité des actes de terrorisme ou d'avoir servi de refuge à des terroristes.

Le Conseil de sécurité a prolongé le régime de sanctions contre les Taliban édicté par la résolution 1267 à Al Qaïda. Outre les obligations de gel des avoirs et des ressources financières ¹, ce dispositif impose également d'autres obligations visant à empêcher l'entrée et le transit ainsi que la fourniture d'armes.

De manière générale, les États se voient également obligés, au titre de la résolution 1373 adoptée le 28 septembre 2001, de « *refuser de donner asile à ceux qui financent, organisent, appuient ou commettent des actes de terrorisme* ». Cette résolution a créé un Comité du contre-terrorisme (CCT) chargé d'examiner la robustesse des régimes juridiques de lutte contre le terrorisme mis en place par les États membres et d'assister ces derniers dans la mise en œuvre de leurs obligations.

2) La montée en puissance de **l'Union européenne** en matière de lutte contre le terrorisme se poursuit.

Largement entamée après les attentats de septembre 2001, cette évolution s'est accélérée depuis les attentats de Madrid en mars 2004. L'Union européenne s'est dotée en juin 2004 d'un plan d'action global de lutte contre le terrorisme, qui comporte sept objectifs stratégiques.

(1) Voir sur ce point la page 59.

Les sept objectifs stratégiques de l'Union européenne dans la lutte contre le terrorisme

- *Fortifier le consensus international et accroître les efforts déployés par la communauté internationale pour lutter contre le terrorisme.*
 - *Réduire l'accès des terroristes aux ressources financières et économiques.*
 - *Développer les moyens des organes de l'Union et des États membres pour identifier les terroristes, enquêter à leur sujet et les poursuivre et empêcher les attentats terroristes.*
 - *Assurer la sécurité des transports internationaux et l'efficacité des systèmes de contrôle aux frontières.*
 - *Développer la capacité de l'Union européenne et des États membres à faire face aux conséquences d'un attentat terroriste.*
 - *Trouver la parade aux facteurs qui contribuent à alimenter le terrorisme et à grossir ses rangs.*
 - *Cibler les actions menées dans le cadre des relations extérieures de l'Union dans des pays tiers dont la capacité de lutte contre le terrorisme doit être renforcée.*
-

Les sept objectifs sont déclinés en près de cent actions concrètes. Afin de renforcer la cohérence stratégique et politique de ces objectifs et de ces actions, l'Union européenne les a regroupés fin 2005 sous quatre grandes rubriques dans le cadre d'une stratégie globale : assurer la **prévention** notamment en empêchant le recrutement de nouveaux terroristes ; assurer une meilleure **protection** des cibles potentielles ; **désorganiser** les réseaux existants ; améliorer nos capacités de **réaction** et de gestion des conséquences en cas d'attentats terroristes.

Malgré ces progrès, l'effort dans le domaine stratégique doit être poursuivi. Il est nécessaire de consolider une approche plus globale et intégrée des différents volets de l'action de l'Union européenne en matière de terrorisme. Dans cette perspective, le Conseil européen a décidé d'instituer un coordinateur européen de la lutte contre le terrorisme à la suite des attentats de Madrid en mars 2004. Ce coordinateur contribue à la mobilisation au sein des structures de l'Union et en direction des États membres.

3) Le **G8** et l'**OTAN** jouent également un rôle utile en matière d'échanges sur la prévention de la menace.

Depuis 1996, à l'instigation de la France, les membres du G8 ont inscrit la lutte contre les menaces représentées par la criminalité organisée, ainsi que par le terrorisme, au cœur de leurs priorités. Parmi les actions du G8 en matière de lutte contre le terrorisme, on peut plus particulièrement citer celles qui ont trait à la sûreté de l'aviation civile, notam-

ment à travers la biométrie et la lutte contre la prolifération des missiles sol-air portatifs (MANPADS ¹⁾, à la traçabilité des avoirs terroristes et à la lutte contre la fraude documentaire.

L'OTAN a de son côté entrepris un effort d'adaptation pour mieux lutter contre le terrorisme dans le domaine militaire qui est le sien. Elle peut ainsi apporter un appui dans la protection d'événements ponctuels (comme les Jeux olympiques d'Athènes, par exemple). L'OTAN effectue également un travail utile en matière de défense NRBC.

Prévenir l'apparition d'un terrorisme pouvant avoir recours aux armes de destruction massive

Des responsables de la mouvance Al Qaïda ont manifesté la volonté de perpétrer des attentats avec des armes nucléaires, radiologiques, biologiques ou chimiques. La coopération internationale s'est très tôt attelée à la prévention du terrorisme NRBC. Celle-ci passe notamment par la lutte contre la prolifération des armes de destruction massive (ADM) et de leurs vecteurs.

1) Le rôle de l'**Union européenne** en matière de lutte contre la prolifération a été substantiellement renforcé depuis l'adoption par le Conseil européen de décembre 2003 de la stratégie de l'Union contre la prolifération des armes de destruction massive. Les chefs d'État ou de gouvernement ont souligné dans ce document le risque de voir des terroristes acquérir de telles armes et ont exprimé la volonté de le réduire.

2) Les travaux menés dans le cadre du **G8** visent à empêcher les terroristes et ceux qui les soutiennent d'avoir accès à des armes de destruction massive et aux matières qui permettraient de les fabriquer. Il s'agit pour l'essentiel de mesures de contrôle et de sécurité traditionnelles en matière de non-prolifération.

En particulier, les dirigeants du G8 ont lancé en juin 2002 le partenariat mondial contre la prolifération des armes de destruction massive et des matières connexes. Ce partenariat entre la Russie et les sept autres membres du G8 vise à réduire la menace provenant du maintien des arsenaux d'armes non conventionnelles (nucléaire, biologique et chimique) de l'ex-Union soviétique. Les pays du G8 se sont engagés à rassembler jusqu'à 20 milliards de dollars pour appuyer des projets allant dans ce sens au cours des dix prochaines années. La France participe activement à ce partenariat. Elle doit poursuivre l'effort engagé en veillant à ce que celui-ci reste bien centré sur la lutte contre la prolifération et le risque de détournement des armes non conventionnelles à des fins terroristes.

(1) Pour *MAN Portable Air Defense Systems*.

3) Les **Nations unies** ont franchi une étape cruciale avec l'adoption de la résolution 1540 du Conseil de sécurité, en avril 2004, qui vise à prévenir le risque d'acquisition d'ADM et de leurs vecteurs par des terroristes. Ce texte est d'autant plus important que le Conseil agit alors dans le cadre du chapitre VII de la charte et qu'il peut demander aux États de prendre des mesures spécifiques pour se conformer à leurs obligations.

L'Agence internationale pour l'énergie atomique (**AIEA**) joue un rôle central dans la sécurité des sources radioactives. Celle-ci reste en effet une préoccupation majeure, en particulier en raison de l'absence de contrôle effectif sur les sources radioactives au regard de la menace terroriste. Dans le cadre du G8, la France a joué un rôle moteur pour lancer cette initiative. Elle suit attentivement son évolution concrète.

4) L'**initiative de sécurité contre la prolifération**¹ (**PSI**) porte sur l'interception des chargements d'armes de destruction massive, de leurs vecteurs ou des équipements et matériels contribuant à leur fabrication, en provenance ou à destination de pays ou d'entités suscitant des préoccupations. Elle continue de se développer. Elle a déjà conduit à des opérations concrètes d'interception et permis de développer des liens opérationnels utiles en cas de crise.

Le fait qu'un très grand nombre d'organisations internationales ou régionales aient adopté des mesures et des plans d'action spécifiques en matière de lutte contre le terrorisme est positif. Il témoigne de la prise en compte de la menace et de la nécessité de la contrer collectivement. Cependant, en matière de lutte contre le terrorisme comme en d'autres domaines, la coopération internationale est un moyen et non une fin. Elle doit s'articuler autour d'un triple objectif d'efficacité, de complémentarité et de subsidiarité.

Dans cette perspective, notre pays doit conforter le rôle prééminent des Nations unies, comme créateur de consensus politique et comme source de légitimité et de pouvoir normatif. Il doit renforcer l'action de l'Union européenne.

(1) Initiative lancée en mars 2003 par le gouvernement américain, la PSI regroupait début 2006 plus de soixante-cinq pays. Lors de la réunion de Paris du 4 septembre 2003, les onze pays du *core group* (dont fait partie la France) ont édicté une « déclaration sur les principes d'interdiction », qui fixe les grands principes de la PSI. Cette initiative s'inscrit dans le cadre du droit international et des législations nationales et a vocation à rassembler tous les États qui luttent contre la prolifération.

Améliorer nos dispositifs

Protéger la population

Consolider la planification de vigilance

Afin de faire face à l'ensemble du spectre des menaces, notre pays adapte en permanence les moyens de prévision et de dissuasion dont il dispose. Le fer de lance de cette stratégie est le plan VIGIPIRATE, créé en octobre 1981 et bien connu de nos concitoyens. Son objectif est double : protéger la population, les infrastructures et les institutions et préparer les réponses en cas d'attaque.

La dernière version de VIGIPIRATE, en vigueur depuis mars 2003, est fondée sur le postulat que la menace terroriste doit désormais être considérée comme permanente. Elle définit ainsi un socle de mesures appliquées en toutes circonstances, même en l'absence de signes de menaces. Le plan se décline ensuite en quatre niveaux d'alerte qui sont rendus publics. Le niveau le plus faible (jaune) est celui d'une menace diffuse. Les mesures qui sont alors mises en œuvre doivent permettre de passer très rapidement aux niveaux supérieurs orange et rouge. Le niveau le plus élevé (écarlate) vise à prévenir le risque imminent d'attentats majeurs.

Le plan VIGIPIRATE a une vocation générale de dissuasion et de prévention antiterroriste. Il est complété par la famille des plans d'intervention « PIRATE », adaptés chacun à un type de risque particulier (PIRATOME, PIRATOX, BIOTOX, PIRANET, PIRATE-MER, PIRATAIR-INTRUSAIR, PIRATE-EXT).

Ces plans sont actualisés en permanence en fonction de l'évolution des menaces et des risques pesant sur notre pays. Ils servent de matrice à la réalisation d'exercices locaux (équipes et cadres de terrain), nationaux (les administrations centrales sont mises à contribution) et « majeurs » (avec la participation de ministres ou de leurs cabinets).

VIGIPIRATE

VIGIPIRATE, plan gouvernemental de vigilance, de prévention et de protection, définit un processus de décision et un catalogue de mesures opérationnelles.

Sur la base d'une évaluation de la menace, un niveau d'alerte est arrêté par le Premier ministre après consultation du président de la République. À chacun des quatre niveaux d'alerte est associé un objectif de sécurité, qui se traduit par la possibilité de mettre en place des mesures couvrant l'ensemble de la palette des risques. À titre d'illustration, le plan prévoit la présence des forces armées dans les gares et les aéroports, la protection renforcée des écoles, des fouilles à l'entrée des grands magasins... Les mesures sont activées sur décision du Premier ministre en fonction du niveau d'alerte et des secteurs menacés. Des plans locaux précisent les modalités pratiques de mise en œuvre des mesures par les préfets, les collectivités locales et les opérateurs économiques.

La famille des plans « PIRATE »

Les plans d'intervention « PIRATE » sont déclenchés par le Premier ministre en cas de menace précise ou d'attaque terroriste utilisant un moyen d'agression spécifique (PIRATOX pour un produit chimique toxique, BIOTOX pour un agent biologique pathogène, PIRATOME pour une matière nucléaire ou radiologique, PIRANET pour une attaque sur les systèmes d'information) ou se déroulant dans un milieu particulier (PIRATAIR-INTRUSAIR contre le terrorisme aérien, PIRATE-MER contre le terrorisme maritime, PIRATE-EXT en cas de menace ou d'attaque contre des ressortissants ou des intérêts français à l'étranger). Les plans définissent une structure de gestion de crise et de traitement des informations, ainsi que les actions que doivent entreprendre les autorités civiles et militaires, dont les unités spécialisées dans l'intervention anti-terroriste et les forces spéciales.

Tous les plans gouvernementaux doivent continuer à être complétés et régulièrement actualisés en fonction de l'évolution des menaces et des risques pesant sur notre pays. Ils doivent également être prolongés par des plans locaux de mise en œuvre.

L'apport de la vidéosurveillance

Dans notre pays, environ 300 000 caméras de vidéosurveillance sont installées dans les espaces publics. Chez certains de nos voisins, on en dénombre plusieurs millions ¹. Outre leur apport déterminant à la résolution des enquêtes criminelles ², ces caméras, installées dans les lieux accueillant du public et les installations sensibles, contribuent à la prévention du terrorisme.

Onze ans après l'adoption de la loi du 21 janvier 1995 qui réglemente la vidéosurveillance dans notre pays, la loi du 23 janvier 2006 relative à la lutte contre le terrorisme complète la couverture des lieux et de la voie publics (commerces, transports, sièges de compagnies aériennes, certains lieux de culte...) pour les protéger contre la menace terroriste. Il est essentiel d'assortir le développement de la vidéosurveillance de garanties assurant le respect des libertés fondamentales. L'installation de ces systèmes est soumise à une autorisation administrative désormais limitée dans le temps, de façon à vérifier périodiquement que les motifs qui ont justifié leur mise en place demeurent pertinents.

Les systèmes de vidéosurveillance existants sont efficaces pour prévenir les tentatives d'effraction ou les menaces dirigées contre les personnes ou les biens. Les circuits de caméras permettent de repérer les premiers indices de l'infraction ; une équipe d'intervention peut être immédiatement envoyée pour éviter que celle-ci soit commise.

Les systèmes de vidéosurveillance traditionnels ne permettent cependant pas de repérer préventivement les terroristes, qui ne procèdent généralement pas par effraction. Pour prévenir plus efficacement la perpétration d'actes terroristes, nous avons besoin de réseaux de vidéodétection capables de repérer des engins explosifs et des comportements suspects. Le saut qualitatif d'un type de réseau à un autre passe par le développement des techniques d'analyse automatique d'images. Ces techniques, qui commencent à être disponibles, sont à même de repérer, dans un flux d'images qui dépasse rapidement la capacité humaine d'observation, un colis abandonné voire un agissement suspect.

Assurer la protection des réseaux de transport

Tous les modes de transports de personnes et de marchandises ont été frappés par le terrorisme : navires pétroliers ou de croisière, ferries, avions commerciaux, réseaux ferrés ou routiers de transport collectif.

Les transports collectifs sont par nature des cibles faciles et « rentables » pour le terrorisme. Leur protection constitue une priorité depuis les attentats du 11 septembre 2001.

(1) Essentiellement en raison, il est vrai, de l'action très dynamique des opérateurs privés.

(2) Le précédent britannique des attentats de Londres de juillet 2005 en constitue une illustration remarquable.

Les transports aériens

La sécurisation du transport aérien a été profondément repensée après les attentats du 11 septembre 2001. Il ne s'agit plus seulement d'empêcher le détournement d'un avion et la prise de ses passagers en otages pour satisfaire une revendication politique, mais aussi de faire obstacle à l'embarquement d'un passager susceptible de détruire l'avion en vol ou d'en prendre le contrôle pour le diriger sur une cible. Simultanément, le risque de chargement de cargaisons dangereuses a été réévalué.

Face à de telles menaces, la définition de mesures de sûreté ne pouvait se faire que dans un cadre international. Pour les États membres de l'Union européenne, cette définition a été harmonisée par un règlement communautaire du 16 décembre 2002, dont ont découlé en France des modifications du Code de l'aviation civile.

Les mesures de sûreté de la navigation aérienne et du transport aérien comportent, en France, trois volets : mesures au sol, mesures à bord, mesures en vol. Elles sont mises en œuvre de façon graduelle à travers le plan VIGIPIRATE et le plan d'intervention PIRATAIR-INTRUSAIR en fonction de l'évaluation de la menace.

Au sol, il a fallu mettre en place un système de sûreté à partir d'une architecture d'aéroports conçue à l'origine pour faciliter l'accès aux avions. Deux espaces sont définis : la zone publique, accessible à tous, professionnels, passagers et accompagnateurs ; la zone réservée, accessible aux seules personnes autorisées : professionnels munis d'une autorisation matérialisée par un badge ou passagers munis d'un titre de transport et préalablement contrôlés. Tout ce qui pénètre en zone réservée (personnes, bagages de soute, bagages de cabine, ravitaillement) est contrôlé pour détecter des produits dangereux (explosifs, produits chimiques toxiques, matières radiologiques). Ces contrôles sont effectués par des appareils de radiographie et des détecteurs de métaux et de traces d'explosifs. Des contrôles similaires ont lieu sur les pistes pour éviter l'embarquement de produits ou d'objets prohibés dans les avions.

À bord de l'avion, les mesures nouvelles les plus marquantes ont été le blindage de la porte d'accès à la cabine de pilotage pour interdire les intrusions et l'obligation d'y installer un système d'alerte codé. Certains vols embarquent des gardes armés.

La phase de vol fait l'objet d'un suivi systématique comparant en permanence le trajet décrit dans le plan de vol et la trajectoire réelle de l'avion.

Les États-Unis et la protection avancée du territoire

Les États-Unis ont instauré une « ligne de défense avancée » de leur territoire. Les compagnies aériennes qui opèrent en direction des États-Unis sont tenues de vérifier que leurs passagers ne se trouvent pas sur une liste des personnes dont l'arrivée sur le territoire américain par la voie aérienne est proscrite (la no fly list).

Si l'identification est faite avant le décollage, le passager n'est pas autorisé à embarquer. Si elle est faite pendant le vol, l'avion est dérotté. La no fly list est actualisée en continu par les services de sécurité américains à partir de multiples sources et selon des critères qui leur sont propres.

Si l'Europe ne s'est pas engagée dans ce type de démarche, certains pays ont recours à la sécurisation de vols par la présence discrète d'agents armés à bord des avions opérant sur des lignes sensibles. En outre, l'accès pour des finalités anti-terroristes aux données des compagnies aériennes renforcera la sécurisation du territoire européen.

Le transport de fret par voie aérienne n'a pas été oublié. Les contrôles sont effectués selon les mêmes principes que pour le transport de passagers, avec une variante organisant une chaîne logistique sécurisée depuis la confection des colis, dont les acteurs doivent tous être agréés : « chargeur connu » préparant des expéditions dénuées d'objets prohibés dans des endroits sécurisés, « agent habilité » les acheminant jusqu'au lieu de chargement, transporteur aérien s'assurant que les procédures de sûreté ont été respectées.

Les États et les compagnies aériennes sont attentifs aux risques d'utilisation, contre des avions commerciaux, de missiles sol-air portables de type MANPADS. Le niveau de performance, le nombre et la dispersion de ces armes en font des menaces redoutables pour l'aviation civile. Des précautions sont prises autour des aéroports. En complément de la politique de contrôle engagée dans les instances internationales compétentes, la recherche et la destruction de ces armes doit continuer à être une priorité des services de renseignement et de sécurité.

Les transports terrestres

Après les attentats du 11 septembre 2001 perpétrés en détournant des avions, les deux attentats les plus meurtriers intervenus dans les pays occidentaux ont été ceux de Madrid en mars 2004 et de Londres en juillet 2005, effectués au moyen d'engins explosifs dans les transports urbains, comme l'avaient été les attentats de Paris en 1995 et 1996.

Les transports collectifs de personnes, en surface comme en souterrain, offrent au terrorisme des champs d'action favorables : fortes

concentrations de personnes dans des espaces restreints, faibles risques de repérage dans la préparation et l'exécution des attaques, nombre élevé de victimes, effets psychologiques importants dans l'opinion publique.

La détection des explosifs est un enjeu majeur de prévention de la menace terroriste dans les réseaux de transports. Elle est rendue difficile par le recours de plus en plus fréquent au masquage des explosifs et par la grande variété des matériaux utilisés.

L'autre enjeu est la détection par un réseau de capteurs de substances biologiques, radiologiques et chimiques. Il s'agit de limiter le contact de la population avec ces matières ou ces agents, puis de prodiguer aux éventuelles victimes les soins nécessaires. La détection permet aussi de circonscrire précisément la zone contaminée et de procéder à sa décontamination. Elle devient cruciale dès lors que l'agent utilisé passe inaperçu tant que les premiers malades n'ont pas été recensés.

Des scénarios d'attentats ont fait l'objet d'études approfondies de faisabilité. Ils ont débouché sur l'élaboration de programmes de renforcement de la sûreté des infrastructures de transport au sens large, comme les tunnels ferroviaires ou routiers et les viaducs, en les équipant de moyens de détection, d'alerte, d'interruption de trafic et d'intervention rapide des secours. La prise en compte de la sûreté intervient désormais dès la conception des grands ouvrages. Cette démarche intégrant les objectifs de sécurité générale contre les risques naturels ou les menaces de malveillance et de terrorisme doit être généralisée à toutes les infrastructures de transport.

La protection des agglomérations contre les risques liés au transport de matières explosives ou toxiques, par voie ferroviaire ou routière, concerne tous les pays. Elle est plus complexe dans les régions d'Europe à forte concentration de population. Des précautions particulières entourent certains transports de matières dangereuses, comme les matières nucléaires. Les efforts de prévention doivent porter sur les infrastructures (en aménageant des déviations pour le transport de ces produits) et sur le contrôle de l'application des règles de sécurité.

Les transports maritimes

La sécurité des transports maritimes a fait l'objet depuis vingt ans d'une attention soutenue ¹.

Après les attentats du 11 septembre 2001, les États-Unis ont réagi par des initiatives unilatérales portant notamment sur la sécurité des containers ². La France a souhaité que ce problème soit aussi traité par les instances internationales. L'Organisation maritime internationale (OMI) s'est saisie de la question et a initié en novembre 2002 un travail qui a abouti à l'édiction du code international de la sûreté des navires et des installations portuaires (sous son abréviation en langue anglaise, le code ISPS), entré en vigueur le 1^{er} juillet 2004.

(1) À la suite de la prise d'otages à bord du ferry Achile Lauro en octobre 1985, en particulier.

(2) Avec l'adoption de la CSI (*Container Security Initiative*).

Le code ISPS impose désormais que tous les navires de commerce effectuant des liaisons internationales soient dotés d'un plan de sûreté certifié. Il prescrit également l'évaluation de la sûreté des installations portuaires. Pour assurer la cohérence des normes internationales avec le plan VIGIPIRATE et le plan d'intervention PIRATE-MER, une doctrine interministérielle de sûreté maritime et portuaire a été arrêtée en octobre 2005 ¹. Cette doctrine repose sur une analyse de la menace et une hiérarchisation des réponses à apporter. Elle définit des actions de surveillance des approches maritimes et des plans d'eau portuaires, de contrôle des passagers et des véhicules embarquant sur les ferries, de vérification des cargaisons.

Une politique de soutien aux pays les plus en difficulté pourrait relayer les actions unilatérales de contrôle. C'est dans le cadre de l'OMI et de l'Organisation mondiale des douanes (OMD) que doivent être promus les programmes de normes à respecter par tous, qu'il s'agisse de l'échange des informations douanières, des méthodes modernes d'inspection à distance des conteneurs ou des techniques permettant de préserver l'intégrité des scelllements de ceux-ci.

Protéger les Français de l'étranger

Les Français vivant à l'étranger ou ceux qui y voyagent n'ont pas été épargnés, au cours des dernières années, par les attentats.

Le ministère des Affaires étrangères ² gère les avertissements ou les recommandations consignées sur le site internet de conseils aux voyageurs ³, dont le contenu est harmonisé, autant que possible, avec ceux de nos principaux partenaires. Il renforce, le cas échéant, les mesures de sécurité protégeant les communautés françaises qui vivent à l'étranger. Ce travail est mené en coordination avec les structures de renseignement, d'analyse ou d'intervention des autres ministères (DGSE, centre de planification et de conduite des opérations du ministère de la Défense, service de coopération technique internationale de la police nationale, centres opérationnels de gestion des crises rattachés au ministère de l'Intérieur : COGIC, COB et CROGEND ⁴) et les structures équivalentes de nos partenaires étrangers.

Sur instruction du directeur du cabinet du ministre des Affaires étrangères, une « cellule de crise opérationnelle » est ouverte sous l'autorité de l'ambassadeur pour organiser et coordonner la réponse, sur place, à la crise, et pour répondre aux appels téléphoniques de nos concitoyens. Cette structure est ouverte à des agents de liaison des pays concernés par

(1) La doctrine interministérielle s'appuie sur le concept de sauvegarde maritime mis en œuvre par la marine nationale.

(2) La Direction des Français à l'étranger et des étrangers en France, en concertation avec les postes diplomatiques.

(3) <http://www.diplomatie.gouv.fr/voyageurs>

(4) COGIC : centre opérationnel de gestion interministérielle des crises ; COB : centre opérationnel Beauvau ; CROGEND : centre de renseignement et d'opérations de la gendarmerie nationale.

les attentats à l'origine de la crise. Elle établit des contacts avec les cellules de crise actives dans ces pays. Sont généralement envoyées sur le lieu de crise des équipes mobiles composées d'agents du ministère et d'autres professionnels (médecins, agents de la sécurité civile, enquêteurs...) qui se coordonnent sur place avec les équipes équivalentes de nos partenaires. Des missions conjointes peuvent être organisées.

Sur le plan européen, le groupe de travail du Conseil de l'Union sur les affaires consulaires a réorienté ses priorités, qui portent désormais moins sur la matière consulaire au sens traditionnel du terme et davantage sur les questions de sécurité. Ce groupe a élaboré des lignes directrices sur la coopération en matière de sécurité des ressortissants de l'Union européenne dans les États tiers. Il doit maintenant définir des planifications communes d'opérations d'évacuation des ressortissants de l'Union dans le cadre de la Politique européenne de sécurité et de défense (PESD) et concevoir des exercices permettant de simuler des situations de crise, à l'instar de l'exercice EVAC06 prévu au premier semestre 2006 et relatif à l'évacuation de 8 000 ressortissants européens d'un pays situé à 10 000 km des frontières de l'Union.

Protéger l'intégrité du pays

Préserver les infrastructures vitales

Dans sa logique de tentative de déstabilisation sociale et politique, le terrorisme mondial cherchera à frapper des cibles à forte valeur économique ou écologique, d'autant plus que la destruction, totale ou partielle, de certaines infrastructures est susceptible d'occasionner aussi de lourdes pertes humaines.

Les terroristes frappant plus là où ils le peuvent que là où ils le voudraient, le durcissement de la sécurité de cibles potentielles est de nature à les faire renoncer à leurs projets ou à réduire l'effet de leurs actes. Il est donc indispensable d'identifier les infrastructures critiques et de mener à leur égard une politique de sécurité impliquant les entreprises des secteurs les plus sensibles.

Tel est l'objet de la réforme engagée récemment par le Gouvernement. Celle-ci est fondée sur les dispositions du code de la défense, qui mettent à la charge des opérateurs publics ou privés d'infrastructures vitales les mesures de protection interne contre « toute menace, notamment à caractère terroriste ».

Sont concernées au premier chef les activités indispensables pour satisfaire les besoins essentiels à la vie de la population et au maintien des capacités de sécurité et de défense du pays : l'alimentation, l'eau, l'énergie, les transports, les institutions financières, les systèmes d'information et de communication, les centres de décision et de commandement.

En concertation avec les professions concernées, l'État établira et tiendra à jour une directive nationale de sécurité pour chacun de ces secteurs d'activité. Cette directive définira la nature des menaces contre lesquelles il convient de se prémunir, les objectifs de sécurité et la combinaison des plans spécifiques préparés par chaque opérateur¹ avec le plan gouvernemental VIGIPIRATE.

Sur le fondement de chaque directive, les principales entreprises du secteur d'activité mettront en œuvre une politique de « défense en profondeur » consignée dans des plans de protection, identifiant leurs installations névralgiques et comportant des mesures concrètes tant physiques (vigiles, clôtures, serrures, caméras de surveillance, détecteurs de produits toxiques, alarmes, moyens de secours) que d'organisation (vérifications plus approfondies à l'embauche, gestion des visiteurs, contrôle des livraisons, flux de circulation, ressources de substitution...).

La démarche engagée sur le plan national est cohérente avec celle de l'Union européenne sur la protection contre les risques de toutes natures pesant sur les infrastructures vitales, notamment sur celles dont l'arrêt ou le dysfonctionnement auraient des conséquences majeures sur plusieurs pays.

Protéger les systèmes informatiques sensibles

Les systèmes d'information constituent les centres nerveux de la plupart des organisations. Ils sont donc une cible de choix pour qui veut désorganiser ou paralyser le fonctionnement du pays.

Or ces réseaux, qu'ils soient publics ou privés, ne fonctionnent pas en vase clos. Quel que soit leur degré de protection, ils disposent le plus souvent d'une ouverture vers l'extérieur, soit en raison de « passerelles » vers internet, soit en raison du développement de la télémaintenance. En outre, l'utilisation généralisée de matériels ou de logiciels standards du commerce, comme Windows ou Unix, augmente la vulnérabilité des systèmes dans la mesure où elle permet une démultiplication standardisée des attaques.

Sur le plan technique, la menace terroriste ne présente pas de spécificités. Les « cyberterroristes » agiraient contre les réseaux informatiques comme des « cybercriminels » de droit commun. D'éventuelles attaques s'appuieraient sur les outils développés par les pirates. Les menaces les plus prévisibles sont les attaques en cascade à l'aide de codes informatiques malveillants diffusés sur le réseau ou dissimulés dans un site web préalablement compromis, qui se dupliqueraient à leur tour une fois introduits dans le système. La menace la plus insidieuse consisterait en des attaques ciblées par des logiciels malveillants diffusés à très peu d'exemplaires (et donc inconnus des fournisseurs de solutions antivirales) et feraient office d'agents dormants jusqu'à leur activation simultanée.

(1) Les « plans de sécurité d'opérateurs ».

L'objectif de ces attaques peut être, en soi, la désorganisation de systèmes vitaux pour le pays. Il peut être aussi de perturber ces systèmes au moment où se produiraient des attentats, dans le but de désorganiser les opérations de secours. On ne peut non plus exclure des motivations plus banales, comme celle de détourner des fonds pour financer des activités terroristes.

Les défenses sont connues. Il s'agit de la mise à jour systématique des logiciels, du respect de rigoureux régimes d'authentification des personnes admises à entrer sur le réseau, de la généralisation de la cryptographie, de l'installation de pare-feu, d'antivirus, d'outils de détection d'intrusion et de l'utilisation d'outils de sécurité labellisés et, dans les cas les plus critiques, de l'isolement des réseaux de l'internet.

La mise en œuvre de ces défenses doit encore être améliorée.

L'État a pris des mesures pour faire face aux menaces pesant sur ses propres systèmes d'information. Améliorer la protection de l'administration contre la malveillance informatique est la mission qui revient au Secrétariat général de la défense nationale (SGDN), qui a un rôle permanent de veille, d'alerte et d'intervention auprès des administrations victimes d'une attaque. Un plan de renforcement de la sécurité des systèmes d'information a été élaboré, avec quatre objectifs principaux : la sécurisation des communications des hautes autorités ; la sécurisation des systèmes d'information des administrations ; la mise en place de capacités opérationnelles de réponse aux attaques informatiques ; l'inscription de cette politique de sécurité dans un cadre européen. Les efforts en termes de moyens et de sensibilisation des utilisateurs doivent être poursuivis dans le domaine de la prévention afin de renforcer le niveau de sécurité des systèmes d'information des administrations.

Les grandes entreprises privées ne sont pas demeurées passives dans ce domaine. Deux freins brident néanmoins une action d'envergure. Certains cadres dirigeants méconnaissent encore le niveau des menaces auquel leur entreprise est soumise. Les dépenses consenties pour la sécurité des systèmes d'information n'ont pas de retour visible. Elles ne sont pas toujours considérées comme des investissements, alors même qu'elles ont pour effet de préserver le patrimoine et plus généralement les actifs de l'entreprise.

Ces obstacles doivent être surmontés par une action de sensibilisation et de coordination associant, sous l'égide de l'État, experts, médias et professionnels du secteur. L'effort à entreprendre en faveur des entreprises les plus vulnérables (PME et PMI) doit en particulier passer par la rédaction à leur intention d'un guide de bonnes pratiques.

Renforcer nos capacités de gestion de crise

Parfaire nos capacités opérationnelles

Les plans d'intervention « PIRATE » et le plan ORSEC récemment rénové sont des outils complets de gestion d'une crise d'origine terroriste. Leur combinaison doit encore être améliorée

Les plans gouvernementaux d'action de la famille « PIRATE ¹ » comportent des mesures d'alerte, d'organisation, de protection et de neutralisation de la menace déclinées à l'échelon de la zone de défense et, pour certains, au niveau du département ². Ils sont principalement consacrés à la prévention.

(1) Pour une description de ces plans, *cf.* p. 70.

(2) En matière de gestion de crise et d'organisation des secours, il existe, au sein de l'État, une strate de responsabilités administratives au-dessus du département, la zone de défense, dans le cadre de laquelle l'événement est géré dès que son ampleur dépasse le niveau départemental et où est assurée la coordination opérationnelle des moyens civils et militaires. Il existe en métropole sept zones de défense.

Le plan ORSEC ¹ est déclenché par le préfet de département en cas d'événement majeur nécessitant l'organisation de secours à la population. Pendant très longtemps, ce plan n'a été regardé que sous son angle purement opérationnel, qui en faisait l'ultime outil en situation de crise. La nouvelle planification ORSEC ² conserve cet aspect essentiel, qui a largement fait ses preuves, mais le replace dans une perspective d'ensemble de protection générale des populations et des biens. Elle est aujourd'hui, sous l'autorité du préfet, l'élément central du dispositif d'organisation et d'intervention permettant de faire face aux conséquences de tout type d'événement majeur, y compris d'un attentat terroriste de grande ampleur.

Le manuel opérationnel ORSEC aborde tout le champ de la gestion de crise : le recensement et l'analyse préalables des risques et des conséquences des menaces communes à tous les services ; un dispositif opérationnel, cœur actif du plan, définissant une organisation unique de gestion des événements majeurs ; des phases de préparation et d'entraînement nécessaires à la mise en œuvre opérationnelle.

Les plans « PIRATE » et ORSEC couvrent ainsi l'ensemble des aspects du traitement d'une crise terroriste : les premiers répondent à la menace et les seconds organisent les secours aux populations. Leur combinaison doit cependant être mieux éprouvée.

Globalement, les plans « PIRATE » traitent d'actes terroristes aériens, maritimes, ou faisant appel à des moyens non conventionnels (nucléaires, radiologiques, biologiques ou chimiques). Ils doivent être complétés par un plan gouvernemental d'intervention consacré à un attentat majeur conventionnel ou à une série d'attentats rapprochés. Dans le détail, les « fiches réflexes » des plans « PIRATE » et les analyses de risques des plans ORSEC doivent être rendues parfaitement cohérentes entre elles.

Il est indispensable que des entraînements réguliers soient effectués pour valider les hypothèses de travail retenues dans les plans, pour éprouver leur mise en œuvre et pour améliorer nos capacités de réponse.

Notre organisation et nos moyens de gestion de crise doivent encore être renforcés

L'organisation

Nous devons resserrer le maillage des centres opérationnels ou des centres de crises des différents ministères.

1) Au niveau central, en 2006, quelques administrations s'appuient sur des centres opérationnels pour tenir une permanence 24 heures sur 24, 7 jours sur 7.

(1) Pour ORganisation des SECours.

(2) Issue du décret n° 2005-1157 du 13 septembre 2005.

Le ministère de l'Intérieur dispose, pour ce qui relève des questions de sécurité intérieure, du Service de veille opérationnelle de la police nationale (SVOPN) et du Centre de renseignement et d'opérations de la gendarmerie nationale (CROGEND). Il dispose aussi du Centre opérationnel de gestion interministérielle des crises (COGIC) pour tout ce qui concerne la sécurité civile. Le ministère de la Défense s'appuie sur le Centre de planification et de conduite des opérations (CPCO) et les centres de conduite des opérations aériennes et maritimes. Une permanence est assurée au ministère des Affaires étrangères.

En dehors des heures habituelles de travail, les autres administrations recourent à des formes diverses d'astreinte, avec des délais d'activation et de réaction adaptés au type de crises qu'elles sont amenées à connaître.

Cet ensemble doit être amélioré sur deux points. Il faut unifier les réseaux sécurisés de transmission de messages et de données et créer un « portail » commun de gestion de crise auquel les agents de permanence seront connectés de manière continue. Il faut également raccourcir les délais de réaction.

L'étape suivante sera la création d'un intranet gouvernemental sécurisé permettant aux autorités d'échanger des informations, confidentielles ou non, avec un haut débit de transfert. Sous le nom d'Isis, ce réseau commence à être déployé au début de l'année 2006.

2) Au niveau territorial, le dispositif de gestion de crise est confié aux préfets et, à Paris, au préfet de police. Cette organisation, claire et rationnelle, bénéficie des prérogatives interministérielles des préfets et d'une longue expérience dans la gestion des situations d'urgence. Au cours des dernières années, les responsabilités et les moyens des préfets de zone de défense ont été renforcés afin de faciliter la coordination et la mutualisation des capacités d'intervention.

La coordination

Au niveau central, le Premier ministre dirige l'action gouvernementale. Il désigne le ou les ministres qui assurent la conduite opérationnelle de l'action gouvernementale, et qui s'appuient pour ce faire sur des cellules ou des centres opérationnels *ad hoc*.

Pour renforcer l'efficacité de ce dispositif et notamment faciliter l'échange d'information et la coordination en cas de crise relevant de plusieurs ministères, il convient de développer l'interopérabilité entre salles de crises, c'est-à-dire la capacité à utiliser des outils de communication et de gestion de crise compatibles, mutualisables et sécurisés.

L'alerte à la population

L'alerte en cas de menace imminente d'attentat pouvant affecter un quartier, une ville ou une région, afin de mettre à l'abri la population dans les meilleures conditions de protection possibles, est un devoir de l'État envers les citoyens.

L'ensemble des États industrialisés ont, pendant la Guerre froide, bâti des systèmes pour gérer les conséquences d'éventuelles hostilités militaires de grande envergure : le Réseau national d'alerte (RNA) qui existe dans notre pays est en grande partie issu de cette période. Constitué d'un réseau de sirènes, le RNA est aujourd'hui assez largement obsolète. Les sirènes n'apportent qu'un message d'alerte brut, indifférencié, inadapté à certains scénarios d'attaque à effet diffus ou différé.

Dans certaines hypothèses d'attentats terroristes, les réseaux de sirènes peuvent cependant demeurer un moyen efficace d'alerte rapide, invitant au confinement ou à l'écoute des radios. Ce constat a suscité un regain d'intérêt pour des réseaux de sirènes locaux, souvent gérés par des communes ou des entreprises.

Des services publics et des entreprises privées ont mis en place des systèmes d'alerte en cas de risque pour la sécurité ou la santé. Ces systèmes utilisent fréquemment des techniques d'appel modernes, correspondant aux nouvelles habitudes de communication : messagerie internet, messages sonores ou écrits sur téléphones mobiles, recours à des plates-formes téléphoniques ou à des centres d'appels automatiques.

Des centres d'information renseignent sur les causes des événements, conseillent les personnes concernées par l'alerte, répondent aux inquiétudes en faisant intervenir des spécialistes. Les messageries électroniques visuelles, urbaines ou routières (accidents, bouchons, risques météorologiques...) permettent la diffusion rapide de messages instantanément actualisés.

C'est par l'utilisation simultanée de ces différents supports que les autorités publiques doivent donner l'alerte aux populations. Des conventions peuvent d'ores et déjà être signées entre l'État, les télévisions et les radios pour relayer les alertes¹. La généralisation des moyens de communication (téléphones fixes et portables, internet...) fournit l'occasion de compléter le maillage du territoire. Les conditions générales d'utilisation des services de téléphonie et de messagerie électronique doivent être conçues pour permettre à l'État d'envoyer des messages vers l'ensemble des téléphones portables situés dans l'aire de desserte des relais d'une zone géographique donnée ou vers le parc d'ordinateurs actifs dans cette zone.

Les moyens de terrain

Si l'attentat n'a pu être évité, il est déterminant que les forces de sécurité et de secours puissent agir même si les conditions d'intervention sont très difficiles.

(1) Voir les prescriptions du décret n° 2005-1269 du 12 octobre 2005 relatif au code d'alerte national et aux obligations des services de radio et de télévision et des détenteurs de tout autre moyen de communication au public. Ce décret a été pris en application de l'article 8 de la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile.

1) Maintenir des moyens de communication efficaces en toutes circonstances.

Le premier effort doit porter sur l'amélioration de l'interopérabilité entre les différentes forces et instances impliquées (parquet de Paris, police, gendarmerie, armées, sécurité civile, pompiers) afin que celles-ci puissent communiquer quelle que soit la situation d'urgence rencontrée. L'interopérabilité doit être recherchée entre les équipements, les systèmes de transmission, les logiciels et les doctrines d'emploi, y compris au niveau européen. À terme, les moyens de communication utilisés par les forces de sécurité devront intégrer la transmission d'images et de vidéo.

La mobilité des forces est essentielle. Il faut donc veiller à ce que les systèmes retenus puissent fonctionner dans des zones sans infrastructures ou dont l'infrastructure serait endommagée. Il faut prévoir des PC de crises facilement transportables dans les zones affectées. Les moyens de commandement et de communication fixes et mobiles des armées peuvent être utilisés si cela s'avère nécessaire.

En matière de télécommunications, la priorité pour les forces de sécurité doit être de disposer en toutes circonstances d'un accès immédiat aux réseaux.

Le réseau ACROPOL de la police et le réseau RUBIS de la gendarmerie assurent aux autorités locales un système de communication avec les forces de l'ordre. Dans certains cas, l'accès aux réseaux civils est cependant l'unique méthode de communication possible. La possibilité de mettre en œuvre une priorité d'établissement des communications au profit de certains acteurs publics doit à cet égard être étudiée.

2) S'équiper, s'entraîner, se préparer par la simulation de crises.

Il appartient à chaque ministère d'équiper ses propres services en tenues de protection, en moyens de transport, en équipements d'intervention et de secours. La loi d'orientation et de programmation pour la sécurité intérieure couvrant la période 2002-2007 et la loi de programmation militaire portant sur la période 2003-2008 ont permis aux ministères de l'Intérieur et de la Défense de moderniser les moyens d'action de la police et des forces armées.

Les unités spécialisées civiles et militaires ont développé une expertise solide dans le domaine terroriste. Les forces de police (RAID, éventuellement assisté des groupes d'intervention de la police nationale) et les forces de gendarmerie (unités regroupées au sein du groupement de sécurité et d'intervention – GSIGN, dont le GIGN et l'escadron parachutiste) s'entraînent au quotidien pour être en mesure de faire face aux situations créées par certains actes de terrorisme, et notamment les prises d'otages ou les détournements d'avions et de navires. Si l'ampleur de

l'attaque l'exige (prise d'otages massive par exemple), les forces spéciales militaires apporteront leur concours, sous un commandement unifié ¹.

Il est nécessaire aussi de poursuivre le développement de logiciens de gestion de crise, indispensables pour optimiser les choix des décideurs travaillant sous pression et dans l'urgence (projections sur le nombre de victimes potentielles, propagation des effets d'une attaque, modélisation et allocation des ressources).

3) Savoir gérer dans la durée les conséquences d'un attentat NRBC.

En cas de déclenchement de crises NRBC, les autorités civiles disposent d'un important éventail de capacités d'analyse, de secours et de traitement : laboratoires du réseau BIOTOX-PIRATOX, SAMU disposant d'équipements NRBC, cellules d'intervention chimique ou radiologique des services départementaux d'incendie et de secours (SDIS), chaînes de décontamination, renforts nationaux des unités d'instruction et d'intervention de la sécurité civile (UIISC), hôpitaux dont les moyens spécialisés sont étendus par des dispositions particulières des plans BLANC ². Le Détachement central interministériel d'intervention technologique (DCI) ³ pourra être mobilisé à tout moment.

Pour l'identification ou la caractérisation des contaminants biologiques les plus dangereux, il existe un maillage par zones de défense du territoire national en laboratoires aux compétences diverses. C'est le réseau de laboratoires BIOTOX/PIRATOX. S'agissant des souches d'agents biologiques les plus pathogènes et pour lesquels il n'existe pas de traitement curatif efficace ni une protection systématique de la population, nos capacités de niveau P4 ⁴ doivent être adaptées pour pouvoir réagir en cas de situation d'urgence et complétées par des moyens mobiles.

Il est également prévu que le ministère de la Défense mette à disposition si nécessaire ses capacités de décontamination, de traitement et de réhabilitation des zones affectées. Il s'agit des centres d'études, des hôpitaux d'instruction des armées et des hôpitaux de campagne dotés pour certains d'une section chirurgicale protégée NBC, du régiment de défense NBC et de certains régiments du génie.

(1) Un escadron d'hélicoptères est depuis le 1^{er} février 2006 spécialement dédié à l'hélicoptère des forces antiterroristes.

(2) Le plan BLANC détermine les dispositions graduées à prendre dans chaque hôpital pour accroître temporairement les capacités d'accueil et d'hospitalisation (rappel de personnel, transfert de patients dans d'autres établissements, report d'interventions sans urgence). Des dispositions particulières sont prévues pour certaines maladies contagieuses et pour les victimes d'attentats chimiques ou radiologiques.

(3) Dirigé depuis sa création par le chef du RAID, le Détachement central interministériel d'intervention technologique (DCI) est chargé de la localisation, de l'identification, du diagnostic et de la neutralisation d'engins nucléaires, radiologiques, biologiques ou chimiques improvisés. Il regroupe les unités spécialisées de divers ministères.

(4) La dénomination P4 (ou plutôt NSB 4 pour « niveau de sécurité biologique 4 ») fait référence au plus haut niveau de confinement nécessaire pour protéger l'environnement et le travailleur lors de la manipulation de micro-organismes pathogènes caractérisés par leur haute dangerosité (transmission interhumaine et absence de traitements efficaces).

Pour faire face aux situations de crise, la palette d'outils juridiques est large mais incomplètement adaptée

En cas d'attaques terroristes dont l'ampleur menacerait gravement le pays, les pouvoirs publics disposent de moyens juridiques exceptionnels pour neutraliser ceux qui les auraient perpétrés et protéger la population.

Pour répondre à des situations d'une extrême gravité, notre droit prévoit trois régimes dont les conséquences sur les libertés publiques sont d'importance croissante.

1) Fixé par la loi du 3 avril 1955, l'état d'urgence s'applique en cas de péril imminent résultant d'atteintes graves à l'ordre public¹. Sa déclaration donne le pouvoir aux préfets d'interdire la circulation des personnes ou des véhicules et d'instituer des zones de protection ou de sécurité où le séjour des personnes est réglementé. Il peut aussi permettre d'ordonner des perquisitions à domicile de jour comme de nuit.

2) Prévu par l'article 36 de la Constitution, l'état de siège, dont la déclaration transfère le maintien de l'ordre des autorités civiles aux autorités militaires, peut être décrété en cas de péril imminent résultant notamment d'une « insurrection armée ». La mise en œuvre de ce régime d'exception, dont l'origine remonte aux lois du 9 août 1849 et du 3 avril 1878², est *a priori* peu adaptée à l'hypothèse d'une attaque terroriste classique. Elle pourrait en revanche se concevoir dans le cas d'une attaque terroriste de grande ampleur faisant appel à des moyens non conventionnels.

3) L'article 16 de la Constitution constitue l'ultime régime juridique d'exception permettant de faire face à des situations d'une extrême gravité³. Ce dispositif se caractérise par l'attribution légale au président de la République de tous les pouvoirs pour une durée limitée.

Les différents régimes qui viennent d'être décrits ont été mis en place dans des circonstances historiques particulières. Aucun d'entre eux n'a été spécifiquement conçu pour lutter contre le terrorisme. Ils permettraient certainement de répondre à une situation d'une exceptionnelle gravité engendrée par des actes terroristes de grande ampleur.

La définition d'un régime juridique plus spécifiquement adapté aux situations de crise terroriste que le pays est susceptible de connaître mérite toutefois une réflexion plus approfondie.

(1) L'état d'urgence a été mis en œuvre en 1955 dans les départements français d'Algérie, puis étendu à la métropole en 1958, pour ne prendre fin que le 31 mai 1963. Plus récemment, l'état d'urgence a été appliqué en Nouvelle-Calédonie en 1985 et en métropole par décret du 8 novembre 2005 avant d'être prolongé pour trois mois par la loi n° 2005-1425 du 18 novembre 2005 et finalement rapporté au 4 janvier 2006 par le décret n° 2006-2 du 3 janvier 2006.

(2) Et est aujourd'hui codifié aux articles L. 2121-1 à L. 2121-8 du Code de la défense.

(3) L'article 16 a été mis en œuvre une seule fois, le 23 avril 1961, par le général de Gaulle à la suite du « putsch des généraux » à Alger.

La mise en place d'une doctrine de communication publique

Le coût élevé d'une mauvaise communication

Toute défaillance en matière de communication publique face au terrorisme se paie d'un prix fort dans le court et dans le long terme.

Dans la crise elle-même, par exemple en cas d'erreur d'attribution dans la responsabilité des attentats, les dommages dans l'opinion publique peuvent être d'une grande intensité immédiate : perte de confiance de la population, difficultés, le cas échéant, à engager l'enquête sur des bases solides.

Les conséquences d'une mauvaise communication publique sont encore plus importantes dans les mois et les années qui suivent. La communication qui accompagne les attaques terroristes ou les grandes calamités naturelles ou industrielles laisse en effet des traces profondes et durables dans la mémoire collective, en raison du climat dans lequel sont vécus les événements ¹. Ce type de souvenir a donc un impact immédiat sur la capacité pour la parole officielle d'être crue, voire même entendue, en cas d'événement comparable ultérieur.

Forces et faiblesses du dispositif actuel

Un dispositif nourri de multiples expériences

Notre pays a eu de multiples occasions de tester des dispositifs de communication destinés à gérer des situations d'urgence qui ne relevaient pas d'un attentat terroriste : inondations, feux de forêt, tempêtes de décembre 1999, canicule de l'été 2003. Nous disposons déjà de concepts et d'une expérience qui peuvent, en partie, être transposés à la communication en cas d'attaque terroriste.

Nous disposons en outre d'une expérience concrète en matière de communication publique après la perpétration d'un attentat terroriste. Elle est cependant limitée car la France n'a pas connu, depuis la fin de la guerre d'Algérie, d'attentat qui ait causé plus de huit morts sur son territoire en une journée. En termes de communication publique, nous n'avons pas eu à gérer les effets de bilans comparables à ceux des attaques les plus meurtrières sur le territoire européen (près de 200 morts à Madrid en mars 2004 ; une cinquantaine de morts à Londres en juillet 2005). Nous n'avons donc pas d'expérience nationale directe en matière de communication publique sur des attentats terroristes très meurtriers.

(1) C'est ainsi que vingt ans après l'accident nucléaire de Tchernobyl, le souvenir de ce qui a été dit à cette occasion par certaines autorités reste vivace.

De même, notre pays n'a pas eu à gérer dans le temps des campagnes terroristes très longues ou de grande ampleur. De 1965 à 2005, c'est-à-dire sur quarante ans, les attentats de toutes origines ont tué 192 personnes sur le sol français. Il faut comparer ce chiffre aux plus de 800 victimes de l'ETA en Espagne durant la même période ou aux 1 700 victimes causées par l'IRA au Royaume-Uni. La qualité actuelle de l'organisation britannique en matière de communication est largement liée aux leçons tirées de la lutte contre le terrorisme irlandais.

Un dispositif centralisé, vertical, et relativement déconcentré

La doctrine et l'organisation de la communication publique face au terrorisme sont à l'image de notre pays et de notre État. Trois mots les caractérisent : centralisation, verticalité et déconcentration.

Compte tenu de la nature des défis auxquels il s'agit de faire face et des objectifs à atteindre, ces caractéristiques traditionnelles sont la source de grandes forces et de nombreux avantages. Elles sont cependant également porteuses de certaines faiblesses.

La centralisation est un avantage. Elle repose sur un *a priori* implicite : en cas de crise, chacun se tourne vers l'État. Cette règle du jeu est connue et admise. La maîtrise de la communication par une seule entité facilite la conduite de la crise. Elle implique en revanche une coordination sans faille entre les différents registres de communication : politique, judiciaire, technique.

Dans notre pays, l'information est traditionnellement montante ou descendante. Une telle logique peut être la source de lourdeurs et de retards, puisque chaque niveau peut avoir tendance à filtrer l'information et donc à la transmettre avec un temps de décalage. La mise en réseau est encore étrangère à la logique du système.

Notre dispositif de communication de crise bénéficie en revanche d'une vraie force : sa large déconcentration dans la chaîne administrative territoriale, au niveau des préfets de zone de défense, des préfets de région et des préfets de département. L'unité de communication y est d'emblée plus aisée qu'à Paris.

Les principes d'une doctrine de communication de crise adaptée face au terrorisme : fédérer et orchestrer

Fédérer

Face à des risques nouveaux et à des menaces de niveau élevé, la communication publique doit être organisée de manière plus intégrée qu'autrefois. La création d'institutions nouvelles ne s'impose pas. Il faut en revanche accroître le rendement et l'efficacité des structures existantes.

La mesure fondamentale à prendre est de conférer un cadre stable – et interministériel – à la communication publique en cas de crise terroriste.

Il faut en premier lieu établir, sur une base permanente, un réseau interministériel, animé par le Service d'information du gouvernement (SIG), auquel participeraient les « communicants » des différents départements ministériels. L'objectif de ce groupe serait double : préparer la conduite de la crise en matière de communication, en particulier au moment des exercices de préparation, et animer la communication lorsque la crise se produit. Ce groupe pourrait élargir certaines de ses réunions aux cellules de communication placées auprès des préfets de zone.

La stabilité du cadre de communication publique passe aussi par la préparation d'un plan de communication pour chacun des ministères qui aurait un rôle à jouer dans la gestion d'une crise terroriste. L'organisation et l'expérience en la matière des ministères de la Défense et des Affaires étrangères devront être mises à profit pour l'élaboration de ces plans.

Orchestrer

1) L'articulation entre la communication politique et la communication opérationnelle.

Deux objectifs fondamentaux justifient de séparer les registres de la communication politique et de la communication opérationnelle.

Il faut en premier lieu conforter la confiance de l'opinion publique en montrant que chacun agit dans sa sphère de compétence (un magistrat, un policier ou un gendarme disposent, pour la communication relative à une enquête, de la crédibilité que leur confère leur fonction).

Il faut en second lieu garantir la crédibilité de la communication dans la durée en évitant de mettre en situation délicate les responsables politiques. Leur crédit pourrait être entamé par une intervention dans des domaines sur lesquels ils n'ont pas de prise directe ou si elle est faite sur la base d'informations incomplètes ou inexactes.

La mise sur pied d'une stratégie combinant les deux niveaux de communication passe par une série de mesures concrètes. Il s'agit d'abord de la décision de principe de séparer les deux registres. À cet égard, les « plans médias » et l'expérience des ministères de la Défense et de l'Intérieur en matière de communication de crise fournissent une bonne base de modèle doctrinal. Il faudra ensuite appliquer de manière systématique ce principe dans les simulations et dans les exercices réalisés au niveau national.

La division des rôles devra en outre se manifester dès le début de crise, sous forme de conférences ou de points de presse réguliers, à l'occasion desquels chaque intervenant sera immédiatement identifié par le spectateur en fonction de son ordre d'intervention, de sa place dans la salle ou de sa tenue (uniforme pour les forces de l'ordre).

2) Préparation et conduite de la communication au niveau de l'Union européenne.

Il est indispensable de mettre sur pied une communication de crise transfrontalière efficace en cas d'attaque terroriste.

Au sein de l'Alliance atlantique, l'existence pendant la crise du Kosovo en 1999 d'un porte-parole de l'organisation s'exprimant quotidiennement, en liaison directe avec les pays impliqués dans les opérations, a grandement facilité l'orchestration des communications proprement nationales. Cette communication s'effectuait en réseau, dont la tête était située au siège de l'organisation.

Cet exemple peut cependant difficilement être transposé à l'Union européenne, dont les missions et l'organisation institutionnelle sont différentes de celles de l'OTAN.

L'absence d'un coordinateur unique chargé de la gestion de crise au sein de l'Union européenne rend difficile la mise en place d'un porte-parolat unique sur ces sujets¹. La coordination en temps réel en matière de communication entre les institutions de l'Union et avec les États membres peut s'organiser sans qu'une telle fonction ne soit institutionnalisée.

La France devra soutenir activement la mise en place de procédures de coordination efficaces entre la Commission et le secrétariat général du Conseil en matière de communication de crise. Ces procédures devraient, comme à l'échelon national, être testées lors d'exercices fréquents associant les États membres.

Fort des outils de communication publique dont il dispose au sein des ministères des Affaires étrangères et de la Défense, notre pays devrait également mettre en place des liens avec les organismes en charge de ces questions chez nos principaux partenaires.

(1) Il existe au niveau de l'Union européenne une instance informelle de préparation et de partage des expériences de communication, à travers le « Groupe de Venise » qui réunit les « communicants » des vingt-cinq États membres et ceux des instances de l'Union. Celui-ci est néanmoins encore embryonnaire. De surcroît, il n'existe pas de mécanisme prédéfini de gestion de crise.



Chapitre 4

Renforcer nos capacités de réparation et de sanction

Réparer les dommages infligés aux victimes

Indemniser

Le fondement du dispositif d'indemnisation des victimes du terrorisme dans notre pays remonte à la loi du 9 septembre 1986. Ce dispositif a ensuite été complété par la loi du 23 janvier 1990, afin de donner aux victimes une véritable reconnaissance et de les faire bénéficier de la solidarité nationale.

Les victimes d'actes de terrorisme bénéficient ainsi des droits et avantages accordés aux victimes civiles de guerre par le Code des pensions militaires d'invalidité : gratuité des soins et des appareillages, emplois réservés, etc. Les enfants devenus orphelins à la suite d'attentats terroristes peuvent, dans certaines conditions, être déclarés pupilles de la Nation, tandis que les successions des victimes sont exonérées de droits de mutation.

Un fonds spécial ¹ a été créé pour faciliter l'indemnisation des victimes d'actes de terrorisme ² et de leurs familles. La procédure suivie est particulièrement simple : informé de l'identité des victimes par le procureur de la République ou par les autorités diplomatiques, le fonds les contacte directement et leur présente une offre provisionnelle d'indemnisation des blessures et du préjudice matériel, et, dans le cas d'un décès, du préjudice moral et économique des membres de la famille.

Naturellement, les victimes et leurs familles conservent à tout moment la possibilité, plutôt que de s'adresser au fonds, de saisir directement les tribunaux. Mais la procédure administrative présente l'avantage d'une aide dans les démarches et de permettre de bénéficier, très rapidement après les faits, de versements provisionnels ³.

Le fonds assure ainsi une réparation financière intégrale du préjudice supporté par les victimes du terrorisme, conformément aux grands principes du droit de la responsabilité. Il est nécessaire aujourd'hui d'aller plus loin, en promouvant, au-delà de l'aspect indemnitaire, un « principe de restauration dans l'état antérieur » de la victime, notamment en fournissant à celle-ci les moyens de réinsertion professionnelle et sociale lorsqu'elle a perdu son travail à la suite de l'attentat.

Réparer par le procès pénal

Au-delà de l'indemnisation, la réparation passe également par le procès pénal. Les dispositions de la loi du 9 septembre 2002, qui permettent aux victimes des infractions les plus graves de bénéficier d'un avocat dont les frais sont pris en charge par l'aide juridictionnelle sans condition de ressources, ont représenté une avancée significative pour les victimes d'actes de terrorisme.

Des progrès doivent encore être réalisés pour prendre en charge les victimes dès le moment de l'attentat et tout au long de la procédure.

(1) Le FGTI, alimenté par une contribution assise sur les primes ou cotisations des contrats d'assurance de biens.

(2) Et, depuis lors, d'autres infractions.

(3) Qui prennent en compte également le préjudice spécifique des victimes du terrorisme (le PSVT), mis en évidence pour la première fois par une étude réalisée en 1987 auprès de victimes.

Poursuivre les suspects : l'approfondissement de la coopération judiciaire internationale

Le pas décisif franchi avec l'adoption du mandat d'arrêt européen

Le 13 juin 2002 était adopté par le Conseil de l'Union européenne la décision-cadre « relative au mandat d'arrêt européen et aux procédures de remise entre États membres ¹ ».

La grande nouveauté réside dans la mise en place d'une procédure d'extradition exclusivement judiciaire, fondée sur le principe de reconnaissance mutuelle des décisions de justice, sans que le dernier mot puisse revenir au pouvoir politique. Elle vise à accélérer les procédures ².

Pour le terrorisme et trente et une autres catégories d'infractions graves, la remise a lieu sans contrôle de la double incrimination du fait reproché : l'autorité judiciaire d'exécution ne peut refuser de faire droit à la demande de remise au motif que les faits reprochés ne constitueraient pas une infraction au regard du droit pénal de son État. Cette souplesse élimine une source de controverses juridiques. La décision-cadre proclame aussi la fin, hautement symbolique, du refus d'extradition des nationaux entre États membres de l'Union européenne.

La Constitution française a été modifiée le 17 mars 2003 pour permettre l'entrée en vigueur de cette décision-cadre, et la loi du 9 mars 2004 en a assuré la transposition. Comme le montrent les statistiques en la matière, nous avons déjà tiré un grand bénéfice de cette réforme : en application de la nouvelle procédure, au 31 décembre 2005, les juridictions françaises avaient ordonné la remise de 336 personnes dont 140 ressortissants français et avaient reçu des autorités judiciaires d'autres pays de l'Union européenne 318 avis favorables dont 69 pour infractions terroristes. Le délai moyen de ces actions était de 45 jours ³.

(1) Le mandat recouvre les deux hypothèses classiques de l'extradition : il peut être émis lorsque les faits reprochés à la personne concernée sont passibles d'une peine privative de liberté d'au moins douze mois, ou, lorsque cette personne a déjà été condamnée, en vue de l'exécution d'une peine d'au moins quatre mois. Les faits de terrorisme entraînent déjà dans le champ des instruments existants.

(2) Des délais sont d'ailleurs fixés, les uns indicatifs, les autres impératifs : ainsi, la décision définitive sur l'exécution du mandat d'arrêt doit normalement intervenir dans les dix jours du consentement lorsque la personne consent à sa remise ou dans les soixante jours de l'arrestation dans le cas contraire, ce délai pouvant être prolongé de trente jours.

(3) Ces données doivent être rapprochées de la situation antérieure à l'entrée en vigueur de la loi du 9 mars 2004, où l'arrestation puis la remise d'une personne à des autorités judiciaires étrangères, même européennes, relevaient d'une procédure dont la durée était d'au moins six mois lorsque la personne consentait à son extradition, et de douze à dix-huit mois lorsque tous les recours étaient exercés.

Tous les États membres de l'Union européenne ont transposé la décision-cadre dans leur droit interne. La France doit néanmoins continuer de veiller à la mise en œuvre du mandat d'arrêt européen, dans un double souci d'efficacité opérationnelle et de promotion d'un instrument qui constitue une étape fondamentale vers l'espace de liberté, de sécurité et de justice que nous soutenons.

Le développement d'équipes communes d'enquête pour contrer le terrorisme international

La coopération judiciaire internationale revêt plusieurs formes.

Elle recouvre la concertation entre magistrats sur l'évolution de la menace, les législations antiterroristes et les pratiques judiciaires (par exemple groupes franco-américain, franco-allemand, franco-italien ou franco-espagnol qui se réunissent une fois par semestre).

Elle se traduit par la présence de magistrats de liaison à l'étranger afin de permettre une meilleure coopération opérationnelle avec les instances judiciaires et garantir ainsi une plus grande réactivité dans le traitement des dossiers sensibles.

Elle se manifeste également par la participation de magistrats français aux instances créées par l'Union européenne, comme EUROJUST. Cette préfiguration d'un parquet européen peut en effet être utile, à condition toutefois que ses conditions de fonctionnement soient précisées, en particulier pour ce qui est des modalités d'échange et de protection du renseignement.

La coopération judiciaire internationale devra aussi se traduire par le recours à des équipes communes d'enquête, ainsi que le permet une décision-cadre adoptée par l'Union européenne¹. De telles équipes, franco-espagnoles, ont déjà permis d'obtenir des résultats dans la lutte contre ETA. La possibilité de mettre en place des équipes opérationnelles du même type avec des pays extérieurs à l'Union européenne doit être recherchée par le biais de conventions bilatérales *ad hoc*.

Sanctionner les coupables

Adapter au plus juste la sanction pénale

Les peines prévues pour les actes à caractère terroriste obéissent à une logique d'aggravation par rapport au droit commun. Lorsqu'une peine punit normalement une infraction de trente ans de réclusion crimi-

(1) Les dispositions qui transposent cette décision-cadre figurent aux articles 695-2 et 3 du Code de procédure pénale.

nelle, elle est portée à la réclusion criminelle à perpétuité si elle est commise dans un but terroriste. Et la même logique s'applique à toutes les infractions.

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a aggravé et complété les sanctions pénales pour certaines infractions en matière de terrorisme. Le fait de participer à un groupement ou à une entente ayant pour objet la préparation d'un ou plusieurs crimes d'atteinte aux personnes, ou la préparation d'une ou plusieurs destructions par substances explosives ou incendiaires susceptibles d'entraîner la mort est désormais puni de vingt ans de réclusion criminelle. Le fait de diriger ou d'organiser une telle entente est quant à lui puni de trente ans de réclusion criminelle.

N'exclure aucune riposte

La France tiendra responsables des actions terroristes, au même titre que ceux qui les ont exécutées, les États qui les auraient commanditées, par leurs services ou par le biais de groupes clandestins.

Si l'action terroriste n'a pu être empêchée contre notre territoire ou contre nos intérêts à l'étranger, notre pays pourra recourir à une réponse militaire dans le cadre de l'article 51 de la charte des Nations unies relatif à la légitime défense. Les modalités et l'intensité de la riposte seront adaptées à la gravité de l'acte commis ainsi qu'aux cibles choisies.

Comme l'a souligné le président de la République après les attentats du 11 septembre 2001, et comme il l'a rappelé lors de son discours à l'Île longue le 19 janvier 2006, la dissuasion nucléaire « *n'est pas destinée à dissuader des terroristes fanatiques. Pour autant, les dirigeants d'États qui auraient recours à des moyens terroristes contre nous, tout comme ceux qui envisageraient d'utiliser, d'une manière ou d'une autre, des armes de destruction massive, doivent comprendre qu'ils s'exposent à une réponse ferme et adaptée de notre part* ».



Troisième partie

**Mener une action
de fond contre
le terrorisme
en gagnant
les batailles
du quotidien,
de la technologie
et des idées**



La France n'est pas en guerre contre les terroristes, mais elle mène une action de fond dont le succès nécessite de remporter les batailles du quotidien, de la technologie et des idées.

Chapitre 1

Gagner la bataille du quotidien : favoriser la détection précoce des activités terroristes par la vigilance et le renseignement humain

La lutte contre le terrorisme se gagnera d'abord par une posture de vigilance au quotidien.

Prévenir concrètement les risques d'attentats implique une mobilisation de tous les instants et une culture de la « détection précoce ». Celle-ci n'est pas spontanée et ne peut être seulement l'affaire des services spécialisés dans la lutte antiterroriste. Cette dimension nouvelle de l'esprit de défense doit être largement diffusée et partagée au sein de la société française.

Les agents des services publics : une vigilance essentielle

Le rôle des forces de sécurité intérieure non spécialisées

La recherche du renseignement opérationnel fait partie des missions premières de toute patrouille de police ou de gendarmerie et, d'une manière plus générale, de l'ensemble des unités du dispositif de sécurité de terrain. Cette responsabilité s'applique aussi au domaine de la lutte antiterroriste.

Notre pays compte près de 245 000 policiers et gendarmes. En raison de la diffusion de la menace et de l'évolution du profil des activistes tentés par le terrorisme, la lutte antiterroriste ne saurait reposer sur les seuls agents spécialisés dans cette lutte. Il est indispensable que l'ensemble des services et des unités contribue à la détection et à la remontée du renseignement à destination des services spécialisés.

La surveillance de la voie publique et le contact avec la population sont un moyen privilégié du recueil d'information. Mais l'efficacité de cette action suppose au préalable une bonne connaissance des enjeux de la lutte antiterroriste par les agents de la sécurité intérieure. Cette connaissance leur permettra de repérer des indices liés à une possible activité terroriste et les rendra capables de sélectionner les informations pertinentes à transmettre aux services spécialisés, mieux à même d'opérer certains recoupements et de donner la suite administrative ou judiciaire adéquate.

Une grande attention doit donc être apportée à la formation initiale et continue des magistrats, des policiers et des gendarmes. L'enseignement doit intégrer la connaissance des réalités sociales et religieuses de la société française contemporaine et des référents idéologiques des groupes terroristes. Le renouvellement récent des programmes de formation initiale et le développement des modules de formation continue portant sur cette question méritent d'être consolidés au cours des prochaines années. Il conviendra également de veiller à ce que l'acquisition et l'exercice de compétences en matière de lutte contre le terrorisme soient valorisés dans les carrières de la police et de la gendarmerie.

L'occupation de la voie publique et des lieux ouverts au public doit prendre en compte le risque terroriste à travers la détermination des lieux, des horaires et de la fréquence des patrouilles de surveillance.

Le nombre des sites à surveiller est tel qu'une coordination s'impose avec les polices municipales, dans le cadre des conventions prévues par la loi. De même, la coopération avec le secteur de la sécurité privée est nécessaire. Ce dernier recouvre aujourd'hui près de 200 000 emplois. Dans les limites fixées par le droit, ces professions réglementées concourent à la prévention du terrorisme et au niveau de sécurité générale.

La vigilance des agents du secteur public

D'autres catégories d'agents, dont les missions ne concourent pas directement à la sécurité, peuvent être confrontées à des situations anormales pouvant révéler les indices d'une activité terroriste.

Les membres des groupes et filières terroristes, qu'ils soient idéologues, recruteurs, logisticiens ou qu'ils préparent directement des attentats, connaissent tout d'abord une trajectoire personnelle qui les amène vers le terrorisme. Par ailleurs, la clandestinité de leur activité ne les dispense pas d'une intégration plus ou moins grande dans la vie courante, ni même des formalités administratives qu'elle implique. Certains sont même étroitement insérés dans des activités sociales. D'autres, à l'inverse, rompent subitement avec leur milieu habituel sous l'influence d'un endoctrinement. Enfin, un acte de terrorisme est précédé par une préparation minutieuse, de l'organisation aux repérages en passant par la confection des moyens de l'attentat, toutes phases durant lesquelles l'action clandestine peut se trahir aux yeux d'un témoin averti.

Il est donc indispensable que chaque catégorie d'agents publics soit régulièrement sensibilisée au phénomène terroriste, ainsi qu'aux comportements suspects qui peuvent en être l'expression.

La sensibilisation relève de l'impulsion des services spécialisés dans la lutte antiterroriste et doit d'abord s'effectuer à travers les relais institutionnels propres à chaque secteur. Son axe majeur devra être la diffusion d'un état de la menace adapté au destinataire. Ce document décrira en termes simples les auteurs potentiels, leurs habitudes comportementales, les modes préparatoires ou opératoires attendus et le type de cibles susceptibles d'être visées. Cette analyse s'accompagnera de fiches relatives à la conduite à tenir au regard des situations décrites.

Il importe tout particulièrement que les personnels, ainsi sensibilisés, trouvent un interlocuteur approprié en cas de doute et soient en mesure de donner l'alerte au bon moment. Pour chaque secteur, le canal de remontée des indices vers les services spécialisés doit être identifié et aisément utilisable.

Au sein de l'État, les Hauts fonctionnaires de défense (HFD) ont vocation à contribuer activement à la diffusion de cet esprit de défense. Le souci de faire prendre en compte de manière permanente la menace terroriste, de servir de relais aux services de renseignement et de veiller à l'application des mesures de vigilance qui s'imposent doit animer leur réseau.

Présents dans chaque ministère, rattachés directement au ministre et coordonnés par le Secrétariat général de la défense nationale, les HFD constituent des référents efficaces. Une réforme de leur statut est en cours. Elle leur donnera une autorité et des moyens plus substantiels en matière de sécurité. Il demeurera cependant nécessaire de faciliter leur travail en réseau à travers le partage d'informations et de retours d'expérience et de les mettre en situation en les chargeant de piloter, dans leur ministère, les exercices de crise.

Avec d'autres services publics ou des exploitants de lieux privés ouverts au public, les services spécialisés dans la lutte antiterroriste préventive peuvent aussi être amenés à nouer des contacts, ponctuels ou réguliers, en fonction de l'état de la menace.

La responsabilité des acteurs sociaux et le rôle du citoyen

La connaissance par le public du dispositif national de lutte antiterroriste

Il n'existe pas de politique préventive efficace dans le domaine de la lutte antiterroriste sans la vigilance de tous. La posture de vigilance doit dépasser la sphère publique.

Chacun connaît l'existence du plan VIGIPIRATE. Cette notoriété est un acquis positif. Mais il faut aller plus loin dans la diffusion d'une culture de prévention. Cette culture doit s'appuyer sur la connaissance de l'organisation du dispositif national de lutte antiterroriste par les citoyens. L'État doit également dire à qui s'adresser pour signaler un indice laissant présumer une activité terroriste.

À qui faire part de l'existence d'une situation suspecte ?

- *Le contact de premier niveau : le commissariat de police ou la brigade de gendarmerie (pour tout signalement ou même en cas de doute) ou les services diplomatiques et consulaires pour les Français résidant à l'étranger.*
 - *Pour les services publics ou les entreprises privées ayant préalablement noué des liens sectoriels au niveau régional : l'une des directions zonales ou des brigades territoriales de la Direction de la surveillance du territoire, la Direction de la protection et de la sécurité de la défense (DPSD), la gendarmerie nationale, ou, le cas échéant, les pôles régionaux de lutte contre l'islamisme radical, dans chaque direction régionale des renseignements généraux.*
 - *Pour des secteurs économiques ou administratifs spécifiques : contact direct avec la Direction de la surveillance du territoire, la Direction centrale des renseignements généraux, la DPSD ou la gendarmerie nationale.*
-

En dehors du dispositif de droit commun, les précédents espagnol et britannique ont montré que l'urgence peut nécessiter la mise en place d'un dispositif exceptionnel en cas de risque imminent ou déclaré d'une campagne d'attentats. Un tel dispositif doit permettre de recueillir dans les délais les plus brefs tout signalement en lien direct avec l'enquête, sur la base d'indications rendues publiques par les autorités en charge de l'enquête.

L'État s'est doté d'une plateforme téléphonique et internet de recueil d'information de la part du public. Il s'agit d'un « numéro vert antiterroriste », activable en cas de nécessité, avec un volet destiné aux victimes et un autre consacré au recueil de témoignages.

Le développement d'une politique d'exercices

Une dynamique nouvelle a été engagée depuis 2002 dans la conception et dans le déroulement des exercices.

Les exercices de défense et de sécurité ont pour objectif de tester régulièrement les procédures et les mesures prévues dans les plans gouvernementaux et dans les plans qui en sont dérivés, en premier lieu dans le domaine de la lutte contre le terrorisme. Ils impliquent tous les échelons de la gestion de crise et préparent les décideurs, leurs « états-majors » et les équipes opérationnelles à des interventions complexes (y compris, pour les intervenants de terrain, en atmosphère contaminée). Ils permettent de tester des équipements et des outils de gestion de crise.

Parmi ces exercices, ceux dits majeurs mettent en œuvre l'ensemble de la chaîne de décision et d'intervention, jusqu'aux plus hautes autorités de l'État (présidence de la République, Premier ministre et son cabinet, ministres et leurs cabinets respectifs).

Aux exercices de défense et de sécurité s'ajoutent les exercices de sécurité civile conduits par le ministère de l'Intérieur. Ils portent sur les opérations d'alerte et de secours après un événement, qu'il soit d'origine naturelle, accidentelle ou terroriste.

La politique nationale d'exercices opérationnels doit être poursuivie et renforcée. Les quatre exercices majeurs organisés chaque année sont un minimum qui doit être complété par des exercices nationaux ministériels et des exercices locaux. Cet ensemble ne prendra tout son sens que si des leçons globales sont tirées après chaque exercice et s'il est complété par un travail de synthèse et d'orientation. Il convient donc de mettre en place une planification indicative d'exercices à l'intention des ministères, d'organiser systématiquement les retours d'expérience, d'en diffuser les résultats et d'en tirer les conséquences pour définir l'adaptation de notre planification et de nos besoins en matière de gestion de crise.

Progressivement, s'organisent également des exercices multinationaux ou internationaux, de niveau stratégique pour la gestion de crises simulées traversant les frontières et les continents, telles que la réapparition de la variole par acte de malveillance ou de terrorisme, ou de niveau opérationnel pour des exercices plus localisés à la frontière de deux

ou de quelques États. Ils mettent en présence une large diversité d'acteurs : autorités publiques nationales et déconcentrées, représentants de collectivités territoriales, opérateurs d'infrastructures vitales, organisations non gouvernementales, etc.

Plusieurs aspects de communication publique sont désormais intégrés aux exercices. Traditionnellement, une information sur l'exercice et sur son déroulement était donnée, en préservant toutefois la discrétion sur certains modes opératoires. Plus récemment, une simulation de la pression médiatique a été incluse dans le déroulement de l'exercice. Cela a amené les acteurs à prendre en compte cette dimension dans leurs décisions : communication sur les événements et sur leur traitement, réactions de l'opinion publique, réactions internationales.

Cette prise en compte de la dimension médiatique dans les exercices de défense et de sécurité devra être renforcée car elle est un élément décisif de la politique de communication publique et de la gestion de crise.

La confiance de la population dans les pouvoirs publics sera plus naturelle si elle s'appuie sur l'expérience de préparatifs visibles à des événements dont l'éventualité ne surprendrait plus. Les citoyens bénéficieront aussi, à l'occasion d'exercices, d'éléments d'apprentissage pédagogique des comportements à adopter face à une crise d'une nature semblable à celle qui est simulée dans l'opération médiatisée.

Les exercices récents

Les exercices les plus fréquents, depuis 2002, ont porté sur des attentats ou des accidents chimiques, avec intervention réelle d'unités de secours sur le lieu de l'événement : PIRATOX en novembre 2003 à Paris, sur un scénario d'utilisation du gaz Sarin, identique à celui auquel la secte Aoum a eu recours dans le métro de Tokyo ; METROTOX en 2003, 2004 et 2005 dans les métros de Toulouse, Lyon et Marseille sur des scénarios d'utilisation de gaz toxique.

Le Détachement central interministériel d'intervention technologique (DCI) a été engagé en janvier 2004 dans un exercice conduisant à la neutralisation d'un engin nucléaire improvisé. Centré sur la phase immédiatement postérieure d'accueil hospitalier, l'exercice R-53 d'octobre 2004 à Paris répondait à un scénario d'attentat par « bombe sale » radiologique.

Le scénario d'AMBROISE 05, exercice d'état-major réalisé en décembre 2005 à Paris, comportait quatre attentats quasi simultanés dans les transports publics, dont un avec diffusion de gaz toxique.

Le domaine biologique a été couvert lors des exercices gouvernementaux BIOTOX 04 de mai 2004, qui portait sur une apparition malveillante de la variole, et « Pandémie grippale 05 » de juin 2005. Même si ce dernier exercice traitait d'un événement naturel et non

d'un acte terroriste, il simulait une situation de crise similaire à des scénarios extrêmes d'attentats majeurs.

Dans le domaine conventionnel, il faut citer les exercices ESTEREL 04 d'octobre 2004 en Méditerranée, ARMOR 05, de mai 2005, en Manche et en Atlantique, qui portait sur le terrorisme maritime, et enfin PIRATAIR 04, de décembre 2004, qui simulait un détournement d'avion, avec interception en vol et intervention au sol. Dans le domaine de la sécurité des systèmes d'information, l'exercice PIRANET 05 a été mené en novembre 2005.

À l'échelon européen, EURATOX, en octobre 2002 sur le plateau de Canjuers (scénario d'attentats chimiques multiples), et EURATECH, en avril 2005, dans la Drôme (attentat sur un transport chimique ferroviaire) ont réuni plusieurs centaines de participants de divers États membres de l'Union européenne pour tester la complémentarité des capacités d'intervention et la compatibilité des procédures et des équipements.

Le maintien de la vigilance de tous

Dans les périodes parfois longues de répit laissées par les terroristes, la vigilance doit pourtant être maintenue. Des actions de communication rappelant la réalité et la permanence du risque doivent être régulièrement menées, notamment à des moments propices : lors de la réalisation d'exercices ou au moment des départs et des retours de vacances.

Dans notre pays, les opérateurs de réseaux de transport en commun ont développé une politique d'appel à la vigilance des voyageurs, notamment au sujet des bagages abandonnés ou des colis suspects. Les appels, régulièrement répétés tout au long de la journée, se bornent néanmoins à prescrire une attitude générale, sans que des consignes précises soient données pour guider les comportements en cas de problème.

Dans le métro de Londres, la police spécialisée a instauré une procédure dite « HOT » résumant les trois caractéristiques d'un objet suspect : il doit être caché (*Hidden*), à l'évidence suspect (*Obviously suspicious*) et ne doit pas être caractéristique (*Typical*) de l'environnement considéré. Des consignes de comportement ont par ailleurs été édictées en cas de découverte d'un objet correspondant à ces trois critères.

Nos opérateurs de transport doivent s'inspirer de ce type d'expérience¹ pour fournir à leurs usagers des guides d'actions concrets au-delà des simples messages à caractère général qui leur sont adressés.

Nous devons aussi mieux gérer les menaces d'attentats. L'expérience a montré que, en France au moins, l'annonce d'un attentat, commis sur notre territoire ou à l'étranger, stimule toujours de mauvais

(1) Alors qu'en 1992 environ 20 % des incidents se traduisaient par une évacuation totale, cette proportion a été aujourd'hui ramenée dans le métro de Londres à moins de 1 %.

plaisants. Après la crise de l'anthrax aux États-Unis en 2001, des milliers d'enveloppes suspectes ont circulé en France et toutes ont été transmises à des laboratoires aux fins d'examen, ce qui a provoqué des engorgements et des délais de traitement excessifs. De même, après les attentats de Madrid en mars 2004, la SNCF a reçu de très nombreux appels anonymes prétendant que des bombes avaient été placées sur des voies ou à bord de trains, ce qui a engendré des retards considérables. Au-delà de la sensibilisation des Français aux dangers de ce type de comportements, une sévérité accrue à l'égard des auteurs des fausses alertes s'impose.

Le rôle de l'école

L'école est un lieu privilégié pour sensibiliser aux risques et aux menaces qui pèsent sur la société dans son ensemble et sur les moyens d'y faire face de manière préventive. Elle permet au futur adulte de prendre conscience de sa place dans la société, du rôle de la collectivité et de l'engagement individuel, et du respect des valeurs communes. Dans ce cadre, la lutte contre toutes les formes de discrimination est un élément essentiel pour prévenir les dérives extrémistes.

Le thème du terrorisme est susceptible d'être abordé en milieu scolaire à des degrés et selon des formats divers. Si la classe de primaire ne paraît pas le lieu le plus opportun, eu égard à la sensibilité du sujet, qui touche aux thèmes de la violence et de la mort, les élèves peuvent toutefois y être sensibilisés à la question du danger et aux règles élémentaires de prudence. Au collège et au lycée, plusieurs modules de programme permettent d'aborder la question du terrorisme, en particulier en cours d'histoire, de géographie et d'éducation civique.

Nous devons proposer aux enseignants des actions pour répondre à leurs attentes en matière d'information sur le terrorisme. Dans le cadre de la formation initiale des maîtres et des personnels d'encadrement, un module spécifique pourrait être consacré au sujet : cela permettrait de sensibiliser l'ensemble du personnel des écoles, des collèges et des lycées. Dans le cadre de la formation continue des enseignants, une journée académique sur les risques du monde contemporain, comprenant une séance sur le terrorisme, pourrait être organisée. La Journée de solidarité pourrait aussi être une occasion pour le corps enseignant et pour l'encadrement de traiter la question.

Des actions de partenariat entre les ministères de l'Éducation nationale, de l'Intérieur et de la Défense pourront être menées pour co-produire des documents, comme par exemple un document de mise en perspective du terrorisme, ou un document de synthèse pédagogique du présent Livre blanc. Une action de formation devra également être entreprise.

L'enseignement des faits religieux est aussi l'affaire de l'école laïque.

L'école ne peut être le lieu d'aucune forme de prosélytisme. C'est le sens de la loi du 15 mars 2004 encadrant, en application du prin-

cipe de laïcité, le port de signes ou de tenues manifestant une appartenance religieuse dans les écoles, collèges et lycées publics.

L'école ne relègue cependant pas les faits religieux à sa porte. Car seule une connaissance objective et circonstanciée des traditions et des textes religieux peut permettre aux jeunes de toutes confessions de tenir en lisière la tutelle d'extrémistes dévoyant le message de leur foi, en faisant des faits religieux des objets d'analyse historique, politique et sociale.

C'est ainsi qu'en termes de méthode, l'enseignement des faits religieux fait l'objet d'un enseignement obligatoire inclus dans les programmes de géographie, d'histoire, de lettres ou de philosophie.



Chapitre 2

Gagner la bataille technologique

L'objectif : toujours précéder la progression de la menace

Les principes

Les terroristes utilisent les technologies les plus modernes tant pour l'organisation de leurs réseaux que pour leurs modes opératoires. Ils progressent donc au rythme de l'évolution technologique. L'action publique ne peut sans risque être en retard.

Jusqu'ici, la politique de sécurité intérieure a privilégié l'achat de produits disponibles sur le marché. Cette approche ne permet pas à l'État de s'assurer que les parades techniques aux éventuels usages criminels des technologies nouvelles sont au point. Il faut savoir anticiper par des programmes de recherche capables de parer aux menaces futures. C'est l'enseignement que l'on peut tirer de la conduite des programmes de défense.

Si le cycle technologique en matière de défense atteint parfois quinze ou vingt ans du fait de la complexité des équipements, l'horizon temporel de la sécurité intérieure est plus ramassé, de l'ordre de trois à cinq ans. La prévention du terrorisme exige une synthèse équilibrée entre les deux modèles.

L'orientation de l'effort de recherche et de développement

Les défis technologiques à relever sont nombreux. Les réponses ne se conçoivent que dans le cadre d'une approche globale et mutualisée des efforts de recherche et de développement (R&D).

Plus que par le passé, une approche pluridisciplinaire s'impose, qui conjugue les sciences humaines (psychologie, linguistique...), les sciences physiques (mécanique, microélectronique...), les sciences du vivant et les technologies de l'information. Un recensement centralisé des besoins est nécessaire ainsi que, dans chaque domaine stratégique, une maîtrise d'ouvrage cohérente, assurée par un pilote identifié.

L'effort de R&D doit s'organiser selon trois volets.

Le premier regroupe la veille et la prospective dans le domaine des menaces, à partir de l'expérience des acteurs de la lutte antiterroriste. L'évolution des modes opératoires utilisés par les terroristes doit être intégrée dans les orientations et dans les choix des pouvoirs publics.

Le deuxième doit stimuler les programmes de recherche dans les domaines technologiques où des évolutions majeures sont attendues. Le rôle de l'Agence nationale pour la recherche (ANR) dans le secteur civil et de la Délégation générale pour l'armement (DGA) dans le secteur de la défense est d'identifier les disciplines qui nécessitent un investissement de long terme.

Le troisième effort concerne le développement industriel et la réalisation d'équipements dans les domaines où la technologie fondamentale est mûre. Il s'agit alors, à partir de l'analyse des besoins, de décliner avec des finalités différentes des applications déjà utilisées dans d'autres secteurs ou d'accélérer la mise au point de matériels spécialement adaptés à la lutte antiterroriste. Il faut là aussi s'appuyer sur les structures existantes, telle que, par exemple, l'Agence pour l'innovation industrielle (AII), le programme de soutien aux pôles de compétitivité dans le secteur civil et la DGA.

Parmi les secteurs qui doivent retenir toute notre attention figurent la protection contre le risque NRBC, la détection des explosifs, le contrôle des flux de télécommunications, la vidéosurveillance, la protection des systèmes d'information et la biométrie.

La protection contre les risques nucléaire, radiologique, biologique et chimique.

Après les attentats du 11 septembre 2001 a été mis en évidence le caractère avéré de la menace d'attentats terroristes ayant recours à des moyens non conventionnels, et pouvant ainsi provoquer un effet nucléaire, radiologique, biologique ou chimique.

Un inventaire des moyens de détection, de diagnostic, de prophylaxie et de thérapeutique, ainsi que de décontamination et de réhabilitation a permis de faire l'état des capacités actuelles de notre dispositif. Celui-ci doit encore être renforcé pour faire face aux caractéristiques parti-

culières de la menace terroriste, comme les « bombes sales » (engins explosifs à dispersion radiologique), les agents chimiques, les agents biologiques pathogènes, les attaques contre la chaîne alimentaire, dont l'eau potable, les ressources agricoles ou le milieu naturel.

Les domaines prioritaires pour lesquels de nouveaux outils doivent être mis au point ont été identifiés.

Dans le domaine nucléaire et radiologique, l'objectif est de pouvoir diagnostiquer et démanteler toute arme et tout engin improvisé dans des conditions optimales de sécurité.

Dans le domaine biologique, nous devons améliorer les capacités de détection et de diagnostic. Il faut compléter la gamme des agents détectables par la mise en œuvre de capteurs fiables et de protocoles communs d'analyse pour les laboratoires experts. Il faut développer encore nos moyens de prophylaxie et de thérapeutique.

L'introduction malveillante de maladies émergentes ou ré-émergentes peut être facilitée par l'évolution rapide des technologies de la biologie. Une capacité renforcée de détection, de diagnostic et de suivi épidémiologique des sujets suspects ou infectés (hommes, animaux, plantes) permettra de développer les réponses adaptées.

Dans le domaine chimique, les besoins portent plus particulièrement sur l'acquisition et l'adaptation de techniques existantes à un contexte civil : détection fiable en continu, levée de doute ou confirmation et alerte automatisée en cas de détection positive.

Les points communs de tous ces domaines sont le développement de capteurs miniaturisés et automatisés, à court délai de détection, et l'élargissement de la gamme de détection à l'ensemble des toxiques susceptibles d'être utilisés par les terroristes.

La détection des explosifs.

Il faut pouvoir détecter les produits explosifs dans des lieux de passage de personnes ou de véhicules sans obérer les flux de circulation. À cet effet doivent être mis au point et développés des capteurs automatiques utilisables en postes fixes ou en stations mobiles.

Les capacités de détection doivent s'étendre à des produits qui, à l'instar du nitrate d'ammonium, ont des comportements explosifs au prix de certaines modalités de préparation et de mise en œuvre. Pour la plupart, ces produits sont très répandus ou faciles à préparer par transformation de matières premières d'accès aisé. Ils sont aujourd'hui détectés par des chiens spécialisés. Il faut développer et fiabiliser les appareils de détection de traces.

Le contrôle des flux de télécommunications.

Le développement du réseau internet et des nouveaux services qu'il offre, en particulier en matière de téléphonie, modifie sensiblement l'architecture des réseaux des opérateurs. Afin de préserver la capacité de l'autorité judiciaire, des forces de police et des services de renseignement

d'accéder au contenu des communications échangées dans le cadre des interceptions judiciaires et de sécurité, il est indispensable que des dispositifs techniques adaptés soient mis en place aussi bien chez les opérateurs qu'auprès des forces de sécurité.

L'automatisation des tâches de détection devra nécessairement intégrer un module consacré à la parole, permettant à terme la reconnaissance du locuteur, celle de la langue employée, la transcription automatique des conversations et leur traduction automatique. Des outils de très bon niveau sont d'ores et déjà disponibles, même si les technologies doivent encore être éprouvées.

Dans le domaine des recherches dans de grands entrepôts de données (combinant texte, son et image numériques), les efforts devront porter principalement sur les capacités de tri sémantique, qui permettent d'ordonner de manière intelligible les informations recueillies dans des textes ou des enregistrements sonores, et sur la reconnaissance d'objets ou de personnes dans un flux continu de photographies ou de vidéos.

Le développement de la **vidéosurveillance** à des fins de lutte antiterroriste recouvre deux volets.

Le premier volet vise à améliorer la qualité des produits disponibles par l'établissement de standards exigeants. La normalisation des produits (caméras, réseaux, dispositifs de visualisation et de stockage, formats d'image, logiciels d'exploitation) devra être fondée sur la généralisation des techniques numériques et l'utilisation des normes dominantes (comme le format vidéo de type Mpeg...). La loi du 23 janvier 2006 relative à la lutte contre le terrorisme prévoit la définition de normes obligatoires.

Le second volet concerne les logiciels. Le développement de la vidéosurveillance ne peut se concevoir sans l'introduction de logiciels experts permettant la reconnaissance faciale, la détection de mouvements, la détection d'objets abandonnés ou le suivi de personnes. Ces logiciels sont en effet les seuls à même de permettre une exploitation rapide et efficace de la masse d'images recueillies. Les résultats obtenus par l'industrie sont encourageants.

Dans le domaine des **systèmes d'informations**, plusieurs actions doivent être menées pour accroître significativement la sécurité.

Face à l'insuffisance avérée de produits de sécurité de confiance, nous devons nous montrer plus ambitieux dans le financement de la recherche, du développement et de l'acquisition de ces outils. L'administration doit systématiquement utiliser, pour ses réseaux ou ses systèmes sensibles, des produits ou des services de sécurité évalués et qualifiés. Les opérateurs privés doivent être associés très en amont à cette démarche. Notre ambition, dans un domaine aussi régalién, doit être de développer des solutions nationales.

La biométrie.

Les techniques de biométrie ont déjà largement pénétré le domaine de l'investigation judiciaire et font la preuve de leur fiabilité. Les risques d'erreur statistique sont très faibles.

À ce jour, la biométrie digitale ¹ demeure le principal support technologique disponible pour développer des systèmes de contrôles fiables ² autour des zones sensibles ou d'accès réglementé. L'effort doit être porté sur le développement opérationnel et sur la diffusion de cette technique.

Dans le domaine génétique, le processus d'analyse reste long et la recherche doit se fixer comme objectif de permettre l'extraction du génome humain en temps quasiment réel à partir d'un échantillon sanguin.

Les techniques de reconnaissance faciale automatisée à partir de la photographie et de reconnaissance de l'iris de l'œil ne sont pas suffisamment mûres pour permettre des applications à grande échelle. Quant à l'identification par l'analyse du spectre de la voix humaine, elle reste un champ de connaissance trop embryonnaire pour que soient d'ores et déjà envisagées de larges applications opérationnelles. La poursuite des programmes de recherche dans ces deux domaines est nécessaire.

La méthode : une collaboration entre l'État et les entreprises, qui privilégie la dimension européenne

Encourager un processus d'élaboration de normes antiterroristes

La conception de produits obéit en 2006 à des normes de qualité de fabrication mais aussi à des normes environnementales nouvelles par rapport aux pratiques en vigueur au début des années 1980. Il faut aller vers une démarche de certification fondée sur l'objectif particulier de lutte contre le terrorisme ³.

L'État doit définir des normes, y compris dans le domaine de la certification, pour les organisations, les systèmes et les équipements concourant à la lutte antiterroriste. Cette action est un corollaire indispen-

(1) Voir la note 2 p. 57.

(2) Le taux d'erreur statistique de cette technique, déjà faible par nature, peut être réduit à un niveau nul par l'utilisation de plusieurs doigts, voire des empreintes de la paume de la main.

(3) À la suite des attentats du 11 septembre 2001, l'ANSI (*American National Standard Institute*) a entamé des travaux sur la lutte contre le terrorisme, sous l'angle global de la « protection du citoyen ». Ce thème a été repris par l'ISO (*International Standardisation Organisation*) et le CEN (Comité européen de normalisation). L'OTAN y participe également, en liaison avec le CEN.

sable à la politique de protection des infrastructures vitales édictée par les directives nationales de sécurité. Elle permet de protéger, de soutenir et d'encadrer l'activité industrielle associée à la sécurité et à la défense.

Les travaux menés dans les enceintes internationales de normalisation concernent de nombreux secteurs associés à la lutte antiterroriste. Il s'agit par exemple de la détection des agents NRBC, des communications d'urgence, des équipements de premier secours, de la biométrie, de la sécurité des chaînes logistiques, des pratiques d'exercices de crise.

Des contributions françaises doivent être apportées dans les instances internationales auxquelles l'agence française de normalisation (AFNOR) participe. À défaut, nous serions confrontés à des solutions auxquelles nos entreprises n'auraient pas été préparées ou qui ne répondraient qu'imparfaitement aux besoins français.

Dialoguer avec les entreprises et soutenir leurs efforts

Les entreprises françaises sont bien positionnées dans le secteur des technologies de sécurité. Elles s'appuient en la matière sur le secteur des technologies de défense avec lequel existe une réelle proximité. Le savoir-faire et les compétences de l'industrie nationale sont reconnus et utilisés par nos partenaires étrangers.

L'État peut donc s'appuyer sur l'expertise nationale pour concevoir les organisations et les équipements que requiert la lutte contre le terrorisme. Il doit soutenir les efforts de recherche et de développement des entreprises. Cette action nécessite un engagement financier inscrit dans la durée.

Pour les secteurs qui doivent recueillir nos efforts principaux (protection contre le risque NRBC, détection des explosifs, contrôle des flux de télécommunications, vidéosurveillance, protection des systèmes d'information et biométrie), l'État doit se fixer des programmes et des objectifs ambitieux. Il doit faire contribuer nos entreprises aux projets par des contrats de recherche ou de développement. Les moyens financiers consacrés à la R&D dans ces secteurs pourraient en outre être présentés dans un document budgétaire unique permettant d'identifier publiquement l'effort réalisé.

Appuyer, soutenir et développer le programme européen de recherche et de sécurité

Le caractère mondial de la menace et l'importance des moyens à mettre en œuvre pour répondre à celle-ci rendent naturelle la recherche de coopérations européennes et internationales.

La coopération est nécessaire pour mutualiser les ressources, et, dans certains cas, atteindre la masse critique susceptible de justifier certaines recherches. Elle permettra de poursuivre l'entreprise de normalisation et

de garantir à terme que les équipements de contrôle et de surveillance communiquent correctement entre eux au-delà des frontières. Elle permettra à notre industrie de s'étalonner par rapport à ses partenaires européens.

La lutte contre le terrorisme est, depuis 2001, une préoccupation importante de l'**Union européenne**.

Des initiatives concrètes ont été prises, avec la création d'agences européennes dans le domaine des transports et des réseaux, telles que l'Agence de sécurité maritime, l'Agence de sécurité aérienne, et l'Agence de sécurité des réseaux et de l'information. Mais les efforts dépassent la simple création de structures.

Des fonds significatifs sont mobilisés, au sein des Programmes-cadres de recherche et développement (PCRD), notamment le 6^e PCRD, en cours de réalisation en 2006. Le 7^e PCRD innove en prévoyant un volet spécifique – le Programme européen de recherche en sécurité (dit « programme PERS ») – qui pourrait être doté de 250 millions d'euros par an durant la période 2007-2013.

Le PERS offre la perspective tangible de développer des technologies européennes en matière de sécurité. Nous entendons y prendre toute notre part. Une organisation interministérielle a été mise en place à cet effet et un dialogue étroit est établi entre les administrations et les industries nationales. Cette concertation permettra de définir notre position, de contribuer à l'orientation du programme et de préparer notre industrie à ce nouveau cadre.

L'Union européenne doit soutenir le développement de systèmes interopérables d'alerte et de bases de données de gestion de crise. Notre pays a identifié les besoins nécessaires, à terme, à la mise en place d'un réseau européen de gestion de crise¹. La vidéosurveillance, la surveillance des marchandises, la détection de matières dangereuses, la protection des transports ont vocation naturelle à figurer aussi dans le PERS. La gestion du PERS par la Commission doit être menée en étroite collaboration avec les États membres, prescripteurs des besoins de sécurité.

Compte tenu de la communauté technologique forte entre les systèmes de lutte contre le terrorisme et ceux développés par les industries de défense en matière de NRBC, de détection, de protection des systèmes en réseau, d'interopérabilité des communications, l'agence européenne de défense peut en outre offrir un cadre approprié pour mener des activités de recherche, en coopération à vingt-cinq ou dans des formations plus réduites.

La sensibilité de certains sujets, pour des raisons de discrétion face aux menaces ou des impératifs de protection de savoir-faire industriels critiques, conduit à privilégier selon les sujets les coopérations restreintes, avec des partenaires européens clés.

Les programmes de coopération avec les États-Unis, notamment dans le domaine du NRBC, doivent par ailleurs être renforcés.

(1) Mise en commun de données, sécurisation des liaisons, mise sur pied de réseaux radio, développement de logiciels d'aide à la décision.



Chapitre 3

Gagner la bataille des idées

Sur le long terme, seule l'adhésion citoyenne est susceptible de constituer un rempart contre la propagation du terrorisme. Cette adhésion implique que notre pays livre bataille sur le terrain des idées, en France et dans le monde. La France a pour elle un crédit initial, celui de la cohérence de principe de son action intérieure et du discours qu'elle tient sur le plan international.

En France, conforter l'adhésion de la population et isoler les terroristes

Pour être entendu, le message doit être simple. Pour être convaincant, il doit se fonder sur les valeurs essentielles de notre tradition démocratique.

Le principe : ne jamais céder sur les valeurs fondamentales de l'État de droit

La France, comme tous les pays menacés par le terrorisme mondial d'inspiration islamiste, est confrontée à la question centrale suivante : comment une démocratie peut, en restant fidèle à ses valeurs, lutter contre une menace qui souhaite l'anéantissement de ce qu'elle représente ?

Deux questions, fondamentales l'une comme l'autre, doivent être tranchées. Devons-nous aller jusqu'à nous considérer en « état de guerre contre le terrorisme » ? Pouvons-nous, en vertu de la prééminence supposée ou réelle du droit fondamental à la sûreté, limiter fortement et durablement les autres libertés fondamentales, telles que le respect de la vie privée ou la liberté d'aller et de venir ?

Si nous étions en guerre, le recours permanent à une législation d'exception se justifierait de lui-même. Et comme la guerre se déroulerait en partie sur notre sol, ceux qui y résident devraient supporter que leurs libertés quotidiennes les plus essentielles soient entamées.

La France a choisi de demeurer dans une logique de temps de paix. Le fait qu'elle engage des forces armées dans la lutte contre le terrorisme ne contredit pas ce choix.

Notre droit pénal en matière de lutte contre le terrorisme demeure un régime spécialisé. Ce n'est pas un régime d'exception. Les mesures les plus novatrices en matière de police administrative, telles que le développement de la vidéosurveillance, la création de fichiers de traitement des informations sur les voyageurs internationaux, sont toujours assorties de garanties ¹ permettant de préserver nos libertés fondamentales.

Les dispositifs les plus innovants ne sont mis en œuvre que pour une durée limitée, avec une clause de rendez-vous devant le Parlement, afin que les pouvoirs publics rendent compte de la façon dont les nouveaux outils ont été utilisés.

Le Parlement doit en outre être informé sur l'activité des services de renseignement en matière de lutte contre le terrorisme. Il pourra l'être dans le cadre plus général de l'information que le gouvernement s'est engagé à lui fournir sur l'activité de ces services.

Cet équilibre général est révélateur d'un consensus clair selon lequel, au-delà du débat entre sécurité et liberté, c'est bien du maintien de nos grands principes démocratiques que pourra naître l'adhésion citoyenne au combat engagé par notre pays contre le terrorisme.

La France doit se battre contre le terrorisme en s'adossant à des valeurs fédératrices et susceptibles de donner une consistance concrète à la lutte. L'État doit informer les citoyens sur les risques et sur les méthodes retenues. La lutte contre le terrorisme passe aussi par une communication publique exigeante.

Refuser l'amalgame

La lutte contre le terrorisme mondial n'est en aucun cas un combat contre l'islam. Elle est dirigée contre des filières, des groupes et des réseaux qui dévoient la tradition humaniste de l'islam et détournent la religion au profit d'objectifs et de causes que des criminels prétendent servir.

(1) Comme l'intervention systématique de la Commission nationale de l'informatique et des libertés (CNIL).

Nous devons refuser l'amalgame entre islam et terrorisme. Le soutien aux autorités représentatives de l'islam de France et au message de paix envoyé par l'immense majorité des imams participe de ce refus absolu de l'amalgame.

Il ne revient pas à l'État de privilégier telle ou telle lecture de l'islam, pas plus d'ailleurs que de toute autre religion. La tenue de propos appelant à la haine, à la provocation ou à la discrimination n'est cependant ni moralement ni juridiquement acceptable et ne sera jamais tolérée.

La forme du message : la politique de communication publique doit rechercher le consensus le plus large en isolant les terroristes

Rassembler la population

Pour lutter contre le terrorisme, il existe deux types possibles de communication de long terme.

La première consiste à rechercher la manifestation d'un soutien majoritaire aux efforts des pouvoirs publics dans la lutte contre le terrorisme et ses effets. Cette approche privilégie la dramatisation, qui provoque souvent un processus d'identification avec l'autorité publique.

La seconde approche a pour objet de bâtir un consensus large, intégrant au premier chef la fraction de la population dont se réclament les terroristes et qu'ils essaient de détacher de la communauté nationale. Une politique de quête du consensus doit viser, à froid et de manière rationnelle, à faire de la population l'acteur lucide et sensibilisé au combat mené par les autorités. C'est cette seconde approche qu'il faut suivre.

Définir des groupes-cibles pour la communication.

Cinq groupes principaux doivent être distingués :

- la population dans son ensemble, y compris les enfants et les adolescents ;
- l'ensemble des personnes et des organisations engagées dans la lutte contre le terrorisme : l'État et ses agents ; les collectivités territoriales et leurs agents ; les opérateurs d'infrastructures vitales (santé, eau, énergie, transports, télécommunications...) ; les établissements recevant du public ainsi que leurs employés ;
- les populations dont les terroristes se prévalent. Elles sont placées dans une position délicate avant la perpétration d'attentats. Elles sont dans une grande vulnérabilité lorsque les terroristes ont frappé¹. Les réactions de cette partie de la population sont en outre décisives dans toute politique d'unité nationale et d'isolement des terroristes. La politique de communication portera tant sur les populations concernées en France que sur les

(1) Voir les réactions violentes contre les écoles et les lieux de culte musulmans aux Pays-Bas en novembre 2004 après l'assassinat du cinéaste Theo Van Gogh.

pays, les populations et les organisations étrangères susceptibles de peser dans le sens de l'isolement des terroristes ;
– les partenaires étrangers de notre pays ;
– en facteur commun, les médias nationaux et étrangers en tant que vecteurs privilégiés de communication.

Sur le plan des principes, les groupes dont la mobilisation est souhaitée doivent être considérés comme des partenaires dans la lutte contre le terrorisme.

Du « besoin d'en connaître » au partage de l'information.

La population est à la fois un enjeu et une cible. Elle doit être considérée comme un partenaire à part entière. Il faut donc passer d'une logique du « besoin d'en connaître », qui régit traditionnellement le domaine de la sécurité, à une dynamique nouvelle de partage de l'information.

Naturellement, ce passage du « besoin d'en connaître » au « besoin de partager » ne signifie pas que tout doit être mis sur la place publique. La population comprendra fort bien qu'une politique de transparence intégrale serait contre-productive dans cette matière. Cependant, affirmer ce nouveau principe revient à déplacer la charge de la preuve en termes de communication. Dans la tradition des États latins, l'information a tendance à être gardée par-devers soi, sauf si l'innocuité en est démontrée. À l'avenir, le principe devra être celui de la communication de l'information, sauf s'il est démontré que celle-ci serait dangereuse.

Le changement est de taille. Mais il est indispensable si l'on veut créer puis entretenir la confiance mutuelle qui est la clef d'une mobilisation réussie et durable du corps social contre le terrorisme.

Distinguer la discrétion nécessaire du mystère inutile.

Que l'on traverse ou non une situation de crise, il est important que les services de renseignement adoptent une politique de communication ciblée. S'ils doivent observer la plus grande réserve sur leurs méthodes opérationnelles et préserver leurs sources d'informations, il est utile que leurs responsables s'expriment sur l'état de la menace et les principaux enjeux de leur action. L'évolution récente de leur pratique à cet égard est un facteur positif qui mérite d'être consolidé.

Un besoin d'interfaces nouvelles.

Pour mettre en œuvre concrètement le changement d'approche, il faut en premier lieu créer à l'échelle nationale des **forums de communication** rassemblant les professionnels de la communication publique et les représentants des divers groupes cibles de la population que l'on souhaite mobiliser : relais d'opinion médiatiques vers la population dans son ensemble (chercheurs, spécialistes reconnus, journalistes), représentants des collectivités et des opérateurs, responsables des populations dont se prévalent les terroristes. La mise sur pied de ce type de forum peut également être envisagée au niveau régional (dans les zones de défense ou dans les régions, au sens institutionnel du terme).

La mise en place d'**enceintes informelles de dialogue avec les journalistes** pourrait être utile à la fois à l'État et à la profession qui se sent parfois isolée lorsqu'il s'agit de faire un choix éthique et déontologique entre préservation de l'intérêt national et révélation d'informations au grand public.

L'organisation de **colloques nationaux ou régionaux** doit être systématisée. Ces rencontres peuvent être organisées à l'initiative de l'État¹ ou d'instituts de recherche, bons relais vers la société civile. Ce type de rencontre visera entre autres à associer aux débats les personnes disposant d'un crédit particulier auprès des populations auxquelles les terroristes prétendent « montrer la voie ». Les travaux des instituts spécialisés dans la sécurité intérieure et la défense² montrent ce qui peut être fait en la matière.

La création de **sources d'information accessibles au grand public**³ comme aux spécialistes sur les diverses facettes du terrorisme doit être encouragée. Cette démarche sera d'autant plus efficace qu'elle associera secteurs public et privé. Cette forme de distanciation permet de dissiper le soupçon d'instrumentalisation qui pèse parfois sur la communication émanant de l'État. Celui-ci peut aussi concourir au développement de la capacité d'analyse des phénomènes terroristes par les centres de recherche.

L'**expertise individuelle sur le terrorisme** doit être développée dans le même esprit. En cas de danger ou de crise, quelle qu'en soit la cause, les médias ont recours à des personnalités réputées détenir une expertise, qui ont pour avantage de fournir une information *a priori* indépendante des intérêts politiques, bureaucratiques ou économiques.

Isoler les terroristes

Les terroristes voudraient discuter d'égal à égal avec les États. Cette logique doit être récusée, sur le fond comme dans la forme.

Les terroristes se disent en guerre. Ils se proclament combattants. Tel était déjà le cas des terroristes de l'ultra-gauche des années 1970 (en « guerre contre le grand capital »). Tel est aujourd'hui le cas d'Oussama Ben Laden et des siens, dont l'horizon est la guerre des civilisations. Cette démarche est destinée à valoriser le terrorisme. Nous ne pouvons l'accepter. Nous devons au contraire marginaliser ceux qui se livrent à des actes de terrorisme, en rappelant que ce ne sont pas des guerriers mais des criminels. On ne fait pas la guerre contre des criminels.

(1) La journée du 17 novembre 2005, « Les Français face au terrorisme », organisée dans le cadre de la préparation du Livre blanc, constitue une bonne entrée en matière.

(2) Comme par exemple l'INHES (Institut national des hautes études de sécurité) ou l'IHEDN (Institut des hautes études de défense nationale).

(3) Comme la base de données sur les actes terroristes, mise en ligne pour le public le 22 septembre 2005 par la Fondation pour la recherche stratégique : www.bdt.frstrategie.org

Il est en outre exclu de mener une politique spécifique de communication envers les terroristes. Car une politique de ce type ne pourrait que conforter ces derniers en les présentant comme des interlocuteurs reconnus. Elle ne ferait que renforcer leur attrait auprès de recrues ou de soutiens potentiels.

Lutter contre le terrorisme au niveau mondial

Contre la propagande islamiste radicale et les discours de haine et d'intolérance

Les organisations internationales ont, sur ce point, un rôle essentiel à jouer. Elles ont commencé à adapter les outils permettant de lutter partout dans le monde contre l'incitation à la haine raciale et la provocation au terrorisme.

La résolution 1624 du Conseil de sécurité des Nations unies, adoptée en septembre 2005, fait ainsi obligation à tous les États de se doter d'un dispositif pénal incriminant une telle infraction. La convention du Conseil de l'Europe sur le terrorisme va dans le même sens. Afin de compléter l'action normative dans le domaine de la lutte contre l'intolérance et l'incitation à la haine, une organisation internationale comme l'UNESCO pourrait constituer une enceinte appropriée pour porter la bataille des idées au niveau mondial, en promouvant des programmes d'éducation et de sensibilisation sur le terrorisme.

Un domaine devra recevoir une attention toute particulière sur le plan international : celui de la diffusion des idées racistes, antisémites ou provoquant au terrorisme dans les programmes de télévision diffusés par satellite.

L'affaire *Al-Manar*¹ survenue en 2003-2004 a fait apparaître l'absence de régulation européenne en ce domaine. Faute d'autre moyen de coercition, les États-Unis ont, de leur côté, inscrit *Al-Manar* sur la liste des organisations terroristes. L'approche française, fondée sur une procédure graduée de mise en garde puis d'interruption du programme, pourrait servir de schéma à l'adoption d'une décision-cadre au niveau communautaire.

(1) La diffusion en novembre 2003 par la chaîne libanaise Al-Manar, proche du Hezbollah, d'un feuilleton syrien au caractère antisémite avait conduit les pouvoirs publics français à élaborer une nouvelle législation relative à la liberté audiovisuelle, adoptée le 9 juillet 2004, dont les dispositions ont permis au Conseil d'État, sur recours en référé du CSA, d'ordonner le 13 décembre 2004 au bouquet satellitaire Eutelsat de cesser de diffuser Al-Manar.

Mieux communiquer

Les terroristes islamistes de la mouvance Al Qaïda rejettent tout dialogue et toute communication : « *Le jihad et le fusil, pas de négociation, pas de conférence, pas de dialogue* » écrivait Abdallah Azzam ¹, le mentor d'Oussama Ben Laden. Quand bien même ils accepteraient le dialogue, on ne voit pas bien quel pourrait être l'objet de celui-ci, tant leur projet s'inscrit en dehors de tout espace politique. Les causes mises en avant sont davantage des prétextes que des revendications : Oussama Ben Laden n'a évoqué le sort des Palestiniens que très tardivement. Ses premiers textes prenaient pour cible la présence américaine en Somalie.

À l'inverse, l'emploi d'une terminologie guerrière, qui exclut par définition tout espace de communication, a pour inconvénient de consolider la menace. Elle peut même constituer la meilleure publicité pour le recrutement de nouveaux terroristes. Plus gravement encore, elle accrédite l'idée, erronée et dangereuse, d'une guerre des civilisations entre l'Occident et le monde musulman, que cherche justement à promouvoir le terrorisme mondial d'inspiration islamiste.

En matière de communication internationale, le travail sur l'environnement des terroristes doit donc s'orienter, en priorité, autour de deux axes.

Le premier consiste à reconnaître, et à réaffirmer, que les pays arabes et musulmans sont plutôt en symbiose qu'en conflit avec la civilisation occidentale.

Le second consiste à cibler, en termes de communication, les classes moyennes et les jeunes générations, y compris lorsque celles-ci voient leurs espaces d'expression bridés par leurs dirigeants.

La France dispose d'une longue tradition orientaliste. Celle-ci a pu jadis apparaître surannée ; elle a, au surplus, certainement été marquée par la période coloniale. Mais elle a connu un renouveau indéniable à partir des années 1980. La compétence humaine qui en résulte doit être mise à profit pour valoriser à l'extérieur nos atouts en matière de dialogue, et pour mener une politique ciblée à l'égard des leaders d'opinion musulmans.

La question d'une communication vers le monde musulman dans son ensemble se pose aussi avec une grande acuité. Depuis les attentats du 11 septembre 2001, les États-Unis ont entrepris de bâtir une *public diplomacy* à l'intention du monde arabe ; ils ont à cet effet créé la radio Sawa et la chaîne de télévision al-Hurra.

La France entretient elle-même depuis longtemps une ambition audiovisuelle internationale, avec des médias comme Radio France internationale (RFI), RMC Moyen-Orient ou le projet de Medi I Sat. La future Chaîne française d'information internationale (CFII) doit aussi être présente dans le monde arabe.

(1) Théoricien de l'islamisme radical et coordonnateur de la participation arabe à la guerre d'Afghanistan, décédé en 1989.

Il faut enfin être présent dans les médias arabophones transnationaux (en 2006, les chaînes de télévision al-Jazira, al-Arabiya et Abou-Dhabi TV ou les quotidiens *al-Hayat* et *al-Sharq al-Awsat*). Ceci permettra de mieux nous faire comprendre et d'éviter des malentendus sur le sens de nos politiques.

Privilégier une approche politique

Au-delà de la définition de concepts d'analyse et d'un langage adéquat de communication, l'endiguement du terrorisme mondial nécessite également une approche politique, qui doit poursuivre trois objectifs : réduire et, idéalement, résoudre les crises régionales dont le terrorisme se nourrit de manière rhétorique et opportuniste ; construire ou reconstruire les États les plus fragiles ; contribuer à l'ouverture des sociétés arabes et occidentales les unes envers les autres.

Réduire ou résoudre les crises régionales

Certains conflits du Proche et du Moyen-Orient sont très présents dans la rhétorique des terroristes islamistes.

Leur résolution ne suffirait bien entendu pas à résorber le terrorisme mondial, qui en est fonctionnellement déconnecté. On peut d'ailleurs remarquer qu'Al Qaïda a pris son envol, en tant qu'organisation, dans la deuxième moitié des années 1990, c'est-à-dire au moment où toutes les énergies étaient mobilisées pour faire aboutir le processus de paix israélo-palestinien.

Toutefois, une implication plus active des Américains et des Européens dans le conflit israélo-palestinien, suivie de résultats, priverait le terrorisme mondial de certains arguments symboliques, ce qui contribuerait à assécher certaines de ses sources de recrutement. Le règlement politique du conflit en Tchétchénie, lui aussi présent dans la propagande terroriste islamiste, doit, pour les mêmes raisons, être recherché.

C'est bien l'Irak qui est toutefois devenu aujourd'hui le point d'abcès principal. Il offre aux terroristes l'image d'un pays arabe occupé par des forces occidentales et, en termes opérationnels, une nouvelle « terre de jihad » encore plus prometteuse que n'avaient pu l'être l'Afghanistan ou la Somalie. Les effets de la situation actuelle se feront durablement sentir, même après que l'Irak aura retrouvé la stabilité.

L'Afrique est également confrontée à des conflits déstabilisateurs dont le terrorisme mondial peut tirer profit. Notre engagement dans la résolution de ces conflits n'en revêt que plus d'importance.

Quelle que soit l'évolution des conflits régionaux dans les années à venir, notre objectif doit être de parvenir à dissocier extrémismes locaux et terrorisme mondial.

Le risque d'alliances ponctuelles, à caractère politique ou opérationnel, est difficilement évitable. La véritable menace est celle d'alliances stratégiques qui permettraient au terrorisme mondial de récupérer la

base militante des extrémismes locaux et à ces derniers de bénéficier dans leurs actions du pouvoir mobilisateur de l'idéologie islamiste internationale.

Notre politique sera d'autant plus efficace qu'elle sera différenciée. Toutes les formes de terrorisme doivent être combattues avec la même détermination, mais, dans un souci d'efficacité, selon des modalités adaptées.

Lorsque le recours au terrorisme se greffe avant tout sur un conflit local, en en recyclant les griefs, il est de notre intérêt de tout faire pour résorber ce conflit : d'abord pour le bien des parties concernées ; ensuite pour priver le terrorisme d'un réservoir de recrutement et d'un moteur de mobilisation. En même temps que nous conduirons l'action nécessaire à l'encontre des groupes terroristes, nous chercherons à conduire au dialogue ceux qui, tout en partageant certains objectifs politiques des terroristes, n'adhèrent pas ou renoncent aux méthodes de ces derniers.

Le terrorisme mondial, s'inscrit en dehors de tout espace politique permettant un dialogue : son objectif est notre destruction ; la violence n'est pas un langage mais une fin en elle-même.

Notre politique de prévention de la menace et de répression des actes doit être poursuivie en coopération avec nos partenaires internationaux.

Consolider les États fragiles et reconstruire les États « faillis »

La consolidation d'États fragiles et la reconstruction des États « faillis », dont toute forme d'autorité a disparu, sont cruciales. Elles sont les clefs des sanctuaires où se réfugient les terroristes. L'objectif premier est de remettre en place dans ces États des institutions qui fonctionnent et auxquelles la population accorde sa confiance car elles lui garantiront un niveau correct de sûreté.

La priorité doit donc être donnée au renforcement des capacités dans le secteur de la sécurité, à l'instar de ce qui est entrepris en Afghanistan et dans les pays de la zone sub-saharienne. Elle implique la remise sur pied de forces de police, militaires et douanières efficaces.

La condition du succès de ces opérations de restauration de l'État dans les zones les plus fragiles dépendra, en dernier ressort, de la capacité des forces de sécurité locales à dialoguer avec les populations hostiles au pouvoir central et de l'aptitude de celui-ci à susciter l'adhésion.

Contribuer à l'ouverture réciproque des sociétés de culture musulmane et des sociétés occidentales

L'intégration des radicaux dans le jeu politique n'est pas toujours possible. Cependant, lorsque la perspective est plausible, nous devons la rechercher.

L'Union européenne a lancé, en 1995, le processus euro-méditerranéen dit « processus de Barcelone ». Ce partenariat entre les deux rives de la Méditerranée joue un rôle utile, en contribuant notamment à aider les États de la rive Sud à assumer leurs responsabilités. Car l'attention aux sociétés civiles ne doit pas nous conduire à ignorer des États déjà fragilisés par les nombreux défis auxquels ils doivent faire face. Comme l'illustre l'exemple irakien, la radicalisation des populations est souvent due aux déficiences des États. L'Union européenne engage des sommes importantes dans le pourtour méditerranéen (de l'ordre de 3 milliards d'euros par an), mais notre approche gagnerait à être plus visible et mieux ciblée.

Au sommet de Barcelone, en novembre 2005, les pays du partenariat euro-méditerranéen se sont retrouvés pour la première fois sur une base commune en matière de lutte antiterroriste en adoptant un « code de bonne conduite ». Ils ont été unanimes à juger le terrorisme injustifiable et à proclamer la volonté de mettre en œuvre les conventions *ad hoc* des Nations unies et de conclure au plus vite la négociation sur la convention globale sur le terrorisme, qui les divise jusqu'à présent.

Des efforts restent à faire, notamment sur la définition du terrorisme, qui ne fait toujours pas l'objet d'un accord. La France continuera d'œuvrer avec détermination pour élargir la base de la mobilisation internationale contre le terrorisme partout dans le monde. D'ores et déjà, le fait d'être parvenus à recueillir un accord de tous les États membres des Nations unies pour condamner « *fermement le terrorisme sous toutes ses formes et dans toutes ses manifestations, quels qu'en soient les auteurs, les lieux et les buts, car il constitue une des menaces les plus graves pour la paix et la sécurité internationales* ¹ » représente une avancée importante. Il faut la faire fructifier.

(1) Extrait de la déclaration finale du sommet de l'assemblée générale célébrant le sixième anniversaire de l'organisation.

Conclusion

Le terrorisme fait peser sur nos sociétés deux périls grandissants : il cherche à les fracturer et à leur faire perdre leur âme.

Au premier rang de cette menace, le terrorisme mondial d'inspiration islamiste poursuit sans relâche son projet de division.

À l'échelle du monde, division entre les sociétés occidentales et les sociétés musulmanes. À l'échelle des pays musulmans, division entre les islamistes extrémistes et les pratiquants modérés. À l'échelle de notre pays, division entre les individus de religion musulmane et les autres. Pour fracturer nos sociétés, le terrorisme mondial recourt à une exploitation criminelle de l'islam, en bafouant les préceptes de paix et de tolérance professés par cette religion. Nous répondrons à ce défi moral en combattant toute idée d'amalgame. C'est l'unité et la cohésion de notre pays qui nous préserveront du « choc des civilisations » dans lequel ce terrorisme prétend nous entraîner.

Le terrorisme mondial cherche aussi à frapper le cœur de nos démocraties.

Tout d'abord en les déstabilisant par la perpétration d'attentats destinés à choquer l'opinion publique et à saper la confiance de celle-ci dans la capacité des pouvoirs publics à les défendre efficacement. Mais surtout en les poussant à renoncer aux principes sur lesquels elles reposent.

La liberté qui constitue le socle fondamental de notre démocratie ne peut être synonyme d'imprévoyance ou de faiblesse. Il faut donc prévenir les attentats et punir avec fermeté ceux qui parviennent à les perpétrer ou tentent de le faire. Le défi consiste à garantir l'efficacité des méthodes de lutte antiterroriste tout en ne s'écarter pas du respect de l'État de droit. Dévier de cette ligne ferait en effet le jeu du terrorisme mondial. À l'occasion de la commémoration du premier anniversaire des attentats perpétrés à Madrid en mars 2004, le secrétaire général de l'ONU déclarait que *« porter atteinte aux Droits de l'homme ne saurait contribuer à la lutte contre le terrorisme. Au contraire, cela permet aux terroristes d'atteindre plus facilement leur objectif en donnant l'impression que la*

morale est dans leur camp et [...] en suscitant la haine et la méfiance [...] précisément chez ceux parmi lesquels les terroristes sont le plus susceptibles de trouver de nouvelles recrues ».

En respectant le droit, la lutte antiterroriste gagne en légitimité. Elle gagne donc en efficacité dans une perspective stratégique de long terme.

Notre pays continuera de cheminer sur cette voie étroite. Il maintiendra le juge au cœur de la lutte antiterroriste, avec le souci de ne jamais basculer dans une justice d'exception. Le recours par nos services de renseignement et de sécurité aux méthodes les plus modernes de surveillance continuera à s'exercer dans le respect des libertés publiques, comme le droit d'aller et de venir et le respect de la vie privée. Les mesures les plus contraignantes ne seront adoptées que pour des durées limitées et régulièrement rediscutées devant le Parlement.

Notre pays a fait le choix juridique, philosophique et stratégique de combattre le terrorisme dans le cadre de l'État de droit. Il n'en dévierà pas.

Annexes



Principales actions attribuées au terrorisme mondial depuis 1992

- **29 décembre 1992** : double attentat à Aden (Yémen) contre des soldats américains, attribué à Al Qaïda.
- **26 février 1993** : attentat contre le *World Trade Center*, à New York (États-Unis), attribué à Al Qaïda. 6 morts et plus de 1 000 blessés.
- **19 novembre 1995** : attentat suicide contre l'ambassade d'Égypte à Islamabad (Pakistan), attribué à un groupe proche d'Al Qaïda. 16 morts et 60 blessés.
- **23 février 1998** : création du Front islamique mondial du Jihad contre les Juifs et les Croisés, sous l'égide d'Oussama Ben Laden.
- **7 août 1998** : double attentat suicide simultané contre les ambassades américaines au Kenya et en Tanzanie, revendiqué par l'Armée islamique pour la libération des lieux saints (AILLS). 224 morts.
- **12 octobre 2000** : attentat suicide contre l'*USS Cole* dans le port d'Aden (Yémen), attribué à Al Qaïda. 17 morts.
- **9 septembre 2001** : assassinat du commandant Massoud par deux membres d'Al Qaïda.
- **11 septembre 2001** : quadruple attentat suicide simultané à New York, Washington et en Pennsylvanie (États-Unis), revendiqué – tardivement – par Al Qaïda. 2 985 morts, dont **5 Français**.
- **11 avril 2002** : attentat suicide contre une synagogue à Djerba (Tunisie), revendiqué par l'AILLS. 15 morts, dont **2 Français**.
- **8 mai 2002** : attentat contre des ingénieurs français de DCN à Karachi (Pakistan) attribué à un groupe proche d'Al Qaïda. 14 morts dont **11 Français**.
- **6 octobre 2002** : attentat suicide contre le pétrolier français Limburg au large du Yémen, revendiqué par Al Qaïda. 1 mort.
- **12 octobre 2002** : double attentat suicide contre une discothèque à Bali (Indonésie), revendiqué par la Jemaah Islamiyah, proche d'Al Qaïda. 202 morts, dont **4 Français**.
- **28 novembre 2002** : double attentat à Mombasa (Kenya), contre un hôtel et un avion de ligne, attribué à Al Qaïda. 11 morts.

- **12 mai 2003** : triple attentat suicide simultané à Riyad (Arabie saoudite) contre des complexes résidentiels occidentaux, revendiqué par Al Qaïda dans la Péninsule Arabique. 34 morts.
- **16 mai 2003** : quintuple attentat simultané à Casablanca (Maroc) contre les communautés juive et occidentale, attribué à un groupe inspiré par Al Qaïda. 41 morts, dont **4 Français**.
- **5 août 2003** : attentat contre l'hôtel Marriott à Jakarta (Indonésie), perpétré par la Jemaah Islamiyah. 12 morts.
- **19 août 2003** : attentat contre le bâtiment des Nations unies à Bagdad. 23 morts, dont le représentant spécial du secrétaire général et **1 Français**. Début de l'intervention jihadiste en Irak.
- 11 septembre 2003** : le Groupe salafiste pour la prédication et le combat (GSPC) prête allégeance à Al Qaïda.
- **8 novembre 2003** : attentat à Riyad (Arabie Saoudite) contre le complexe résidentiel de Mouhaya. 18 morts.
- **15 et 20 novembre 2003** : attentats à Istanbul (Turquie), respectivement contre la communauté juive (23 morts) et les intérêts britanniques (27 morts), attribués à Al Qaïda.
- **11 mars 2004** : quatre vagues d'attentats simultanés (10) à Madrid (Espagne), attribuées à un groupe inspiré par Al Qaïda. 191 morts, dont **1 Français**.
- **9 septembre 2004** : attentat contre l'ambassade d'Australie à Jakarta (Indonésie), réalisé par la Jemaah Islamiyah. 9 morts.
- **7 octobre 2004** : triple attentat suicide à Taba (Égypte), attribué à un groupe proche d'Al Qaïda. 34 morts.
- **7 avril 2005** : attentat suicide au Caire (Égypte) attribué à un groupe inspiré par Al Qaïda. 4 morts, dont **2 Français**.
- **7 juillet 2005** : quadruple attentat suicide à Londres (Royaume-Uni), revendiqué par Al Qaïda. 56 morts, dont **1 Français**.
- **23 juillet 2005** : triple attentat suicide à Sharm el Sheikh (Égypte). 62 morts.
- **9 novembre 2005** : triple attentat suicide à Amman (Jordanie). 57 morts.

Les principales menaces contre la France depuis 1998

- **5 mars 1998** : démantèlement à Bruxelles (Belgique) d'une cellule terroriste islamiste soupçonnée de préparer des attentats en France (cellule Melouk).
- **18 mai 1998** : déclarations d'Oussama Ben Laden dans le quotidien pakistanais *Aousaf* menaçant vingt-trois installations militaires occidentales dans la région du golfe arabo-persique dont la base française de Djibouti.
- **26 mai 1998** : série d'arrestations en France, en Italie, en Allemagne, en Belgique et en Suisse de terroristes maghrébins préparant des attentats contre la coupe du monde de football.
- **11 et 25 juin 1999** : diffusion de deux communiqués menaçant la France et la Belgique attribués à une cellule de terroristes algériens issus du GIA.
- **25 et 26 décembre 2000** : arrestation à Francfort (Allemagne) de terroristes maghrébins planifiant une attaque vraisemblablement contre la cathédrale et/ou le marché de Noël de Strasbourg.
- **20 septembre 2001** : démantèlement en France, en Belgique et au Royaume-Uni d'une cellule d'Al Qaïda préparant un attentat suicide contre l'ambassade des États-Unis à Paris, prévu en juillet 2002 (réseau Beghal).
- **5 octobre 2001** : démantèlement à Saint-Denis d'une cellule islamiste algérienne soupçonnée de préparer un attentat à l'occasion du match de football France-Algérie du 6 octobre 2001.
- **17 octobre 2001** : lettre de menaces contre la France du Groupe des gardiens de la prédication salafiste, dissidence du GIA.
- **22 décembre 2001** : tentative d'attentat, attribuée à Al Qaïda, contre un vol d'Air France entre Paris et Miami.
- **12 novembre 2002** : communiqué d'Oussama Ben Laden justifiant les attentats commis depuis le 11 septembre 2001, dont celui du 8 mai 2002 à Karachi contre les ingénieurs français.
- **16 décembre 2002** : démantèlement d'une cellule à La Courneuve soupçonnée de préparer une attaque non conventionnelle (produits toxiques) contre l'ambassade de Russie à Paris.

- **24 décembre 2002** : poursuite de cette opération à Romainville.
- **16 février 2003** : intervention d'Oussama Ben Laden dénonçant la politique occidentale, dont les accords Sykes-Picot.
- **2 juin 2003** : arrestation, à Roissy, du ressortissant marocain, Karim Mehdi, jihadiste lié à la cellule de Hambourg, qui projetait de se rendre à la Réunion pour y préparer une action terroriste contre des sites touristiques.
- **16 septembre 2003** : arrestation à Sanaa (Yémen) du responsable d'une cellule, liée à l'organisation Al Qaïda dans la Péninsule Arabique, planifiant des attentats, notamment contre le Centre culturel français et l'ambassade des États-Unis.
- **24 février 2004** : communiqué d'Ayman Al Zawahiri, adjoint d'Oussama Ben Laden, dénonçant la loi française sur la laïcité.
- **14 octobre 2004** : courrier d'Abdelmalek Droukhal, émir du GSPC, à Abou Moussab Al Zarqawi dénonçant la France en raison de ses relations avec le gouvernement algérien.
- **18 mai 2005** : communiqué d'Abou Moussab Al Zarqawi dénonçant la loi française sur la laïcité.
- **Juin 2005** : menaces contre l'ambassadeur de France à Bagdad.
- **Juillet 2005** : menaces proférées contre la France par l'hebdomadaire pakistanais *Dharb Al Moumin* (édition du 8 au 14 juillet).
- **Septembre 2005** : communiqué sans date précise (mis en ligne le 14 septembre) du GSPC menaçant la France, qualifiée d'« ennemi n° 1 ».
- **26 septembre 2005** : opération de police menée en France contre une cellule d'anciens membres du GIA soupçonnés de préparer des attentats contre le siège de la DST, l'aéroport d'Orly et le métro parisien.
- **6 janvier 2006** : communiqué d'Al Zawahiri critiquant la France pour sa politique en Algérie.
- **4 mars 2006** : intervention d'Al Zawahiri appelant au boycott économique de plusieurs pays européens, dont la France, et stigmatisant à nouveau la loi française sur la laïcité.

Les travaux et les groupes de travail

Les travaux du Livre blanc ont été lancés en mai 2005 par Jean-Pierre Raffarin, Premier ministre, sur proposition de Dominique de Villepin, alors ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales. Un comité de pilotage du Livre blanc a été constitué sous la présidence de Nicolas Sarkozy, ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire.

Six groupes de travail ont été mis en place. Ils étaient présidés par le directeur général de la sécurité extérieure, le directeur de la surveillance du territoire, l'ambassadeur délégué pour le sommet mondial de la société de l'information, le directeur des affaires criminelles et des grâces du ministère de la Justice, le directeur général des affaires politiques et de sécurité du ministère des Affaires étrangères et le conseiller spécial du directeur de la fondation pour la recherche stratégique.

Le secrétaire général de la défense nationale était le rapporteur général du Livre blanc. Il était assisté par quatre hauts fonctionnaires issus du Conseil d'État, du ministère de l'Intérieur, du ministère de la Défense et du ministère des Affaires étrangères.

Dans le cadre de la préparation du Livre blanc, une journée de réflexion ouverte au public, intitulée « Les Français face au terrorisme », a eu lieu le 17 novembre 2005 sous la présidence du Premier ministre.



Table des matières

Avant-propos	5
Introduction	7
Première partie	
Le terrorisme mondial : une menace stratégique	13
Chapitre 1	
Un discours efficace, une volonté de maîtrise de l'espace, des structures évolutives	15
Une vision du monde simpliste et complexe à la fois	15
Une vision du monde qui permet de délivrer un message simple et puissant	15
Une stratégie plus complexe qu'il n'y paraît	17
Le discours tactique du proche et du lointain	17
Une volonté de maîtrise de l'espace	18
Les sanctuaires	19
Les terres de combat	19
Les zones de transit et de soutien, à mi-chemin entre sanctuaires et terres de combat	20
Les zones d'opérations où le terrorisme mondial d'inspiration islamiste est à l'œuvre	20
Des structures difficilement saisissables	20
Le premier niveau : l'organisation Al Qaïda	22
Le deuxième niveau : les entités terroristes qui disposent d'un enracinement territorial	22
Le dernier niveau de la mouvance : les individus, regroupés ou non en cellules	22
Chapitre 2	
Le terrorisme mondial renouvelle ses recrues, adapte ses méthodes et signe son mode opératoire	25
Des terroristes plus difficiles à repérer	25
Une minorité aux profils variés	25
La succession de trois générations	26
Une procédure de ralliement bien rodée	27
Une troisième vague plus problématique que les précédentes	28
Une gestion efficace des flux d'information, de financement et de déplacements	29
L'usage par les terroristes des moyens de communication	29
Les flux de financement du terrorisme	30
Les déplacements de personnes	31

Des modes opératoires classiques
et pourtant reconnaissables entre tous **31**

Chapitre 3

**Des perspectives préoccupantes
pour la France** **33**

La France est un objectif particulier au sein de l'Europe,
cible du terrorisme **33**

Le terrorisme mondial d'inspiration islamiste n'épargne pas la France **33**

L'Europe, cible du terrorisme **35**

Les facteurs d'une menace aggravée pour la France
et pour l'Europe **35**

Deuxième partie

**Le dispositif français de lutte contre
le terrorisme doit continuer à s'adapter** **39**

Chapitre 1

**Prévenir le risque : surveiller, détecter,
neutraliser** **45**

Renforcer les capacités des services de renseignement
et de sécurité **46**

Renforcer les capacités de repérage **46**

Assurer la coordination des services de renseignement
et de sécurité en matière de lutte contre le terrorisme **49**

Coopérer avec nos partenaires étrangers **52**

Conforter notre dispositif pénal et adapter notre système
pénitentiaire à la menace terroriste **53**

Conforter un dispositif pénal efficace **53**

Un traitement carcéral à adapter **55**

Neutraliser les flux dangereux de personnes, de biens,
de capitaux et d'idées **56**

Contrôler les flux de personnes dangereuses **56**

Tarir les flux de capitaux qui contribuent au financement du terrorisme **58**

Neutraliser les flux d'idées porteuses de haine, de violence
ou appelant au terrorisme **60**

Protéger le territoire des intrusions et neutraliser
les terroristes à l'étranger par l'action des armées **61**

Les forces armées protègent et contrôlent en profondeur les espaces
nationaux et ceux où la France a des intérêts **61**

Les forces armées contribuent à la prévention contre le terrorisme
en engageant leurs moyens à l'extérieur du territoire national **62**

Renforcer la coopération internationale **63**

Prévenir la menace **63**

Prévenir l'apparition d'un terrorisme pouvant avoir recours
aux armes de destruction massive **67**

Chapitre 2	
Améliorer nos dispositifs	69
Protéger la population	69
Consolider la planification de vigilance	69
L'apport de la vidéosurveillance	71
Assurer la protection des réseaux de transport	71
Protéger les Français de l'étranger	75
Protéger l'intégrité du pays	76
Préserver les infrastructures vitales	76
Protéger les systèmes informatiques sensibles	77
Chapitre 3	
Renforcer nos capacités de gestion de crise	79
Parfaire nos capacités opérationnelles	79
Les plans d'intervention « PIRATE » et le plan ORSEC récemment rénové sont des outils complets de gestion d'une crise d'origine terroriste. Leur combinaison doit encore être améliorée	79
Notre organisation et nos moyens de gestion de crise doivent encore être renforcés	80
Pour faire face aux situations de crise, la palette d'outils juridiques est large mais incomplètement adaptée	85
La mise en place d'une doctrine de communication publique	86
Le coût élevé d'une mauvaise communication	86
Forces et faiblesses du dispositif actuel	86
Les principes d'une doctrine de communication de crise adaptée face au terrorisme : fédérer et orchestrer	87
Chapitre 4	
Renforcer nos capacités de réparation et de sanction	91
Réparer les dommages infligés aux victimes	91
Indemniser	91
Réparer par le procès pénal	92
Poursuivre les suspects : l'approfondissement de la coopération judiciaire internationale	93
Le pas décisif franchi avec l'adoption du mandat d'arrêt européen	93
Le développement d'équipes communes d'enquête pour contrer le terrorisme international	94
Sanctionner les coupables	94
Adapter au plus juste la sanction pénale	94
N'exclure aucune riposte	95

Troisième partie

Mener une action de fond contre le terrorisme en gagnant les batailles du quotidien, de la technologie et des idées

97

Chapitre 1

Gagner la bataille du quotidien : favoriser la détection précoce des activités terroristes par la vigilance et le renseignement humain

99

Les agents des services publics :
une vigilance essentielle

100

Le rôle des forces de sécurité intérieure non spécialisées

100

La vigilance des agents du secteur public

101

La responsabilité des acteurs sociaux
et le rôle du citoyen

102

La connaissance par le public du dispositif national
de lutte antiterroriste

102

Le développement d'une politique d'exercices

103

Le maintien de la vigilance de tous

105

Le rôle de l'école

106

Chapitre 2

Gagner la bataille technologique

109

L'objectif : toujours précéder la progression
de la menace

109

Les principes

109

L'orientation de l'effort de recherche et de développement

110

La méthode : une collaboration entre l'État
et les entreprises, qui privilégie la dimension européenne

113

Encourager un processus d'élaboration de normes antiterroristes

113

Dialoguer avec les entreprises et soutenir leurs efforts

114

Appuyer, soutenir et développer le programme européen
de recherche et de sécurité

114

Chapitre 3

Gagner la bataille des idées

117

En France, conforter l'adhésion de la population
et isoler les terroristes

117

Le principe : ne jamais céder sur les valeurs fondamentales
de l'État de droit

117

Refuser l'amalgame

118

La forme du message : la politique de communication publique
doit rechercher le consensus le plus large en isolant les terroristes

119

Lutter contre le terrorisme au niveau mondial

122

Contrer la propagande islamiste radicale et les discours de haine
et d'intolérance

122

Mieux communiquer

123

Privilégier une approche politique

124

Conclusion	127
Annexes	129
Annexe 1	
Principales actions attribuées au terrorisme mondial depuis 1992	131
Annexe 2	
Les principales menaces contre la France depuis 1998	133
Les travaux et les groupes de travail	135