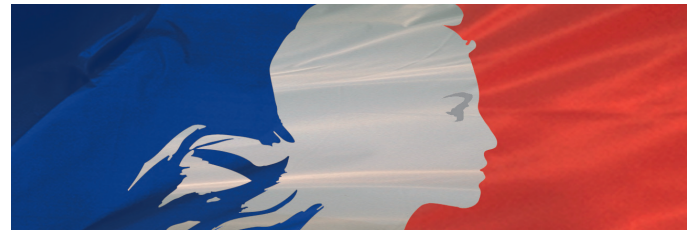
LA FRANCE FACE AU TERRORISME



Livre blanc du Gouvernement
sur la sécurité intérieure
face au terrorisme

La **documentation** Française

Sommaire

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

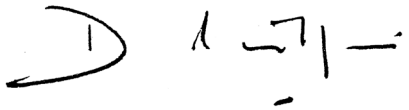
des attentats et aux poseurs de bombes. Seule une connaissance approfondie des réseaux, des relais et des outils de ces groupes peut nous permettre de protéger nos concitoyens.

• 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 Assassins [1], 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 an [1]. 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. Décriée 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 combattrons efficacement le terrorisme qu'avec l'adhésion de l'ensemble de nos concitoyens. Nous ne le combattrons 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 initial [1] 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'Afghanistan [1], 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 entrerait 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 Gogh [1] 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.

Chapitre 2

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 accréditent 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'accommodent, 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 incommensurables 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 anonymes [2].

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.

Chapitre 3

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'école [1], 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 Taliban [2], 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 DCN [3], 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 parisienne [4], 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 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 VIGIPIRATE [1] 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 fomente 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 forums [2] 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 réservation [1] et les fichiers de contrôle des départs [2]. 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 renseignement [3] » 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 priorités [1]. 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 sécurité [3].

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 72ème 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 soumise [1] 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 droit [2].

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 TRACFIN [1] 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 cultuelles 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 préfigurait 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 liste [1], 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 iranienne), 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 montant [2]. 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 délictuels 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 violent [1].

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 militaires [3] : 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 règlerait 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'exécuterait 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 « extrader 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.

Chapitre 2

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 antiterroriste 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 dérouté. 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 antiterroristes 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 1er 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 scellements 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 opérateur [1] 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.

Chapitre 3

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 nº 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 alertes [1]. 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 logiciels 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 1er février 2006 spécialement dédié à l'hélitransport 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 perpétrées 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 public [1]. 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 1878 [2], 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 gravité [3]. 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 sujets [1]. 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 entraient 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 européenne [1]. 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'expérience [1] 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 régalien, 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 6e PCRD, en cours de réalisation en 2006. Le 7e 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 crise [1]. 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 frappé [1]. 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'État [1] 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 défense [2] 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.frstratégie.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

Contrer 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 soixantième 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'écartant 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 déviera pas.

Annexes

Annexe 1

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.

Annexe 2

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 Droukdal, 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

Summary

Preface

With this White Paper on Domestic Security against Terrorism, our country has for the first time developed a genuine doctrine for dealing with a scourge it has had to face many times in its history.

We have, of course, constantly been adapting our efforts to protect our territory and our citizens. Our security and intelligence forces are now trained to anticipate and fight the terrorist threat. Why, then, did we want to go further and formulate a comprehensive security strategy?

• The first reason is that the threat to our country has never been so great: since the Madrid and London attacks we know that Europe is clearly a target. France is thus not sheltered from such attacks. To ensure the security of French citizens, it has become necessary to understand this threat better.

• Another reason is that this is a strategic threat, which targets our interests all over the world. This was demonstrated by the attacks in Karachi, which claimed 11 French lives in May 2002.

• Finally, we need a comprehensive strategy because the terrorist threat has been constantly changing. This means that we must constantly adapt our tools and our system if we want to stay a step ahead of the terrorist groups. We began doing this with the creation of regional centres for the fight against radical Islamism and with the adoption of the 23 January 2006 counter-terrorism law. But we need an adaptation strategy for the long term, similar to the one developed in the 1994 French White Paper on Defence.

The goal of this endeavour is threefold.

• We must first better understand the workings of terrorist groups. We know that they take advantage of well-developed operational networks in European countries. These networks cover a spectrum running all the way from extremist preachers and organizations that send young people to terrorist training camps and battlegrounds to the organizers of attacks and the people who plant the bombs. Only a thorough knowledge

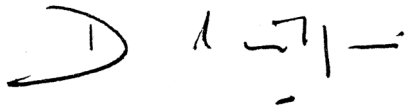
of the networks, the facilitators, and the tools of these groups will allow us to protect our fellow citizens.

• The second objective of this White Paper is to define a counter-terrorist strategy tailored to the threat we face. This strategy must take into account the new technological tools and modern means of communication used by the terrorist groups. It will also develop active international cooperation. This is indispensable to deal with groups that are connected by constantly changing affiliations and to understand the financial networks that they use. We have already developed effective bilateral partnerships. Now we must develop multilateral cooperation.

• Finally, the goal of this White Paper is to better inform our fellow citizens about a threat that concerns them and about the tools we are putting into place to protect them. Faced with a threat that seeks to divide our societies, our fight must be everybody's fight. It must build on a shared conviction about the seriousness of the threat and the importance of the rules that must govern counter-terrorism.

In the fight against terrorism, our democratic principles are our best weapon. Our strength lies in our tolerance, our respect for civil liberties, and our respect for the identities that our country has always defended. To renounce these values would be to play into the terrorists' hands. To give in to the temptation to change our standards would be to begin to lose the fight. So let us remain faithful to our values: they are our greatest strength in our fight against terrorism.

Dominique de Villepin
Prime Minister



Introduction

To fight terrorism effectively, we must be able to name it and define it:

'any action that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a Government or an international organization to do or to abstain from doing any act.'[1]

This is the definition of terrorism the United Nations Secretary General proposed at the General Assembly Summit celebrating the UN's 60th anniversary in September 2005. Although there is not an international consensus behind this definition yet, France accepted it from the start. It describes a form of violence that our country has known for more than two centuries.

Past, Present and Future Threats

As an active player in international affairs, France has been the target of numerous attacks for the entire second half of the 20th century. We have been victims of terrorism linked to domestic policy issues, including attacks committed in the context of the Algerian War, and terrorism fostered by ideological or regionalist demands.

But we have also been hit by a form of terrorist violence linked to external crises, first when Palestinian terrorist groups started attacking the interests of their adversaries wherever they were, erasing geographical limits. In France, but also in Italy (the Rome airport attack), in Austria (the attack on the headquarters of the Organization of Petroleum Exporting Countries,

(1) *In Larger Freedom: Towards Security, Development and Human Rights for All*, Report of the Secretary General of the United Nations for Decision by Heads of State and Government in September 2005 (New York: March 2005).

OPEC), in Uganda (hostage-taking at Entebbe) and elsewhere, we began to witness the first 'globalization' of a cause through terrorist action.

Step by step, other movements started to adopt this type of action. The Armenian Secret Army for the Liberation of Armenia (ASALA), founded in 1975 in Beirut, is an example of this. Until it was disbanded in 1984, it committed more than 35 attacks in France, demonstrating that one did not need to be the main enemy of a movement to become one of its victims.

During the 1960s and 1970s, violent extreme leftist and autonomous movements also propagated terror. A handful of these, such as Direct Action, continued to carry out attacks through the 1980s before their ability to do damage was gradually eroded.

The most recent major attacks on French territory go back to 1995 and 1996: the attacks in Metro and express subway in Paris at the Saint-Michel, Maison-Blanche and Port-Royal stations. Although linked to the Algerian civil war, these attacks in a way foreshadowed Islamist terrorism. They were the work of terrorists supported by cells that had been pre-positioned in France and which went from providing logistical support to armed groups in Algeria to taking direct action against a Western state. This issue, new at the time, prefigured the threats that France faces today.

France has not been spared from regionally inspired terrorism. Corsican, Basque and Breton independence movements resort to violence. This type of terrorism is not unique to France. In Spain and the United Kingdom, ETA and the IRA have for more than three decades fought intensely against the government in the name of Basque independence and Irish unity. Regionalist terrorism has not disappeared. In the recent past it went so far as to include the assassination of a representative of the French Republic. Governments must continue to pay close attention to it over the long-term.

But the terrorism with which we are confronted today is the lineage of the September 11, 2001 terrorist attacks in the United States, which cost nearly 3,000 lives. This is the threat we must be prepared for in order to protect our fellow citizens.

An Increasingly Lethal Issue

Terrorist movements' capacity for doing harm depends in part on the means of destruction to which they can gain access. The daggers of the 'Assassins'[1] and the guns and firebombs of anarchists in the late 19th century made possible only targeted murders or killings of at most a few dozen victims.

(1) The Assassins were a ruthless Ismailian religious group in Persia, then Syria, from the end of the 10th to the 13th century and which attacked leadership elites.

In the second half of the 20th century, much more extensive massacres and hostage-taking became possible through access to modern means of transport – which became terrorists' targets and tools at the same time – as well as through the availability of powerful explosives on the open market. On 19 April 1995, two isolated individuals in Oklahoma City in the United States carried out an attack that killed 168 people and wounded 600 others.

The capacity to manufacture chemical agents such as powerful nerve agents, as well as the acquisition of biological expertise and technologies, are henceforth within reach of various groups and individuals. This was confirmed by the Sarin gas attacks carried out by the *Aum Shinrikyo* sect in the Tokyo subway in March 1995, and by the distribution of envelopes containing anthrax in autumn 2001 in the United States. These attacks, which only caused a few deaths, revealed how difficult it was to carry out mass attacks with these techniques.

Over the past 25 years, the number of victims caused by terrorist attacks has crossed several thresholds. Before 1983, the bloodiest terrorist attack had killed 85 people (an attack in the Bologna railway station in Italy, in 1980). The threshold of 100 victims was crossed for the first time in 1983, with the double attack in Beirut, Lebanon, against American and French military forces (299 deaths). Until 2001, the deadliest attack had killed 329 people (the destruction of an Air India plane over the Irish Sea in 1985). The threshold of 1,000 victims was crossed with the al Qaeda attack in the United States on 11 September 2001.

Whereas the numbers have fallen since September 2001, the accounting measure for the deadliest attacks has gone from tens to hundreds to thousands of victims in a generation.

The examination of the past and of ‘traditional’ threats against France enables us to determine the evolving characteristics of the type of terrorism that might pose a lasting threat to France. It is distinguished by violent acts prepared in secret. It is carried out by non-state actors, which makes it less predictable. Its perpetrators are ideologically motivated individuals, committed to an international cause whose rhetoric is rooted in history. One of its goals is to kill as many French people – or foreigners on French soil – as possible, even if its analytical framework, as a matter of principle, does not stop at French borders or at civilian victims. In its logic all attacks are fair game. It seeks the maximum psychological effect on governments and public opinion.

The potential increase in the level of destruction sought by the terrorists is the primary justification for a re-examination of France's counter-terrorism system.

The Emergence of 'Global Terrorism'

The second factor that calls for this White Paper is the appearance, at the start of the 21st century, of a new type of terrorism.

Since the second half of the 1990s, globalization has brought about an unprecedented transformation of all societies. Global public opinion now has access to the same images, often in real time. Distances have been abolished and the repercussions of various regional crises are increasingly powerful. The countries of the Near and Middle East are particularly affected by this instability. The legacy of history, political stagnation in a number of countries, and the consequences of possessing oil resources have left the region in a fragile situation. The disarray of populations facing considerable social and economic difficulties has made them a prime recruiting ground for terrorist groups who take advantage of their feeling of injustice by turning it against the West, which they blame for the region's fate. They have also instrumentalised the message of Islam by imposing an unbending and violent reading of the Muslim religion.

Terrorism has thus undergone a change in nature and degree similar to the changes provoked by globalization. This transformation has led to the emergence of a global Islamist-inspired terrorism, which indiscriminately attacks Western, Arab, or more generally Muslim countries, with unprecedented means of destruction.

This new type of terrorism – embodied by al Qaeda – has had global ambitions from the very start. Since 1998, it has struck in some 20 countries, at an average rate of three or four major attacks per year.[1] It has shown a capacity for action in Europe twice, in Madrid in March 2004 and in London in July 2005. It is distinguished by its ability to borrow from globalization the very tools that have enabled globalization to succeed. It manages to combine very personal individual concerns with lofty international perspectives; it shows a preference for people-to-people networks; it uses electronic means; it places a premium on publicity; and it shows a capacity for permanent evolution, even advance planning. Globalization is thus denigrated out of principle – yet at the same time its most effective elements are accepted, integrated, and exploited operationally.

We have entered the era of what we shall call 'global terrorism.' This terrorism differs from regionalist terrorism or state-sponsored terrorism. It cannot escape the general rule that all terrorist movements only manage to mobilize a small number of activists. Yet global terrorism alone claims to carry a historical legacy and to stand on a geopolitical base. It seeks to flaunt its ambitions, innovate, and develop the means to attain results that would elevate it immediately to the level of a global and generational adversary. It wants to be capable of inflicting far greater

(1) These figures exclude attacks carried out in war zones.

damage and exercising far greater influence over our societies than the rather more limited objectives of other forms of terrorism.

Anchored in a still young generation, the global terrorist threat will likely prove longlasting. It has acquired a strategic dimension. France is one of its targets. Many French nationals have been among its victims abroad.

We must analyse this threat in order to measure it well, determine how to adapt our counter-terrorism system to counter it, and establish a long-term strategy to limit it. We must avoid the trap of a 'clash of civilizations' that has been set by global Islamist-inspired terrorism and we must refuse the conflation of Islam and terrorism that this movement seeks to provoke.

It is this refusal to conflate Islam and terrorism that France is demonstrating when it encourages the organization of Islam in France, namely through the French Council of the Muslim Faith; when it consistently presses at the global level for a better dialogue among peoples, especially toward our neighbours from the South and in the Muslim world; and when it fights against all forms of hate speech. This policy is all the more well-received because most French Muslims demonstrate respect for the Republican values of tolerance and secularism and condemn the manipulation of Islam's message by extremist factions.

The goal of this White Paper is to formulate France's counter-terrorism doctrine. This doctrine should be known to all, for we will only succeed in fighting terrorism effectively if we have the backing of all our citizens. Only by developing international cooperation will we be able to fight it effectively.

Part I

Global Terrorism: A Strategic Threat

Part of the reason for the strength of global terrorism is the effectiveness of its rhetoric. Its originality lies in its functionally differentiated use of various territories. It adapts its structures and procedures, renews its recruits and knows how to make good use of the means of communication that globalization provides. Today embodied by Islamist terrorism, it is a strategic threat to France.

Chapter 1

Effective Rhetoric, a Strategy for Managing Territory, Evolving Structures

A Simplistic – Yet Complex – World View

The apparent – and well-displayed – simplicity of the world view proposed by global Islamist-inspired terrorism provides a common reference for a movement that at first glance seems to be rather disparate.

A global vision with a simple and powerful message

Global terrorism draws its ideological inspiration from Salafism.[1] Based on the rejection of political and social progress, this school of thought is by nature hostile to democracy. Its point of reference is the memory – partly based on fantasy – of a 'golden age' of original

(1) From the 'Salafs,' or 'ancient ones,' the earliest companions of the Prophet Mohammad.

Islam. It rejects the world as it has evolved. It offers itself as an alternative to globalization. It proposes a return to the practices of the original caliphate based on a narrow interpretation of the Koran.[1]

Yet this desire to go back to basics hides a movement that actually advocates an Islamic 'renaissance.' In this sense, Salafism can also be seen as the vehicle for a negative interpretation of a painfully and unjustly endured history. It is the history of the decline of a civilization 'humiliated' by successive physical, economic and cultural invasions by the 'Christian West,' from the time of the Crusades until today.

In this view, as a victim of 'aggression' – its very survival threatened on its own territory – Islam has no choice but to defend itself with the most extreme violence. For global Islamist-inspired terrorism, this 'clash of civilizations' has entered a critical phase of the 'jihad,' thus hijacking this central element of the Muslim religion. This is the powerfully simple message that it puts forth relentlessly.

Jihad and Jihadism

In Europe we tend to translate jihad as 'holy war.' Etymologically, jihad means 'determined effort to reach a goal' – in other words, on one hand, that of defending or promoting Islam and, on the other, what a Believer does to conform to the rules of the Koran. This reference can be found in various parts of the Koran, under different forms: spread Islam through persuasion, fight to repel an attack on Islam, etc. Considering Islam to be a universal value, all of the different movements within Islam accept that its propagation is a duty for the Muslim community.

Just as we make a distinction between 'Islam' and its political exploitation ('Islamism'), it is necessary to distinguish the religious notion of jihad from 'jihadism,' which is its deviation into violence. For the past few years, jihad has often been assimilated – wrongly – with terrorism. This lumping together of two different things only helped the terrorists themselves.

After Afghanistan in the late 1980s, jihadism reached its peak in Algeria in the 1990s, when the Armed Islamic Group (GIA) began to go after Europeans – in Europe or in Algeria – as well as Muslims judged to have been excessively influenced by Western culture.

(1) The word 'caliphate' refers to the authority of the caliph, the successor to the Prophet Mohammad, over the entire Muslim community as well as over the territories under its control.

A strategy more complex than it seems

The most immediate goal of the exponents of global Islamist-inspired terrorism is to 'cure' the Muslim people of what they consider as an inferiority complex that they see as a product of colonialism. To do that they seek to undermine the belief of the 'oppressed' in the supremacy of the 'oppressors' by revealing the latter's vulnerabilities. This was the goal of the 11 September 2001 attacks in New York and Washington.

Once this symbolic power relationship is disrupted, the next goal is to seriously and enduringly impede the functioning of Western societies, by making their energy sources (such as oil and gas) vulnerable and threatening their modes of transport, both domestic and international.

The following stage is to provoke a split, including through physical separation, between the West and Muslims by driving Westerners (including permanent residents, military troops or tourists) out of Muslim lands and by attacking 'intermingling' areas such as tourist sites, and public transport networks in big cities.

To complete the separation, the Islamists terrorists seek the exhaustion of Western governments and public opinion.

Global Islamist-inspired terrorism also manages to recycle non-religious causes whose flames have died out due to lack of support. To the extent possible, it seeks to occupy the political space created by the collapse of communist revolutionary or Third-Worldist ideologies. It occupies the anti-imperialist space that no one else fills any longer. By doing so it seeks to place itself in the continuity of anti-colonial wars. In the rejectionist movement against the West and the fight against the great economic powers, we cannot exclude that it will one day seek a rapprochement with the most radical of the anti-globalization movements.

Rhetoric about 'the near enemy' and 'the far enemy'

The launch of the second Iraq war in 2003 allowed Islamist terrorism to reposition itself in the tradition of nationalist struggles and the defence of identity, and to recreate the combination that worked so well against the Soviet occupation of Afghanistan.

The military intervention in Iraq led to a threefold convergence that consolidated the terrorists' position: an ideological convergence between transnational 'jihadism' and Arab nationalism; an operational convergence between the terrorists and the Ba'athist security services; and finally a geographical convergence that allowed al Qaeda – which until then had always fought in the margins of the Arab world like Afghanistan, Bosnia, Chechnya and East-Africa – to take a position in its heart.

The terrorists' message is boosted by this new set of factors, allowing them to return to the tactic of painting a picture of 'near' and 'far' enemies. The near enemies are the local 'apostate' regimes they accuse of having abandoned their religious identity; the far ones are their

Western ‘protectors.’ Taking advantage of this new situation, the terrorist movement can even pretend to take a pragmatic approach, such as when Osama bin Laden twice proposed a truce with the Europeans, in April 2004 and in 2006.

The terrorist movement achieves three main benefits from the wide scope of its rhetoric:

The first is an attractiveness that goes beyond the hard core of its original audience and allows it to seduce Western converts. This issue remains marginal. But it has enormous symbolic power. It shows the capacity to overcome ethnic and cultural barriers in the name of universal brotherhood.

The second benefit is to conceal the movement's internal differences. These differences, however, are very real. They have to do with how to characterize the enemy, in particular the possible existence of a tactical hierarchy among Western countries. Such a hierarchy would lead the terrorists to attack first the members of the 2003 coalition of countries that supported the second Iraq war, on the basis of the importance henceforth attributed to this natural battleground.

The third benefit is to reconcile political and ideological terrorism. This is most ‘promising’ in the long-term, since it makes it possible to combine the mobilization powers of each of these distinct forms of terrorism. Political terrorism is utilitarian. It sets concrete, limited, and asserted goals. It uses violence as a tactical lever. Ideological terrorism, on the other hand, expresses an existential rejection of the world. It refuses any possibility of dialogue or deterrence. Its only end is itself. Its power to harm is therefore, in principle, unlimited.

A Strategy for Managing Territory

The al Qaeda movement's rhetoric is inclusive. It also displays a strategy for differentiated use of territory. The territories in which it now operates can be divided into several different zones, whose purposes are precisely defined but whose borders are constantly evolving. These are sanctuaries, battlegrounds, transit zones, and operational areas.

Sanctuaries

Terrorism needs ‘sanctuaries’ for shelter, as possible training grounds, and sometimes to help organize the trafficking that provides financial support. After being forced to leave their open-air sanctuary in Afghanistan in 2001, the al Qaeda terrorists went looking for alternatives.[1]

(1) Prior to Afghanistan, al Qaeda's sanctuary was in Sudan, which Osama bin Laden left in 1996.

In the absence of states willing to welcome them, they went to places where state authority no longer existed. Thus they took up residence in the desert or mountain zones that are scattered all around the arc of crisis that runs from the Maghreb to Southeast Asia, and which are devoid of state authority or monitoring. These areas include the tribal zones on the Pakistan-Afghanistan border, the borders of Kashmir and the borders of Iran. That is where the remnants of the original al Qaeda remain. Farther away, these areas include some refugee camps in Lebanon, the tribal regions of Yemen as well as Somalia. Still farther is the Sahel region in Africa, which has become a supply and shelter zone for some small groups, and at the other extreme some remote islands on the Philippine or Indonesian archipelagoes which play the same role.

These hideouts offer effective protection. All indications suggest that the hunt for new sanctuaries continues.

Battlegrounds

The second type of zone consists of the 'lands of jihad,' direct battlegrounds against the enemy, where terrorists gain legitimacy and experience and develop relationships.

During the first part of the 1990s, Bosnia was one of these combat zones. To various degrees, Afghanistan, Chechnya and the North Caucasus remain in this category. But now it is Iraq that has become the centre of gravity of these 'lands of jihad.' By creating a focal point for all the grievances of the Arab and Muslim worlds, the 2003 military intervention in Iraq led to increased radicalization by validating the most simplistic rhetoric of Islamist terrorism. This movement was able to portray the intervention as an attempt to use military power to impose democratic values and as an example of alleged collusion between Shiites and 'Crusaders.'

The dynamic at work in Iraq today thus contributes to the consolidation and spreading of terrorism. Thousands of volunteers from across the Arab world, as well as a smaller number from the European continent, are flocking to Iraq. After gaining valuable experience there, these volunteers find their calling in returning to their homelands. Because of the lack of adjacent sanctuaries, this issue has not yet reached the proportion it once did in Afghanistan. But it takes full advantage of globalization to amplify its message.

Transit and Support Zones, Half-Way between Sanctuaries and Battlegrounds

Global Islamist-inspired terrorism organizes networks to move people, money and weapons. These transit and support zones are of critical importance to the movement, which explains why they are relatively free from violence. Their centre of gravity today is in the area around Iraq, serving either as special entry points into Iraq or as practical communications corridors with Afghanistan or even the North Caucasus.

Operational Zones Where Global Islamist-Inspired Terrorism is at Work

Since 2001, most of the areas where terrorists operate have been concentrated in the Muslim world, as this often makes it easier for them. In the vast majority of cases they take action where they can, when they can, and how they can. Most often, this equation produces a simple result: they act at home, in their own countries, where Western targets representing the 'collaboration' between their governments and the 'occupiers' are normally present.

From the Sahel to the Indonesian archipelagoes, fewer and fewer countries are spared by the spread of terror at an average rate of one major attack every three months (except for Iraq, where the attacks happen daily). The targets are in big cities (Riyadh, Jakarta, Casablanca, Istanbul, Karachi, Amman) as well as in tourist centres (Djerba, Bali, Mombassa, Taba, Sharm el-Sheikh)

Since March 2004, Europe has been among these operational zones. There as elsewhere, the terrorists are acting at home, where they were born, and where they have been living for a long time.

Evolving and Complex Structures

Global Islamist-inspired terrorism is an amorphous collection of entities and individuals, organized horizontally and connected to each other to varying degrees.

The movement's original structure was different and relatively simple. It was vertical, with al Qaeda at the top and a few hundred Mujaheddin groups of varying backgrounds and affiliations at the bottom. These groups had passed through Afghanistan or other combat zones.

Initially, al Qaeda had an underground structure based on narrow recruitment from the middle-classes and created from the coming together of the Gulf Wahabis and Egyptian jihadists. Since 1998 under the joint leadership of Osama bin Laden and Ayman al Zawahiri, it dragged the world into the new form of terrorism that we know today with three key actions.

The first stage was the incorporation of the thousands of Mujaheddin who came from the world over to fight the Soviets in Afghanistan (between 1979-89), and then to join the Taliban (from 1996-2001). By creating this original model, al Qaeda earned the legitimacy that enables it now to symbolise global Islamist-inspired terrorism in general and to act as its spokesperson in the media.[1]

(1) Osama bin Laden's stay in Afghanistan from 1996-2001 also enabled him to bring together individuals and groups from all over the world and to reinforce his influence over them – especially by using his money.

The second key set of events was of course the 11 September 2001 attacks, whose stunning results made it possible for terrorism itself to change the course of world history. Indeed, it was the collapse of the World Trade Centre towers that simultaneously elevated what was once a threat from a few hundred individuals to the strategic level and led the United States to launch a 'war on terrorism.'

Finally, after the intervention in Afghanistan in 2001, al Qaeda organized the exfiltration and dissemination of terrorists all around the world.

The original model, however, has been significantly modified since 2001.

Through forced exile from its Afghan sanctuary, the original al Qaeda core group has lost a significant number of its leaders as well as its ability to play the role of single command centre. And the foot soldiers have been obliged to disperse among local militants. They have become part of an increasingly composite landscape never seen before on a global level. The best analogy for understanding it is the Internet: the terrorists form a huge, interconnected web, in which neutralizing one part has little effect on the functioning of the whole.

The network can be broken down into three levels, which – atypically – sit side by side, rather than on top of one another pyramid-style. It is fair to describe it as a network of networks whose borders are porous.

The First Level: the al Qaeda Organization

While partially dismantled, al Qaeda continues – though not without difficulty – to try to plan attacks from its Afghan and Pakistani redoubts. Its direct influence today is mostly concentrated along the axis linking Afghanistan to Iraq, in the Arabian peninsula and in the Horn of Africa. It does, however, still have the will, and even the means, to strike anywhere in the world.

It is in any case the core leadership that maintains the responsibility of keeping the movement ideologically coherent in its public message. This it does via the numerous video messages – around 40 since 2001, not including their many press releases – made by Osama bin Laden and Ayman al Zawahiri.

The Second Level: Terrorist Entities with Regional Roots

The types of relationships between these groups and the original al Qaeda vary enormously. They range from 'subsidiary' relationships and partnerships to simple imitations. There are many such organizations, but the ones in Iraq and Saudi Arabia are those most willing to display their attachment to the 'centre.'

While the Iraqi movement has many unique characteristics, the model of a 'regional branch' has spread throughout the Persian Gulf region. The *Organization of Al Qaeda for Jihad in the Arabian Peninsula*, for example, seeks to bring together all the cells working in and around Saudi Arabia. There are also other organizations, all organized in different ways: *Osbat al Ansar* in Southern Lebanon; *Al Ittihad Al Islami* in Somalia, the 'combatant Islamic groups' in different North African countries (Morocco, Tunisia and Libya); the *Salafist Group for Preaching and Combat* (GSPC), in Algeria; and the *Jamaa Islamiyya* in Southeast Asia.

The Final Level: Individuals Acting Alone or in Cells

Individuals have widely varying roles within the global terrorist movement.

At the top are the 'officers.' They have the address books, compiled in battle zones, training camps or prisons. That enables them to become 'facilitators,' organizers of the groups that support the national networks with false documents, money, lodging, and help crossing borders.

Other members of the movement might be called the 'experts.' Their job is to provide some specialized skill (in explosives, counterfeiting, finance, and computers) to a cell, network, or even the entire amorphous movement.

Cells are normally organized around an individual distinguished by his past accomplishments or personal charisma. The cell is the basic element in the terrorist galaxy, gathering a limited number of individuals around a hard core typically consisting of five to 15 people. By varying its composition according to its missions, it can play a logistical role, an operational role, or the role of ideological radicalization – and it can move easily back and forth among these roles.

Whatever the circumstances, and even in the context of a guerilla war as in Iraq in 2006, the cell constitutes the basic unit around which the struggle is organized. To understand how a cell functions, it is necessary to determine how independent it is from other cells and from potential external superiors. The study of the major attacks claimed by al Qaeda has made it possible to put forward a basic analytical framework that is based on the 'theory of the three circles.'

The 'Theory of the Three Circles'

This theory places al Qaeda attacks in three categories: The 'first circle' consists of attacks planned and executed directly by al Qaeda in the strictest sense of the term, acting alone. In the 'second circle' are attacks planned by al Qaeda and carried out with outside actors. And in the 'third circle' are attacks decided on and carried out by outside actors, but who claim to belong to the al Qaeda movement.

Thus according to these criteria, the March 2004 Madrid attacks would probably fall in the third category, the July 2005 London attacks might be in the second category, and the 11 September 2001 attacks would clearly be in the first category.

The last possibility is the individual, influenced by the movement but acting alone, or nearly alone, on his own, in his own way, and with his own hands.

As of 2006 this last possibility is still only a hypothesis. But the example of Theo Van Gogh's assassination in Amsterdam in November 2004 suggests that this possibility is no longer unrealistic.[1]

(1) Theo Van Gogh was a Dutch film-maker who had made critical references to Islam and some radical Islamist religious groups in his work.

Chapter 2

Global Terrorism Renews its Recruits, Adapts its Methods, and Displays a Signature Modus Operandi

Elusive Terrorists

Only a small number of marginalized individuals will ever resort to violence and engage in terrorist activities. This rule of thumb applies to global Islamist-inspired terrorism as well. It consists of a tiny minority of people, even within Muslim communities.

This type of terrorism nonetheless represents a growing threat that is harder to contain than in the past because of the diversification of its methods and its targets for recruitment.

A Minority with Diverse Backgrounds

Although reality cannot be easily reduced to stereotypes, it is primarily in Muslim areas that terrorist networks inevitably seek their recruits. The most likely profile to this day would be that of a young Muslim male, less than 40 years old. Women are only rarely involved.

But the origins, backgrounds and personalities of terrorists are of an unexpectedly wide variety. They have no obviously common bonds and their decision to engage in terrorism is not based on some simplistic determinism. A decline in social position or economic, social or cultural suffering can matter. But this is certainly not as important a factor as is sometimes said.

What comes through among individuals is a feeling of frustration and injustice. They feel frustration at what they believe is the Muslim community's loss of identity. And they believe Muslims to be victims of injustice in the world order.

The cosmopolitan and socially diverse nature of the global terrorist movement's members demonstrates the reality and power of the collective rage that unites them. It would be a grave error to assume it will disappear anytime soon.

Three Successive Generations

The hard core of global terrorism is made up of at least three generations :

• veterans of the first Afghan war, many of whom have been neutralized or have retired;
• militants trained in Afghan camps during the Taliban era;
• new recruits who signed up under the banner of the 'Iraq generation,' and who seem to have a greater propensity to carry out suicide attacks.

These three waves of recruits are intermingled with the current networks. The first, even if decimated, provides historical figures; the second provides active leadership; and the last provides the foot soldiers.

The first two groups remain dangerous. They now belong to the category of professional revolutionaries, old hands from the battle zones, used to operating under cover, exalted for their glorious accomplishments and their status as trained fighters, for their stays in prison, or, for some, for their theological expertise. For all these reasons their identities – even if sometimes multiple – and location are more or less known to the authorities. Some are on international data bases like the lists published under the authority of the United Nations Security Council, which entail the freezing of their assets and bans from staying in or transiting other countries.

Taken as a whole, they constitute a closed group of a few thousand individuals, of which a significant number have in 2006 already been rendered unable to do any harm or have decided on their own to retire. Some of the survivors nonetheless remain active. They use their prestige and experience to rally young recruits of the third generation to the cause.

Well-Honed Recruitment Methods

The recruiter takes advantage of the links that are created by regions, tribes, clans, families or neighbourhoods (in cities, mosques,

sports clubs or prisons) to enroll candidates in all the traditional ways. In this sense, mobilization stems more from political and psychological mechanisms than religious ones.

In Muslim countries, the technique is to invoke notions of purity and unselfishness, to which young people are particularly sensitive, as a means of getting those young people to rise up against the 'occupier' or against a corrupt power.

In the West, recruiters instead seek to exploit the vulnerabilities of the successive generations of immigrants, including those who come from non-Muslim countries (the Caribbean). The goal is to channel the malaise that exists in some big cities toward religious revival or revolt.

The 'Born Again'

The issue of 'born again' Muslims constitutes one of the possible responses to the need to find an identity that many of the most vulnerable people in our society feel. This is especially true for young people, children of immigrant origin and from difficult neighbourhoods, whose personal or professional development has stopped.

Seeking to resolve their personal problems, they turn to radical Islamism, which offers a simple and comprehensive ideological 'solution.' This type of conversion – expressed through sectarianism or political radicalization, and in conflict with the prevailing family and social milieu – has little in common with a return to the religious values of Islam that derive from family and cultural tradition.

Taken in by a charismatic recruiter and hardened by the influence of a narrow group of peers, the 'born-again' believer rediscovers his reference points and starts to believe once again in himself and to gain the respect of those around him.

Happily, the path toward terrorist violence is not automatic. But the stage of 'rebirth' can in some cases lead some more gullible individuals in that direction when the political circumstances, in their eyes, validate the thesis of a humiliated Islam under siege.

The exploitation of the recruits' psychological fallibility is in practice always strongly reinforced by the group dynamic produced by the cell. Indeed, it offers a framework of social links between people who lack such a framework. Most importantly, it puts peer pressure that can reinforce their original commitment in case it might be wavering. It is also within the cell that 'ideologisation' takes place – when personal motivations of a social or familial nature turn into a political-religious commitment to a collective goal.

The more closed the environment, the more these methods are effective. That is why they are so successful in prisons.

Finally, it is worth noting that while the decision to take action is ultimately always an individual one, taken after solitary reflection, that decision almost always comes in a collective framework, especially if it involves the suicide of the person carrying out the attack.

A More Problematic Third Wave

The description of the way in which new terrorists are enrolled shows why the third wave poses different problems from those posed by the first two.

Except for the 'Iraq returnees' who, like the veterans of the Afghan and Bosnian wars, have common, identifiable traits, the main characteristic of the new recruits is that of being difficult to pinpoint.

The new recruits can appear to be successfully integrated. They do not stand out for any particular religious fervour or militancy or from any past clashes with the police. They are indistinguishable, or at most barely distinguishable, from youth in general, with whom they share the same diverse social origins and levels of education. This intentional blending into general society helps to widen considerably the number of communities that could be at risk, which is all the more problematic because the radicalization process has accelerated.

This description fits the terrorists who struck Madrid in March 2004 and London in July 2005.

* * *

The threat of global Islamist-inspired terrorism is likely to endure. Although the spillover effects from Iraq have led it to spread since 2003, it has not been transformed into a mass movement. But it will have no trouble maintaining its strength, even if it continues to take significant losses.

Effective Management of the Flow of Information, Financing and People

Those who promote global Islamist-inspired terrorism are at home in modern society, even if they deny it. In any case, they systematically exploit all the opportunities it presents.

A key characteristic of globalization is the expansion and acceleration of the flow of information and money. Terrorists take full advantage of these hard-to-control exchanges to hide their secret activities or, on the contrary, to promote their accomplishments by taking full advantage of the media.

The flexibility of the terrorist networks' structures allows them to take better advantage of globalization than the states whose responsibility it is to fight those networks.

How the Terrorists Communicate

The Internet as a Tool of Modern Terrorism

The 'web' is the best symbol of global terrorist activity. Not only is it perfectly suited to the structure of the terrorist movement but it has in particular become an all-purpose tool. The terrorists feel at home on the web.

The Internet enables an individual or a group, even a tiny or secret one, to send messages instantly and openly to the entire world. It also makes it possible to get in touch, also immediately but privately, with a limited number of carefully chosen partners. The particular characteristics of the Internet – through which countless data transits – provide good conditions for anonymity.

To meet their needs in the areas of propaganda, recruitment, long-distance training, or transmission of messages, the terrorists use all the Internet's resources, including both open and closed areas. The most recent types of services offered by the Internet can even help them improve their ability to identify potential targets, thanks to all sorts of data – including geographical data and even satellite imagery – that can be found on the web.

The result of this intensive use of the Internet is the creation of a virtual space whose reach goes beyond the framework of terrorism. The community of sympathetic web-users brought together in this way can create the feeling of a reunified *Umma* (the community of believers), without borders or nationalities, united against a common enemy. Some even believe that global Islamist-inspired terrorism seeks to create a 'virtual Caliphate.'

The Use of Television for Propaganda Purposes

Satellite television – received all over and watched by those of all ages – is another of the terrorists' favourite propaganda tools.

In the rhetoric of Islamist terrorism, the West uses pictures and sounds as a means of intruding in every Muslim household to impose its values. Nonetheless, it must be pointed out that the terrorists – and certain extremist Muslim religious groups more broadly – now use television to promote their goals. Television is used to broadcast images of hostages begging to be spared before their decapitation and of suicide attacks, punctuated by the insistent appeals of Osama bin Laden and Ayman al Zawahiri. The terrorists' objective is to send messages to mobilize those in whose name they claim to speak and to demoralise the adversary.

While the major Arab and Muslim international media generally demonstrate the professionalism necessary to avoid being taken advantage of, the same cannot be said for all satellite channels.

Mobile Phones are Also Well Suited to the Activities of Highly Fragmented Terrorist Networks

The ability to track mobile phone use is greater than it used to be. But the advantages cell networks offer are too tempting, and the means to preserve anonymity still too effective, for terrorists to refrain from using them, whether for operational or personal purposes.

Terrorist Financing

Terrorist financing is a particularly important matter in the 'lands of jihad.' In these areas, paramilitary fighting and all that it involves (such as buying arms and ammunitions, and transport and supply for fighters and even their families), is in fact very expensive. As much as the materials necessary for attacks, it is the need to hire 'full-time terrorists' that entails high costs. It requires structured financing, which has two main sources. The first comes from skimming off oil income, particularly in the Persian Gulf. The second comes from collection networks set up in Western countries. In addition, certain preachers divert part of the *zakat*, the contributions that believers make to their mosques.

The security of transfers is ensured by the diversification of funding channels, which are to the extent possible kept outside of the banking system in order to thwart the surveillance and alert measures that apply to international financial flows.

Money orders, in small denominations, are used. Humanitarian Islamic NGOs were for a long time a primary tool, before their activities were subjected to more careful monitoring in France in 2002. But other equally inconspicuous means are still used. This is the case for the oldest and most traditional means, which remain as effective as ever. Human

money carriers are used, as is the *Hawala* channel.[1] Finally, modern kinds of money, which make anonymous money transfers possible, have appeared.[2]

In Europe, the local needs are smaller because the operational activities are rare and inexpensive. This makes the issue of terrorist financial flows different. The cost of carrying out the March 2004 attacks in Madrid and the July 2005 London attacks is estimated to have been between 15,000 and 20,000 euros. To ensure their financing, the cells may simply resort to delinquency, or even petty crime.

The Movement of People

Moving people remains indispensable in some cases, such as getting volunteers to the 'lands of jihad,' arranging for specialists to make temporary trips, or having human couriers transmit messages or money. These activities thus require the making of false travel documents and identity papers by the group's experts, whose work is vital to the terrorist business.

One of the most disturbing traits in the recent evolution of terrorism is, in fact, that these movements – which are dangerous to the terrorists because they can be tracked – are becoming less and less necessary because of the growing possibility of recruiting locals, including within Europe, and of using the services provided by the Internet.

A Traditional Yet Distinctive Modus Operandi

Global terrorism leaves an immediately recognisable imprint on its operations, wherever they may take place, seeking thus to validate the idea of a global enterprise capable of striking any time and anywhere (see Annex 1).

With the exception of the 11 September 2001 attacks, it must be noted that the promoters of global terrorism have most often sought to keep things as simple as possible. They have so far stuck to expanded use of explosives and suicide attacks. Their 'trademark' is thus not revealed by the nature of the attacks.

(1) *Hawala* is an informal system of international money transfer used in the Islamic world. It works using a compensation system among the participants.
(2) One example is prepaid smart cards – called 'Cash U Cards' – used in Arab countries and in the United Kingdom. Less secure than credit cards, they are anonymous and do not require the user to open a bank account. They make it possible to transfer money or make purchases without using a bank as an intermediary.

Rather, their originality lies in how the attacks are conducted. The first characteristic is the use of simultaneous explosions in one or several sites (13 bombs in four trains in Madrid in March 2004; simultaneous attacks on three subway lines and one bus in London in July 2005; several hundred small bombs in Bangladesh in 2005). Next are the 'soft targets' – civilian targets not directly protected – and the desire to cause as many casualties as possible. Finally there is the issue of timing, initially characterized by the effect of surprise – divorced from the timing of political events – and by the insistent repetition of attacks.

The trademark of global terrorist attacks since 2001 has, nonetheless, undergone a certain evolution, under the effect of the movement's 'Iraqisation' process. In Iraq itself, the development of an old-style guerilla movement that quickly became widespread has led to the return of targeted assassinations and hostage-taking. Suicide attacks have multiplied. These practices have spread contagiously and have begun to expand beyond Iraq – first to Saudi Arabia, and then to Afghanistan, the Maghreb, and even Europe.

The attacks carried out in Europe seem to have been timed to coincide with political events (the Spanish legislative elections in 2004 and the G8 summit in the United Kingdom in 2005). Some saw in this the desire to directly affect national politics. It could simply be a matter of seeking to maximise the symbolic or media impact of the attacks. While successful, the attacks carried out in Europe were also characterized by the relative amateurism of local recruits trained on the job and probably self-financed.

As of early 2006, our continent had experienced all those terrorist practices ever used before by global terrorism: indiscriminate and simultaneous attacks, targeted attacks, and attacks that crossed the suicide barrier.

Global terrorism continues to give top priority to causing as many immediate casualties as possible. This choice is driven by the desire to send a message of direct hostility to a world symbolized by the targets chosen. But whatever the effectiveness of this operating procedure, repeating it seems to be in long-term contradiction with the need for novelty and for ever more spectacular results that the terrorists have imposed on themselves.

Chapter 3

Troubling Prospects for France

France is a Designated Target at the Heart of a Europe under Threat

Global Islamist-Inspired Terrorism Does Not Spare France

France conducts a balanced foreign policy, which promotes respect for the rule of law and multilateralism and which listens to disadvantaged countries. This policy is in no sense directed against any specific state. Nonetheless, our country has been the object of attacks by the promoters of global terrorism.

The indictment always includes the same grievances: a past depicted as particularly burdensome (from the Crusades through colonialism); a military presence in Muslim lands (for example Djibouti); solid support for 'apostate' regimes, especially in the Maghreb; the secularism of the Republican State; the pretension to organize Islam according to a national model (with the 2003 creation of the French Council of the Muslim Faith); and finally, the constant determination of French judges and security agencies to preventively neutralize terrorists and their accomplices.

Two further factors have recently emerged. One was the 15 March 2004 law on religious symbols in schools,[1] proof of our unwavering attachment to secularism. The other was the participation of French forces in the operations conducted in Afghanistan.

France is directly and repeatedly the object of various declarations of war put forward by the spokesmen of global Islamist-inspired terrorism.

Starting in 1998, the year al Qaeda was created in its original form, Osama bin Laden listed French military bases in Djibouti among the 23 objectives of his organization. Subsequently, the April 2001 visit to France by the Taliban's avowed enemy Commander Ahmad Shah Massoud, led the al Qaeda leader to speak out virulently against France, which he called his main adversary after the United States.[2]

Since 11 September 2001, no fewer than nine communiqués have called for France to be punished. The main ones include that of Ayman al Zawahiri of 24 February 2004 and that published 18 May 2005 by Abu Musab al Zarqawi, leader of 'al Qaeda in Iraq,' both denouncing the law banning religious symbols in schools. Even more worrisome are the declarations of the 'emir' of the Salafist Group for Preaching and Combat (GSPC) which, in summer 2005, labelled France 'enemy number one,' confirming the overt hostility of Maghrebian extremists toward the former colonial power.

The attack in Karachi on engineers from DCN (the French naval shipbuilder then known as the *Direction des Constructions Navales*) on 8 May 2002, the attack on the tanker 'Limburg' on 6 October 2002, and the kidnapping of French hostages in Iraq starting in 2004 have confirmed that France got no 'special treatment' and that it was not spared from attack either. In addition, the numerous foiled attacks on French soil since 1998, in Strasbourg or in the Paris region, demonstrate that certain groups have already developed plans to carry out large-scale attacks directly in France (see Annex 2).[3]

(1) Law no. 2004-228 of 15 March 2004, which, according to the principle of *laicité* (secularism), provides the framework for the wearing of symbols or clothing manifesting religious affiliation in public elementary schools, secondary schools, and high schools.

(2) Massoud was assassinated on 9 September 2001, two days before the attacks in the United States, by affiliates of Osama bin Laden.

(3) Examples include, among others: 5 October 2001 – dismantlement of an Algerian Islamist cell suspected of preparing an attack at the time of a France-Algeria football match on 6 October 2001; 16 December 2002 – dismantlement at La Courneuve of a cell suspected of preparing non-conventional (chemical) attacks; 26 September 2005 – French police operation against a cell of former GIA members suspected of preparing attacks against the headquarters of the *Direction de la Surveillance du Territoire* (Directorate of Territorial Surveillance, DST), the Orly airport and the Paris Metro.

Europe Targeted by Terrorism

Nearer to the Middle East and thus more accessible than the United States, Europe represents a desirable alternative to anyone thinking about striking the 'far enemy.' It contains a wide range of spectacular targets, some linked to the United States or Israel, which if attacked would create global reverberations. Finally insofar as there are large numbers of Muslims in Europe, it is in direct contact with crisis zones.

The Schengen Area, of which France is a part, has a single external border where entry is monitored by each country according to identical procedures, using a data base of undesirable individuals.[1] It is also characterized by the abolition of checks at internal borders. The setting up of this area was an important step in the European integration process. It must be consolidated because, while this area is not easy to get into, the free movement of people within it can facilitate the organization and movement of networks set up in Europe.

The reasons why Europe has become an operational zone can be found in a range of recently emerged aggravating factors.

Reasons for the Growing Threat to France and Europe

The first of the aggravating factors is the development of a generation of 'home-grown rebels,' with or without French nationality, who are either longstanding Muslims or recent converts.

If Islamists who left France to fight in Iraq were to come back or if some of the thousands of Maghrebian fighters who have gone there did the same, a second aggravating factor would immediately appear. Such prestigious terrorists could represent a considerable force of attraction for many young people of the same generation. These new 'officers' could become the inspiration for new networks, to which they would also bring expertise in urban terrorism.

The third aggravating factor is the movement of 'transnationalisation' of terrorism among Algerian, Libyan, Moroccan and Tunisian groups. Goaded by certain terrorists at the forefront of the fight in Iraq, and bolstered by the feeling of belonging to a unifying cause, many of the support cells that are found in France and its neighbours – in particular

(1) The Schengen Area is named after two conventions signed in the Luxemburg city of Schengen in 1985 and 1990 by five countries, including France. This cooperation was legally incorporated into European Union common policies with the entry into force of the Amsterdam Treaty in 1999. It now involves the first 15 members of the EU, with special regimes for Denmark and the United Kingdom, and it was widened, with certain conditions, to non-EU member states Norway, Iceland and Switzerland.

those of the GSPC – could be tempted to follow the path opened ten years ago by those linked to the GIA. This would mean turning from logistical support for the fighting in Algeria toward violent acts directed against France.

A final factor aggravating the threat has to do with its growing invisibility and decentralization. The access by Internet to all sorts of expertise or, on a different level, the radicalization of the prison milieu, mean that apprentice terrorists no longer need to be integrated into a fundamentalist movement or to attend Koranic schools (such as the Pakistani *madrassas*)[1]. Nor do they need to go to the less numerous and more distant training camps. Relations with the veterans can thus be established more discreetly.

The threat now develops almost invisibly and is much more difficult for the intelligence and security agencies to detect.

One would expect that the recent trend within global terrorism toward smaller and less integrated units would lead it in the direction of less sophisticated actions. It remains to be seen whether this trend will not be affected by an opposite movement in the direction of more spectacular or deadly operational methods.

We cannot exclude another mutation that would lead to chemical, biological, radiological or nuclear terrorism. No moral objection to such actions exists in the terrorists' minds. They have in fact clearly shown that no atrocity is too repulsive to them, and they would not in principle reject any operational method if it matched their criteria for effectiveness. There is no doubt, moreover, that some of them have already thought about using such weapons and that they have envisaged to acquire them. Osama bin Laden has in fact often referred to Islam's need to endow itself with nuclear or chemical weapons.[2] Numerous extremist theologians have in their writings legitimized the use of weapons of mass destruction against Western civilians. The operations undertaken by the coalition in Afghanistan, moreover, have made it possible to establish that al Qaeda had already before 2001 undertaken rather advanced research in the chemical and biological areas, with help from high-level experts. Several terrorists arrested in France since 2001 had been involved with terrorist projects that included a rudimentary non-conventional aspect.

Numerous obstacles still stand in the way of the desire to commit this sort of attack. It is first necessary to have a minimal level of scientific and technical knowledge. It often remains very difficult to acquire the necessary materials, components or equipment. Working with these materials is often complex and dangerous. An attack undertaken with unconventional means can only succeed under very precise conditions. It thus entails a risk of failure. The loss of the Afghan sanctuary thus deprived the terrorists of the capacity to develop major unconventional projects. These

(1) Some of these schools have been identified as training centres for global Islamist-inspired terrorism.
(2) His words, however, could be taken to refer more to Muslim nations in general than to his own organization.

potential complications are probably what has led al Qaeda to adopt, other than on a few rare occasions, a more basic operational process, combining proven techniques (such as the systematic use of explosives) with original tactics (widespread simultaneous attacks in public places).

But other factors darkly suggest a resort to forms of terrorism that would make use of non-conventional weapons. The need to innovate in using terror is one. The growing spread of the technology, equipment and knowledge necessary for chemical and especially biological terrorism is another. This, in fact, makes it possible to cross certain technical obstacles. The recruitment of individuals well-integrated in European societies and trained in chemistry and biology can make it possible to apply expertise in highly toxic chemical products – widely available in business and industry – and publicly accessible procedures for biological production and use.

Part II

France's Counter-Terrorism System Must Continue to Adapt

The global terrorist threat could produce highly varied kinds of attacks that our country must be able to counter. To be prepared for any eventuality, we must test our system by envisaging scenarios that would call on the main measures designed to prevent terrorist acts and responding if an attack cannot be prevented.

Seven Scenarios for Testing Our Counter-Terrorist System

The following scenarios are not predictions. Many of them are today highly improbable because of their degree of complexity. Taken as a whole, they nonetheless allow us to outline the policies we must follow to fight terrorism effectively in all its forms.

A Campaign of Bomb Attacks

A terrorist group tries to conduct a campaign of repeated attacks, spread out over several months, with explosions in public places (metro stations, buses, airports, schools, etc.)

The aspects of our counter-terrorist system most in demand would be:
• The capacity to identify and neutralize the bombers as quickly as possible;
• The capacity of all our judicial, intelligence and security agencies to work at an intensive pace for an extended time;
• The capacity to maintain the vigilance of the public and state agencies as the country begins to function at the pace required by the constraining measures of the Red – or even Scarlet – level of the 'VIGIPIRATE'[1] plan for several months;
• The application over time of drastic and coherent security measures to all national public places.

Multiple Simultaneous Attacks

A terrorist organization seeks to use suicide attacks to cause simultaneous explosions in public buildings. The targets are large shopping centres, for example.

The aspects of our counter-terrorist system most in demand would be:
• Early actions of our intelligence agencies;
• Precautionary, preventive and protective measures taken in the context of the 'VIGIPIRATE' plan;
• Increased internal security in a large number of public buildings;
• Rapid dissemination of warning signals;

(1) See p. 68.

• The simultaneous implementation of several plans to help the victims;
• The strengthening of security measures pertaining to the raw materials used for making the types of explosives used (access, tracability) in order to avoid a second wave of attacks.

Diversified Cross-Border Attacks

Three teams of terrorists try to act simultaneously in several neighbouring countries. The objective of the first team is to seize a cargo ship arriving from a nearby country in order to cause damage in an oil terminal in one of our ports. The second team provokes an attack designed to sow confusion in the immediate neighbourhood of a nuclear plant near the border. The third team tries to attack computer systems to interfere with emergency response activities.

The aspects of our counter-terrorist system most in demand would be:
• Operational procedures between France and its neighbours, including in the area of public communication;
• Cyberterrorism prevention measures;
• The neutralization and reaction measures foreseen in the dedicated reaction plans ('PIRANET,' 'PIRATE-MER,' 'PIRATOME'...)[1]

Radiological Attack

A terrorist tries to set off a 'dirty bomb' (a device made of explosives and radioactive materials) in an underground public transport network.

The aspects of our counter-terrorist system most in demand would be:
• National and international measures to control radioactive materials;
• The capacity of early detection of explosives and dangerous substances;
• Public communication;
• Decontamination of the sites polluted by the dispersed radioactive materials;
• The neutralization and reaction measures foreseen in the 'PIRATOME' plan.

Chemical Attack

A terrorist group tries to spread a powerful nerve agent of industrial origin in a large railway station at rush hour, with the goal of causing a large number of casualties.

The aspects of our counter-terrorist system most in demand would be:
• The capacity of early detection of the acquizition and transformation of the precursor products for nerve gas;
• The protective measure of the 'VIGIPIRATE' plan and the alert and preventive neutralization measures in the dedicated 'PIRATOX' reaction plan;

(1) See p. 68.

• The capacity of the emergency and security services to immediately identify nerve gas and to take rapid action in a potentially contaminated atmosphere;
• Public communication;
• Decontamination of the areas polluted by the nerve agent.

Infectious Biological Attack

A terrorist group tries to acquire a highly contagious and deadly infectious agent. It seeks to spread it in a number of places to set off an epidemic that could last several months.

The aspects of our counter-terrorist system most in demand would be:
• Early detection of the epidemic via the identification of clinical signs and the comparison of analyses among different laboratories;
• The elaboration of procedures designed to isolate infected households, treat the sick, and allow economic and social services to continue to operate;
• The production and distribution of prophylactic and therapeutic treatments;
• Public communication;
• The application of emergency public health restrictions to limit the movement and activities of the population;
• Measures of neutralization and reaction foreseen in the 'BIOTOX' plan.

Attempt to Divert a Nuclear Weapon

A terrorist group tries to move a nuclear weapon from overseas to an urban centre in order to trigger an explosion.

The aspects of our counter-terrorist system most in demand would be:
• International action against nuclear proliferation;
• The capacity to detect the movement of the weapon and to put in place an intercept operation while it is in transit;
• The capacity to rapidly neutralize the weapon;
• The reaction measures foreseen in the 'PIRATOME' plan;
• The capacity to evacuate the population;
• If the terrorist group succeeds, the capacity to treat casualties both short-term and long-term, the maintenance of basic communication capabilities in such an environment, and the rebuilding of affected areas.

The list of scenarios described above is not exhaustive. Other threats that could be carried out are taken into account by the national counter-terrorist system.

To stop all possible attacks, we must continue to adapt our system. Our goal must be to prevent risks and threats through surveillance, detection and neutralization of potential terrorists, to reduce our vulnerabilities, to reinforce our capacities for management of a terrorist crisis and to strengthen our capacity for rebuilding and punishment.

Chapter 1

Countering Risk: Surveillance, Detection, Neutralization

The mission of prevention is essential in the fight against terrorism. We have the means to identify the most dangerous individuals, to neutralize those who are planning to act, and to monitor groups that might be at risk. This is all the more effective in that the French penal system – and this is its strength – does not establish a rigid separation between prevention and punishment.

Every day, this prevention mission mobilizes our intelligence agencies and our internal security forces responsible for monitoring the people and goods that enter, exit and cross our territory; our counter-terrorist magistrates; our armed forces; and our diplomatic service.

The terrorism prevention system in place in our country is sound and has proven its effectiveness. But the evolution of the terrorist threat, characterized by the development of global terrorism, makes it necessary for us to continue to adapt this system. This was the imperative that guided the elaboration of the counter-terrorism law of 23 January 2006.

Strengthening the Capabilities of our Intelligence and Security Agencies

Strengthening our Detection Capabilities

The effectiveness of our security and intelligence agencies, police and gendarmerie stems from their capacity for anticipating violent action and analysing the full range of mechanisms that contribute to the development of terrorism to better counter it. This requires the improvement of our capability to monitor electronic communications, the facilitation of the security and intelligence agencies' access to certain administrative data bases, and a better identification of dangerous travellers.

Improving Surveillance of Electronic Communications

As noted, those involved in global terrorism are comfortable on the Internet, whose characteristics offer them privacy.

(1) Given the technical standards that govern it, the Internet makes it difficult to identify users since the idea of a ‘user name’ is often virtual and temporary.

(2) An individual can have numerous user names. He or she can thus maintain many different electronic addresses, supplied either by an Internet operator or by global service providers which allow the user, without any identity checks, to create email addresses. Similarly, these same service providers offer the possibility, without further checks, to create websites.

(3) There are many Internet access providers. Some are less sensitive to security concerns than traditional telephone operators.

(4) The services on offer are proliferating. At the start of the decade, email and ‘news groups’ – where particular topics could be discussed – were the most widely used tools. Today there are many other ways of communicating on the web. People can use ‘chat rooms’ – which enable users to communicate instantly with others; they can use instant messaging; they can create semi-private communications systems; they can exchange files, even very large ones, via ‘peer to peer’ (P2P), in other words directly from computer to computer without the data passing through a centralized system; they can call without using the usual telephone networks (for example thanks to free, downloadable software, which can be used with only a user name and a password); they can encrypt communications thanks to commercial software that makes this possible; and they can even talk very easily via videoconference.

(5) The ways of accessing the Internet are being diversified. At first one used fixed telephone lines from home. Now many also use cable, mobile phone networks, or satellites to do so. Access points are also prolif-

erating. It is possible to 'navigate' on the Internet, and thus check email remotely, in Internet cafés, or in most public places that are equipped with 'wifi' (wireless networks). These types of connection are developing on physical networks and communications nexuses; they can be found in hotels, railway stations, airports, and service stations on highways.

There are two parts to the Internet. One is open. It provides free access to information through websites, chats, forums, blogs, so long as one is connected to the right address. The other part is closed. It consists mainly of traditional email, instant messaging, and telephone accounts. Access to information is often protected with user names and passwords.

The creation in the counter-terrorism law of 23 January 2006 of a procedure enabling governmental access to connection data (under the monitoring of an independent authority) allows the specialized agencies to act more effectively and more rapidly to prevent terrorist acts. This system can be activated 24 hours a day in case of an emergency.

The intelligence agencies must be able to identify and extract relevant data from the mass of information that is available in the open part of the Internet. Under certain conditions, they must also be able to access data that circulate on the closed part.

It will likely be necessary to adapt the 10 July 1991 law that governs security intercepts, if only to be able to target not only a predetermined telephone number but an individual, with the full range of means of communication and services that he or she uses.

We must also become more active in shaping Internet standards. To do that, we need a policy that seeks more actively to influence the authorities that regulate the Internet, both in terms of its operational development (at the level of the Internet Engineering Task Force, IETF) and in the area of research (under the auspices of the Internet Research Task Force, IRTF). It is particularly necessary to advocate technical and legal decisions that make it possible to limit anonymous communication.

Authorising Security and Intelligence Agencies to Access Certain Ordinary Administrative Data Bases

The growing discretion of the terrorists and their ability to communicate or move around in relative anonymity are obstacles to effective preventive action of the specialized services. The services have to take into account the evolution of the profile of new recruits. These recruits have not drawn previous attention by the police, or are known for an ordinary criminal past that shows no signs of developing into radical Islamism.

However, the identification of a terrorist before he acts can depend on the verification of a simple piece of operational information, often on short notice.

Until 2006 and unlike most of their counterparts in foreign countries, the intelligence agencies did not have legal access to ordinary

administrative data bases (for identity cards and passports; visas and residence permits; vehicle registrations and drivers licences). The counter-terrorism law of 23 January 2006 allowed access to the personal data in these data bases, managed by the Interior Ministry, so that the necessary verifications could be made within operationally useful time limits.

All such investigations carried out by the police are kept and put under the control of the National Commission on Data Processing and Liberties (*Commission Nationale de l'Informatique et des Libertés* or CNIL). They only involve personal data that is not sensitive, such as one's civil status or address. The possible access to more sensitive data, such as that contained in banking, tax, or social security data bases, is only allowed in the framework of a judicial procedure.

Identifying Dangerous Travellers Better

For the branches of the police responsible for counter-terrorism, it is absolutely essential to have access to information about individuals who travel regularly or for extended stays to countries known to shelter areas of radicalization, as well as about the travel movements of people already identified.

The National Cross-border Index (*Fichier National Transfrontière*, FNT) is designed with this goal in mind. The way in which it is supplied with information, however, has become ineffective and obsolete. The boarding and landing cards that passengers fill out are entirely declaratory and cannot be systematically monitored. Moreover, the manual handling of the cards has become an enormous job with the growth in air travel. It unduly occupies the agents needed to carry out security checks and border checks. By authorising automatic information feeding of the FNT with optical reading of the travel papers and visas at the time of the border controls, the counter-terrorism law of 23 January 2006 opened the way to the rapid modernisation of this data base.

The data bases of airlines are also a source of useful information in counter-terrorism. Two types of such data bases exist: commercial reservation databases[1] and departure-monitoring data bases.[2] Both contain identifying information relative to the travellers as well as information about the flights taken.

Access to data from reservations, departure checks and border checks prior to the flight enables the agencies in charge of counter-terrorism to run checks sometimes several days before the trip. Effective use of counter-terrorism information requires that the data be compared with each

(1) 'Passenger Name Records' (PNR) data bases include a variety of data collected by companies for their business needs. The International Civil Aviation Organization has issued recommendations, but PNR do not conform to any standard. Depending on the destination the airlines must share the information they have with the police.

(2) 'Advanced Passenger Information System' (APIS) data bases are being standardized internationally. Airlines must gather certain data from their passengers, check them, and transmit them to the authorities responsible for border controls in the country of destination before the airplane takes off.

other and sometimes kept in a single data base. They must always be cross-checked with the data base of suspects.

The counter-terrorism law of 23 January 2006 enables the regulations governing air travel to be extended to international sea and rail travel whenever an external European Union border is crossed.

Ensuring Coordination Among Intelligence and Security Agencies in the Fight Against Terrorism

To be as effective as possible, the activities of the various specialized counter-terrorism agencies require close cooperation.

Since the 11 September 2001 terrorist attacks in the United States, our main partners have been moving to restructure their intelligence coordination agencies. The United States created the post of 'Director of National Intelligence' (DNI) under the U.S. President.[1] In the United Kingdom, in 2003, the authorities put in place a new inter-agency terrorism analysis structure, the Joint Terrorism Analysis Centre (JTAC). Operating 24 hours per day and bringing together officials from 11 different ministries and agencies, the JTAC's goal is to centralize, analyse and evaluate all terrorism-related information, both on British territory and abroad. The creation of the JTAC brings the operational level (the everyday work of the agencies on the ground) closer to the strategic level, represented by the Joint Intelligence Committee (JIC) under the direction of the Prime Minister's Security and Intelligence Coordinator.

In France, the main decisions in the area of counter-terrorism are taken in a number of different high-level bodies. Chaired by the President of the Republic, the *Conseil de Sécurité Intérieure* (Internal Security Council, CSI) defines the orientation for domestic security policy and establishes priorities.[2] The Prime Minister brings together the ministers involved with counter-terrorism to coordinate their actions and establish their orientation. He chairs the *Comité Interministériel du Renseignement* (Interministerial Intelligence Committee, or CIR).[3] This committee also leads the work of technical groups. The Interior Minister leads the *Comité Interministériel de Lutte Antiterroriste* (Interministerial Counter-Terrorist Committee, CILAT) in order to coordinate action undertaken at the interministerial level. The Prime Minister's chief of staff extends the Prime

(1) The 2004 Intelligence Reform and Terrorism Prevention Act also created a new coordination structure – the National Counterterrorism Centre (NCTC) – directly under the Director of National Intelligence.

(2) According to decree no. 2002-890 of 15 May 2002 relating to the Internal Security Council. The CSI includes the Prime Minister, the Ministers involved and the Permanent Secretary for National Defence. The Secretary General of the CSI is appointed by the President of the Republic and serves under him.

(3) According to ordinance nº 89-258 of 20 April 1989, the CIR is in charge of ensuring the orientation and coordination of the activities of the intelligence agencies. It is staffed by the *Secrétariat Général de la Défense Nationale* (Permanent Secretariat for National Defence), which is under the Prime Minister.

Minister's leadership by chairing regular meetings of the senior officials responsible for security.[1]

At the operational level, the *Unité de Coordination de la Lutte Anti-Terroriste* (Anti-Terrorist Coordination Unit, UCLAT), created in 1984 within the Interior Ministry, ensures the coordination of all the counter-terrorism agencies, through the daily analysis and synthesis of information about terrorism. It works closely with the DST, the DCRG, the national gendarmerie, the DGSE and the *Direction Générale des Douanes* (Customs Service). It makes sure that relevant operational information is shared with all the counter-terrorism agencies and authorities, including the counter-terrorist magistrates and the prison management authorities.

Specialized Counter-terrorism Agencies in France

*The **judicial arm** includes a public prosecutor (parquet), an investigating branch (pôle d'instruction) and a panel of judges (formations de jugement) specialized in judging terrorist crimes. All of their files are centralized in Paris.*

*In the **Interior Ministry**, most of the specialized counter-terrorism agencies are under the Direction Générale de la Police Nationale (Central Directorate of National Police, DGPN). The Direction de la Surveillance du Territoire (Territorial Surveillance Directorate, DST), in addition to traditional counter-espionage missions, works directly on the prevention and repression of terrorist activities thanks to its judicial and administrative policing attributions. The role of the Direction Centrale des Renseignements Généraux (Central Directorate of General Intelligence, DCRG) is to monitor dangerous groups. The Direction Centrale de la Police Judiciaire (Central Directorate of Judicial Police, DCPJ) undertakes numerous investigations through its Division Nationale Anti-Terroriste (National Counter-Terrorist Division, DNAT). In cases of financial crime, one of its specialized offices can be used as well.*

The Unité de Coordination de la Lutte Anti-Terroriste (Anti-Terrorism Coordination Unit, UCLAT) brings together the information supplied by all the operational agencies, whether in the Interior Ministry, the Defence Ministry or the Ministry of the Economy, Finance and Industry. This unit is also responsible for regularly exchanging information with judicial authorities. The RAID (research, assistance, intervention and deterrence), intervention force of the national police, is constantly available to the DGPN in

(1) The 'intelligence meetings' chaired by the Prime Minister's chief of staff include the representatives of the President of the Republic's private office (état-major particulier), of the CSI, the chiefs of staff of the Interior, Defence, and Foreign Ministers and the Permanent Secretary for National Defence (SGDN), as well as the directors of the main intelligence services (DGSE, DST, DRM).

case of crisis. The Police aux Frontières (Border Police, PAF) watches out for suspicious persons entering and exiting the country. In Paris, the police prefecture maintains specialized administrative and judicial police units. The national gendarmerie under the operational control of the Interior Minister, participates in counter-terrorism through its widespread coverage of the national territory.

*In the **Defence Ministry**, the Direction Générale de la Sécurité Extérieure (Central Directorate of External Security, DGSE) plays an essential role by providing intelligence gathered outside of France. The Direction du Renseignement Militaire (Military Intelligence Directorate, DRM) has detection and analysis capabilities (notably through satellite imagery). By virtue of its military attributions, particularly for external operations, the national gendarmerie also plays an important role. Moreover, within its Groupement de Sécurité et d'Intervention (Security and Intervention Group, GSIGN), it makes the Groupement d'Intervention de la Gendarmerie Nationale (Gendarmerie Nationale Intervention Unit, GIGN) constantly available for counter-terrorist action. Finally, the Direction de la Protection et de la Sécurité de la Défense (Defence Protection and Security Directorate, DPSD) ensures that the personnel and installations of the wider defence sector (state and industry) are protected against terrorism.*

*The **Ministry of the Economy, Finance and Industry** has several agencies associated with counter-terrorism. The Direction Nationale du Renseignement et des Enquêtes Douanières (National Intelligence and Customs Inquiries Directorate, DNRED) gathers, analyses, and distributes customs information related to terrorist financing. The cell called Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins, (Treatment of Information and Action Against Clandestine Financial Circuits, TRACFIN) gathers information that it adds to by comparing it with information from other ministries before passing it on to the judicial system. The main role of the FINATER cell (created in October 2001 to prepare and relay ministerial guidelines on the fight against terrorist financing) is to freeze terrorists' financial assets.*

Cooperating with Our Foreign Partners

Traditionally, international cooperation in the area of intelligence is primarily a bilateral relationship between services. It is in this framework that most information, especially operational information, circulates. It has, however, become necessary to expand cooperation in a multilateral framework, given the convergence of interests and risks with our partners.

In the **European Union**, after the March 2004 Madrid attacks, a terrorism threat analysis cell was created in the Situation Centre ('SITCEN') that was placed under the authority of the Secretary-General

of the Council, High Representative for the Common Foreign and Security Policy (CFSP). This Situation Centre, which France actively contributes to, establishes a threat assessment based on the sources provided to it by intelligence agencies, military, diplomats, and the police. The Sitcen can also make useful contributions to operational issues, such as the terrorists' destinations, motives and movements, in order to sensitize all Member States and help them to take appropriate measures. Experience shows that Member States have very different threat perceptions and that their harmonization is highly useful.

The retention of fixed telephone, mobile phone and internet traffic data plays a key role in counter-terrorism. This is often what makes it possible, notably in the case of the March 2004 Madrid attacks, to track down the terrorist network. Connexion data show the identification, place and time of the calls, but not the content of the communications. Already in 2001, France took the decision to require electronic communications operators to keep these data for a year. The adoption in early 2006 of the European directive on the retention of communications traffic data, which requires the data to be kept for at least six months, will be an important step forward. It will allow better cooperation among Member States in identifying terrorists.

The heads of internal security agencies of several European countries meet in the context of the **Club of Bern**, an informal forum for exchanging information in areas such as counter-espionage, organized crime and terrorism.[1] After the 11 September attacks and on the recommendation of the European Union, the Club of Bern created a counter-terrorism group (GAT) that brings together the leaders of counter-terrorist units. This group draws together assessments of terrorist threats and thematic studies on issues such as false documents networks and the chemical, biological, radiological and nuclear (CBRN) threat.

At the **multilateral level**, information exchanges on threat analysis take place mostly within the G8[2] and the North Atlantic Treaty Organization (NATO). Within the G8, the Practitioners Group carries out threat analysis. In NATO, the Special Committee prepares analytical documents on terrorist threats that could affect the Alliance.

(1) Created in 1968, the Club of Bern includes heads of internal security in 19 European Countries.

(2) The G8 is an informal multilateral institution made up of 8 states: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States. France proposed its creation at the Rambouillet summit in 1975. This led to the formation of the G7 the following year, which was expanded to include Russia in 1998.

Consolidating our Penal System and Adapting our Prison System to the Threat of Terrorism

Consolidating an effective penal system

To be effective, a judicial system for counter-terrorism must combine a preventive element, whose objective is to prevent terrorists from acting, and a repressive element, to punish those who commit attacks as well as their organizers and accomplices.

The French system follows this logic. But its originality and strength lie in the fact that the barrier between prevention and punishment is not airtight.

On the level of principles, France has chosen to develop a unique penal system to prevent and punish terrorism. The main element is the law of 9 September 1986, adopted after the wave of attacks conducted in 1985 and 1986. It is not a matter of creating extraordinary legislation. It is a specialized penal system tailored to the particular nature of terrorism. Specialized law applies not only to the fight against terrorism, but also to organized crime.

In our legal system, a terrorist act is defined first by the combination of a crime with 'an individual or collective act whose goal is to seriously disturb public order through intimidation or terror' (article 421-1 of the penal code). The terrorist aspect of the crime brings into application a penal system that includes, most importantly, an increase in the severity of the penalties imposed and an extension of the normal statute of limitations (extended to 30 years for felonies and 20 years for misdemeanours).

There are three unique aspects to our antiterrorist penal system.

The first is the existence of a specific offence that enables not only the suppression of support structures of terrorists or their accomplices but also the prevention of attacks still under preparation. Elevated to the level of a specific offence by the law of 22 July 1996, it is without question the cornerstone of the system. It enables the legal system to intervene even before an attack is perpetrated. It is thanks to this law that the terrorist networks' logistical cells and the peripheral structures that surround them can be dismantled. The application of this offence requires an exchange between magistrates and intelligence services. The exchange is facilitated by the fact that the DST is at the same time an internal intelligence agency responsible for preventing activities that threaten national security and a judicial police agency that undertakes sensitive investigations on international terrorism. This dual nature makes possible the use of information acquired through intelligence during judicial procedures, whereas in the other direction, the information gathered in the context of judicial procedures is used to guide the security police work.

The second specificity of the French system is to take into account the seriousness of terrorist acts in the definition of procedural

rules which are more flexible than for normal offences. A terrorist suspect can be held for up to 96 hours, compared with 48 hours under the normal system. The intervention of a lawyer is pushed back to the 72nd hour. In case of an imminent risk of attack or necessity linked to international cooperation, the counter-terrorism law of 23 January 2006 authorizes an extension of up to six days. The means of investigation have also been expanded: it is possible, under certain conditions, to carry out searches and seizures at night and infiltration and 'bugging' of automobiles and residences is permitted. Finally, the serious risks involved justify special protection for witnesses and even investigators. Witnesses can thus be heard anonymously, and the anonymity of investigators can, under certain conditions, be maintained.

The specialization of counter-terrorist magistrates is the third specificity of the counter-terrorist penal regime. Its main characteristic is the centralization of the prosecution, investigation, and judgment of cases in Paris. Seven magistrates of the public prosecutor's office and seven specialized *juges d'instruction* (investigating magistrates) are responsible for terrorism cases. The judgment of misdemeanours is delegated to the Tribunal de Grande Instance of Paris, while that for felonies is the responsibility of a *cour d'assises* (trial court) made up entirely of professional magistrates, as opposed to a *cour d'assises* for normal offences, in which the jury is made up of ordinary citizens. This specialization of the magistrates has made it possible over time to develop a genuine counter-terrorist culture: the terror network's evolution is better controlled, and relationships of confidence built up over time have been developed with foreign security agencies and magistrates.

All in all, the French judicial system for counter-terrorism, constantly adapted since 1986, gives cause for satisfaction.[1] It does not need major reform.

Prison Conditions in Need of Adaptation

Prison has become a place where dangerous proselytization takes place. If we are not careful, this will eventually produce a reservoir of radical activists available to conduct terrorist acts. An examination of past incidents makes it possible to draw a national map of proselytization in prisons and a genuine increase has been observed in certain regions, including Paris region.

Various short-term measures can be contemplated to slow the rise of proselytization. A modification of regulations in the legal code governing prison life should solve some of the problems. It is also necessary to pay close attention to the recruitment of Muslim chaplains in prisons.

The phenomenon also requires structural treatment over the long term. Centralizing the application of penalties at the Tribunal de Grande

(1) The main reforms include the laws of 22 July 1996, 15 November 2001, 9 September 2002, 18 March 2003, 9 March 2004, and most recently 23 January 2006.

Instance of Paris as foreseen in the counter-terrorism law of 23 January 2006 will make it easier to follow-up on prisoners being held for a terrorist offence, wherever they are being held and wherever they may be from. This policy could be bolstered by establishing a computerized national data-base of people sentenced for a terrorist offence.

Neutralizing Dangerous Flows of People, Goods, Funds and Ideas

Monitoring the Movement of Dangerous Individuals

The Entry and Stay in France of People Suspected of Links with Terrorist Activities

With the exception of the special case of people from Member States of the European Union, foreigners who enter and reside in France are subject to a system of administrative authorization.

(1) Entry into France normally requires the issuing of a visa by consular authorities.[1]

Heads of French consular posts have the legal right to refuse the granting of a visa in cases where the applicant has terrorist links. This is the case whether it is an application for a long-term visa, which are still handled by France, or for a visa for a stay of less than three months, which is handled under a common regime of the Schengen countries. The Convention implementing the Schengen agreement allows short-term visas to be rejected for this reason, which leads the people in question to be listed in the 'Schengen Information System' (SIS data base).

(2) Contrary to widespread assumptions, even an official visa in good order does not grant an unconditional right of entry into the country.

The visa does allow its holder to depart his or her country with France as a destination. But the border police can refuse the visa holder entry into France for reasons of public security resulting from a link with terrorism. Entry can be refused not only to a foreigner with a regular entry visa, but also to a foreigner holding a residence permit (*carte de séjour*).

Typically, in the process running from getting a visa to entry into France to staying in France, the issue of a threat to public security, specifically linked to a risk of terrorism, can be raised at any time: at the time the visa is applied for; upon admission into the territory; or when the

(1) Except in cases of reciprocal agreements that exempt citizens from certain countries from this requirement.

application for a residence permit is being considered, even for a foreigner who could otherwise claim every right to have one.[1]

(3) Links with terrorism, which constitute a legal obstacle to entry into and residence in France, in the same way constitute a legal basis for forced deportation from France. 'Conduct linked to activities of a terrorist nature' thus justifies the deportation of a foreigner, however extensive his or her links with France.[2]

'Explicit and deliberate acts of incitement to discrimination, hatred or violence' can also lead to deportation. It was on this basis that the Interior Ministry announced the deportation of some ten fundamentalist imams during 2004-05.

Identifying Individuals: the Biometrics Issue

It is necessary to have the ability to prevent dangerous individuals from entering or staying in France. And it is just as necessary to have the ability to deport some of them from the country. But the impact of these measures on civil liberties, especially on the right to come and go, is not negligible. We must therefore be sure that the coercive measures are being applied to the right people, without risk of error. The more certain we can be about identifying the right people, the more certain we can be not to take action against the wrong ones.

Identity falsification and identity theft are big challenges. They raise questions about the reliability of registry office data, identity papers and passports. Using biometrics can help limit fraud by offering a limited number of all-purpose means of identification.

Biometrics makes use of different techniques, including facial recognition; optical (iris pattern) recognition; fingerprints or palmprints; spectral voice analysis; and genetic data comparison.

The advantage of biometric data is that they are unique and indistinguishable from the individual in question. Biometrics thus makes it possible to identify an individual who is present by establishing a link between the person and the identifying documents that is almost impossible to falsify. Biometrics also makes it possible to identify someone by comparing his biometrical data with those contained in a data base.

A number of our neighbouring countries have already begun making use of fingerprint and palmprint biometrics not only for travel documents but also for identity cards. This is the case in Belgium, Spain, Italy and the United Kingdom. France has already decided to start issuing biometric visas. Making passports and identity papers more secure through fingerprint and palmprint biometrics is a priority. This should take place in

(1) According to Articles L. 314-11 and 12 of the code governing entry and residence of foreigners and right to asylum.
(2) This is clearly expressed in the language of Article L. 521-3 of the code governing entry and residence of foreigners and right to asylum.

a balanced legal framework, taking into account both the protection of civil liberties and the demands of the combat against terrorism.

Stopping Capital Flows that Contribute to Terrorist Financing

Reinforcing our Judicial Apparatus Against Terrorist Financing

Financing terrorism is a criminal offence, banned by Article 421-2-2 of the penal code. It is thus legally possible to track down the networks and, if necessary, to sanction the network's financial support. Practitioners are completely satisfied with the fact that the financial and the counter-terrorism departments of the Tribunal de Grande Instance of Paris can be seized jointly.

The effectiveness of prevention is less certain.

Information circulates appropriately among the different actors: magistrates, intelligence agencies, the Economy, Finance and Industry Ministry's TRACFIN cell, whose responsibility it is to track secret financing in France. It would, however, be desirable to strengthen the legal basis of the exchanges between TRACFIN and the police and intelligence agencies that participate in the combat against terrorist financing and money-laundering.

The way in which certain religious organizations and charities use the money they raise is highly opaque. A number of options are possible to try to lessen the doubts that this absence of transparency can create.

One option would be to require that beyond a certain level of activity, organizations be required to work with an accounting commissioner to certify the legality of all their transactions, or that their obligation to present their accounts to clerks from Grande Instance tribunals be reinforced. These requirements, which are not particularly burdensome and serve the general interest, do not interfere with the right to free association guaranteed by the law of 1901. A reinforcement of the regime that oversees fundraising from the public could also complement the application of this sort of declaratory requirement.

Finally, the procedure for freezing assets of people or organizations with links to terrorist organizations, recently reformed by the counter-terrorism law of 23 January 2006, should enable the neutralization of suspicious assets, by giving the Ministry of the Economy, Finance and Industry the power even over funds held by EU citizens.

Developing Effective International Cooperation

Already in 1999, at France's initiative, the Convention for the Suppression of the Financing of Terrorism was adopted at the United Nations. This text prefigured a number of measures that were taken up again in UN Security Council Resolutions 1267 and 1373, and also contains other

measures that are enormously helpful in the combat against terrorist financing, such as extradition measures and mutual legal assistance, preventive measures for financial institutions to take, and the lifting of banking secrecy.

Following the 11 September 2001 terrorist attacks, different international legal instruments were adopted. Their objective is to freeze the financial resources of individuals and organizations that commit or are accomplices in terrorist acts. The main instruments are UN Security Council Resolution 1267, which delegates to a committee the job of updating a 'black list' of names, and Resolution 1373, which accepted the principle of a general obligation to freeze assets linked to terrorism. The system was initially created to fight the Taliban protectors of al Qaeda. Today the lists include more than 350 names of individuals and entities.

Based on Resolution 1373, the European Union created its own list in December 2001, which in particular includes European terrorist organizations (those linked to ETA, Northern Irish, Greek and Italian groups) and external groups (Palestinian Islamic Jihad, the PKK, Shining Path, and the Iranian MEK), as well as individuals linked to these groups.[1] The system is nonetheless incomplete in the sense that the freezing of assets that is prescribed in Europe only applies to non-residents.

The Financial Action Task Force on Money Laundering (FATF), set up by the Paris G7 summit in 1989, has made action against terrorist financing its top priority. Now composed of 33 members, the FATF is an active organization in the combat against international micro-financing of illicit activity. It proposes to raise the level of security of international transfers, by obliging financial institutions to note the identity of the person making the transfer, so that the state where the person receiving it lives can easily identify the transaction. In this area, the European Union is seeking to have the system applied to all transfers, of whatever amount.[2] France must support the adoption, under UN auspices, of a range of international instruments based on the logic at work in the FATF.

Neutralizing Flows of Ideas that Incite Hatred, Violence or Terrorism

Our legal system contains arrangements that make it possible to fight the dissemination of extremist ideas.

(1) Common Positions 2001/930 and 931/CFSP of 27 December 2001, taken in the context of the common foreign and security policy, and regulation 2580/2001 of the Council of the European Union, taken on the basis of Articles 60, 301, and 308 of the Treaty establishing the European Community. Taken together, these three instruments of binding legal force for Member States constitute the mechanism known as the 'Clearing House.'

(2) In 2005 France already managed to get the level at which transfers are followed lowered from $3,000 to $1,000.

The law of 10 January 1936 on combat groups and private militias gives the President of the Republic the authority, by decree in the Council of Ministers, to disband associations or 'de facto' groups that promote discrimination, hatred or violence toward a person or a group of people based on their origin or their belonging (or not) to a particular ethnic group, nation, race or religion. Groups acting 'on French territory to undertake activities designed to provoke terrorist acts in France or from French territory to provoke such acts abroad' are also covered by this legislation.

Appropriate tools thus exist against these groups. It is more complicated however to launch legal action when it is a matter of prosecuting similar illegal acts attributed to individuals acting alone.

The penalty for direct incitement to terrorist acts and the justification of such acts by **individuals** is five years in prison and a 45,000 euro fine. In theory, the punitive regime thus seems a good deterrent. This offence, however, does not appear in the penal code but in the law of 29 July 1881 on freedom of the press. It is thus this law's particular legal framework that applies to the prosecution of illegal acts: the statute of limitations is shortened to three months; seizures or preventive arrest of the person in question is not permitted; and accelerated anti-crime procedures (such as immediate court-appearances, for example), are not possible. In addition, the acts in question must have been public, which excludes individual-to-individual proselytizing done for the purpose of committing a violent act.[1] Finally, the application of this law does not come under the jurisdiction of Paris as part of its national counter-terrorism responsibilities.[2]

Thus applicable law does not seem well suited to the situation. Two possible routes to improve it exist.

The first consists in taking the offence of incitement or justification of terrorism out of the scope of the press law and integrating it directly into the penal code. Such an approach would not be unprecedented. It is what was done in the case of the offence of incitement to drug use or trafficking. In addition, by dropping the requirement that the incitement be public, this option would easily widen its coverage to include proselytization whose goal or result is the commitment of a violent act.[3]

The second option would be to incorporate this offence into the penal code while leaving in place the scope of the law of 1881. Illegal acts could thus be prosecuted on the basis of either of the two laws.

(1) In fact, Article 24 of the law of 29 July 1881 requires that the incitement takes place in a public place, real or virtual (electronic means of communication were added to the law with part II of Article 2 of law no. 2004-575 of 21 June 2004).
(2) For a description of the counter-terrorism penal regime, see p. 53.
(3) This would have the added value of dealing with part of the problem of proselytization in prisons.

Protecting the Homeland from Intrusions and Neutralizing Terrorists Abroad Through Action of the Armed Forces

'The object of defence is to ensure, at all times, in all circumstances, and against all forms of aggression, the security and the integrity of the territory, as well as the life of its population.'[1]

Backed by this mandate, the military forces contribute to the prevention of terrorism by accomplishing two principal missions, for which they continuously employ 35,000 military personnel. One mission is to protect and control in depth France's national territory, air and maritime space and other areas where France has interests. The other is to undertake external operations whose main goal is to neutralize the terrorist threat before it reaches our country.[2]

The Armed Forces Protect and Thoroughly Monitor National Territory and Areas Where France Has Interests

(1) Approximately one hundred fixed radars permanently watch over and control the 10,000 aircraft that fly over the national territory every day. Mobile tactical radars complement the system whenever there is a particular need.

In the case of suspect behaviour of an aircraft or troubles on board a plane, combat aircraft and armed helicopters are in a position to intervene very rapidly at the highest state of alert.

To optimize even further its capacity to defend its territory against any intrusion from the air, by detecting the threat before it penetrates French airspace, France must continue its policy of concluding bilateral air security agreements. Agreements have already been reached with Belgium, Spain, and Switzerland. They must be complemented with agreements with Germany, Italy, Luxembourg, and the United Kingdom, as well as with Brazil and Suriname, which neighbour the French Department of Guyane, where the Kourou Space Centre is.

(2) Maritime traffic in the waters around France, its Departments and Overseas Territories, and the areas where we have economic interests[3] is monitored with civilian and military assets. In Metropolitan

(1) Article L. 1111-1 of the defence code.
(2) The participation of the armed forces in the 'Vigipirate' plan, and the work done by the national gendarmerie under the direction of the Interior Ministry, are described elsewhere in this White Paper.
(3) The Exclusive Economic Zone extends 200 nautical miles from French coasts, including around the overseas departments and territories.

France, surveillance is undertaken with support from the SPATIONAV network, built around French coastal semaphores and their radars.[1] This network also benefits from information provided by the International Maritime Organization (IMO), by allied navies, as well as by French navy ships on mission in oceans around the world. Suspicious naval activity can be dealt with on short notice by the most appropriate combat tool: surface ship, submarine, commandos, airplane or helicopter.

The safeguard system could usefully be promoted and harmonized within the European Union.

The Armed Forces Help Prevent Terrorism by Acting Outside French Territory

Beyond our borders, our intelligence services, our armed forces, and our diplomatic service work together to identify and prevent threats as early as possible.

As asserted in the report annexed to the Military Programme Law for 2003-2008, the possibility of a pre-emptive action may be envisaged in case a clear and established threat situation is recognized.[2] Recourse to such action would be in keeping with the framework of Article 51 of the UN Charter, in other words in a situation of self-defence.

In a more general sense, the participation of the armed forces in peace restoration or stabilization missions – alongside national and international civilian participants – contributes to the elimination of terrorist havens by stabilizing crisis zones. In 2006, France is actively contributing, at both the civilian and military level, to such missions in territories that have sheltered or continue to shelter terrorists, such as the Balkans, Afghanistan or the Sahel region. In all these actions, the armed forces are supported by the *Direction du Renseignement Militaire* (Military Intelligence Directorate, DRM). With its satellites and interception capabilities, and in cooperation with other domestic and foreign intelligence agencies, the DRM evaluates the threat to our forces.

Parallel to the efforts of prevention in the broad sense, the armed forces participate in the combat against terrorism by attacking it in its bastions. Thus, after the 11 September 2001 attacks, France immediately took part in counter-terrorism operations in Afghanistan and the Indian Ocean under American command. UN Security Council Resolution 1368, adopted on 12 September 2001, notes that such operations are in keeping with the framework of the legitimate right to self-defence recog-

(1) SPATIONAV stands for *Surveillance des espaces sous jurisdiction nationale et des approaches maritimes* – Surveillance of areas under national jurisdiction and maritime approaches.

(2) 'Pre-emptive' action is commonly understood to mean an action against an imminent threat, whereas 'preventive' action is action against a merely potential threat.

nized by the UN Charter. Our force known as HERACLES involved air forces, naval forces and land forces, and both regular and special forces.[1]

Preventive use of enforcement measures, including the use of armed force, may also be considered. It should be authorized by the Security Council under the framework of Chapter VII of the UN Charter.[2]

Strengthening International Cooperation

A characteristic of global terrorism is to refuse to recognize any territorial limits. Any attempt to deal with a movement that disregards borders without the help of others would be doomed to failure.

France did not wait for the 11 September attacks before seeking a concerted and coordinated international response to the terrorist threat. Confronted with the rise of global terrorism, international cooperation was expanded and intensified. Besides the prevention of attacks, its main objective is to reduce the vulnerability of our societies.

Preventing the Threat

The protection of national territory is a responsibility of national states. But international cooperation is indispensable to enable states to uphold this responsibility in a context distinguished by the expansion of financial, economic and human interactions.

(1) The **United Nations** offers a universal framework to mobilize all states in the combat against terrorism at the political level. This combat is often seen as a concern of northern countries. As of early 2006, however, global terrorism had caused more casualties in the countries of the south than in those of the north.

The United Nations also provides a universal framework to set up binding legal norms. UN action in this area has two components. One is the thirteen conventions concluded under the auspices of the UN or its agencies between 1960 and 2005. The other consists of the resolutions the Security Council took under Chapter VII of the Charter.

(1) HERACLES conducted reconnaissance, supply, transport and combat missions, as well as offensive air operations, conducted by the air force and naval aviation, for example, in direct support of American ground troops in Operation Anaconda in spring 2002. France has also deployed a carrier battle group around the nuclear aircraft carrier *Charles de Gaulle* for more than 7 months .

(2) Chapter VII of the UN Charter authorizes the Security Council in order to maintain or restore international peace and security to take compulsory measures that States are obliged to follow.

The 13 UN Anti-Terrorism Conventions

Thirteen UN anti-terrorism conventions were negotiated between 1963 and 2005. They define criminal offences that Member States must incorporate into their internal legal systems and rules of judicial competence, extradition and mutual legal assistance that apply to these offences, according to the principle of 'extradite or judge.'

These conventions remain imperfectly applied: many States have still not signed them; others that have signed them have nonetheless not implemented them.

France is already a party to 12 conventions and has started ratification procedures regarding the International Convention for the Suppression of Acts of Nuclear Terrorism.

- *Convention on Offences and Certain Other Acts Committed on Board Aircraft (1963)*
- *Convention for the Suppression of Unlawful Seizure of Aircraft (1970)*
- *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971)*
- *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (1988)*
- *Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents (1973)*
- *International Convention Against the Taking of Hostages (1979)*
- *Convention on the Physical Protection of Nuclear Material (1980)*
- *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (1988)*
- *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (1988)*
- *Convention on the Marking of Plastic Explosives for the Purpose of Detection (1991)*
- *International Convention for the Suppression of Terrorist Bombings (1997)*
- *International Convention for the Suppression of the Financing of Terrorism (1999)*
- *International Convention for the Suppression of Acts of Nuclear Terrorism (2005)*

The UN Security Council has several times deemed international terrorism to be a 'threat to international peace and security,' leading it to oblige States to take binding measures under Chapter VII of the Charter. It thus imposed sanctions on Libya, Sudan and Afghanistan, three

States accused of having conducted or ordered acts of terrorism or of having served as a haven for terrorists.

The Security Council extended the sanctions regime against the Taliban under Resolution 1267 to al Qaeda. In addition to the obligation of freezing financial assets and resources,[1] this mechanism also entails obligations designed to prevent the entry, transit of individuals as well as the provision of weapons.

More generally, under Resolution 1373 (adopted on 28 September 2001), States are also required to 'deny safe haven to those who finance, plan, support or commit terrorist acts.' This Resolution created a Counter-Terrorism Committee (CTC) tasked with monitoring the robustness of Member States' counter-terrorism legislation and to help those States to fulfil their responsibilities.

(2) The **European Union's** build-up in the area of counter-terrorism is being pursued.

Well underway after the 11 September attacks, this evolution was accelerated after the Madrid attacks of March 2004. In June 2004 the European Union adopted an Action Plan on Combating Terrorism, which contains seven strategic objectives.

The European Union's Seven Strategic Objectives in the Fight against Terrorism

1 – To deepen the international consensus and enhance international efforts to combat terrorism.

2 – To reduce the access of terrorists to financial and other economic resources.

3 – To maximize capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and prevent terrorist attacks.

4 – To protect the security of international transport and ensure effective systems of border control.

5 – To enhance the capability of the European Union and of Member States to deal with the consequences of a terrorist attack.

6 – To address the factors which contribute to support for, and recruitment into, terrorism.

7 – To target actions under EU external relations toward priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.

(1) See page 57 on this point.

The seven objectives are broken down into nearly 100 concrete actions. To strengthen the strategic and political coherence of these objectives and actions, the European Union in 2005 grouped them under four main categories in the context of a global strategy: ensure **prevention**, especially by preventing the recruitment of new terrorists; ensure better **protection** of potential targets; **disrupt** existing networks; improve our **reaction** and consequence management capabilities in case of terrorist attacks.

Despite this progress, the effort in the strategic domain must be continued. It is necessary to consolidate a more comprehensive approach that better integrates the different components of EU counter-terrorism action. In light of this, the European Council decided to name a counter-terrorism coordinator following the March 2004 Madrid attacks. This coordinator plays a useful mobilizing role within the EU structures and among the Member States.

(3) The **G8 and NATO** also play a useful role in the area of **information sharing** on the prevention of the threat.

Since 1996, at France's instigation, the members of the G8 put the combat against threats represented by organized crime, as well as by terrorism, at the heart of their priorities. Among the actions of the G8 in the area of counter-terrorism, the most important include those that have to do with the security of civil aviation, particularly through biometrics and the fight against the proliferation of ground-to-air missiles ('man-portable air-defence systems', or MANPADS); the traceability of terrorist assets; and the fight against documents fraud.

NATO has also undergone an effort to adapt to better combat terrorism in the military domain, which is precisely its area of competence. It can thus help in the protection of specific events (such as the Athens Olympics, for example). NATO is also doing useful work in the area of chemical, biological, radiological and nuclear (CBRN) defence.

Preventing Terrorist Access to Weapons of Mass Destruction

Senior members of the al Qaeda movement have demonstrated the will to carry out attacks with chemical, biological, radiological or nuclear weapons. The international community has long focused on the prevention of CBRN terrorism. The way to do this is primarily through the fight against the proliferation of weapons of mass destruction (WMD) and their means of delivery.

(1) The role of the **European Union** in the fight against proliferation has been substantially strengthened by the December 2003 European Council's adoption of the EU strategy against the proliferation of weapons of mass destruction. The heads of state and government underscored in this document the risk of seeing terrorists acquire such weapons and expressed the desire to counter this risk.

(2) The goal of the work done in the context of the **G8** is to prevent terrorists and those who support them from gaining access to weapons

of mass destruction and the materials that would make it possible to build them. For the most part this is a matter of traditional control and security measures in the area of non-proliferation.

In particular, the G8 leaders launched in June 2002 the Global Partnership against the Spread of Weapons and Materials of Mass Destruction. This partnership between Russia and the seven other members of the G8 seeks to reduce the threat stemming from the continued existence of non-conventional (nuclear, biological and chemical) weapons arsenals in the former Soviet Union. The G8 countries committed to devote up to $20 billion over the next ten years to support projects in this area. France participates actively in this partnership. It must continue the effort begun while ensuring that it remains focused on the fight against proliferation and the risk of non-conventional weapons getting diverted for terrorist use.

(3) The **United Nations** took a critical step in April 2004 with the adoption of Security Council Resolution 1540, which seeks to prevent the risk of terrorists acquiring WMD and their means of delivery. This text is particularly important as the Council was acting in the framework of Chapter VII of the Charter and can ask States to take specific measures to comply with their obligations.

The **International Atomic Energy Agency** (IAEA) plays a central role in the security of radioactive materials. This issue remains a major concern, particularly because of the absence of effective control over radioactive materials with regard to the terrorist threat. France, in the context of the G8, played a driving role in launching this initiative. We are carefully following its evolution.

(4) The **Proliferation Security Initiative**[1] (PSI) focuses on intercepting shipments of weapons of mass destruction, their means of delivery, and equipment and materials used in their construction, being sent to or from countries or entities of concern. This initiative is still being developed. It has already led to concrete interception operations and enabled the development of useful operational contacts in case of a crisis.

The fact that numerous international or regional organizations have adopted specific counter-terrorism measures and action plans is positive. It demonstrates that the threat and the need to counter it collectively are being taken seriously. In the area of the fight against terrorism as in other areas, however, international cooperation is a means, not an end. It must be based on a threefold goal of effectiveness, complementarity, and subsidiarity.

With this in mind, our country must reinforce the pre-eminent role of the United Nations, as a creator of political consensus and as a source of legitimacy and normative power. It must reinforce the action of the European Union.

(1) Launched in March 2003 by the U.S. government. As of early 2006 PSI involved more than 65 countries. At the Paris meeting on 4 September 2003, the 11 'core group' countries (a group that includes France) put forward a 'Statement of Interdiction Principles,' which sets forth the main principles of PSI. This initiative is within the framework of international law and national laws and its goal is to bring together all States that are combating proliferation.

Chapter 2

Improving our System

Protecting the Population

Consolidating Planning to Maintain Vigilance

To deal with the full range of threats, our country is constantly adapting its forecasting and deterrence tools. The spearhead of this strategy is the VIGIPIRATE plan, created in October 1981 and well known to our citizens. It has a dual objective: protect France's population, infrastructure and institutions and prepare responses in case of attack.

The most recent version of VIGIPIRATE, in force since March 2003, is based on the premise that the terrorist threat must henceforth be considered to be permanent. It thus defines a baseline of measures that are always in force, even in the absence of threat indications. The plan then has four levels of alert, which are made public. The lowest level (yellow) is that of a vague threat. The measures that are then put in place must make it possible to very rapidly move up to the higher levels, which are orange and red. The highest level (scarlet) seeks to prevent an immediate risk of major attacks.

The VIGIPIRATE plan's general objective is to deter and prevent terrorism. It is complemented by the series of 'PIRATE' intervention plans, each of which is tailored to a particular risk (PIRATOME, PIRATOX, BIOTOX, PIRANET, PIRATE-MER, PIRATAIR-INTRUSAIR, PIRATE-EXT).

These plans are constantly updated in response to the evolution of the threats and risks faced by our country. They serve as a matrix for carrying out exercises at the local level (first responders and local officials), the national level (central administrations) and the 'senior' level (involving the participation of ministers or their cabinets).

VIGIPIRATE

VIGIPIRATE, the governmental plan for vigilance, prevention and protection, defines a decision-making process and a list of operational measures.

On the basis of a threat evaluation, a level of alert is established by the Prime Minister, after consultation with the President of the Republic. Each of the four alert levels has a security objective associated with it, which makes it possible to put in place measures to deal with the full range of risks. For example, the plan envisages a military presence in railway stations and airports, enhanced protection for schools, and searches at the entrances of department stores. Such measures are activated by decision of the Prime Minister depending on the alert level and the sectors that are under threat. Local plans set out in detail the practical ways in which local representatives of the State (prefects), local authorities and economic operators will put the measures into place.

The 'PIRATE' Family of Plans

The 'PIRATE' intervention plans are launched by the Prime Minister in case of a specific threat or terrorist attack using a given means of aggression (PIRATOX for a toxic chemical product, BIOTOX for a biological pathogen agent, PIRATOME for nuclear or radiological material, PIRANET for an attack on information systems) or in case of an attack taking place in a particular area (PIRATAIR-INTRUSAIR against terrorism related to aircraft, PIRATE-MER against maritime terrorism, PIRATE-EXT in case of a threat or attack against French nationals or interests abroad). These plans define crisis-management and information-processing structures as well as the actions that should be taken by civil and military authorities (including special anti-terrorist units and special forces).

All the governmental plans must be continually adapted and updated depending on the evolution of the threats and risks our country faces. They must also be extended through local implementation plans.

The Contribution of Video-Surveillance

In our country, approximately 300,000 video-surveillance cameras are installed in public spaces. In some neighbouring countries, there are several million.[1] Beyond their decisive contribution to resolving criminal investigations,[2] these cameras – installed in public areas and sensitive locations – contribute to the prevention of terrorism.

Eleven years after the adoption of the law of 21 January 1995 which regulates video-surveillance in our country, the counter-terrorism law of 23 January 2006 extended the coverage of public places and thoroughfares (including businesses, transport, offices of airline companies, certain religious sites, etc.) to protect them from the terrorist threat. We must pair the development of video-surveillance with guarantees of the respect for basic freedoms. The installation of video systems requires administrative authorization with time limits and periodic reviews to ensure that the basis for the systems' installation is still appropriate.

The existing video-surveillance systems are effective in preventing burglaries and threats to people and goods. The camera circuits make it possible to identify the first indications of the offence; an intervention team can be immediately sent to prevent it from being committed.

Traditional video-surveillance systems, however, do not make it possible to preventively spot terrorists, who do not normally burglarize. To prevent terrorist attacks more effectively, we need video-detection networks able to find explosive devices and suspicious behaviour. The qualitative jump from one type of network to another requires the development of automatic image analysis techniques. These techniques, which are starting to come onto the market, are able to identify an abandoned package or even suspect behaviour in a tide of images that goes beyond the human capacity for observation.

Ensuring Transport Safety

All modes of transport of people and goods have been hit by terrorism: oil tankers and cruise ships, ferries, commercial planes, public transports, road and railway networks.

Public transport is by nature an easy and ‘profitable’ target for terrorism. Protecting it has been a priority since the 11 September 2001 attacks.

Air Transport

Methods for ensuring air transport security have been fundamentally rethought since the 11 September 2001 attacks. It is no longer

(1) This is, of course, largely because of the high level of activity among private operators.
(2) A remarkable example of this was the precedent set by the British in the July 2005 London attacks.

only a matter of preventing hijackings and passenger hostage-taking to satisfy political claims, but also of preventing the boarding of any passenger who might destroy the plane in the air or who might take control of it to fly it into a target. At the same time, the risk of loading dangerous cargo has been re-evaluated.

Confronted by such threats, security measures can only be defined in an international framework. For Member States of the European Union, this process was harmonized by an EU Regulation of 16 December 2002, which required modifications of France's civil aviation code.

Security measures for air navigation and air transport in France have three components: ground measures, boarding measures, and in-flight measures. They are gradually called into action by the VIGIPIRATE plan and the PIRATAIR-INTRUSAIR intervention plan depending on the evaluation of the threat.

On the ground, we had to put in place a security system based on airport architecture originally designed to facilitate access to the planes. There are two areas: the public area accessible to all, including airport workers, passengers and those accompanying them; and the restricted area accessible only to those authorized to enter it – airport workers with identification or previously verified ticket holders. Everything that enters into the restricted area (people, checked baggage, carry-on baggage, food) is checked for dangerous products (explosives, toxic chemicals, radiological materials). These checks are carried out by x-ray machines, metal detectors, and explosive traces detectors. Similar checks take place on the runways to prevent banned objects from being loaded onto planes.

On board the plane, the most notable new measures have been the reinforcement of the flight deck doors and the requirement to install encoded alert systems to prevent intrusions. Some flights take along armed guards.

The flight itself is subject to systematic tracking that constantly compares its flight plan with its actual path.

The United States and Forward Territorial Defence

The United States has installed a 'forward line of defence' of its territory. The airlines that fly to the United States must verify that their passengers are not on a list of individuals banned from flying into the country (the 'no fly list'.)

If the identification is made before take-off, the passenger is not allowed to board. If the passenger is identified in flight, the plane is diverted. The 'no fly list' is updated continuously by U.S. security agencies based on a variety of sources and according to their own criteria.

While Europe has not taken such a step, some countries have increased security on certain flights though the discreet presence of armed sky marshals on board planes flying sensitive routes. Moreover, access to airline company data for counter-terrorism purposes will reinforce the security of European territory.

Freight transport by air has not been forgotten. Checks are carried out according to the same principles as for passenger transport, with a variation that allows for a secure logistical chain starting with the putting together of packages, and only accredited individuals. 'Approved packagers' prepare consignments free of goods that are banned from secure areas, 'entitled agents' take them all the way to the loading area, and airlines ensure that the security procedures have been respected.

States and airlines are well aware of the risks of MANPAD ground-to-air missiles being used against commercial airlines. The performance level, number and dispersion of these arms make them serious threats to civil aviation. Precautions have been taken around our airports. To complement the surveillance policy undertaken by the relevant international authorities, the search and destruction of these arms must remain a priority for the intelligence and security agencies.

Ground Transport

After the 11 September 2001 terrorist attacks with hijacked airplanes, the two most deadly attacks taking place in the West were those of Madrid in March 2004 and London in July 2005, both carried out with explosives in public transport, just as the Paris attacks of 1995 and 1996 were.

The public transport of people, whether above or under ground, presents favourable conditions for terrorists: high concentrations of people in limited spaces; small risk of being caught while preparing and executing the attacks; high numbers of victims; large psychological effects in public opinion.

The detection of explosives is a major issue in the prevention of the terrorist threat to transport networks. It is made difficult by the growing use of techniques to conceal explosives and the wide variety of materials used.

The other issue is the detection by a network of detectors of biological, radiological and chemical substances. The goal is to limit the public's contact with these agents and to provide necessary care to possible victims. Detection also makes it possible to circumscribe precisely the contaminated zone and to move forward with decontamination. Detection is critical when the agent used goes unnoticed until the first illnesses become apparent.

Extensive feasibility studies of attack scenarios have been conducted. They have resulted in the development of programmes to

strengthen transport infrastructure security broadly speaking, such as train or automobile tunnels or bridges, by equipping them with means for detection, alert, traffic interruption and fast emergency services. Security issues are now taken into account in the conception phase of major construction projects. The idea of taking into account the objective of security against natural disasters or threats of malicious intent or terrorism should be broadened to include all transport infrastructures.

The protection of cities from the risks associated with the transport of explosive or toxic materials, by rail or truck, is a concern for all countries. It is most complicated in Europe's highly populated regions. Particular precautions are taken regarding the transport of certain dangerous materials, such as nuclear materials. Preventive efforts should be focused on infrastructure (by managing transport routes for dangerous products) and on the enforcement of security regulations.

Maritime Transport

Maritime transport has been an area of sustained attention for twenty years (in particular following the hostage-taking on board the ship *Achille Lauro* in October 1985).

After the 11 September 2001 attacks, the United States took unilateral initiatives in the area of container security (with the adoption of the Container Security Initiative, CSI). France preferred that this problem also be dealt with through international organizations. The International Maritime Organization (IMO) took up the issue and in November 2002 began work that led to the establishment of an International Ship and Port Facility Security Code (known as ISPS code), which came into effect on 1 July 2004.

The ISPS Code requires that all commercial ships making international journeys have a certified security plan. It also calls for the evaluation of port facility security. To ensure that the international norms are consistent with the VIGIPIRATE plan and the PIRATE-MER intervention plan, an inter-ministerial port and maritime security doctrine was adopted in October 2005.[1] This doctrine is based on an analysis of the threat and a hierarchy of responses. It establishes procedures for surveillance of coastal waters and ports, passenger and vehicle checks on ferries, and cargo verification.

A policy of support to states in difficulty could complement the unilateral checks. In the framework of the IMO and the World Customs Organization (WCO), universal norms should be promoted, whether through the exchange of customs information, modern methods of inspections of containers at a distance, or techniques that make it possible to keep their seals intact.

(1) The interministerial doctrine is based on the maritime safeguard concept applied by the navy.

Protecting French Nationals Abroad

French nationals who live abroad and those who travel have also been struck by terrorism.

The Ministry of Foreign Affairs (the Directorate for French Nationals Abroad and Foreign Nationals in France, together with diplomatic posts) is responsible for the warnings or recommendations posted on the website giving guidance to travellers (http://www.diplomatie.gouv.fr/voyageurs), the content of which is harmonized, to the extent possible, with that of our primary partners. It strengthens, when necessary, the security measures protecting the French communities that live abroad. This work is conducted in coordination with the intelligence, analysis or intervention structures of the other ministries, including the DGSE, the Ministry of Defence's Planning and Operations Centre, the international technical cooperation department of the National Police, the operational crisis management centres under the Interior Ministry (COGIC, COB and CROGEND[1]) and the equivalent structures of our foreign partners.

At the request of the chief of staff of the Minister of Foreign Affairs, an 'operational crisis cell' is opened under the authority of the Ambassador to organize and coordinate the crisis response locally, and to answer telephone calls from our fellow citizens. This structure is open to liaison agents from concerned countries at the origin of the crisis. It establishes contacts with active crisis cells in these countries. Generally, mobile teams made up of agents from the ministry and other professionals (doctors, civil security agents, investigators) are sent to the place of the crisis and coordinate on the ground with the equivalent teams of our partners. Joint missions may be organized.

At the European level, the consular affairs working group of the Council has reoriented its priorities, which are now less focused on traditional consular matters and more on security issues. This group has set forth guidelines on security cooperation of EU nationals in third countries. They must now define common operational plans for evacuation of EU nationals in the framework of the Common Foreign and Security Policy (CFSP), along the lines of the EVAC06 exercise planned for the first quarter of 2006, which relates to the evacuation of 8,000 European nationals in a country 10,000 kilometers away from the EU.

(1) COGIC is the *Centre Opérationnel de Gestion Interministérielle des Crises* or Inter-Ministerial Operational Crisis Management Centre; COB is the *Centre Opérationnel Beauvau* or Beauvau Operational Centre; CROGEND is the *Centre de renseignement et d'opérations de la gendarmerie nationale* or National Gendarmerie Intelligence and Operations Centre.

Protecting Territorial Integrity

Preserving Critical Infrastructure

Following the logic of its social and political destabilization efforts, global terrorism will seek to strike targets of high economic and ecological value, especially as the partial or total destruction of certain infrastructures can also cause massive casualties.

As the terrorists prefer to strike where they can as opposed to where they would like to, the hardening of potential targets can lead them to abandon their projects or reduce the effect of their actions. It is thus indispensable to identify critical infrastructures and to have a security policy for them involving the firms of the most sensitive sectors.

This is what the Government's recent reform seeks to do. The reform is based on the arrangements of the defence code, which make public or private operators of vital infrastructures responsible for internal protection measures against 'all possible threats, notably threats of a terrorist nature.'

The top priorities are those activities that are indispensable to the public's essential needs and the maintenance of the security and defence capabilities of the country: food, water, energy, transport, financial institutions, information and communications systems, and command and decision centres.

Working closely with those responsible, the State will establish and keep updated a national security directive for each of these sectors. This directive will define the nature of the threats against which protection is necessary, the security objectives and the combination of the specific plans prepared by each operator (the 'operator security plans') with the VIGIPIRATE plan.

Basing their action on each directive, the main companies in each sector will put into action an 'in depth defence' policy required by the protection plans. It will identify their sensitive installations and include both concrete physical measures (guards, secure entrances, locks, surveillance cameras, toxic product detectors, alarms, rescue tools) and organizational measures (more thorough background checks during the hiring process, closer watch over visitors, checks on deliveries, supply chain monitoring, alternative sources).

What is being done on the national level is consistent with efforts on the EU level to protect against all risks to vital infrastructures, especially those functions whose shutdown or malfunction would have major consequences for several countries.

Protecting Sensitive Computer Systems

Information systems are the nerve centres for most organizations. They are therefore a priority target for those who want to destabilize or paralyse the country's functioning.

Yet these networks, whether public or private, do not operate in isolation. Whatever their degree of protection, they are normally open to the outside world, whether through links to the Internet or because of the expanded use of remote maintenance. In addition, the widespread use of standard commercial hardware or software such as Windows or Unix makes the systems more vulnerable to the extent that hackers can do widespread damage with a single attack.

On the technical level, the terrorist threat is not unique. 'Cyberterrorists' would attack information networks just like regular 'cybercriminals.' Attackers could use the tools developed by hackers. The most foreseeable threats are cascade attacks based on malicious computer codes sent out on the web or hidden in an already infected website, which would then be duplicated once introduced in the system. The most insidious threat would consist of attacks targeted by malicious software and sent out in very limited numbers (thus keeping them unknown to anti-virus software providers) and would act as sleeper cells until their simultaneous activation.

The goal of these attacks could be the disruption of vital national systems. It could also be to disorganize these systems at the same time as a terrorist attack, in order to interfere with rescue operations. Nor can more mundane motivations be excluded, such as diverting funds to finance terrorist activities.

The defences are well known. They include systematic updating of software; the application of strict rules for authenticating individuals allowed onto the network; the increasingly general use of cryptography; the installation of firewalls, anti-virus software, and intrusion-detection tools; the use of security certification tools; and in the most critical cases, the isolation of internet networks.

The application of these defences, however, must still be improved.

The State has taken measures to deal with threats to its own information systems. Improving protection of the administration against information attacks is the job of the Permanent Secretariat for National Defence (*Secrétariat général de la défense nationale*, SGDN), whose role is to monitor, warn and intervene in case of an attack on a public administration. A security reinforcement plan for information systems has been developed, with four main objectives: securing the communications of high officials; securing government information systems; putting in place operational capabilities for responding to information attacks; the incorporation of this security policy in a European framework. The efforts (both in terms of means and sensitizing users) must be pursued in the area of prevention in order to reinforce the level of security of government information systems.

Major private companies have not remained passive in this area. Yet there are two major obstacles to broader action. Some business leaders still underestimate the level of threat their companies face. Expenses for information security systems do not have any visible return. They are not always considered to be investments, even if their effect is to preserve the physical capital – and more generally the other assets – of the company.

These obstacles must be overcome through action by experts, the media, and information security professionals, led by the government, to raise business leaders' awareness and coordinate their efforts. A ‘best practices’ guide should be developed for the most vulnerable businesses (small and medium-sized enterprises).

Chapter 3

Strengthening our Crisis Management Capabilities

Improving our Operational Capabilities

The recently updated 'PIRATE' and ORSEC intervention plans are comprehensive tools for managing a terrorist crisis. Their coordination must still be improved

The governmental action plans of the PIRATE family of plans[1] include measures of alert, organization, protection and neutralization of the threat broken down according to different levels of defence and in some cases to the departmental level.[2] They are mostly devoted to protection.

(1) For a description of these plans, see p. 68.
(2) In the area of crisis management and emergency relief organization, there is, within the State, a level of administrative responsibilities above the Department known as the 'defence zone.' In case of an attack large enough to surpass the departmental level, it is at this level that an event is managed and where operational coordination of civilian and military means takes place. There are seven defence zones in metropolitan France.

The ORSEC[1] plan is triggered by the departmental prefect in case of a major event requiring the organization of emergency relief for the population. For a long time, this plan was only viewed from the operational point of view, for which it was the final tool in a crisis situation. The new ORSEC plan[2] maintains this essential aspect, which has been proven to work, but places it into a broader context of the general protection of people and goods. It is now, under the authority of the prefect, the central element of the system of organization and intervention that makes it possible to deal with the consequences of any kind of major event, including a large-scale terrorist attack.

The ORSEC operational manual addresses the entire range of crisis-management needs: the advance surveying and analysis of risks and consequences of threats common to all agencies; an operational system, at the heart of the plan, which calls for a single organization to manage major events; preparation and training phases necessary to operational implementation.

The 'PIRATE' and ORSEC plans thus cover the full spectrum of elements involved in dealing with a terrorist crisis: the former covers the threat and the second organizes the aid for the population. Their coordination, however, must be improved.

Overall, the 'PIRATE' plans deal with terrorist attacks in the air, on the sea, or which use unconventional means (chemical, biological, radiological or nuclear). They must be complemented by a governmental intervention plan focused on a major conventional attack or on a rapid series of attacks. The standard operating procedures designated by the 'PIRATE' plans and the risk analysis of the ORSEC plans must be made perfectly consistent with each other in every detail.

It is essential that we conduct regular exercises to validate the working hypotheses of the plans, to test their implementation and to improve our response capacities.

Our Crisis Management Assets and Organization Must be Further Strengthened

Organization

We must tighten the network of operational and crisis centres of the various ministries.

(1) On the national level, in 2006, some ministries rely on operational centres to provide 24-hour service seven days per week.

For internal security matters, the Interior Ministry relies on the *Service de Veille Opérationelle de la Police Nationale* (Operational Watch of the National Police, SVOPN) and the *Centre de Renseignement et*

(1) ORSEC stands for *ORganization des SECours* or Emergency Relief Organization.
(2) Resulting from decree no. 2005-1157 of 13 September 2005.

d'Opérations de la Gendarmerie Nationale (National Gendarmerie Intelligence and Operations Centre, CROGEND). It also has the *Centre Opérationnel de Gestion Interministérielle des Crises* (Inter-Ministerial Operational Crisis Management Centre, COGIC) for civil security. The Defence Ministry relies on the *Centre de Planification et de Conduite des Opérations* (Planning and Operations Execution Centre, CPCO) and the air and maritime execution centres. Someone is continuously on duty at the Ministry of Foreign Affairs.

Outside of normal business hours, other ministries resort to different forms of coverage, with activation and reaction times tailored to the types of crises they may face.

This set of arrangements must be improved in two ways. The secure networks for transmitting messages and information must be unified, and a common portal for crisis management – to which on-duty agents are continuously connected – must be created. Reaction times must also be reduced.

The next stage will be the creation of a secure, governmental intranet that allows the authorities to exchange information, confidential or not, at high speed. Such a network, under the name Isis, will progressively be deployed in early 2006.

(2) At the regional level, the crisis management system is the responsibility of prefects, and in Paris of the police prefect. This clear and rational organization takes advantage of the prefects' inter-ministerial prerogatives and long experience in dealing with emergency situations. Over the past few years, the responsibilities and assets of the prefects in the defence zones have been strengthened in order to facilitate the coordination and pooling of intervention capabilities.

Coordination

At the national level, the Prime Minister directs governmental action. He designates the minister or ministers who ensure the operational execution of governmental action and who rely on ad hoc cells or operational centres to do so.

To reinforce the effectiveness of this system, and in particular to facilitate the exchange of information and coordination in case of a crisis involving numerous ministries, we must develop interoperability among crisis centres by developing the capacity to use compatible, shared and secure communications and management tools.

Alerting the Population

The State has the duty to its citizens to alert them in case of an imminent threat that could affect a neighbourhood, a city or a region, in order to shelter the population in the best possible conditions.

During the Cold War, all industrialized States built systems to manage the consequences of potential large-scale military hostilities: the national alert network (*réseau national d'alerte*, RNA) that exists in

France is largely derived from this period. Consisting of a network of sirens, the RNA is now largely obsolete. The sirens only carry a basic, undifferentiated message of alert, badly suited for certain attack scenarios whose effects might be vague or delayed.

In certain attack scenarios, the siren network could nonetheless remain an effective means of quick alert, getting people to stay at home or turn on their radios. This observation has led to new interest for local siren networks, often managed by towns or businesses.

Public services or private companies have put alert systems in place in case of risks to security or health. These systems often use modern calling techniques, corresponding to new communication habits: emails; voice or text messages on mobile phones; recourse to telephones or automated call centres.

Information centres investigate the causes of the events, advise people affected by the alert, and respond to concerns by bringing in specialists. Visual electronic message services, in cities or on the roads (accidents, traffic jams, weather risks...) make possible the quick diffusion of instantly updated messages.

It is by using all of these different tools simultaneously that public authorities must alert their populations. The State can now sign agreements with television and radio stations to pass on the alerts.[1] The expansion of means of communication (such as fixed and portable telephones and the Internet) provides the opportunity to complete the coverage of all of France. General conditions for using telephone and email services must be developed to enable the State to send messages to all mobile phones in an area that has such service in a given geographical zone and to the computers operating in this zone.

Assets on the Ground

If an attack cannot be prevented, it is essential that security and emergency forces be able to act even if the conditions in which they must do so are very difficult.

(1) Maintaining Effective Means of Communication in All Circumstances

The first priority must be improvement of the interoperability between the different forces and agencies involved (Paris prosecutor's office, police, gendarmerie, armed forces, civil security, fire departments) so that they can communicate whatever the circumstances. Interoperability must be sought between equipment, transmission system, software and operational doctrines, including at the European level. Ultimately, the

(1) See decree no. 2005-1269 of 12 October 2005 concerning the national alert code and the obligations of radio and television stations as well as those who control all other means of public communication. This decree was taken pursuant to Article 8 of civil security modernization law no. 2004-811 of 13 August 2004.

means of communication used by the security forces must include the transmission of still images and video.

Force mobility is essential. We thus need to ensure that the systems chosen can operate in areas with no infrastructure or where the infrastructure might be damaged. We must arrange for crisis operations centres that are easily transportable in the affected areas. The military's fixed and mobile means of communications and command may be used if that proves necessary.

In the area of telecommunications, the priority for security forces must be to always have immediate access to the networks in all circumstances.

The ACROPOL police network and the RUBIS gendarmerie network ensure that local authorities have a system to communicate with the security forces. In some cases, however, access to the civilian networks is the only possible means of communication. We must thus explore the possibility of putting into place a system for giving priority to restoring communication of certain public actors in case of a crisis.

(2) Equipping, Training, and Preparing Through Use of Crisis Simulations

Each ministry must equip its own agencies with protective suits, means of transport, and emergency relief equipment. The orientation and programme law for internal security for 2002-07 and the military programme law for 2003-08 enabled the interior and defence ministries to modernize the assets of the police and the military.

Specialized civil and military units have developed solid expertise in the field of terrorism. The police forces (*Recherche, Assistance, Intervention, Dissuasion*, Search, Assistance, Intervention and Deterrence Unit RAID, potentially assisted by Intervention Groups of the National Police) and the gendarmerie forces (units with the security and intervention group GSIGN, including the *Groupe d'intervention de la gendarmerie nationale* (Gendarmerie nationale intervention unit, GIGN) and the parachute squadron) train daily to be able to deal with terrorism contingencies, notably hostage taking and hijacking of airplanes or ships. If the scope of the attack requires it – in case of a large-scale hostage-taking, for example – military special forces will help, under a unified command.[1]

It is also necessary to pursue the development of crisis management software, which is indispensable to optimise the choices of decision-makers working under pressure and in emergency situations – on issues like projecting the number of potential victims and the degree to which the effects of the attack will spread, and modelling and allocating resources.

(1) Since 1 February 2006, a helicopter squadron is dedicated to the transport of counter-terrorist forces.

(3) Knowing How to Handle the Long-Term Consequences of a CBRN Attack.

In case of CBRN crises, the civil authorities have at their disposal a wide range of analysis, emergency relief, and treatment capabilities: laboratories in the BIOTOX-PIRATOX network, SAMU (*Service d'aide médicale urgente* or Emergency Medical Assistance Services) units with CBRN equipment, chemical or radiological intervention cells of the departmental fire and emergency services (SDIS), decontamination processes, national reinforcements from the *unités d'instruction et d'intervention de la sécurité civile* (Civil Security Intervention and Training Units, or UIISC), and hospitals with special capabilities enhanced by the measures of the BLANC[1] plans. The Central Inter-Ministerial Technological Intervention Unit (*détachement central interministériel d'intervention technologique*, or DCI[2]) can be mobilized at any time.

For identifying and characterizing the most dangerous biological contaminants, we have a system of laboratories with different capabilities that are integrated across the defence zones of the national territory. This is the network of BIOTOX/PIRATOX laboratories. For the most pathological strains of biological agent, for which there is no effective curative treatment or systematic protection of the public, our capacities at the 'P4' level must be tailored to make it possible to react in case of an emergency and enhanced by mobile assets.[3]

If necessary, the Ministry of Defence can also make available its decontamination, treatment and rehabilitation capabilities for the affected areas. This includes research centres, army training hospitals and field hospitals (some of which have an NBC-protected surgical division), the NBC defence regiment, and certain engineering regiments.

To Deal with Crisis Situations, the Range of Legal Tools is Broad but Must be Further Enhanced

In case of terrorist attacks whose scope would seriously threaten the country, the state authorities can use exceptional legal means to neutralize the perpetrators and protect the population.

(1) The BLANC plan sets forth measures to be taken gradually in each hospital to temporarily enhance its ability to receive and hospitalize patients, including recalling of personnel, transfers of patients to other hospitals, delaying non-urgent treatment. Particular measures are foreseen for certain contagious diseases and for the victims of chemical or radiological attacks.

(2) The DCI, under the direction of the head of RAID since its inception, is responsible for locating, identifying, diagnosing and neutralizing improvised chemical, biological, radiological and nuclear devices. It brings together specialized units from different ministries.

(3) The name 'P4' (or rather biosafety level 4) is a reference to the highest level of confinement necessary to protect the environment and people working on highly hazardous pathogenic micro-organisms (those that can be transmitted among humans and for which there is no effective treatment.)

To respond to very serious situations, our law provides for three regimes whose consequences for civil liberties are of growing importance.

(1) Set out in the law of 3 April 1955, the state of emergency applies in the case of imminent danger resulting from serious infringements on public order.[1] The declaration of a state of emergency gives prefects the power to ban the movement of people and vehicles and to implement protection or security zones where individuals' activities are regulated. It also makes it possible to order house searches during the day or at night.

(2) Foreseen by Article 36 of the Constitution, the state of siege, whose declaration transfers the maintenance of order from the civilian authorities to military authorities, can be decreed in case of imminent danger resulting in particular from an 'armed insurrection.' The application of this extraordinary regime, whose origins go back to the laws of 9 August 1849 and 3 April 1878,[2] would seem to be poorly suited to dealing with the case of a traditional terrorist attack. It could, on the other hand, be conceivable in the case of a major terrorist attack with non-conventional means.

(3) Article 16 of the Constitution constitutes the final extraordinary legal regime for dealing with extremely serious situations.[3] This system legally gives the President of the Republic complete power for a limited duration.

These different regimes were established in particular historical circumstances. None of them was specifically conceived for the fight against terrorism. They would certainly make it possible to respond to a situation of exceptional seriousness provoked by major terrorist attacks.

The elaboration of a legal regime more specifically tailored to the types of terrorist crisis situations that the country risks facing nonetheless deserves deeper study.

(1) The state of emergency was declared in 1955 in the French departments of Algeria, then in 1958 in all of France, lasting until 31 May 1963. More recently, the state of emergency was applied in New Caledonia in 1985, and in all of France by the decree of 8 November 2005, which was then extended for three months by law no. 2005-1425 of 18 November 2005 and finally cut back to 4 January 2006 by decree no. 2006 of 2 and 3 January 2006.

(2) It is today codified in Articles L. 2121-1 to L. 2121-8 of the defence code.

(3) Article 16 was applied only once, on 23 April 1961, by General de Gaulle following the 'Generals Putsch' in Algiers.

Establishing a Public Communications Doctrine

The High Cost of Poor Communication

Any failures in the area of public communication when confronting terrorism can carry a high price in the short and long term.

During the crisis itself – for example in case of a mistaken attribution of responsibility for attacks – the damage in public opinion can be immediate and considerable: loss of public confidence and, in some cases, difficulty finding solid bases on which to pursue the investigation.

The consequences of poor public communication are even greater in the months and years that follow. Indeed, the way governments communicate to the public after terrorist attacks or large-scale natural or industrial disasters leaves deep and lasting marks on the collective memory, because of the climate in which the events are experienced.[1] This type of memory thus has an immediate impact on the likelihood that official pronouncements will be believed, or even heard, in case of a similar event later on.

Strengths and Weaknesses of the Current System

A System Enriched Through Experience

Our country has had a number of opportunities to test the communications systems for managing emergency situations which were not caused by terrorist attacks: floods, forest fires, the December 1999 storms, and the heat-wave of summer 2003. We already have concepts and experience that can, in part, be transposed to communications in case of a terrorist attack.

We also have concrete experience in the area of public communications after the perpetration of a terrorist attack. This, however, is limited, as France has not suffered an attack that caused more than 8 deaths on its territory in one day since the end of Algerian War. In terms of public communication, we have not had to manage the effect of results like those of the most deadly attacks on European territory (nearly 200 deaths in Madrid in March 2004; more than 50 deaths in London in July 2005). We therefore do not have direct national experience in public communications on very deadly terrorist attacks.

Similarly, France has not in the past had to manage extended or large-scale terrorist campaigns. From 1965-2005, thus over forty years, attacks of all sorts killed 192 people on French soil. This figure must be compared to more than 800 victims of ETA in Spain during the same

(1) Thus 20 years after the Chernobyl nuclear accident, the memory of what was said at the time by certain officials remains vivid.

period and to 1,700 victims of the IRA in the United Kingdom. The current quality of the British organization in the area of communications is largely linked to the lessons learned from the fight against Irish terrorism.

A Centralized, Vertical, and Geographically Dispersed System

Our public communications doctrine and organization for counter-terrorism are made in the image of France and the French state. The system is characterized by three ideas: centralization, verticality, and geographic dispersal**.**

Given the nature of the challenges we face and the objectives we seek to reach, these traditional characteristics are the source of great strengths and numerous advantages. They also, however, create certain weaknesses.

Centralization is an advantage. It is based on an implicit assumption: in the case of a crisis, everyone looks to the State. This rule of the game is well-known and accepted. The control of communications by a single entity facilitates the handling of the crisis. On the other hand it requires seamless coordination among the different categories of communication: political, judicial, and technical.

In our country, information normally moves both up and down. This approach can cause delays, since each level can tend to filter the information and thus lag in transmitting it. Networking remains alien to the logic of this system.

Our communications system benefits from a genuine strength: its wide devolution across the territorial administrative hierarchy, at the level of defence zone prefects, regional prefects, and departmental prefects. Given the prefects' powers, unified communication at the local level is from the start easier than in Paris.

The Principles of a Communications Doctrine Appropriate for Terrorism: Federate and Orchestrate

Federate

Confronting new risks and high-level threats, public communication must be organized in a more integrated way than before. The creation of new institutions is not necessary. What is necessary, on the other hand, is to increase the performance and effectiveness of the existing structures.

The fundamental step to take is to provide a stable – and inter-ministerial – framework for public communication in case of a terrorist crisis.

We must first establish, on a permanent basis, an inter-ministerial network, led by the *Service d'information du Gouvernement* (Government Information Service, SIG) in which 'communicators' of the different

ministerial departments would participate. The objective of this group would be twofold: to prepare the handling of the crisis in the area of communications, in particular at the time of preparation exercises, and lead the communication during an actual crisis. This group could open up some of its meetings to communications cells set up under the prefects at the zone level.

The stability of the framework for public communication also requires preparation of a communications plan for each of the ministries that would have a role to play in the management of a terrorist crisis. The organization and experience of the defence and foreign ministries in this area should be taken advantage of in the development of these plans.

Orchestrate

(1) The link between political communication and operational communication

The separation of political communication and operational communication is justified by two fundamental objectives.

The first objective is to consolidate public confidence by showing that everyone is operating in his or her area of competence (for communications about an investigation, a magistrate, a policeman and a gendarme each have the credibility their job gives them.)

Second, we must guarantee the credibility of the communication over time by avoiding putting political leaders in difficult situations. They could lose credibility by commenting on areas they have no direct role in, or if their comments are based on incomplete or inexact information.

Putting together a strategy that combines these two levels of communication requires a series of concrete steps. The first thing that is needed is the decision on principle to separate the two types of communication. In this respect, the 'media plans' and the experience of the Defence and Interior Ministries in the area of crisis communications provide a good basis for a doctrinal model. Next, it is necessary to apply this principle in a systematic way in the simulations and exercises conducted at the national level.

The division of roles must also be maintained from the start of a crisis, in the form of regular press conferences and statements, during which each speaker will be immediately identifiable to the audience through the order of the speakers, each speaker's place in the room, or by what he or she is wearing (uniforms for security forces).

(2) Preparation and handling of communication at the level of the European Union

It is essential that we put in place an effective cross-border communications system in case of a terrorist attack.

During the Kosovo crisis in 1999, the coordination of separate national communications was greatly facilitated by the existence within

NATO of a spokesman from the organization speaking every day, in direct liaison with the countries participating in operations. This communication was carried out in a network, whose leader was at the organization's headquarters.

This example would be hard to transpose to the European Union, however, whose missions and institutional organization are different from those of NATO.

The absence of a single coordinator in charge of crisis management in the European Union makes it difficult to put in place a single spokesperson's office on all these subjects.[1] The real-time coordination in the area of communication among the institutions of the Union and with the Member States can be organized without institutionalizing such a function.

France must actively support the implementation of effective coordination procedures between the Commission and the Secretariat-General of the Council in the area of crisis communications. Just as on the national level, these procedures should be tested during frequent exercises involving the Member States.

Building on the public communication tools that it maintains within the foreign and defence ministries, France should also develop ties with the bodies in charge of these issues among our main partners.

(1) The European Union does have an informal body for preparation and the sharing of communications via the 'Venice Group,' which brings together the 'communicators' of the 25 Member States and those of the Union's institutions. This group, however, is embryonic. In addition, the EU has no single pre-designated crisis management mechanism.

Chapter 4

Better Reparation and Sanction

Reparation for Damage Suffered by Victims

Compensation

The basis of the system for compensating victims of terrorism in France goes back to the law of 9 September 1986. This system was then extended by the law of 23 January 1990, to give victims genuine recognition and allow them to benefit from national solidarity.

Victims of terrorist acts thus benefit from the rights and advantages accorded to civilian war victims by the disabled military pension code: free health care and artificial limbs, jobs designated for disabled people, etc. Children made orphans by terrorism can, under certain conditions, be declared war orphans, and the children of victims are exonerated from having to pay inheritance tax.

A special fund (the *Fonds de Garantie des Victimes des Actes de Terrorisme et d'autres infraction*s, Compensation Fund for Victims of Acts of Terrorism and Other Offenses, FGTI, funded by taxes on insurance premiums or contributions) was created to facilitate payments to victims of acts of terrorism and their families.[1] The applicable procedure is particularly simple: informed of the identity of the victims by the chief prosecutor

(1) This now applies to victims of other crimes as well.

(*Procureur de la République*), or by diplomatic authorities, the fund contacts them directly and makes them a provisional offer of compensation for injuries and material damages, and in case of a death, for moral and economic damages of family members.

Naturally, the victims and their families keep the possibility, at any time, of taking the issue to the courts rather than appealing to the fund. But the administrative procedure offers the advantage of helping with the proceedings and of enabling victims to benefit from provisional payments very soon after the incident.[1]

The fund thus ensures complete financial reparation for damage suffered by victims of terrorism, in conformity with core principles of law of responsibility. It is now necessary to go further, by supporting, beyond the question of money, a 'principle of restoring the prior condition' of the victim, notably by providing him or her with the means of professional and social rehabilitation in the case of a lost job following an attack.

Reparations via the Penal System

Beyond compensation, reparation is done via the penal system. The provisions of the law of 9 September 2002, which allow victims of the most serious offences to benefit from a lawyer paid for by legal aid regardless of their resources, represented significant progress for the victims of terrorist acts.

Progress must still be made to provide for victims from the time of the attack and all throughout the procedure.

Prosecuting Suspects: Strengthening International Judicial Cooperation

The Adoption of the European Arrest Warrant: A Major Step Forward

On 13 June 2002, the Council of the European Union adopted the framework decision 'on the European arrest warrant and the surrender procedures between Member States.'[2]

(1) These payments also take into account the specific damages to victims of terrorism (*préjudice spécifique des victimes du terrorisme* – PSVT) that was first demonstrated by a study of victims undertaken in 1987.

(2) The warrant covers two traditional extradition scenarios: it can be issued when the acts a person is charged with are punishable by a custodial sentence or a detention order of at least twelve months, or when the person has already been convicted, with sentences of at least four months. Acts of terrorism already fall within the scope of existing instruments.

The great innovation was to put in place an exclusively judicial extradition procedure, based on the principle of mutual recognition of legal decisions, without the political authorities getting a chance to reverse them. The aim is to speed up the procedures.[1]

For terrorism and 31 other categories of serious offences, the surrender takes place without verification of the double criminality of the alleged act: the executing judicial authority cannot refuse to grant the request for surrender on the grounds that the alleged act is not an offence according to the penal law in his country. This flexibility eliminates a source of legal controversy. The framework decision thus marks the end – highly symbolic – of the refusal to extradite nationals among Member States of the European Union.

The French Constitution was modified on 17 March 2003 to allow this framework decision to come into effect, and the law of 9 March 2004 carried out the transposition. As statistics show, we have already greatly benefited from this reform: as of 31 December 2005, French jurisdictions had ordered the surrender of 336 people, including 140 French nationals, and had received 318 positive decisions from the judicial authorities in other EU countries, of which 69 were for terrorist offences. The average length of time for these actions was 45 days.[2]

All the EU Member States have transposed the framework decision into their domestic law. France must nonetheless continue to carefully watch the implementation of the European arrest warrant for two reasons: to ensure that it is operationally effective and to promote an instrument that is a fundamental stage in the creation of the area of freedom, security and justice that we support in the European Union.

The Development of Joint Investigation Teams to Counter International Terrorism

International judicial cooperation comes in many forms.

It covers close cooperation among magistrates regarding the evolution of the threat, anti-terrorist legislation, and judicial practices (for example the French-American, French-German, French-Italian and French-Spanish groups that meet twice a year).

(1) The time allowed for the process is set, in some cases voluntarily and in other cases obligatorily: Thus the final decision on the execution of the arrest warrant should normally take place within 10 days when the person consents to surrender or within 60 days of the arrest when consent is not given. The latter period can be extended by 30 days.

(2) These data should be compared to the situation prior to the coming into effect of the law of 9 March 2004, when the arrest and surrender of a person to foreign judicial authorities, even European ones, were subject to a procedure that lasted at least six months when the person consented to his extradition, and 12-18 months when all appeals had been exhausted.

It is expressed by the presence of liaison magistrates abroad to ensure better operational cooperation with judicial bodies and to thus guarantee better responsiveness in handling sensitive cases.

It is also expressed through the participation of French magistrates in EU bodies such as EUROJUST. This foreshadowing of a European prosecutor's office can be useful, provided that the conditions of its operation are made very clear, especially regarding the exchange of information and the protection of intelligence.

International judicial cooperation must also be expressed through the use of joint investigation teams, as authorized by a framework decision adopted by the European Union.[1] French-Spanish teams have already made possible some success in the fight against ETA. The possibility of establishing similar operational teams with countries outside the European Union should be explored through ad hoc bilateral agreements.

Punishing the Guilty

Tailoring Legal Penalties

The sentences foreseen for terrorist acts follow an augmentative logic compared with ordinary law. When an offence is normally punished with a sentence of 30 years of imprisonment, it is extended to a life sentence if it is committed with a terrorist goal. The same logic applies for all offences.

The counter-terrorism law of 23 January 2006 increased and extended legal penalties for certain terrorist offences. Taking part in a group or in a conspiracy whose goal is to prepare one or more crimes against people, or preparation of one or more acts of destruction by explosive or incendiary lethal substances, is henceforth punishable by 20 years of prison. Directing or organizing such a conspiracy is punishable by 30 years of imprisonment.

Keeping All Options Open

Just as it will for those who commit terrorist acts, France will hold responsible States that order them, through their services or via clandestine groups.

If a terrorist action against our territory or against our interests overseas cannot be prevented, our country can respond militarily in the context of Article 51 of the UN Charter relating to self-defence. The means

(1) The provisions that transpose this framework decision are in Articles 695-2 and 3 of the *Code de procédure pénale* (penal procedure code).

and the intensity of the response will be tailored to the seriousness of the act committed and to the targets chosen.

As the President of the Republic stressed after the 11 September 2001 attacks, and as he reiterated in his speech at Île Longue on 19 January 2006, nuclear deterrence 'is not intended to deter fanatical terrorists. Yet, the leaders of States who would use terrorist means against us, as well as those who would consider using, in one way or another, weapons of mass destruction, must understand that they would lay themselves open to a firm and adapted response on our part.'

Part III

Taking Substantive Action Against Terrorism by Winning the Battle in Everyday Life, the Technological Battle and the Battle of Ideas

France is not at war against the terrorists, but it is undertaking substantive action whose success requires it to maintain constant vigilance, improve technology and win the battle of ideas.

Chapter 1

Winning the Battle in Everyday Life: Promoting Early Detection of Terrorist Activities Through Vigilance and Human Intelligence

First of all, the fight against terrorism will be won through daily vigilance.

Concretely preventing the risk of attack requires constant mobilization and a culture of 'early detection.' This does not come naturally and can not be left solely to the specialized counter-terrorism security agencies.

This new dimension of the '*esprit de défense'* must be widely promoted and shared throughout French society.

Public Agents: Vigilance is Essential

The Role of Non-Specialized Internal Security Forces

One of the primary missions of all police or gendarmerie patrols – and more generally all units in the internal security system in the field – is the search for operational intelligence. This responsibility also applies in the area of counter-terrorism.

There are nearly 245,000 policemen or women and gendarmes in France. Because of the spreading of the threat and the evolution of the profile of activists who might be tempted by terrorism, counter-terrorism cannot rely solely on specialized agents. It is essential that all agencies and units contribute to the detection and upward flow of intelligence for use by the specialized agencies.

Surveillance of public areas and contact with the population is a preferred means for gathering information. But a prerequisite for the effectiveness of this work is that internal security agents have a good understanding of the stakes of the anti-terrorist fight. This understanding will allow them to spot indications of possible terrorist activity and enable them to choose the relevant information to transmit to specialized agencies, better placed to do some cross-checking and appropriate administrative or judicial follow-up.

Careful attention must thus be paid to the initial and continued training of magistrates, police forces, and gendarmes. Their instruction must incorporate knowledge of the social and religious realities of contemporary French society and the ideological references of the terrorist groups. The recent renewal of initial training programmes and the development of continuing education and training modules on these issues should be consolidated in the coming years. It would also be appropriate to ensure that the career advancement process for police and gendarmerie takes into account the acquisition and exercise of skills in counter-terrorism.

The risk of terrorism should also be taken into account when determining the places, times and the frequency of surveillance patrols on the street and in other public places.

The number of sites to be watched is such that coordination with municipal police is necessary, in the framework of agreements concluded with the State. Similarly, cooperation with the private security sector is necessary. The latter now employs some 200,000 people. Within the limits set by the law, these regulated professions work toward the prevention of terrorism and promote the level of general security.

Vigilance of Public Agents

Other categories of officials – whose missions do not directly involve security – may be confronted with abnormal situations that could provide indications of terrorist activity. Members of terrorist groups and networks – whether ideologues, recruiters, logisticians, or individuals directly preparing attacks – first undergo a personal trajectory that carries them toward terrorism. In other respects, the clandestine nature of their activity does not keep them from greater or lesser integration in normal life, nor from the administrative formalities that normal life entails. Some are even highly active in social activities. Others, on the contrary, are indoctrinated to break suddenly with their normal circles. Finally, acts of terrorism are preceded by meticulous preparation – organizing the attack,

choosing targets, putting together the means to be used – all phases during which clandestine activity can be revealed to a well-informed witness.

It is thus essential that all categories of public officials be regularly sensitized to terrorism issues and the types of suspect behaviour that it can produce.

The sensitization must be led by the specialized counter-terrorism agencies and must first be carried out via institutional intermediaries in each sector. Its main avenue must be the distribution of an analysis of the threat tailored to those who receive it. This document will describe, in simple terms, potential terrorists, their behavioural habits, their expected modes of preparation or operation and the type of targets that could be struck. This analysis will be accompanied by guidance on what to do in the types of situations described.

It is especially important that personnel, thus sensitized, find an appropriate interlocutor in case of doubt and that they be able to sound the alert at the right time. For each sector, the channel for passing tips to specialized agencies must be identified and easily usable.

At the State level, senior defence officials (*hauts fonctionnaires de défense*, HFD) are responsible for contributing actively to spreading this *esprit de défense*. Their network should be guided by the desire to raise awareness of the terrorist threat permanently, to support the intelligence agencies, and to ensure that measures designed to promote vigilance are applied.

Present in every ministry, working directly under the minister and coordinated by the Permanent Secretariat for National Defence (Secrétariat général de la défense nationale, SGDN), the HFDs are effective points of contact. A reform of their status is underway. The reform will give them greater authority and means in the area of security. It will nonetheless remain necessary to enhance their ability to work in a network by sharing informations and lessons learned and to enhance their role by tasking them to lead crisis exercises in their respective ministries.

The specialized preventive counter-terrorism security agencies should also develop contacts with other public services or owners of private places open to the public. These contacts may be periodic or regular depending on the state of the threat.

The Responsibility of Civil Society and the Role of the Citizen

Public Knowledge of the National Counter-Terrorism System

There can be no effective preventive policy in the area of counter-terrorism without the vigilance of everybody. And vigilance must go beyond the public domain.

Everybody is aware of the existence of the VIGIPIRATE plan. This degree of knowledge is a good thing. But we must go further in extending a culture of prevention. This culture should be based on our citizens' knowledge of the organization of the national counter-terrorism system. The State must also tell the public whom to turn to with information about possible terrorist activities.

Whom to Tell About a Suspicious Situation?

• *The first level of contact: the police station or the gendarmerie brigade (for any report or even in case of doubt) or the diplomatic and consular service for French people abroad;*

• *For public services or private companies having already developed sectoral links at the regional level: one of the zonal directorates or territorial brigades in the Direction de la Surveillance du Territoire (Territorial Surveillance Directorate, DST), the Direction de la Protection et de la Sécurité de la Défense (Defence Protection and Security Directorate, DPSD), the gendarmerie, or, as appropriate the regional centres in the fight against radical Islamism, in each regional directorate of the Renseignements Généraux (Central Directorate of General Intelligence, DCRG).*

• *For specific economic or administrative sectors: direct contact with the DST, the DCRG, the DPSD or the gendarmerie.*

The Spanish and British precedents have shown that an emergency can make it necessary to have in place an exceptional system in case of imminent or announced risk of a campaign of attacks. Such a system must make it possible to very quickly receive any report having a direct link with the investigation, on the basis of indications made public by the authorities in charge of the investigations.

The State has acquired a telephone and Internet system for receiving public information. It provides a ‘counter-terrorist green number’ that can be activated in case of necessity, with one branch set up for victims and another for taking testimony.

Developing an Exercise Policy

A new dynamic has been underway since 2002 in the conception and execution of exercises.

The objective of defence and security exercises is to regularly test the procedures and measures foreseen in the official plans and sub-plans, in the first instance in the area of counter-terrorism. They involve every level of crisis management and prepare decision-makers, their 'headquarters,' and operational teams for complex operations (including, for emergency responders working in a contaminated climate). They make it possible to test equipment and crisis management tools.

Among these exercises, so-called 'major exercises' mobilize the entire decision-making and operational chain of command, all the way up to the State's highest authorities (Presidency of the Republic, Prime Minister and his private office, Ministers and their respective private office).

On top of security and defence exercises there are civil security exercises conducted by the Interior Minister. They relate to alert or emergency operations following an event, whether of a natural, accidental or terrorist nature.

The national operational exercise policy must be pursued and strengthened. The four major exercises, organized every year, constitute a base-line that should be extended with national ministerial and local exercises. This system will only be fully effective if comprehensive lessons are drawn after each exercise and if it is complemented by efforts of synthesis and orientation**.** We therefore need to put in place an indicative exercise planning system for ministries; systematically organize lessons-learned; disseminate results; and draw consequences to guide the adaptation of our planning system and our crisis-management needs.

Progressively, multinational or international exercises are being organized. At the strategic level they concern management of crises that can cross borders and continents such as the reappearance of smallpox by malicious act or terrorism. At the operational level they involve exercises that take place on the borders of two or more countries. They involve a wide range of actors: national and local state authorities, representatives of local governments, vital infrastructure operators, non-governmental organizations, etc.

Several aspects of public communication are now integrated into the exercises. Traditionally, some information about the exercise and its results was provided, while certain operational methods were not revealed. More recently, the simulation of media pressure has become part of the exercise itself. This has led the players to take media issues into account when making their decisions: these include communication about the events and how they are being handled, reactions of public opinion, and international reaction.

We must increasingly take media issues into account in defence and security exercises because they are such a key element in the public communications and crisis management policies.

Public confidence in government will be all the more natural if it is based on the experience of visible preparation for events which, if they occurred, would no longer be a surprise. As part of the exercises, citizens would also benefit from getting experience learning about how to behave during a crisis similar to the one being simulated in the publicized exercise.

Recent Exercises

The most frequent exercises, since 2002, have been about chemical attacks or accidents, with real intervention by emergency units at the site of the event: PIRATOX in November 2003 in Paris, following a scenario in which Sarin gas (the same type used by the Aum Shinrikyo sect in the Tokyo metro) was used; METROTOX in 2003, 2004 and 2005, following a scenario in which toxic gas was used in metro stations in Toulouse, Lyon and Marseille.

The Central Inter-Ministerial Technological Intervention Unit (détachement central interministériel d'intervention technologique, DCI) was used in January 2004 leading to the neutralization of an improvised nuclear device. The 'R-53' exercise in October 2004 in Paris dealt with a 'dirty bomb' radiological attack scenario and was focused on the hospitalization phase.

The scenario 'Ambroise 05' (Ambrosia), a headquarters exercise carried out in December 2005 in Paris, simulated four nearly simultaneous attacks on the public transport system, including one with the diffusion of toxic gas.

The biological area was covered with the governmental BIOTOX 04 exercise in May 2004, which simulated a malicious appearance of smallpox, and with PANDEMIE GRIPPALE 05 (Flu Pandemic 05) in June 2005. Even though the latter exercise dealt with a natural event rather than a terrorist attack, it simulated a crisis situation similar to the extreme scenarios of major attacks.

In the conventional area, three exercises should be mentioned: ESTEREL 04 in the Mediterranean in October 2004; ARMOR 05, focused on maritime terrorism in the English Channel and the Atlantic in May 2005; and finally PIRATAIR 04 in December 2004, which simulated an airplane hijacking, with mid-air interception and intervention on the ground. In the area of the security of information systems, the exercise PIRANET 05 was conducted in November 2005.

At the European level, EURATOX, which simulated multiple chemical attacks on the Plateau of Canjuers in October 2002, and EURATECH in April 2005, which simulated an attack on a chemical railway transport in Drôme, brought together many hundreds of participants from different EU Member States to test the complementarity of the interventional capabilities and the compatibility of procedures and equipment.

Maintaining Public Vigilance

In the sometimes long periods of respite left by the terrorists, vigilance must nonetheless be maintained. Communications efforts reminding people of the reality and permanence of the threat must be undertaken regularly, especially at propitious times such as when exercises are being conducted or during departures and returns from holidays.

In France the operators of the public transport networks have developed a policy of calling for vigilance among travellers, especially regarding abandoned luggage or suspicious packages. These calls, repeated regularly during the day, are nonetheless limited to prescribing a general attitude, without giving precise instructions for what to do in case of a problem.

In the London Underground, the specialized police initiated a procedure called 'HOT' to sum up the three characteristics of a suspicious object: it must be 'Hidden', 'Obviously suspicious' and not 'Typical' of the environment in question. Instructions have also been issued describing what to do in case an object with these three characteristics is discovered.

Our public transport operators must learn from this type of experience to give their users practical guidelines for action beyond simple messages of a general character that are addressed to them.[1]

We must also better manage threats of attacks. Experience has shown that, at least in France, the announcement of an attack, committed on our territory or abroad, always stimulates hoaxes. After the anthrax crisis in the United States in 2001, thousands of suspicious envelopes circulated in France and all were transmitted to laboratories for examination, which led to backups and excessive processing period. Similarly, after the Madrid attacks in March 2004, the *Société Nationale des Chemins de Fer* (French National Railways, SNCF) received numerous anonymous calls claiming that bombs had been placed on trains or train tracks, which led to considerable delays. Beyond sensitizing the French to the dangers of this sort of behaviour, it is necessary to increase the severity of punishment for those who sound false alarms.

The Role of Schools

School is a good place to sensitize children to the risks and threats that weigh on our society in general and on the means to deal with those threats in a preventive way. Schools enable future adults to take conscience of their place in society, of the role of the group and of individual engagement, and of respect for common values. In this framework, the fight against all forms of discrimination is an essential element to prevent the development of extremism.

(1) Whereas in 1992 approximately 20% of incidents in the London Underground led to total evacuations, this proportion has now been lowered to less than 1%.

The theme of terrorism may be taken up in a school setting to differing degrees and according to different formats. While elementary school does not seem to be the right place, given the sensitivity of the subject that touches on themes like violence and death, the pupils can nonetheless be sensitized to the question of danger and to the basic rules of caution. In middle school and high school, several programme modules make it possible to take up the question of terrorism, especially in history, geography, and civil education classes.

We must propose paths of action to teachers to respond to their expectations in the area of information about terrorism. In the framework of the initial training of teachers and school officials, a specific module could be focused on the subject that would make it possible to sensitize the entirety of the personnel in elementary schools, middle schools, and high schools. In the framework of teachers' continuing education and training an academic day on risks of the contemporary world, including a session on terrorism, could be organized. The *Journée de Solidarité*[1] could also be an opportunity for the teachers and school officials to deal with the question.

Partnership between the Education, Interior and Defence Ministries could also be promoted to co-produce documents for example putting terrorism into perspective or summarising this White Paper. Training should also be undertaken.

Teaching about religions must also be the business of the secular school.

School cannot be a place open to any form of proselytization. This is the meaning of the law of 15 March 2004 which, in application of the principle of *laïcité* (secularism), provides the framework for the wearing of symbols or clothing manifesting religious affiliation in public elementary schools, secondary schools, and high schools.

Yet schools do not exclude religions from their curricula. Only an objective and detailed knowledge of religious traditions and texts can make it possible for young people of all faiths to avoid falling under the sway of extremists distorting the message of their faith, by applying historical, political and social analysis to religions.

It is thus that in terms of method, teaching about religions is part of the required curriculum in areas like geography, history, literature, or philosophy.

(1) A ‘day of solidarity’, introduced in 2005, on which workers' salaries are allocated to the elderly

Chapter 2

Winning the Technological Battle

The Objective: Always Stay Ahead of the Threat

Principles

Terrorists use the most modern technologies both in the organization of their networks and in their operating procedures. They thus progress according to the pace of technological evolution. Government cannot afford to lag behind.

Until now, our internal security policy gave priority to the purchase of products available on the open market. This approach does not enable the State to ensure that technological efforts to block potential criminal use of the new technologies are up to date. We must get ahead by developing research programmes capable of blocking future threats. This is the lesson that can be drawn from the development of defence programmes.

Whereas the technological cycle in the defence area sometimes lasts 15 or 20 years because of the complexity of the equipment, the time horizon for internal security is shorter, on the order of three to five years. Preventing terrorism requires striking the right balance between the two models.

Orienting the Research and Development Effort

We face numerous technological challenges. The responses can only be found in the framework of a comprehensive and pooled approach in the area of research and development (R&D).

Even more than in the past, our approach must be multi-disciplinary, involving human sciences (psychology, linguistics), physical sciences (mechanics, microelectronics), biotechnology, and information technologies. We need a centralized survey of needs as well as a coherent master plan with a clear leader, for each strategic area.

The R&D effort should be organized in three parts:

The first involves keeping watch and carrying out forward-looking analysis in the area of threats, based on the experience of counter-terrorism officials. The evolution of the terrorists' operating procedures should be integrated in government guidelines and choices.

The second part should promote research programmes in the technological areas in which major developments are expected. The role of the National Research Agency (*Agence Nationale de la Recherche*, ANR) in the civilian sector and of the General Delegation for Armament (*Délégation Générale pour l'Armement*, DGA) in the defence sector is to identify the fields that require long-term investment.

The third effort has to do with industrial development and the production of equipment in the areas where the basic technology is mature. Based on an analysis of needs, what is necessary is to adjust applications already being used in various sectors to different objectives, or to speed up the development of specially tailored counter-terrorist equipment. Here, too, we should build on existing structures, for example the Agency for Innovation in Industry (*Agence de l'Innovation Industrielle*, AII), the support programme for competitive clusters in the civilian sector of the DGA.

The sectors that deserve particular attention include protection against the CBRN risk, the detection of explosives, the monitoring of telecommunications, video-surveillance, the protection of information systems and biometrics.

Protection against chemical, biological, radiological and nuclear threats

The 11 September 2001 attacks demonstrated the clear risk of terrorist attacks with non-conventional weapons, which could thus have chemical, biological, radiological or nuclear effects.

An inventory of our detection, diagnostic, prophylactic and therapeutic means – as well as of our means for decontamination and rehabilitation – made it possible to evaluate the current capabilities of our system. This system must be strengthened to deal with the particular characteristics of the terrorist threat, such as ‘dirty bombs’ (explosives that spread radioactive materials), chemical agents, pathogens, attacks on the

food chain (including drinking water), agricultural resources or the environment.

The priority areas for which new tools must be developed have been identified.

In the nuclear and radiological area, the goal is to be able in optimal security conditions to diagnose and dismantle any weapon and any improvised device.

In the biological area, we must improve our detection and diagnostic capabilities. We must extend the range of detectable agents by developing reliable sensors and common procedures of analysis in the expert laboratories. We must further develop our prophylactic and therapeutic means.

The malicious spreading of emerging or re-emerging diseases can be made easier by the rapid evolution of biological technologies. An enhanced epidemiological detection, diagnostic, and follow-up capability for infected or potentially infected people, animals or plants can make it possible to develop appropriate responses.

In the chemical area, the greatest needs are the acquisition and adaptation of existing techniques to a civilian context: reliable and continuous detection, confirmation and automatic alert in case of detection and reassurance in the opposite case.

The common points in all these areas are the development of miniaturized and automatic sensors that can detect threats rapidly and the extension of the detection capability to the whole range of toxic agents that could be used by terrorists.

Detection of Explosives

We need to be able to detect explosives in areas of significant human or automobile traffic without interfering with freedom of movement. For this we need to develop and perfect automatic sensors that can be used in fixed sites or mobile stations.

Our detection capabilities must cover products, such as ammonium nitrate, that have explosive characteristics when they are prepared and applied in a particular way. These products are for the most part very widely available or easy to prepare via the transformation of easily obtainable raw materials. They are currently detected by specialized dogs. We must develop trace detection devices and make them more reliable.

Monitoring Telecommunications

The development of the Internet and of the numerous services that it offers, especially in the area of voice telephony, significantly changes the architecture of the operators'networks. To maintain the capability for judicial authorities, police forces and intelligence services to access the content of communications as part of judicial or security intercepts, appropriate technical systems must be implemented both by operators and by security services.

The automation of detection will have to include an element focused on voice – eventually enabling recognition of the speaker's voice, his or her language, and automatic transcription and translation of the conversations. High-capacity tools are already available, but the technologies must still be fully validated.

In the area of research in large stocks of data (combining text, sound and digital images), work should focus on word-sorting, which makes it possible to organize the information gathered in texts or in sound recordings in an intelligible manner, and on the recognition of objects or people in a continuous flow of photographs or videos.

The development of **video-surveillance** in the area of counter-terrorism has two components.

The goal of the first is to improve the quality of available products by establishing demanding standards. The standardization of products (cameras, networks, visualization and storage systems, image formats, operating software) must be based on the generalization of digital techniques and the use of dominant standards (such as the Mpeg video format). The counter-terrorism law of 23 January 2006 requires the definition of mandatory standards.

The second component has to do with software. The development of video-surveillance must include the introduction of specialized software capable of face-recognition, movement detection, detection of abandoned objects, and tracking individuals. Only this kind of software makes it possible to quickly and effectively make use of the volume of images received. The results obtained so far by industry are encouraging.

In the area of **information systems**, several steps should be taken to improve security significantly.

Given the recognized lack of trusted security products, we have to be more ambitious in funding research, development and acquisition of such tools. In its networks and sensitive systems, the government must systematically use tested and validated security products and services. Private operators must be involved with this approach from early on. Our goal, in such a sensitive area of national affairs, must be to develop national solutions.

Biometrics

Biometric techniques are now widely used in the area of judicial investigation and they have proven their reliability. The risk of statistical error is very low.

At present, fingerprint and palmprint biometrics remain the primary technological tool available to develop these systems of reliable checks in sensitive or restricted-access areas.[1] The focus needs to be placed on operational development and on diffusion of this technique.

(1) The rate of statistical error for these techniques, already naturally very low, can be reduced to zero by using several fingers or palmprints.

In the area of genetics, the analysis process remains long, and research should focus on making it possible to extract DNA in practically real time from a blood sample.

Automatic face-recognition technology based on photographs and iris-recognition technology is not sufficiently mature to make possible large-scale operational application. Identification via voice spectrum analysis is a field of knowledge that is still too embryonic for it to be operationally applied on a large scale at present. Research programmes in these two areas must be pursued.

The Method: Cooperation between State and Business, which Emphasizes the European Dimension

Encouraging a Process for Developing Anti-Terrorist standards

Compared to the practices of the early 1980s, the conception of products now takes new environmental norms into account in addition to standards for the quality of production. We have to move toward a certification process that takes the specific objective of the fight against terrorism into account.[1]

The State must set standards, including in the area of certification, for the organizations, systems and equipments that contribute to the fight against terrorism. This is an indispensable corollary to the policy of vital infrastructure protection decreed by the national security directives. It makes it possible to protect, support and frame the industrial activity associated with security and defence.

The work done in international standardization bodies focuses on a number of different sectors associated with counter-terrorism. These include CBRN detection, emergency communications, first aid equipment, biometrics, logistics chain security, and crisis exercise practices.

French input should be given to the international bodies that the French Standardization Agency (*Agence Française de Normalisation*, AFNOR) participates in. Otherwise, we would be presented with solutions for which our companies would not be prepared or that do not reflect French needs.

(1) After the 11 September 2001 attacks, the American National Standards Institute (ANSI) began work on the fight against terrorism, from the point of view of 'citizen protection.' This issue was taken up by the International Organization for Standardization (ISO) and the European Committee for Standardization (CEN). NATO also participates, in liaison with the CEN.

Communicating with Companies and Supporting their Efforts

French companies are well placed in the security technologies sector. In this area they benefit from the defence technology sector, with which they work closely. The expertise of our national industrial sector is recognized and used by our foreign partners.

The State can thus rely on national expertise to develop the systems and equipment required by the fight against terrorism. It must support the research and development efforts of businesses. This requires a long-term financial engagement.

For the sectors that require our main efforts (protection from the CBRN threat, detection of explosives, the monitoring of telecommunications, video-surveillance, the protection of information systems and biometrics), the State should establish ambitious programmes and set ambitious objectives. It must get our companies to contribute to projects with research and development contracts. The financial resources devoted to R&D in these sectors could, moreover, be presented in a single budget, making it possible to publicly identify the effort undertaken.

Further Supporting and Enhancing the European Security Research Programme

The global character of the threat and the importance of the means to deploy in response to the threat make European and international cooperation natural.

Cooperation is necessary to pool resources and, in some cases, to attain the critical mass needed to justify certain research projects. Cooperation will make it possible to pursue the standardization project and eventually to guarantee that monitoring and surveillance equipment can communicate beyond borders. It will enable our industry to measure itself against its European partners.

Since 2001, the fight against terrorism has been an important concern of the **European Union.**

Concrete initiatives have been taken with the creation of European agencies in the areas of transport and information networks, including the European Maritime Safety Agency, the European Aviation Safety Agency and the European Network and Information Security Agency. But EU efforts go beyond merely creating new institutions.

Significant funds have been allocated within the Framework Research and Development Programmes (FRDP), notably the 6th FRDP underway in 2006. The 7th FRDP breaks new ground by offering a specific element – the European Security Research Programme (known as 'the ESRP programme') that could be endowed with 250 million euros per year for the 2007-2013 period.

ESRP offers concrete prospects for developing European security technologies. France plans to take full part in this. An inter-ministerial organization for this purpose has been set up and a close dialogue between government and national industries has been established. This dialogue will make it possible to establish our position, to contribute to the orientation of the program and to prepare our industrial sector for this new framework.

The European Union must support the development of interoperable alert systems and crisis management data-bases. France has identified what is needed in the long run to establish a European crisis management network.[1] The ESRP should also cover video-surveillance, surveillance of goods, detection of dangerous materials, and protection of the transport system. Management of the ESRP by the Commission should be carried out in close collaboration with Member States, who establish security needs.

Given the strong technological commonality between the systems for counter-terrorism and those developed by the defence industries in areas like CBRN, detection, protection of networked systems, and communications interoperability, the European Defence Agency can also offer an appropriate framework for conducting research activities, through cooperation among the 25 or in smaller teams.

The sensitivity of certain subjects – given the need for discretion in the face of certain threats and the need to protect industrial know-how – makes it necessary to focus on limited cooperation with key European partners, depending on the issue.

The cooperation programmes with the United States, especially in the CBRN area, must also be reinforced.

(1) This includes data sharing, secure information links, the setting up of radio networks, and the development of software to help with decision-making.

Chapter 3

Winning the Battle of Ideas

In the long run, the only real way to stop the spread of terrorism is with the support and solidarity of citizens. This means that France must fight a battle of ideas, in France and throughout the world. France begins this battle with some initial credit, including the coherence of the principles that guide its internal action and the position it takes in international affairs.

In France, Consolidating Public Support and Isolating the Terrorists

To be heard, a message must be simple. To be convincing, it must be based on the basic values of our democratic tradition.

The Principle: Never Compromise the Fundamental Values of the Rule of Law

France, like all countries threatened by global Islamist-inspired terrorism, faces this fundamental question: How can a democracy, while remaining faithful to its values, fight against a threat that seeks the destruction of what that democracy represents?

Two questions, one as fundamental as the other, must be resolved. Should we go so far as to consider ourselves in a 'state of war against terrorism'? Can we – by virtue of the supposed or real pre-eminence of the fundamental right to security, strictly and durably limit our

fundamental liberties, such as respect for private life or the freedom to come and go?

If we were at war, permanent recourse to emergency legislation would be justified. And if the war took place in part on our soil, those living there would have to accept the curbing of their most essential daily liberties.

France has decided to remain within a peacetime logic. The fact that it is using its armed forces in the fight against terrorism does not contradict this choice.

Our penal law in the area of the fight against terrorism remains a specialized system. It is not an extraordinary system. The most innovative measures in the field of policing civil liberties – such as the development of video-surveillance and the creation of data-bases that process information about international travellers – are accompanied by guarantees that protect our basic freedoms.[1]

The most innovative systems are only implemented for limited periods of time, with a 'rendez-vous' clause requiring parliamentary review, so that the government reports on the way in which the new tools have been used.

The Parliament must also be informed about the activity of the intelligence agencies in the area of counter-terrorism. This can take place in the more general framework of the information that the government has pledged to provide to parliament about the activity of these agencies.

This general balance demonstrates a clear consensus that beyond the debate between security and liberty, popular support for our country's battle against terrorism derives from the conservation of our great democratic principles.

France must fight terrorism by remaining firm on the values that hold this country together and which can give substance to the fight. The government must inform citizens about the risks involved and the methods being used. The fight against terrorism also depends on rigorous public communication.

Rejecting the Conflation of Terrorism and Islam

The fight against global terrorism is in no sense a fight against Islam. It is focused on the groups and networks that hijack Islam's humanist tradition and pervert the religion for the goals and causes that the criminals claim to be serving.

We have to reject any conflation of Islam with terrorism. Support for Islam's representative authorities in France and for the message of

(1) These guarantees include the systematic intervention of the National Commission on Data Processing and Liberties (*Commission Nationale de l'Informatique et des Libertés*, CNIL).

peace sent by the immense majority of imams is part of the absolute refusal of conflation of Islam with terrorism.

It is not up to the State to favour one or another reading of Islam, nor of any other religion for that matter. But language inciting hatred, provocation or discrimination is neither morally nor legally acceptable and will never be tolerated.

The Form of the Message: Public Communications Policy Must Seek the Widest Possible Consensus by Isolating the Terrorists

Rallying the Population

To fight against terrorism, there are two possible types of long-term communication.

The first seeks to create the expression of majority support for the government in the fight against terrorism and its effects. This approach favours dramatiszation, which often provokes a process of identification with government.

The second approach seeks to build a wide consensus, integrating first and foremost the fraction of the population the terrorists claim to speak for and that they try to detach from the national community. A policy of seeking consensus must coldly and rationally seek to make of the public a clear-eyed ally that is sensitized to the battle being waged by the authorities. It is this second approach that we must follow.

Defining target groups for communication

Five main groups can be distinguished.

• The broad population, including children and adolescents;

• People and organizations engaged in the fight against terrorism: the State and its agents; local authorities and their agents; critical infrastructure operators (health, water, energy, transport, telecommunications); institutions that deal with the public and their employees;

• Populations the terrorists claim to be fighting for. They are put in a delicate position before attacks are committed. They are extremely vulnerable when the terrorists have struck.[1] The reactions of this part of the population are also decisive for any policy that seeks to promote national unity and isolate the terrorists. The communications policy will target both the relevant populations in France and the countries, populations and foreign organizations that could contribute to the isolation of the terrorists;

(1) See the violent reactions against Muslim schools and the religious sites in the Netherlands in November 2004 after the assassination of the director Theo Van Gogh.

• France's foreign partners;

• Both the national and foreign media as special communication channels;

On the level of principles, the groups whose mobilization is desired must be considered as partners in the fight against terrorism.

From the 'need to know' to the 'need to share'

The public is both a stake and a target at the same time. It must be viewed as a full partner. We therefore need to move from a logic of 'need to know,' which traditionally governs the security domain, to a new dynamic of sharing information.

Naturally, this passage from the 'need to know' to 'need to share' does not mean that everything must be made public. The general public will understand perfectly well that a fully transparent policy would be counter-productive in this area. Affirming this new principle, however, moves the burden of proof in terms of communication. In the tradition of Latin States, people have a tendency to keep information to themselves, unless it is obviously harmless. In the future, the principle should be that of communicating information, unless it is obviously dangerous.

This is a major change. But it is indispensable if we want to create, and maintain, the mutual confidence that is the key to a successful and durable mobilization of society against terrorism.

Distinguishing necessary discretion from useless mystery

Whether in time of crisis or not, it is important for the intelligence agencies to adopt a policy of targeted communications. While they must be extremely circumspect about their operational methods and protect their sources, their leaders can usefully speak about the state of the threat and the main goals of their activities. The recent evolution of their practices in this respect is a positive factor worthy of being consolidated.

A need for new interfaces

To concretely apply the new approach, we must first create **communications forums** on a national scale bringing together public communication professionals and the representatives of diverse target groups from the population we seek to mobilize: general opinion leaders (researchers, recognized specialists, and journalists), representatives of local government and operators, leaders from the parts of the public the terrorists claim to speak for. The setting up of this type of forum can also be envisaged at the regional level (in the defence zones or in France's *Régions*.)

The establishment of **informal dialogues** with the press could be useful both to the State and to the journalists, who sometimes feel isolated when it comes to making an ethical choice between defending the national interest and revealing information to the public.

The organization of **national or regional conferences** must be made systematic. These meetings can be organized at the State's initiative

or by research institutes, which are good intermediaries with civil society.[1] This type of gathering will, among other goals, seek to involve in the debate people with particular standing among the populations the terrorists claim to be 'showing the way.' The work of institutes specialized in internal security and defence show that this can be done in this area.[2]

The creation of **information sources accessible to the wider public**[3] and specialists on different aspects of terrorism must be encouraged. Such efforts will be all the more effective if they involve the public and private sectors. Having the State distancing itself in this manner can help lessen the suspicion of manipulation that sometimes surrounds information put out by the government. Making more information public can also help research centres develop their capacity for analyzing terrorism.

Individual expertise on terrorism must be developed in the same spirit. In case of a danger or a crisis, whatever the cause, the media can turn to people known for their expertise, who in principle have the advantage of being able to provide information independently from political, bureaucratic or economic interests.

Isolating the terrorists

The terrorists would like to speak to States as equals. This logic must be refused, both in terms of substance and of style.

The terrorists say they are at war. They call themselves combatants. This was already the case for the extreme-left of the 1970s (at 'war against big capital'). Now it is the case for Osama bin Laden and his supporters, who see themselves in a clash of civilizations. This approach seeks to legitimize terrorism. We cannot accept it. On the contrary, we must marginalize those who undertake terrorist acts, reminding everyone that these are not warriors but criminals. You do not go to war against criminals.

Trying to open dialogue with the terrorists is also out of the question. This is because such a policy would only bolster the terrorists by treating them like appropriate interlocutors. Treating them like this would only enhance their attraction in the eyes of potential recruits or supporters.

(1) The 17 November 2005 conference 'The French in the face of terrorism', organized in the framework of the preparation of this White Paper, is a good example of a conference organized by the State.

(2) Examples include the *Institut National des Hautes Etudes de Sécurité* (National Institute of Higher Security Studies, INHES) and the *Institut des Hautes Etudes de Défense Nationale* (Institute of Higher National Defence Studies, IHEDN).

(3) Such as the data base on terrorist attacks, made available to the public on-line on 22 September 2005 by the *Fondation pour la Recherche Stratégique* (Foundation for Strategic Research), www.frstrategie.org

Fighting Terrorism at the Global Level

Countering Radical Islamist Propaganda and the Rhetoric of Hatred and Intolerance

On this point, international organizations have an important role to play. They have started adapting the tools that make it possible to fight all over the world against incitement to racial hatred and provocation of terrorism.

UN Security Council Resolution 1624, adopted in September 2005, compels all states to adopt a penal system that criminalizes these offences. The Council of Europe's convention on terrorism goes in the same direction. To further develop this normative action in the area of the fight against intolerance and incitement to racial hatred, an international organization such as UNESCO could prove to be an appropriate body to carry the battle of ideas to a global level. It could do this by promoting education programmes and sensitizing people to the terrorist threat.

Another area that should receive priority attention at the international level is the use of satellite television to spread racist or anti-Semitic ideas or that promote terrorism.

The *Al-Manar* affair of 2003-2004 demonstrated the absence of European regulation in this area.[1] Without any other coercive means available, the United States, for their part, put *Al-Manar* on the list of terrorist organizations. The French approach, based on a procedure of gradual warning and then cutting off of the programme, could serve as a model for the adoption of an EU Framework Decision.

Communicating Better

Islamist terrorists of al Qaeda's persuasion reject all dialogue and all communication: 'The jihad and the rifle alone, no negotiation, no conference, no dialogue' wrote Abdallah Azzam, the mentor of Osama bin Laden.[2] Even if they would accept dialogue, it is hard to see what the objective of such dialogue could be, given that their project lies beyond any political bounds. The causes put forward are more pretexts than claims: Osama bin Laden only focused on the fate of the Palestinians belat-

(1) In November 2003, the Lebanese television station *Al-Manar*, which is close to Hezbollah, broadcast an anti-Semitic Syrian soap opera. This broadcast led the French authorities to develop new legislation relating to audiovisual freedom, which was adopted on 9 July 2004. Its provisions allowed the Conseil d'Etat, to which the issue was referred by the *Conseil supérieur de l'audiovisuel* (Higher Audiovisual Council, CSA), to order the Eutelsat satellite system to stop carrying *Al-Manar* on 13 December 2004.

(2) Azzam was a radical Islamist theoretician and coordinator of the Arab participation in the Afghanistan war; he died in 1989.

edly. His first statements focused on the American presence in Somalia as a target.

Conversely, the use of warlike terminology, which by definition excludes any room for communication, has the disadvantage of consolidating the threat. It can even constitute the best publicity for the recruitment of new terrorists. Even more seriously, it gives credit to the false and dangerous idea of a 'clash of civilizations' between the West and the Muslim world, which is exactly what global Islamist-inspired terrorism seeks to promote.

In the area of international communication, the work on the terrorists' environment must primarily focus on two things.

The first is to recognize, and to reaffirm, that the Arab and Muslim States are more in symbiosis than in conflict with Western civilization.

The second consists in targeting, in terms of communication, the middle classes and the young generations, including when they see their room for expression curbed by their leaders.

France has a long tradition of Middle East studies. In the past this might have seemed outmoded; it was, in addition, certainly marked by the colonial period. But this tradition underwent an undeniable renewal in the 1980s. The skills that French scholars developed in this period must be put to use to promote our assets in the area of dialogue and to conduct a targeted policy with respect to Muslim opinion leaders.

The question of communication toward the Muslim world in general is also highly relevant. Since the 11 September 2001 attacks, the United States has pursued 'public diplomacy' toward the Arab world; to this end they created the Sawa radio station and the al-Hura television channel.

France itself has long had international audiovisual ambitions, with media such as Radio France Internationale (RFI), RMC Moyen-Orient (RMC Middle East) and the Medi I Sat project. The future French international information channel (CFII) will also have to be present in the Arab world.

Finally, we must also be present in the international Arabic media (in 2006 the al-Jazeera, al-Arabiya and Abu Dhabi TV television channels and the al-Hayat and al-Sharq al Awsat newspapers). This will make it possible for us to be better understood and to avoid misunderstanding about our policies.

Emphasizing a Political Approach

Beyond the elaboration of analysis and language concepts appropriate for communication, containing global terrorism also requires a political approach, which must pursue three objectives: reduce and, ideally, resolve regional crises on which terrorism thrives rhetorically and

opportunistically; build or rebuild the weakest States; contribute to the opening of Arab and Western societies toward one another.

Reducing or Resolving Regional Crises

Certain Near or Middle East conflicts are very present in the rhetoric of Islamist terrorists.

Their resolution would of course not reduce global terrorism, which functionally has nothing to do with them. It is, moreover, worth noting that al Qaeda took off as an organization in the second half of the 1990s, in other words at the very moment when so much was being done to bring the Israeli-Palestinian peace process to a successful conclusion.

Nonetheless, more active American and European involvement in the Israeli-Palestinian conflict, followed by positive results, would deprive global terrorism of some symbolic arguments, which would contribute to the drying up of some of its recruitment sources. The political resolution of the Chechen conflict, also very present in the Islamist terrorist propaganda, must, for the same reason, be pursued.

But it is Iraq that has today become the main aggravating factor. It offers the terrorists the image of an Arab country occupied by Western forces and, in operational terms, a new 'land of jihad' even more promising than Afghanistan or Somalia had been. The effects of the current situation will be felt for a long time, even after Iraq will have stabilized.

Africa is also confronted with destabilizing conflicts of which global terrorism can take advantage. This only makes our engagement in the resolution of these conflicts even more important.

Whatever the evolution of the regional conflicts in the coming years, our objective must be to succeed in dissociating local extremism and global terrorism.

The risk of alliances of convenience, of an operational or political character, is hard to avoid. The true threat is that of strategic alliances that would allow global terrorism to win over the militant base of the local extremist groups and enable them to benefit from the mobilizing power of international Islamist ideology.

Our policy will be all the more effective if it is diversified. All forms of terrorism must be fought with the same determination, but, with the goal of effectiveness in mind, in different ways.

When the resort to terrorism links up with a local conflict, by recycling its complaints, it is in our interest to do everything possible to resolve the conflict: first of all for the good of all parties concerned; then to deprive terrorism of a recruitment reservoir and a motor of mobilization. At the same time that we undertake the required actions against terrorist groups, we will seek a dialogue with those who, while they may share certain political objectives with the terrorists, either do not share or renounce the terrorists' methods.

Global terrorism lies outside the political space in which dialogue is possible: its objective is our destruction; violence is not a language but an end in itself.

Our policy of preventing the threat and stopping terrorist acts must be pursued in cooperation with our international partners.

Consolidating Weak States and Reconstructing Failed States

The consolidation of weak states and the reconstruction of failed states, where all form of authority has disappeared, are crucial. They are the keys to the sanctuaries where the terrorists find refuge. The main goal is to restore in these states institutions that function in which the public is confident because these institutions will provide people with an appropriate level of security.

The priority must therefore be to reinforce the capabilities in the area of security, along the lines of what has been undertaken in Afghanistan and in the countries of sub-Saharan Africa. This implies re-establishing effective police, military and customs forces.

The condition for success of these state building operations in the most fragile areas will ultimately depend on the capacity of the local security forces to collaborate with those hostile to the central authority and on the ability of the government to win them over.

Contributing to the Reciprocal Opening of Muslim Cultures and Western Societies

The integration of radicals into politics is not always possible. When it is plausible, however, we should seek it.

In 1995, the European Union launched the Euro-Mediterranean process, called the 'Barcelona Process.' This partnership between the two shores of the Mediterranean plays a useful role, notably by helping the countries on the southern side uphold their responsibilities. The focus on civil societies must not lead us to ignore States already weakened by the numerous challenges they must face. As the Iraqi case shows, the radicalization of populations is often due to the deficiencies of States. The European Union allocates large amounts of money in the Mediterranean region (approximately 3 billion euros per year), but our approach would benefit from being more visible and better targeted.

At the Barcelona summit, in November 2005, the countries of the Euro-Mediterranean partnership agreed for the first time on a common basis for counter-terrorism by adopting a 'code of good conduct.' They unanimously declared terrorism to be unjustifiable and committed themselves to implementing the ad hoc UN conventions on terrorism and to concluding the negotiation on the global convention on terrorism – which has until now divided them – as soon as possible.

More needs to be done, in particular regarding the definition of terrorism, on which there is still no agreement. France will continue to work determinedly to broaden the basis of international mobilization against terrorism everywhere in the world. Already, an important step forward was taken with the agreement of all UN Member States to 'strongly condemn terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, as it constitutes one of the most serious threats to international peace and security.'[1] This declaration must be made to bear fruit.

(1) Excerpt from the final declaration of the General Assembly Summit celebrating the 60th anniversary of the UN in September 2005.

Conclusion

Terrorism presents two growing threats to our societies: it seeks to splinter them and to make them lose their souls.

At the forefront of this threat, global Islamist-inspired terrorism relentlessly pursues its divisive project.

At the global level, it seeks to divide Western and Muslim societies. In Muslim countries, it seeks to divide Islamist extremists and moderate believers. In France, it seeks to divide individuals of the Muslim faith from others. To splinter our societies, global terrorism resorts to exploiting Islam for political purposes, scorning the precepts of peace and tolerance taught by this religion. We will respond to this moral challenge by fighting any attempt to conflate Islam and terrorism. It is the unity and cohesion of our country that protect us from the clash of civilizations into which global terrorism seeks to drag us.

Global terrorism also seeks to strike at the heart of our democracies.

It seeks this first by destabilizing them with the perpetration of attacks designed to shock public opinion and to undermine its confidence in the capacity of government to defend them effectively. But it especially seeks this goal by pushing citizens to renounce the principles democracies are built on.

The freedom that constitutes the bedrock of our democracy can not be synonymous with improvidence and weakness. We must thus prevent attacks and severely punish those who manage to perpetrate them or who attempt to do so. The challenge is to ensure the effectiveness of counter-terrorism methods while complying with the rule of law. To deviate from this course would in fact be to play into the hands of global terrorism. On the occasion of the commemoration of the first anniversary of the March 2004 attacks in Madrid, the UN Secretary General declared that ‘compromising human rights cannot serve the struggle against terrorism. On the contrary, it facilitates achievement of the terrorist's objective – by

ceding to him the moral high ground, and provoking tension, hatred and mistrust [...] among precisely those parts of the population where he is most likely to find recruits.'

By respecting the law, the fight against terrorism gains legitimacy. It therefore gains effectiveness, from a long-term strategic perspective.

Our country will continue to travel down this narrow path. It will keep the judge at the heart of counter-terrorism, being careful never to go down the slippery slope of developing extraordinary procedures. Our intelligence and security agencies will use the most modern surveillance methods with continued respect for civil liberties, such as the right to come and go and the respect for privacy. The most restrictive measures will only be adopted for limited periods of time and they will be regularly and repeatedly discussed in Parliament.

Our country has made the legal, philosophical, and strategic choice to fight terrorism within the framework of the rule of law. It will not deviate from this course.

Appendix

Main acts attributed to global terrorism since 1992

• **29 December 1992**: double attack at Aden (Yemen) against American soldiers, attributed to al Qaeda

• **26 February 1993**: attack on the World Trade Center in New York (United States) attributed to al Qaeda. 6 deaths and more than 1000 injured.

• **19 November 1995**: suicide attack against the Egyptian Embassy in Islamabad (Pakistan), attributed to a group close to al Qaeda. 16 deaths and 60 injured.

• ***23 February 1998****:* creation of *World Islamic Front for Jihad Against Jews and Crusaders* under the aegis of Osama bin Laden.

• **7 August 1998:** double suicide attacks simultaneously on the American Embassies in Kenya and Tanzania, responsibility claimed by Islamic Army for the Liberation of the Holy Places. 224 deaths.

• **12 October 2000:** suicide attack on the U.S.S. Cole in the port of Aden (Yemen), attributed to al Qaeda. 17 deaths.

• **9 September 2001:** assassination of Commander Massoud by two members of al Qaeda.

• **11 September 2001:** quadruple suicide attacks simultaneously in New York, Washington, and Pennsylvania (United States), responsibility claimed belatedly by al Qaeda. 2985 deaths, **5 of which were French**.

• **11 April 2002:** suicide attack on a synagogue in Djerba (Tunisia), responsibility claimed by Islamic Army for the Liberation of the Holy Places. 15 deaths, **2 of which were French**.

• **8 May 2002:** attack on French engineers of DCN at Karachi (Pakistan) attributed to a group close to al Qaeda. 14 deaths, **11 of which were French**.

• **6 October 2002:** suicide attack on the French oil tanker Limburg offshore Yemen, claimed by al Qaeda. 1 death.

• **12 October 2002:** double suicide attack in a night club in Bali (Indonesia), responsibility claimed by Jemaah Islamiyah, close to al Qaeda. 202 deaths, **4 of which were French**.

• **28 November 2002:** double suicide attack in Mombasa (Kenya) against a hotel and an airliner, attributed to al Qaeda. 11 deaths.

• **12 May 2003:** triple suicide attack simultaneously at Riyadh (Saudi Arabia) against western residential complexes, claimed by al Qaeda in the Arabic Peninsula. 34 deaths.

• **16 May 2003:** quintuple simultaneous attacks in Casablanca (Morocco) against western and Jewish communities, attributed to an al Qaeda-inspired group. 41 deaths, **4 of which were French.**

• **5 August 2003:** attack on a Marriott hotel in Jakarta (Indonesia), carried out by Jemaah Islamiyah. 12 deaths.

• **19 August 2003:** attack on the United Nations building in Baghdad. 23 deaths, among them the Special Representative of the Secretary-General and **1 French**. Debut of the jihadist intervention in Iraq.

• **11 September 2003:** the Salafist Group for Preaching and Combat pledges its allegiance to al Qaeda.

• **8 November 2003:** attack in Riyadh (Saudi Arabia) on the residential complex of Mouhaya. 18 deaths.

• **15 and 20 November 2003:** respectively, attacks in Istanbul (Turkey) against the Jewish community (23 deaths) and British interests (27 deaths), attributed to al Qaeda.

• **11 March 2004:** four simultaneous waves of attacks (10) in Madrid (Spain), attributed to an al Qaeda-inspired group. 191 deaths, **among them 1 French**.

• **9 September 2004:** attack against the Australian Embassy in Jakarta (Indonesia), carried out by Jemaah Islamiyah. 9 deaths.

• **7 October 2004:** triple suicide attack in Taba (Egypt), attributed to a group close to al Qaeda. 34 deaths.

• **7 April 2005:** suicide attack in Cairo (Egypt) attributed to a group inspired by al Qaeda. 4 deaths, **2 of which were French**.

• **7 July 2005:** quadruple suicide attacks in London (United Kingdom), claimed by al Qaeda. 56 deaths, **1 of which was French**.

• **23 July 2005:** triple suicide attack in Sharm el-Sheikh (Egypt). 62 deaths.

• **9 November 2005:** triple suicide attack in Amman (Jordan). 57 deaths.

Appendix 2

Principal Threats against France since 1998

• **5 March 1998:** dismantling of an Islamic terrorist cell in Brussels (Belgium), suspected of preparing for attacks in France (Melouk cell).

• **18 May 1998:** declarations by Osama bin Laden in the Pakistani daily *Aousaf* threatening 23 western military installations in the region around the Persian Gulf, including the French base in Djibouti.

• **26 May 1998:** a series of arrests in France, Italy, Germany, Belgium and Switzerland of Maghreb terrorists planning attacks against the World Soccer Cup.

• **11 and 25 June 1999:** diffusion of two communications threatening France and Belgium attributed to an Algerian terrorist cell issued by GIA.

• **25 and 26 December 2000:** arrest in Frankfurt (Germany) of Maghreb terrorists planning an apparent attack against the cathedral and/or the Christmas market in Strasbourg.

• **20 September 2001:** dismantling of an al Qaeda cell in France, Belgium, and in the United Kingdom which was preparing for a suicide attack on the American Embassy in Paris, which was forecasted for July 2002 (Beghal network).

• **5 October 2001:** in Saint-Denis, dismantling of an Algerian Islamic cell suspected of planning an attack at the France-Algeria football match on 6 October 2001.

• **17 October 2001:** threat letters against France by the Salafist Group for Preaching and Combat (GSPC), a dissident branch of the GIA.

• **22 December 2001:** attempted attack against an Air France flight between Paris and Miami, attributed to al Qaeda.

• **12 November 2002:** communiqué from Osama bin Laden justifying the attacks committed on 11 September 2001, as well as the 8 May 2002 attacks in Karachi against French engineers.

• **16 December 2002:** dismantling of a cell in La Courneuve suspected of preparing a non-conventional attack (toxic agents) against the Russian Embassy in Paris.

• **24 December 2002:** continuation of this operation in Romainville.

• **16 February 2003:** statement by Osama bin Laden denouncing Western policy, including the Sykes-Picot Agreement.

• **2 June 2003:** arrest at Charles de Gaulle airport of Moroccan national Karim Mehdi, jihadist linked to the Hamburg cell, who was planning to go to Reunion Island to prepare a terrorist act against tourist sites.

• **16 September 2003:** arrest in Sanaa (Yemen) of a cell leader linked to the organization al Qaeda in the Arabian Peninsula planning attacks, especially against the French Cultural Centre and the US Embassy.

• **24 February 2004:** communiqué from Ayman al Zawahiri, deputy of Osama bin Laden, denouncing the French law on *laïcité* (secularism).

• **14 October 2004:** letter from Abdelmalek Droukdal, Emir of the GSPC, to Abu Musab al Zarqawi, denouncing France because of its relations with the Algerian government.

• **18 May 2005:** communiqué from Abu Musab al Zarqawi denouncing the French law on *laïcité* (secularism).

• **June 2005:** threats against the French Embassy in Baghdad.

• **July 2005:** threats made against France by the Pakistani weekly Dharb al Munim (8-14 July issue).

• **September 2005:** undated communiqué (posted online on 14 September) of the GSPC threatening France, qualified as 'enemy no. 1'.

• **26 September 2005:** police operation in France against a cell of former GIA members suspected of preparing attacks on the DST headquarters, Orly airport and the Paris Metro.

• **6 January 2006:** communiqué by al Zawahiri criticizing France for its policy in Algeria.

• **4 March 2006:** Call by al Zawahiri for an economic boycott of a number of European countries, including France, again condemning the French law on *laïcité* (secularism).

• **23 April 2006:** declaration by Osama bin Laden criticizing the French law on *laïcité* (secularism) and the muslims' status in France.

Drafting and Working Groups

Work on this White Paper was begun in May 2005 by Prime Minister Jean-Pierre Raffarin at the proposal of Dominique de Villepin, then Minister of the Interior, Internal Security and Local Freedoms. A Directing Committee for the White Paper was set up under the presidency of Nicolas Sarkozy, *Ministre d'Etat*, Minister of the Interior and Country Planning.

Six Working Groups were set up. They were chaired by the Director General for External Security (DGSE), the Director for Territorial Surveillance (DST), the Ambassador-Delegate to the World Summit on the Information Society, the Director of Criminal Affairs and Pardons of the Justice Ministry, the Director General for Political and Security Affairs of the Ministry of Foreign Affairs and the Special Advisor to the Director of the Foundation for Strategic Research.

The Permanent Secretary for National Defence (Secrétaire général de la défense nationale, SGDN) was the overall rapporteur of the White Paper. He was assisted by four senior officials from the State Council (*Conseil d'Etat*), the Interior Ministry, the Ministry of Defence and the Ministry of Foreign Affairs.

In the framework of the preparation of this White Paper, a conference open to the public, entitled 'The French in the face of terrorism,' was organized on 17 November 2005 under the chairmanship of the Prime Minister.

Table of Contents

La menace terroriste n'a jamais été aussi forte. Elle a aussi profondément changé de nature. Comme la plupart de ses partenaires, la France a adapté ses moyens d'action à ce nouveau contexte. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a ainsi permis de renforcer notre prévention face aux évolutions des moyens de transport et de communication.

En définissant une stratégie de long terme, le Livre blanc s'inscrit dans cet effort pour améliorer notre dispositif de lutte contre le terrorisme. Il est le fruit d'une réflexion associant des professionnels du renseignement, des magistrats, des hauts fonctionnaires, des journalistes et des universitaires.

Au-delà de l'adaptation de nos dispositifs, au-delà des atouts de la coopération internationale, seule une mobilisation la plus large possible nous permettra de relever le défi du terrorisme. Cela suppose une information claire sur la réalité de la menace et sur les moyens mis en œuvre pour y faire face. C'est le sens même de ce Livre blanc.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

Prix : 10 €
ISBN : 2-11-006101-4
DF : 5 8434-7
Imprimé en France

La Documentation française
29-31, quai Voltaire
75344 Paris Cedex 07
Téléphone : 01 40 15 70 00
Télécopie : 01 40 15 72 30
www.ladocumentationfrancaise.fr

9 782110 061010