



**CONSEIL DE
L'UNION EUROPÉENNE**

**Bruxelles, le 22 octobre 2010 (25.10)
(OR. en)**

**13153/2/10
REV 2**

**ENFOPOL 237
PROCIV 102
PARLNAT 78**

NOTE

du: Secrétariat général

au: COREPER

n° doc. préc.: 13154/10 ENFOPOL 238 PROCIV 103
8568/10 ENFOPOL 98 PROCIV 47 + COR 1
6090/2/10 REV 2 ENFOPOL 38 PROCIV 15 + COR 1
6090/10 ENFOPOL 38 PROCIV 15 RESTREINT UE

Objet: Informations sur le contenu et les résultats des évaluations

On trouvera dans le présent document le rapport final du deuxième cycle d'évaluation par les pairs dans le domaine de la lutte contre le terrorisme concernant "la préparation et la gestion des conséquences en cas d'attentats terroristes".

Le COREPER a approuvé, lors de sa réunion du 22 septembre 2010, la transmission du rapport au Parlement européen et aux parlements nationaux.

- I. Historique
- II. Base de l'évaluation par les pairs
- III. Processus d'évaluation
- IV. Principales conclusions
- V. Résultats

I. HISTORIQUE

1. À la suite des attentats commis aux États-Unis le 11 septembre 2001, le Conseil a lancé le 20 septembre 2001 un exercice d'évaluation des dispositifs nationaux de lutte contre le terrorisme sous la forme d'une évaluation par les pairs, en se fondant sur des considérations d'ordre législatif, administratif et technique. Le principal objectif consistait à recenser et à bien comprendre les mécanismes mis en place dans chacun des vingt-sept États membres.
2. Les visites d'évaluation ont été effectuées entre 2003 et 2005 et font l'objet d'un rapport final¹ qui énonce des recommandations adressées à l'ensemble des États membres à titre individuel ou collectif, en vue d'améliorer encore leurs dispositifs antiterroristes nationaux. En outre, les meilleures pratiques ont été répertoriées et un aperçu général des dispositifs antiterroriste dans tous les États membres a été dressé. La mise en œuvre de ces recommandations a été évaluée par le groupe "Terrorisme" en 2006² et un rapport de suivi concernant la mise en œuvre des recommandations du Conseil de l'UE sur des mesures de lutte contre le terrorisme dans les États membres a été achevé en 2007³.

¹ Document 12168/3/05 REV 3 ENFOPOL 109.

² Ces recommandations générales ont été mises en œuvre à 95%.

³ Document 5356/2/07 REV 2 ENFOPOL 30.

3. L'évaluation par les pairs a contribué de façon significative à la réforme des dispositifs antiterroristes dans les États membres. Cette démarche commune des États membres, qui ont œuvré dans la même direction, a permis de renforcer la capacité collective de l'UE dans ce domaine.

Compte tenu de ces résultats encourageants, les États membres ont décidé d'effectuer un deuxième cycle d'évaluation par les pairs, qui contribuerait à la poursuite de la mise en œuvre de la stratégie antiterroriste dans l'UE.

II. BASE DE L'EVALUATION PAR LES PAIRS

4. Parmi les neuf sujets potentiels proposés pour le deuxième cycle par le Secrétariat du Conseil, les États membres et la Commission, on citera la vidéosurveillance, le financement du terrorisme et la lutte contre la radicalisation et le recrutement. Il est ressorti des discussions que dans leur grande majorité (vingt-trois), les États membres jugeaient nécessaire de renforcer la capacité de l'UE à réagir de façon appropriée en cas d'attentats terroristes. C'est pourquoi il a été convenu que la préparation et la gestion des conséquences⁴ constitueraient le thème central du deuxième cycle d'évaluation par les pairs.
5. Les dispositifs nationaux de gestion de crise n'ont pas fait jusqu'ici l'objet d'une évaluation en profondeur ni de considérations politiques au niveau de l'UE. Le deuxième cycle d'évaluation par les pairs devait se concentrer sur ces dispositifs. Il était essentiel d'éviter les chevauchements avec les travaux en cours dans le domaine de la protection civile et notamment de la protection des infrastructures critiques, qui constituent un sujet plus étendu que la protection des cibles faciles et sont examinées par un groupe de travail spécifique. Cela favoriserait l'adoption d'une démarche cohérente et compatible dans les États membres et jetterait les bases d'une réaction coordonnée face à un attentat terroriste dans le cas où plusieurs États membres seraient touchés.

⁴ Document 7188/07 ENFOPOL 39 RESTREINT UE.

6. En mai 2007, le comité de l'article 36 a approuvé le thème du deuxième cycle d'évaluation et désigné le groupe "Terrorisme" comme étant le groupe compétent pour poursuivre les travaux dans ce domaine, conformément aux articles 2, 3, 4, 5 et 8 de la décision du Conseil du 28 novembre 2002⁵.

III. PROCESSUS D'EVALUATION

7. Le deuxième cycle d'évaluation comportait quatre volets: le questionnaire, les visites dans les pays, les rapports nationaux et le rapport final.
8. Une fois qu'un consensus a été dégagé sur le thème général, il a été nécessaire de définir les sous-thèmes plus spécifiques sur lesquels porteraient les questions. Il a été jugé important de limiter le nombre de sous-thèmes à trois au maximum, afin de garantir un processus réaliste et efficace.

Il était également essentiel de garantir la cohérence et la complémentarité des trois sous-thèmes, pour faire en sorte, en particulier, que chaque équipe d'évaluation dispose des capacités et des compétences nécessaires pour traiter l'ensemble des questions.

9. Aussi le questionnaire a-t-il été divisé en trois parties:
- structures et organisation des centres de crise nationaux;
 - formation/exercices pour tester les centres de crise et les systèmes de communication nationaux en cas d'attentats terroristes;
 - cibles faciles.
10. Ces trois parties étaient couvertes par un ensemble de questions spécifiques destinées à recueillir des éléments pour alimenter les visites d'évaluation et le futur rapport final. Le questionnaire a été envoyé aux États membres le 1^{er} août 2007 afin qu'ils l'examinent une dernière fois et formulent le cas échéant des propositions. Certaines propositions des États membres ont été incorporées dans la version finale, qui a été approuvée par le groupe "Terrorisme" le 16 octobre 2007.

⁵ Décision 2002/996/JAI (JO L 349 du 24.12.2002, p. 1).

11. Les réponses au questionnaire ont servi de base aux travaux menés lors des réunions et aux questions posées lors des visites dans les États membres. Les États membres, Europol et la Commission ont été invités à désigner des experts pour constituer les équipes d'évaluation. Chaque équipe d'experts comprenait en principe un expert désigné par le Secrétariat général, deux experts désignés par les États membres, un expert désigné par Europol et un expert désigné par la Commission.
12. Les visites, d'une durée moyenne de trois jours, ont été préparées par les États membres, en coopération avec le Secrétariat du Conseil. Les États membres évalués étaient chargés de désigner les services et les personnes les plus à même de répondre aux questions et de lever les doutes des experts constituant la délégation, l'objectif étant de se faire une idée plus claire du dispositif de gestion des crises et de leurs conséquences mis en place dans le pays considéré.
13. Les visites ont été effectuées selon l'ordre indiqué à l'annexe 1.
14. Au terme de chaque visite d'évaluation, les experts ont été invités à élaborer un projet de rapport destiné au Secrétariat général du Conseil. Les projets de rapports, les réponses au questionnaire ainsi que tous les éléments fournis par chaque pays⁶ ont été utilisés comme sources d'information pour l'élaboration des rapports nationaux/par pays. Les rapports nationaux/par pays ont été soumis à l'État membre concerné pour observations. Celui-ci a fait part de son avis sur le rapport, habituellement dans un délai de six semaines, et le rapport a été modifié lorsque l'État membre concerné l'a jugé nécessaire. Les rapports nationaux/par pays figurent aux addendums 1 à 27 du présent document.
15. L'avancement du cycle d'évaluation a été présenté lors de plusieurs réunions du groupe "Terrorisme", et un rapport intermédiaire (document 12287/09 ENFOPOL 199) a été établi à la demande de la présidence suédoise.

⁶ Transparents PowerPoint, exposés, brochures, plans, etc.

IV. PRINCIPALES CONCLUSIONS

16. Lors des visites, il a été constaté que s'ils visent tous à répondre à la même préoccupation, les systèmes mis en place pour gérer les conséquences des attentats terroristes présentent néanmoins de nombreuses différences. Ils sont adaptés à la taille, la géographie et la répartition de la population du pays considéré ainsi qu'à la perception de la menace. Cette dernière varie en fonction des États membres, selon des facteurs historiques, politiques ou juridiques, les frontières, les réseaux sociaux et les relations avec les pays à risque. Aussi les meilleures pratiques recueillies traduisent-elles une approche nuancée de la question.
17. Le principal paramètre est le cadre juridique propre aux différents modèles politiques qui caractérisent les vingt-sept États membres; il en va de même en ce qui concerne la gestion de crise. Certains pays sont dotés de structures politiques particulièrement dynamiques, qui interviennent jusqu'au niveau des décisions opérationnelles, alors que dans d'autres, les autorités politiques jouent un rôle davantage stratégique et définissent les grands objectifs à atteindre. Dans le premier cas, on est en présence d'un modèle relativement bureaucratique, qui peut être extrêmement tributaire d'un système de communication efficace, et dans le second, une distance est maintenue entre l'autorité politique et les décisions les plus importantes (par exemple, recours aux forces armées pour renforcer les structures civiles).
18. Les orientations régissant les activités des forces et des structures intervenant dans la gestion de crise, ainsi que leur coordination politique, peuvent émaner directement du cabinet du Premier ministre, de différents ministères, ou encore d'un ministère unique, généralement le ministère de l'intérieur ou le ministère de la défense. À condition que le processus de coordination ne soit pas exagérément complexe ni abstrait, ces différents modèles de gestion, dont le degré de centralisation varie, peuvent se révéler aussi efficaces les uns que les autres. Dans tous les cas, les équipes de premiers secours sont mobilisées immédiatement et enclenchent l'ensemble des procédures habituelles destinées à faire face à un attentat terroriste et mettent en œuvre les plans d'urgence, dans la mesure du possible et lorsqu'il en existe.

19. Certains États membres disposent de plans spécifiques pour faire face aux situations d'urgence, le terrorisme n'étant qu'un cas parmi d'autres. Les différents plans peuvent être combinés et des mesures générales peuvent être adoptées en fonction des besoins et des circonstances. Il arrive que ces plans débouchent sur une solution trop rigide pouvant poser des problèmes lorsqu'il faut adapter les mesures prédéfinies à la situation concrète. D'autres États membres ne disposent pas de plans spécifiques, mais seulement d'un plan général, sorte de plan parapluie destiné à faire face aux conséquences d'un attentat terroriste au même titre que de toute autre situation de crise.

Dans ce dernier cas, le plan général s'appuie sur les mesures et l'organisation propres aux différentes autorités de police et services de secours, ce qui le rend plus souple, certes, mais aussi plus difficile à mettre en œuvre.

20. Dans quelques États membres, une crise est gérée au niveau local dans un premier temps, et ce n'est qu'en cas de manque de ressources que la gestion de la situation est transférée au niveau régional ou national, selon le principe de subsidiarité. Dans d'autres États membres, la gestion de crise est considérée comme une question d'importance nationale, et l'échelon central prend la tête des opérations dès qu'une urgence est déclarée. La formule retenue dépend souvent des ressources disponibles dans le pays et de leur répartition sur le territoire national. Une approche centralisée est fréquemment un moyen de compenser le caractère limité des ressources disponibles pour gérer les crises.
21. Une autre différence manifeste entre les États membres tient aux centres de crise. Dans certains cas, le centre de crise est une structure permanente disposant de locaux et d'un personnel spécifiques et jouant en permanence un rôle important dans le dispositif de gestion de crise. Dans d'autres cas, la crise est gérée par un organisme ad hoc constitué des principales autorités concernées, qui ne se réunit qu'en cas de besoin. Enfin, il existe dans certains États membres un troisième modèle dans lequel le centre de crise est une structure physique comprenant tous les éléments nécessaires pour gérer une situation de crise (salles de réunion, matériel de communication, systèmes informatiques, etc.) mais activée uniquement pour faire face à une situation particulière (visite d'État, grandes manifestations sportives, catastrophes naturelles, entre autres).

22. En ce qui concerne la formation nécessaire pour tester le centre ou le dispositif de crise national et le système de communication en cas d'attentat terroriste, différentes solutions ont été rencontrées. Tous les États membres organisent des exercices, mais dans certains cas, il s'agit uniquement d'exercices de simulation n'impliquant pas tous les services concernés, parfois pas même les intervenants en première ligne. Dans certains cas, le nombre d'exercices menés en coopération avec les pays voisins (États membres ou pays tiers) est insuffisant.
23. Lors des visites, les équipes d'experts ont constaté que les pays avaient progressé de façon très différente dans le passage des réseaux analogiques, parfois non cryptés, aux réseaux numériques cryptés. Toutefois, tous les pays disposent à tout le moins de plans prévoyant une telle transition. Certains ont déjà mené à bien la mise en place d'un réseau numérique crypté national ou l'auront menée à bien très prochainement.
24. En ce qui concerne les cibles faciles, un nombre significatif d'États membres les assimilent aux infrastructures critiques et adoptent les mêmes mesures de sécurité dans les deux cas. D'autres États considèrent et traitent les cibles faciles comme un problème distinct. La question des cibles faciles peut, entre autres, être du ressort d'une autorité nationale ou la compétence en la matière peut être déléguée au niveau local. En tout état de cause, il incombe à l'instance responsable non seulement de répertorier les cibles faciles, mais aussi de proposer les mesures et les procédures de sécurité nécessaires.

V. RESULTATS

25. Du point de vue national, l'évaluation par les pairs a permis aux États membres d'étudier et de réévaluer leurs propres structures. Les considérations formulées au moment de répondre au questionnaire ainsi que dans le cadre du deuxième volet, durant la visite d'évaluation, ont permis d'opérer un rapprochement entre les différentes structures nationales participant à la gestion de crise et de renforcer les liens entre elles. Elles ont aussi permis de clarifier les compétences de chaque instance concernée et de répertorier les défaillances du système. De la même manière, les réunions avec les équipes d'experts ont été l'occasion dans quelques États membres de réunir les différentes instances concernées autour de la même table, ce qui a contribué à renforcer les contacts personnels et institutionnels dont l'importance est primordiale en temps de crise.

26. Chaque rapport par pays énonce des recommandations spécifiques qui tiennent compte des cadres juridiques et politiques nationaux et ciblent le modèle mis en place.
- Ces recommandations spécifiques, étayées par des procédures existant dans d'autres États membres, sont conçues pour améliorer les dispositifs en place en proposant des mesures à adopter. Elles sont en outre destinées à confronter les autorités nationales à un regard extérieur, afin de leur permettre de remettre en question les dispositifs nationaux de gestion des crises et de leurs conséquences.
27. Outre les recommandations, l'un des principaux objectifs de cette entreprise consistait à recueillir les meilleures pratiques. Les meilleures pratiques ont été répertoriées dans l'ensemble des vingt-sept États membres en fonction des différents modèles mis en place et regroupées à l'annexe 2 du présent rapport. Si l'on se place à un niveau supranational, le regroupement des meilleures pratiques permettra aux États membres d'appliquer les solutions mises en place par d'autres États membres pour résoudre des problèmes similaires, en adaptant des mécanismes compatibles à leur modèle national. Le recensement des meilleures pratiques permettant de résoudre un problème dans un État membre contribuera sans conteste à intensifier le dialogue entre les États membres de l'UE, autour de la question capitale que constitue la sécurité.
28. Sur la base des recommandations spécifiques et des meilleures pratiques, le présent rapport formule des recommandations générales qui vont au-delà des modèles et des structures nationales et visent à améliorer la gestion des crises et de leurs conséquences à l'échelon européen ainsi qu'à mieux aligner les modèles de gestion de crise des vingt-sept États membres de l'UE.
29. Les dix recommandations générales ci-après sont regroupées selon les quatre thèmes suivants:
- a) questions structurelles;
 - b) communications;
 - c) amélioration de la coopération;
 - d) communication avec le public.

a) Questions structurelles

1. Élaboration d'un plan général de gestion de crise

Pour la plupart, les États membres ont mis en place des plans spécifiques pour faire face à des scénarios de crise concrets; certains ont prévu un nombre significatif de plans de cette nature. Il est essentiel de faire en sorte que tous les plans existants soient compatibles au niveau de l'ensemble du territoire du pays, ainsi que de remédier à tout conflit de compétence entre les différents organismes participant à la gestion de crise. Par conséquent, un plan général compatible avec les plans existants et répondant à toute lacune ou incertitude qui apparaîtrait lors de la mise en œuvre de plusieurs plans différents, constitue un document indispensable pour coordonner efficacement les mécanismes de gestion de crise.

2. Centre de crise national

Tous les États membres ont créé un centre de crise national ou une structure similaire conçue pour faire face à une crise de grande envergure, qu'elle soit ou non liée au terrorisme. Selon les États membres, le centre de crise national est organisé de différentes manières: dans certains, il s'agit d'une structure permanente disposant d'installations, d'un personnel permanent et de compétences définies par voie législative. Dans d'autres États membres, le centre de crise national est un concept étayé par des plans permettant de regrouper ses membres en cas de crise, dans les installations de l'organisme qui prend la tête des opérations dans le cas d'espèce. Il est impossible d'évaluer l'efficacité relative des différents modèles parce que seuls quelques États membres de l'UE ont été appelés à faire face aux conséquences d'attentats terroristes. Toutefois, quel que soit le modèle mis en place dans chaque État membre, le rôle du centre de crise national doit être clairement défini. Le centre de crise devrait être bien connu au niveau national; sa composition de base et son rôle devraient être bien déterminés.

Pour pouvoir faire face à une crise liée au terrorisme, les instances nationales participant à la gestion des crises et de leurs conséquences doivent être en mesure de reconnaître le centre de crise national comme étant formellement chargé d'assurer la coordination. Il importe d'éviter les chevauchements entre les structures existantes et le centre de crise national, ce dernier devant se concentrer sur son rôle de coordination au niveau national.

b) Communications

3. Réseaux numériques cryptés et gestion des conséquences en cas d'attentats terroristes

- 3 a) Mise en place ou développement des réseaux numériques cryptés permettant à l'ensemble des services de secours de travailler de concert

Vu les développements et les progrès techniques dans le domaine du terrorisme, il est désormais impossible aux services de secours de s'acquitter de leur mission au moyen de réseaux non cryptés. De même, il est nécessaire sur le plan technique de disposer de réseaux numériques cryptés pour assurer la coordination étroite requise entre les différentes parties concernées.

Afin aussi bien d'assurer au public un service efficace que de garantir la sécurité des différents services de secours, il est important que tous les États membres achèvent de doter les services concernés d'un réseau de communication numérique crypté.

- 3 b) Améliorer la compatibilité des réseaux numériques cryptés dans les régions frontalières

Il faut s'efforcer de mettre en place des solutions simples pour rendre les réseaux radio compatibles dans les régions frontalières, notamment lorsque des normes techniques différentes sont utilisées (TETRA ou TETRAPOL).

En vue de contribuer à remédier à ce problème, les États membres devraient participer au groupe d'experts institué par la *recommandation du Conseil relative à l'amélioration des radiocommunications entre unités opérationnelles en zone transfrontalière*⁷, afin d'étudier les questions liées à la mise au point d'une interface inter-systèmes pour TETRA et TETRAPOL et de tirer les leçons du rapport du groupe "Coopération policière" sur la viabilité de la mise en place de telles interfaces, prévu pour juin 2010⁸.

⁷ Document 10141/09 ENFOPOL 143 TELECOM 116 COMIX 421, approuvé par le Conseil les 4-5 juin 2009.

⁸ Des réunions sur ce sujet sont prévues en mai et octobre 2010.

4. Établissement de communications directes entre les centres de crise des différents États membres

Les centres de crise sont chargés de l'ensemble de la coordination stratégique des mesures adoptées pour faire face à un événement tel qu'une situation d'urgence liée au terrorisme. Alors qu'au niveau interne, la plupart des États membres ont défini clairement les compétences des différents organismes concernés, davantage d'incertitudes doivent être levées en ce qui concerne les contacts internationaux.

En cas de crise transfrontière, et lorsqu'il faut coordonner les mesures prises par les différents États membres touchés par un même événement, il est nécessaire que les centres de crise puissent se mettre en rapport avec leurs homologues dans les autres États membres. Aussi est-il recommandé d'établir une liste claire, complète et à jour de l'ensemble des centres de crise et des points de contact, pour les questions liées au terrorisme, dans les différents États membres. Une telle liste a déjà été établie par le groupe "Protection civile"⁹ et incorporée dans le Manuel sur la coordination des situations d'urgence et des crises par l'UE. Cette liste devrait être mise à jour le plus souvent possible, par l'intermédiaire des groupes de travail existants au niveau de l'UE, et une liste de diffusion appropriée devrait être établie.

Il faut aussi établir une communication directe entre ces structures non seulement pour qu'il soit plus facile d'arrêter d'un commun accord les décisions requises, en cas de besoin, mais aussi pour permettre un échange d'informations, durant la crise, entre l'État membre touché et les autres États membres.

⁹ Voir le document 7154/10.

c) Améliorer les différentes formes de coopération

5. Partenariat public-privé

En règle générale, le contact, au niveau des États membres, entre les autorités publiques et le secteur privé en ce qui concerne les cibles faciles est insuffisant. Les contacts entre les secteurs public et privé en matière de lutte contre le terrorisme ne sauraient se limiter à l'octroi de permis de construire ou à l'exécution d'inspections incendie. Il est nécessaire d'établir une relation fondée sur la confiance et le dialogue, permettant aux entreprises privées de consulter les autorités compétentes sur différents aspects de leurs activités. Il peut s'agir aussi bien des mesures à adopter à des fins de protection passive dans le cadre de la construction d'un bâtiment ou de la gestion d'un espace public que des accords avec les hôpitaux privés en ce qui concerne la coordination des secours lorsque se produit un événement faisant un grand nombre de victimes, par la mise en place d'activités de formation ou d'évaluation communes.

En ce qui concerne les cibles faciles, la mise en place d'un interlocuteur officiel tel que le National Counter Terrorism Security Office (Royaume-Uni), chargé d'étudier les menaces éventuelles et les risques liés à une cible déterminée ainsi que de conseiller les partenaires publics/privés, constitue donc un progrès significatif.

6. Renforcer la coopération entre les autorités civiles et militaires

Les autorités civiles et les forces armées nationales possèdent une expérience considérable en matière de gestion de situations de crise, acquise notamment dans le cadre des interventions menées à l'étranger dans ce domaine, par exemple en ce qui concerne la gestion de crises au jour le jour et les missions internationales, et des activités de formation à l'utilisation de nouveaux équipements. Alors que dans la plupart des États membres, l'armée vient épauler les moyens civils en cas de crise majeure, il n'en est pas moins toujours possible d'améliorer la coopération entre l'armée et les secours d'urgence en amont, en instaurant des échanges d'expérience et de connaissances et en poussant plus loin l'intégration de l'armée aux procédures d'urgence civiles ainsi que par l'acquisition et la mise en œuvre pratique de matériel. Cela permettra d'harmoniser les procédures et d'assurer la compatibilité des moyens disponibles en cas de crise liée au terrorisme.

7. Formation transfrontière

Il est ressorti clairement de l'ensemble des visites effectuées que la coopération transfrontière constitue un sujet de préoccupation pour tous les États membres, en particulier les pays limitrophes, qu'ils soient ou non membres de l'UE. Les exercices tels que ceux effectués par le réseau ATLAS pour les unités spéciales d'intervention devraient être organisés à l'intention des différentes autorités participant à la gestion des crises et de leurs conséquences en cas d'attentats terroristes.

Ces exercices offrent l'occasion aux différents interlocuteurs d'apprendre à se connaître personnellement, ce qui ne peut que contribuer à simplifier les contacts en cas de crise. Ils sont aussi l'occasion d'actualiser les approches et de trouver des solutions à un certain nombre de difficultés qui risqueraient d'avoir des conséquences graves si elles ne sont pas mises en évidence avant qu'une crise ne se produise. Les exercices transfrontière doivent être menés aussi bien parmi les États membres qu'avec les pays tiers, selon qu'il conviendra.

Sans pour autant remplacer les exercices transfrontière, la participation d'observateurs des pays voisins doit aussi être développée.

La participation de membres du personnel des services de secours, en qualité d'observateurs, aux exercices des pays voisins est moins onéreuse que les exercices transfrontière et peut constituer un moyen supplémentaire d'entretenir les contacts et de maintenir à jour la connaissance des moyens et des techniques d'intervention respectifs.

d) Communication avec le public

8. Site Internet spécifique pour les situations de crise

De nombreux États membres s'efforcent de tenir le public informé au moyen de sites Internet. Dans la plupart des cas, il s'agit des sites habituels des pouvoirs publics, sur lesquels les informations concernant la crise sont publiées au même titre que les renseignements habituels, les listes des membres du personnel des différents services ou les déclarations de personnalités. Il en résulte une certaine confusion, la priorité n'étant pas donnée à l'accès aux informations essentielles.

Toutefois, d'autres États membres ont opté pour des sites consacrés exclusivement à la gestion de crise. Ces sites offrent au public un accès plus clair et rapide aux informations importantes et lui permettent de mieux suivre la situation. Le nom de domaine doit être clair et facile à mémoriser, et le contenu du site doit concerner exclusivement la gestion de la crise en cours (information sur l'évolution de la situation, conseils, etc.). Ces sites ne sont pas alimentés en dehors des périodes de crise. Ils doivent être conçus de manière à résister à toutes les formes de cyberattaques.

9. Centraliser tous les appels d'urgence au moyen du numéro d'appel d'urgence européen 112

Bien que tous les États membres aient instauré le numéro central 112, celui-ci coexiste toujours dans certains cas avec un autre numéro central. Dans d'autres cas, il coexiste avec plusieurs numéros d'appel d'urgence de différents services, parfois sans aucune interconnexion. Il existe des solutions techniques permettant de changer les habitudes héritées du passé ou de remédier à des problèmes logistiques. En tout état de cause, priorité devrait être donnée à la mise en œuvre du numéro central 112, qui devrait être organisé de manière à permettre une distinction immédiate entre les différents types de situations d'urgence et de répondre aux demandes du public.

10. Création d'une unité d'aide psychologique ou renforcement des unités existantes

Il est communément admis qu'à côté des victimes souffrant de traumatismes physiques à la suite d'un attentat, un nombre plus élevé encore de victimes souffrent de traumatismes psychiques. On citera parmi ces personnes celles qui ont perdu un membre de leur famille, un ami ou un collègue, ou qui ont simplement survécu à un attentat. Il est par conséquent recommandé de créer des unités de spécialistes de ce type d'assistance chargées de proposer à ces victimes une aide aussi bien immédiate qu'à long terme ou de renforcer ces unités lorsqu'il en existe déjà.

ANNEXE 1 DE L'ANNEXE

<i>État membre</i>	<i>Dates</i>
<i>Lettonie</i>	<i>28-30/05/2008</i>
<i>République tchèque</i>	<i>11-13/06/2008</i>
<i>Grèce</i>	<i>18-20/06/2008</i>
<i>Hongrie</i>	<i>02-04/07/2008</i>
<i>Chypre</i>	<i>10-12/09/2008</i>
<i>Malte</i>	<i>17-19/09/2008</i>
<i>Royaume-Uni</i>	<i>08-10/10/2008</i>
<i>Bulgarie</i>	<i>22-24/10/2008</i>
<i>France</i>	<i>19-21/11/2008</i>
<i>Pays-Bas</i>	<i>26-28/11/2008</i>
<i>Belgique</i>	<i>21-23/01/2009</i>
<i>Autriche</i>	<i>28-30/01/2009</i>
<i>Lituanie</i>	<i>18-20/02/2009</i>
<i>Pologne</i>	<i>25-27/02/2009</i>
<i>Finlande</i>	<i>11-13/03/2009</i>
<i>Luxembourg</i>	<i>18-20/03/2009</i>
<i>Espagne</i>	<i>01-03/04/2009</i>
<i>Portugal</i>	<i>15-17/04/2009</i>
<i>Estonie</i>	<i>06-08/05/2009</i>
<i>Suède</i>	<i>10-12/06/2009</i>
<i>Slovénie</i>	<i>17-19/06/2009</i>
<i>Roumanie</i>	<i>16-18/09/2009</i>
<i>Italie</i>	<i>23-25/09/2009</i>
<i>Danemark</i>	<i>14-16/10/2009</i>
<i>Slovaquie</i>	<i>28-30/10/2009</i>
<i>Irlande</i>	<i>18-20/11/2009</i>
<i>Allemagne</i>	<i>25-27/11/2009</i>

MEILLEURES PRATIQUES EN MATIÈRE DE PRÉPARATION ET DE GESTION DES CONSÉQUENCES EN CAS D'ATTENTATS TERRORISTES

La présente annexe dresse l'inventaire des principales bonnes pratiques qui figurent dans les rapports nationaux d'évaluation par les pairs relatifs aux États membres évalués.

1. DISPOSITIONS PRÉVUES EN CAS D'ATTENTATS TERRORISTES

1.1. Dispositions prévues à l'échelle nationale

1.1.1. Mesures d'ordre législatif ou organisationnel

- L'élaboration de lignes directrices et leur diffusion au niveau des différents ministères, dans le but de créer une approche commune en matière de sécurité et de mesures de gestion des crises, constitue une avancée importante. Cette élaboration de normes communes permet une planification plus aisée ainsi qu'une gestion plus efficace de toute situation de crise éventuelle. (Autriche)
- En cas de crise, les différentes autorités publiques peuvent demander l'aide de l'armée, et des accords correspondants existent au niveau des Länder. L'armée ne fait pas office de premier intervenant, mais fournit un appui très important pour la gestion des crises, grâce à ses forces bien entraînées et extrêmement bien équipées. La participation de l'armée, avec son personnel et son équipement moderne, s'avère généralement obligatoire en matière de gestion des crises et de leurs conséquences, et il pourrait en être de même pour tous les États membres de l'UE. En outre, il peut être fait appel aux compétences spécialisées que possède l'armée en ce qui concerne des types de dangers bien précis, par exemple dans le domaine des armes chimiques ou nucléaires. Le fait que cette coopération et ce soutien soient déjà inscrits dans la Constitution constitue un élément prospectif. (Autriche)

- L'organisation du centre national de coordination. La structure organisationnelle du centre national de coordination comprend deux grandes divisions: la Gestion opérationnelle et la Planification d'urgence. L'existence d'une division chargée de la planification reflète l'intégration de la planification d'urgence, qui constitue l'une des tâches principales du centre national de coordination. Ce dispositif organisationnel mérite une mention positive. Il établit principalement un lien solide et très important entre la planification d'urgence (qui est essentiellement une activité "de temps de paix") et la gestion des activités au cours des crises, étant donné que la gestion efficace des crises dépend de la planification qui est effectuée dans le cadre des activités quotidiennes.

Ce dispositif permet en outre de fournir des orientations à l'intention des responsables de la planification aux niveaux fédéral, provincial et communal; il facilite la coordination et l'harmonisation des plans d'urgence et donne au centre national de coordination une connaissance approfondie de la qualité de la planification d'urgence réalisée par les différentes autorités. Par ailleurs, le personnel du centre de crise semble avoir pour philosophie de faciliter la coordination entre les autorités et/ou les disciplines concernées, sans chercher à empiéter sur les responsabilités ou les compétences respectives de celles-ci, en incitant d'autres départements à coopérer étroitement et de manière transparente avec le centre de crise. (Belgique)
- Cinq "disciplines" sont présentes dans tous les forums pluridisciplinaires qui interviennent dans la gestion des incidents ou des crises, que ce soit sur le site de l'incident ou dans les centres de coordination mis sur pied aux niveaux communal, provincial ou national.

Les forces armées sont déjà intégrées dans la phase de planification des plans globaux au sein de la Discipline 4. Un déploiement peut être organisé par l'intermédiaire du commandement militaire de la province concernée, sans qu'il soit nécessaire de passer par l'ensemble de la hiérarchie gouvernementale. En termes de meilleures pratiques, l'intégration de la cinquième discipline (communication d'informations au public) mérite également que l'on s'y intéresse. Cette tâche revêt une grande importance, en particulier lorsqu'il s'agit d'incidents de grande ampleur, comme c'est le cas pour les attentats terroristes. Il est dès lors très satisfaisant de constater que les autorités belges considèrent l'information au public comme faisant partie intégrante du dispositif de gestion des crises dans tous les forums où des autorités coopèrent afin de gérer des incidents ou des crises. (Belgique)

- La gestion des situations de crise et des catastrophes est codifiée dans deux actes juridiques qui ont été régulièrement modifiés (pour tenir compte de l'expérience acquise dans leur mise en œuvre et de besoins nouveaux) depuis leur adoption, à savoir la loi sur la gestion des crises de 2005 et la loi sur la protection en cas de catastrophes, adoptée en 2006. (Bulgarie)
- La loi attribue des compétences à différents organes concernés par la gestion des crises et par la direction des opérations sur le lieu des crises. (Bulgarie)
- La création, en 2008, de l'Agence de l'État pour la sécurité nationale, ainsi que du centre de coordination de la lutte contre le terrorisme. (Bulgarie)
- Le dispositif de commandement à trois niveaux mis en place pour la police (or - argent - bronze) a fait ses preuves dans le domaine du terrorisme et d'autres grands événements et devrait répondre efficacement aux impératifs de gestion des organisations de crises. La répartition des tâches prévue dans le cadre de ce dispositif semble avoir été bien prise en compte par la direction de la police. (Chypre)
- Du personnel militaire peut être déployé, en nombre limité, pour exécuter les tâches de police, sur la base des règlements publics. Dans ce cas, les forces armées sont placées sous le commandement de la police et reçoivent une formation concernant leur mission avant le déploiement. (République tchèque)
- L'existence du plan d'action national visant à lutter contre le terrorisme. La République tchèque s'est dotée d'un plan national, qui a été mis à jour à cinq reprises (une fois par an depuis 2002) et qui fixe des objectifs non seulement stratégiques, mais aussi opérationnels. Des organisations ont été désignées et des délais leur ont été impartis pour atteindre l'objectif fixé. Chaque objectif est assorti des indications suivantes: le délai pour atteindre le résultat escompté, un organisme compétent, des indicateurs de performance, ainsi que le montant estimé et les sources du financement lié à la mission. (République tchèque)

- L'Estonie a fait un effort pour réduire le nombre des agences appelées à intervenir lors d'une situation de crise, en fusionnant plusieurs agences en un seul organisme responsable en cas d'urgence. Cela réduira les coûts, améliorera l'accessibilité du service pour le citoyen et contribuera à éviter les conflits d'intérêts et de compétences. Même si l'Estonie est comparativement un petit pays, où il est peut-être plus facile de mener à bien une telle réforme administrative, l'exemple estonien pourrait encourager d'autres États membres à examiner si la fusion d'agences pourrait également créer des synergies chez eux et permettre de délimiter clairement les responsabilités. (Estonie)
- Les principaux acteurs de la communauté de sécurité estonienne semblent très bien se connaître, ce qui facilite la gestion des crises. Cela s'explique par le fait que de nombreux échanges de personnel sont organisés entre les autorités concernées. (Estonie)
- Le ministère de l'intérieur a dressé une liste comprenant 26 scénarios d'urgence différents, afin d'élaborer des plans d'intervention spécifiques, adaptés à chaque incident. Même si la liste peut paraître longue et contient peut-être quelques redondances, le principe consistant à mettre au point des procédures opérationnelles normalisées adaptées à des scénarios spécifiques peut contribuer à réagir plus rapidement et plus efficacement en cas d'urgence, pour autant que les plans d'urgence soient élaborés en faisant preuve d'une souplesse suffisante. (Estonie)
- La Finlande est résolument déterminée à simplifier autant que possible le modèle de gestion de crise et un réel effort a été fait en ce sens. Cet effort a débouché sur une gestion des crises extrêmement efficace. (Finlande)
- Considéré comme étant une forme de menace contre la sécurité publique, le terrorisme constitue à ce titre une matière relevant de la compétence de la police finlandaise et est assimilé à une infraction pénale. D'autres autorités apportent leur soutien à la police pour exécuter ces missions et, pour cette raison, la police est autorisée à utiliser les ressources des forces de défense ainsi que d'éventuelles autres ressources provenant de tout organisme quel qu'il soit, qui pourraient être considérées comme importantes pour gérer une situation liée au terrorisme. En raison du manque de ressources, toutes les fonctions sont exécutées en partageant les ressources. Les autorisations, qui reposent sur une base juridique solide, ainsi qu'une formation et une communication régulières, donnent des garanties suffisantes quant au fait que les ressources seront utilisées de la manière la plus efficace possible. Étant donné que cette gestion permet d'éviter les doubles emplois, des économies importantes peuvent être réalisées sur l'acquisition d'équipements ainsi que sur leur utilisation en cas d'urgence. (Finlande)

- L'équipe spéciale d'intervention (Karhu) consacre 40 % de son temps de travail aux activités quotidiennes de la police. Cette méthode de travail permet aux membres de l'unité de se tenir informés des travaux d'ordre général de la police et d'établir des contacts personnels avec les officiers chargés des tâches quotidiennes de la police. (Finlande)
- Les échanges réguliers de personnel entre la sûreté nationale et les services centraux de la police judiciaire assurent une meilleure compréhension mutuelle par ces deux entités de leurs activités et tâches respectives et permettent une coopération harmonieuse en cas d'enquêtes connexes. (Finlande)
- Considérés dans leur ensemble, l'éventail des plans d'intervention VIGIPIRATE, créés sous l'égide du secrétaire général de la défense nationale, couvrent pleinement le spectre de la menace terroriste. (France)
- La centralisation autour d'une chaîne hiérarchique bien définie semble particulièrement efficace. La tâche de gestionnaire et de coordinateur, que le préfet de zone de défense est appelé à exercer lorsqu'une crise se produit dans la région relevant de sa responsabilité, constitue un mécanisme utile. (France)
- L'organisation de l'État sur une base fédérale est conçue de manière à ne pas nuire à la cohérence des dispositifs globaux et à ne pas entraîner de problèmes d'ordre organisationnel. La coordination entre les missions locales et fédérales semble être organisée d'une manière harmonieuse et n'engendre pas de lacunes ou de doubles emplois. Les différents aspects, allant de l'évaluation de la menace à l'organisation de l'aide, en passant par la phase de planification, semblent être correctement pris en compte. (Allemagne)
- Le système bien élaboré de gestion de crise et de réaction aux incidents "Polydeukis" et les différents niveaux de menace. Il s'agit d'un document qui est constamment mis à jour. Il met à profit le savoir-faire acquis par la Grèce dans le domaine de la gestion des crises avant et au cours des Jeux olympiques de 2004. (Grèce)

- Une structure d'évaluation intéressante: le groupe OSINT (Open Sources Intelligence group) actif dans le domaine du renseignement de source ouverte, au sein du ministère des affaires étrangères. Ce groupe a été constitué en 2007 et placé sous l'autorité du ministère des affaires étrangères. Il fournit des évaluations portant sur divers thèmes, en particulier des informations relatives à la sécurité des citoyens hongrois et concernant d'autres sujets liés aux intérêts hongrois à l'étranger, tels que par exemple les organisations terroristes, les personnes impliquées dans des activités terroristes, la prolifération. (Hongrie)
- L'existence d'un document intitulé "*A Framework for Major Emergency Management*", établissant un cadre pour la gestion des situations d'urgence majeure, permet d'assurer la coordination et la coopération entre toutes les autorités chargées de la gestion des crises selon les mêmes lignes directrices, en définissant clairement les compétences et l'organisation stratégique. (Irlande)
- La méthode consistant à utiliser un questionnaire annuel et à examiner ensuite les réponses qui y sont données avec le département et l'autorité responsables, afin de s'en servir comme point de départ pour la révision annuelle des plans, ainsi que la transmission d'un rapport annuel au gouvernement, sont uniques en Europe. (Irlande)
- Même si la structure de gestion des crises existant en Italie est complexe et repose sur un certain nombre d'institutions qui ont été mises sur pied pour des raisons historiques, l'échange d'informations et la coordination entre ces institutions (y compris le service de protection civile, les pompiers, etc.) semblent bien fonctionner. En particulier, l'unité chargée des crises se caractérise par la grande souplesse de ses dispositifs qui permettent à différentes institutions d'être représentées en son sein à diverses occasions (c'est-à-dire selon le type de crise). (Italie)

- Les méthodes mises en œuvre par le comité d'analyse stratégique sur le terrorisme (C.A.S.A.) semblent être un modèle particulièrement utile pour assurer l'échange d'informations entre tous les acteurs concernés en évitant les doubles emplois qui pourraient résulter d'un système de gestion des crises complexe.
La chose la plus importante dans toute situation de crise, et en particulier en cas d'attentat terroriste, est de disposer d'un bon mécanisme de partage des informations, c'est-à-dire d'un mécanisme grâce auquel les informations sont rapidement transmises à l'organisation compétente, ce qui permet de prendre les mesures qui conviennent. Le comité d'analyse stratégique C.A.S.A. est une institution de ce type, qui permet d'évaluer la menace terroriste, sur la base du flux continu d'informations transitant par ce mécanisme. (Italie)
- Le bureau de coordination et de planification des forces de police mis en place constitue un bon instrument permettant d'optimiser et d'harmoniser les services et de planifier les activités des forces de police. (Italie)
- Le plan national de lutte contre le terrorisme définit les mesures préventives de lutte contre le terrorisme qui devraient être mises en œuvre par les institutions publiques et d'autres organisations. Le plan national définit également le rôle de chacune des institutions concernées par la lutte contre le terrorisme et fournit des lignes directrices essentielles qui seront cruciales en cas d'attentat terroriste. Ce plan doit être passé en revue une fois tous les deux ans. (Lettonie)
- Le personnel du centre de crise semble avoir pour philosophie de faciliter la coordination entre les autorités et/ou les disciplines concernées, sans chercher à empiéter sur les responsabilités ou les compétences respectives de celles-ci, en incitant d'autres départements à coopérer étroitement et de manière transparente avec le centre de crise. (Luxembourg)

- Le fonctionnement et la teneur du plan VIGILNAT constitue un autre exemple de bonne pratique. (Luxembourg)
- Le recours très efficace à des ressources limitées, à des organes existants et à des outils disponibles, y compris aux forces armées. La législation maltaise institue et régit le soutien que l'armée doit fournir à la police maltaise et aux forces de sécurité, en particulier en termes de gestion des incidents terroristes. Ce soutien permet une utilisation la plus optimale possible des ressources et évite les doubles emplois au niveau des équipements et des services. La manière dont les forces coopèrent au quotidien les familiarise avec le concept de coopération, ce qui pourrait constituer un avantage en cas de crise. (Malte)
- Les cinq scénarios qui ont été élaborés et leurs listes de vérification respectives fournissent les lignes directrices nécessaires au commandant sur le terrain et aux centres de commandement, tout en leur laissant une marge de manœuvre suffisante pour réagir adéquatement à toute situation d'urgence. (Pays-Bas)
- Une caractéristique très spécifique du système mis en place aux Pays-Bas est qu'il s'appuie fortement sur une approche régionale, même s'il est apparu clairement que, en cas de crise provoquée par un incident terroriste, la responsabilité de la gestion de cette crise incombera au coordinateur national de la lutte contre le terrorisme(CTC). Cette structure semble parfaitement correspondre à la culture administrative et gouvernementale néerlandaise. Certains problèmes se posent en termes de coordination de l'approche lorsqu'un attentat terroriste a des ramifications interrégionales, nationales ou internationales, mais on s'emploie à les résoudre dans une certaine mesure en effectuant des exercices associant plusieurs régions et en s'appuyant sur le rôle de coordination assuré par le CTC, qui est responsable dès qu'une crise revêt un caractère terroriste. (Pays-Bas)

- La loi sur la gestion des crises. L'existence d'une disposition juridique très générale qui définit les compétences et le rôle de chacune des institutions tant au niveau politique qu'opérationnel constitue une étape importante vers la définition des compétences et des rôles de chaque institution dans le domaine de la gestion des crises. Le plan indique non seulement qui est concerné et quelles sont les tâches qui incombent à chacune des institutions ou des organes concernés, mais précise également dans le détail les calendriers comprenant les délais fixés pour la présentation, par exemple, de plans pour la protection des infrastructures critiques. (Pologne)
- Les dispositions budgétaires en matière de planification de la gestion des crises et la gestion des situations de crise sont précisées dans la loi sur la gestion des crises et définissent le cadre financier ainsi que les subsides. Ces dispositions évitent les discussions qui pourraient survenir au cours d'une crise ou après celle-ci et fournissent un niveau de certitude élevé. (Pologne)
- Les exploitants d'infrastructures critiques sont obligés d'élaborer et de mettre en œuvre leurs propres plans de protection des infrastructures critiques. Il relève également de leur responsabilité de communiquer le nom de personnes de contact à l'administration publique. Toutefois, les autorités centrales ont accès à tous ces plans et en assurent la coordination, ce qui permet d'assurer une approche plus cohérente en matière de gestion des crises. (Pologne)
- L'existence de la fonction de secrétaire général chargé du système de sécurité intérieure, désigné par le premier ministre et soutenu par un cadre juridique. (Portugal)
- L'existence d'un organe de ce type, doté d'une direction et d'un centre de commandement opérationnel, permet un rapprochement entre les décideurs politiques et le commandement opérationnel. Cela crée en outre un lieu d'échange de vues, où les représentants des différentes entités concernées par la gestion des crises sont présents, ce qui permet de réaliser une planification plus efficace. (Portugal)
- Les premiers intervenants clés sont regroupés au sein du ministère de l'intérieur. Cela permet non seulement de réduire les risques de désaccord politique, mais aussi de garantir l'existence d'une structure de commandement claire en cas de crise. (Portugal)

- L'équipement dont dispose l'autorité nationale chargée de la protection civile répond à des normes de qualité élevées. Plusieurs postes de commandement mobiles entièrement équipés sont à la disposition de tous les premiers intervenants. Tous ces équipements peuvent être déployés facilement en cas d'urgence, et sont mis à la disposition des entités concernées. (Portugal)
- Le cadre organisationnel vertical est bien défini et une distinction claire est établie entre les tâches et les responsabilités politiques/stratégiques, opérationnelles/techniques et tactiques. À chaque niveau, les tâches sont clairement définies et les procédures sont exposées dans des protocoles et d'autres dispositions. (Roumanie)
- Le système national de prévention et de lutte contre le terrorisme (SNPCT) dispose d'une structure globale qui regroupe en permanence tous les acteurs concernés dans le domaine de la prévention et de la lutte contre le terrorisme. Sur la base de cette structure, des dispositions juridiques et des protocoles pertinents, le système de gestion existant du centre de commandement national chargé de la coordination de missions d'ordre public (CCOA) garantit un échange permanent d'informations entre les organisations concernées au sein du SNCPT. Par conséquent, toutes les conditions préalables nécessaires pour réagir en temps utile à une situation de crise sont réunies. (Roumanie)
- Outre la collecte permanente de renseignements par le SRI et les autres services de renseignements, les autorités roumaines renforcent actuellement la police de proximité. La pleine mise en œuvre de ce principe permettra aux autorités de se préparer à une situation d'urgence de grande ampleur. (Roumanie)
- Une copie de sauvegarde de la base de données de la police est conservée en dehors de la capitale Ljubljana. La vulnérabilité éventuelle du système est de ce fait encore réduite. (Slovénie)
- Le centre de gestion national des crises (établi au sein du ministère de la défense de la République de Slovénie) fournit des facilités et des ressources techniques, ainsi que dans les domaines de l'information et des télécommunications, pour les activités du gouvernement et des services opérationnels nationaux. Ce centre national constitue un bon exemple en termes d'environnement sécurisé, d'installations informatiques et de communications, autant de ressources qui améliorent la coordination entre les différents acteurs concernés par la gestion de crises. (Slovénie)

- La cohésion générale et l'organisation efficace du système national de gestion des crises dans son ensemble constitue en soi une bonne pratique. Les dispositifs et les mécanismes énumérés ci-après peuvent toutefois aussi être considérés comme étant des bonnes pratiques. (Espagne)
- L'existence d'un centre de gestion des crises national, pour tous les types de crises, opérationnel 24 heures sur 24 et 7 jours sur 7, constitue un gage d'efficacité. (Espagne)
- La base de données de référence centralisée au sein du centre national de protection des infrastructures critiques concernant les infrastructures critiques semble être très efficace. Elle contient également le nom exact des personnes à contacter en cas d'incident et une première série de mesures à prendre par les premiers intervenants. (Espagne)
- Le fait que les services répressifs et les agences chargées de la protection civile fonctionnent selon le même système à quatre niveaux de menaces leur permet de bien comprendre leurs évaluations respectives et de les appréhender de manière cohérente. (Espagne)
- Le centre national de coordination a un rôle strictement stratégique, ce qui contribue à éviter toute interférence des instances gouvernementales dans les procédures opérationnelles. (Suède)
- Le principe consistant à fusionner toutes les agences chargées de réagir à des situations d'urgence en un seul organisme de coordination dénommé MSB constitue probablement un bon moyen pour assurer la coordination lors de la phase de réaction en cas d'événements de grande ampleur et d'opérations internationales. (Suède)
- La forte participation du gouvernement local aux services de réaction aux crises et aux plans d'intervention d'urgence explique la bonne qualité des systèmes de sécurité locaux. La réalisation d'une planification d'urgence au niveau communautaire garantit une réaction satisfaisante lors d'incidents et d'événements de faible ampleur. (Suède)

- La stratégie du Royaume-Uni en matière de lutte contre le terrorisme (CONTEST2) constitue la pierre angulaire de toutes les activités de lutte contre les menaces terroristes. Toutes les autorités compétentes doivent suivre une liste comportant 4 points, que l'on appelle les 4 "P" (prévention, protection, poursuite et réaction), ce qui permet d'assurer la cohérence dans la mise en œuvre des programmes et des plans d'action existants. (Royaume-Uni)
- Les équipes de liaison du gouvernement soutiennent et conseillent les autorités locales, et constituent en outre un canal important de communication et d'information. (Royaume-Uni)
- Du point de vue de la préparation et de la gestion des crises, la structure des autorités de police, allant de l'Association des chefs de Police (ACPO) aux sièges régionaux et locaux (Commandements d'Or, d'Argent et de Bronze), constitue la base idéale pour planifier et exécuter les opérations d'une manière optimale. (Royaume-Uni)
- La gestion transparente des informations par les instances gouvernementales (registre accessible sur Internet, niveau de menace, dépliants consacrés aux différents scénarios, etc.) a pour effet de sensibiliser le grand public et de mieux faire comprendre les mesures destinées à accroître la sécurité. (Royaume-Uni)
- La coopération étroite mise en place entre l'Office for Security and Counter-Terrorism (OSCT), le National Counter Terrorism Security Office (NaCTSO) et les agences compétentes du gouvernement garantit l'adoption d'un ensemble équilibré de programmes et de mesures. (Royaume-Uni)
- La mise en œuvre du plan HERMIS vise à informer convenablement et en temps utile toutes les missions diplomatiques présentes à Londres en cas d'incidents entraînant des pertes massives ou en cas d'autres événements graves qui pourraient se produire dans le pays. Cela est considéré à juste titre comme une bonne pratique étant donné que, toutes les ambassades étant régulièrement informées des événements, la police peut faire son travail sans être distraite de sa mission. (Royaume-Uni)

1.1.2. *Participation des citoyens, des ONG et des volontaires*

- Le principe consistant à faire participer les citoyens à la gestion des crises, qui s'est imposé au vu du grand nombre de volontaires actifs dans les services de secours, est un élément positif. Cela permet non seulement de sensibiliser la population aux risques probables liés à la catastrophe, mais aussi de renforcer la capacité des citoyens à faire face à ce type de situations. (Autriche)
- La bonne intégration des organisations non gouvernementales, telles que la Croix-Rouge, dans les opérations de sauvetage et dans la gestion des services médicaux d'urgence. (Autriche)
- En plus du personnel permanent, le recours, à titre complémentaire, à des volontaires s'est avéré être une méthode efficace et celle-ci est considérée comme une bonne pratique. Les volontaires chypriotes de la défense civile ont apporté une contribution efficace lors de la crise du Liban de 2006, en portant secours à des milliers de ressortissants de l'UE et d'autres pays qui ont été rapatriés. Il en a été de même dans le cas de la contribution apportée par la défense civile chypriote lors de plusieurs catastrophes naturelles et, récemment, au cours des incendies sauvages de forêts qui ont eu lieu à Chypre et en Grèce en 2007. (Chypre)
- Il existe un système de volontariat très élaboré dans le pays (Ligue de défense, volontaires qui assistent la police). Afin d'améliorer la coopération avec la police, un accord-cadre est conclu annuellement entre l'état-major de la Ligue de défense et la direction de la police. Conformément à cet accord, on a commencé à mettre en place des cellules chargées de la protection de l'ordre public dans toutes les unités régionales de la Ligue de défense. Ces cellules se composent de membres de la Ligue de défense ayant le statut d'assistant policier, qui aident les officiers de police dans la protection de l'ordre public et qui peuvent également exécuter les tâches de la police militaire en cas de crise. En plus d'une formation militaire immédiate, la Ligue de défense dispense à ses membres un grand nombre d'autres connaissances et apprentissages pratiques nécessaires dans la vie. En utilisant les compétences acquises au sein du groupe de formation dans le domaine paramédical et dans celui des premiers secours, les membres de la Ligue de défense ont souvent été en mesure d'agir rapidement et de manière déterminante, sauvant nombre de leurs concitoyens dont la vie était en danger. (Estonie)

- L'approche avancée adoptée en ce qui concerne le partenariat public-privé figure certainement au nombre des bonnes pratiques. La séparation entre les niveaux de menace (politique) nationale exposée dans la DTN (évaluation de la menace terroriste) et le système d'alerte du secteur privé constitue un avantage pour l'élaboration d'une coopération fructueuse entre les deux parties. (Pays-Bas)
- La description des structures de gestion des crises mises en place, donnée par ministère de l'intérieur, comporte une dimension intéressante, à savoir la reconnaissance explicite du rôle joué par les organisations non gouvernementales tant au niveau national que régional. Leur représentation au niveau national est destinée à faciliter la contribution qu'elles apportent à l'élaboration de la politique en matière de gestion des crises, alors qu'au niveau des voïvodies, leur apport se traduit par une liste de moyens existants au niveau des ONG auxquels il peut être fait appel en fonction de la nature d'une crise bien spécifique. (Pologne)

1.1.3. Organisation des travaux sur le terrain

- L'organisation du travail de la police en cas d'incident terroriste. L'approche consistant à désigner une personne responsable de la gestion des sites d'attentat à la bombe pourrait être instaurée au niveau européen. Cette fonction a pour but d'assurer une coordination efficace entre les missions d'investigation et les tâches administratives de la police, ainsi que d'assurer la liaison entre la police et les autres services d'urgence. (Belgique)
- En termes de compétences générales en matière d'enquête, la police finlandaise peut demander toute information quelle qu'elle soit (y compris les listes de passagers) dans le cadre de son mandat sans avoir besoin d'une autorisation supplémentaire. (Finlande)
- En rationalisant et en prévoyant un cadre pour les enquêteurs, la capacité de réaction aux attentats mise en place par la Direction centrale de la police judiciaire (DCPJ) facilite le déroulement des phases initiales critiques de l'enquête après qu'un attentat terroriste a été perpétré. (France)

- Au sein du CCOA des services de renseignements roumains (SRI), une ligne téléphonique d'urgence a été mise en place pour permettre la notification d'éventuelles menaces terroristes. Cette ligne est gratuite et disponible 24 heures sur 24 et 7 jours sur 7. Des experts dans le domaine du terrorisme sont disponibles pour dépister les canulars et procéder à une évaluation immédiate des informations pertinentes (limitées). (Roumanie)
- L'équipe de soutien de la police chargée de la gestion des attentats terroristes majeurs, créée en janvier 2006 et composée d'experts du corps national de police (CNP) et de la Guardia civil (GC), est très utile en cas d'attentat terroriste majeur. La direction de ce groupe, assurée alternativement par le CNP et la GC, constitue également une bonne pratique. (Espagne)
- Le principe de base, qui consiste à maintenir les responsabilités le plus possible au niveau local et à bénéficier du soutien et des conseils stratégiques du gouvernement, est une excellente façon de partager les compétences, et permet d'éviter des procédures décisionnelles longues et complexes. (Royaume-Uni)

1.1.4. Relations avec le secteur privé

- Les relations que le centre national de coordination entretient avec le secteur privé par l'intermédiaire du système mis en vigueur par la FEB (Fédération des Entreprises de Belgique) s'avèrent à la fois souples et extrêmement efficaces. Une telle approche pourrait également être introduite au niveau européen. (Belgique)
- Les obligations concernant la participation et la coopération de personnes physiques et morales et d'entrepreneurs individuels dans les crises sont exposées dans la législation relative à la gestion des crises; des sanctions sont prévues en cas de non-respect (ainsi que le remboursement des frais exposés lors d'actions menées sur ordre des autorités publiques lors des crises). (Bulgarie)

1.1.5. Menaces chimiques, biologiques, radiologiques ou nucléaires (CBRN)

- Les équipes de secours en place (présentes dans chacune des 28 régions dès la fin de 2008), qui sont équipées pour la gestion d'incidents CBRN. (Bulgarie)
- La menace CBRN est très bien couverte en termes à la fois d'intervention préventive et d'intervention consécutive à un attentat. (France)
- Les forces armées et les pompiers ont reçu les mêmes équipements, ou du moins des équipements compatibles, pour réagir aux incidents CBRN. Il en va de même des équipements fournis aux premiers intervenants en Irlande du Nord. Cette approche transfrontalière atteste de la volonté des autorités irlandaises de s'engager dans une coopération transfrontalière et européenne. (Irlande)
- L'achat d'équipements, en particulier en ce qui concerne la protection CBRN, est décidé d'un commun accord par les différentes instances concernées. Ce débat ouvert entre institutions permet de mieux comprendre les besoins réels de chacun des organes concernés et d'échanger les expériences acquises avec les différents équipements. Il va sans dire que cette procédure plus interactive débouche sur une meilleure utilisation du budget disponible. (Portugal)
- Étant donné le nombre limité d'installations sanitaires spécialisées dont le pays dispose dans le domaine du CBRN, le ministère slovaque de la santé a conclu des accords de coopération avec l'Autriche et la République tchèque, et a étendu ces accords à la réalisation d'exercices d'entraînement. Le ministère de l'intérieur a fait savoir qu'il était actuellement en train de finaliser un accord avec le ministère de la santé afin de donner un accès prioritaire à ces installations aux premiers intervenants. Cet accord comprend l'accès aux installations de soins de santé publiques et privées et les premiers secours fournis sur place par l'intermédiaire du corps des ambulanciers. De la même façon, les laboratoires chimiques de contrôle de la protection civile du ministère de l'intérieur investissent dans des centres mobiles afin de fournir une assistance sur place et des installations d'essais pour les incidents liés au CBRN. (République slovaque)

- La centralisation au niveau national des achats d'équipement CBRN de base garantit la compatibilité entre les premiers intervenants concernés par les affaires CBRN. Il est prévu d'équiper les 44 unités de pompiers importantes (parmi lesquelles 13 sont des unités professionnelles) de matériel CBRN de qualité d'ici la fin de 2013. (Slovénie)
- Le service de police suédois a élaboré une norme uniforme pour réagir aux incidents CBRN. Celle-ci comprend une formation, des procédures et des équipements communs au niveau national, ce qui facilite une approche commune en la matière à l'échelle nationale. (Suède)

1.1.6. Coopération interservices

- Afin d'améliorer la coopération entre les services de police, les douanes et les garde-frontières, un organe conjoint a été créé. Ces trois instances utilisent une même base de données et des réunions hebdomadaires sont organisées pour examiner les questions d'intérêt commun. (Finlande)
- Excellent système de gestion de crise en amont grâce à l'évaluation de la menace réalisée par l'UCLAT (Unité de coordination de la lutte antiterroriste). Cette évaluation de la menace, qui fait appel à tous les services concernés, est essentielle dans le cadre du processus consistant à évaluer le niveau de la menace en vue de la mise en oeuvre du plan VIGIPIRATE. (France)
- La base de données commune au niveau des Länder (ville de Berlin) concernant les ressources techniques et les effectifs, associée à une liste des mesures à prendre et à une série d'autres options semblent constituer des outils appropriés dans le cadre d'une coopération interservices. (Allemagne)
- La structure et le fonctionnement du GTAZ (Centre commun de lutte contre le terrorisme de la République fédérale d'Allemagne), qui concentre les efforts de lutte contre le terrorisme de 40 instances analysant le terrorisme à motivation religieuse en Allemagne, permettent une évaluation efficace de la menace. (Allemagne)

- Coopération entre l'AGS (forces de police irlandaises) et les forces armées, et en particulier participation des forces armées aux opérations de désamorçage des engins explosifs improvisés (EEI). (Irlande)
- Le centre de lutte contre le terrorisme . L'existence d'un centre permanent de lutte contre le terrorisme, susceptible d'activer un centre de commandement opérationnel en cas de danger imminent, est essentielle. Le centre de lutte contre le terrorisme est également responsable de l'élaboration, de la mise à jour et de la mise en œuvre du plan national de lutte contre le terrorisme, ainsi que de l'élaboration de plans de réaction à des situations particulières. (Lettonie)
- En tant que service de renseignement et service répressif, la police de sécurité constitue toujours la principale institution de prévention du terrorisme en Lettonie. Le fait que les capacités juridiques de la police et les compétences des services de renseignements soient regroupées au sein d'un même organe permet de réaliser un travail de prévention efficace ainsi que des évaluations plus réalistes de la menace. (Lettonie)
- Le fait que les services de sécurité maltais soient composés de personnel détaché des services de police, des douanes et des forces armées accroît le flux d'informations et la coopération entre les services ainsi que l'efficacité du fonctionnement des services de sécurité. (Malte).
- Existence d'un coordinateur de la lutte contre le terrorisme qui prend en charge la coordination en cas d'acte terroriste. La préparation et la capacité de réaction aux crises, notamment de nature terroriste, ont été considérablement améliorées, tant sur le plan de l'expertise technique qu'en termes de mise à niveau des procédures. (Pays-Bas)

- Valeur ajoutée qu'apportent aux processus de "vérification" les compétences en termes d'analyse de l'information et des renseignements du centre de lutte contre le terrorisme. Une présentation a clairement démontré l'existence d'un système complexe et cohérent de notification (Intranet du centre) fournissant des rapports opérationnels et situationnels, même si les particularités et la valeur ajoutée de la vérification effectuée par le centre n'ont pas été clairement exposées.
L'introduction de modèles-types de procédures de notification du centre de lutte contre le terrorisme auprès des différents acteurs de la sécurité nationale renforcerait l'échange d'informations entre ces acteurs et leur compréhension mutuelle. On a déjà pu constater les avantages d'un regroupement des divers acteurs au sein de forums de lutte contre le terrorisme. (Pologne)
- Le SIRESP est une structure de communication interservices bien développée. Permettre à des partenaires privés d'accéder au SIRESP constitue une excellente approche pour une communication rapide entre organismes publics et privés en cas d'urgence. La participation, au sein d'un même réseau, de toutes les structures concernées par la gestion de crise se traduit par l'utilisation des moyens les plus appropriés en cas de nécessité. (Portugal)
- La création, en mai 2004, du Centre national pour la coordination de la lutte contre le terrorisme (CNCA), qui permet de fournir au ministre de l'intérieur tous les renseignements collectés par l'ensemble des instances administratives concernées par la lutte contre le terrorisme, représente un atout considérable. (Espagne)

1.2. Coopération sur d'éventuels objectifs transfrontaliers

- La coopération semble être particulièrement poussée entre les pays du Benelux, qui échangent des informations sur les analyses de risque, la gestion des situations d'urgence et la mise en place d'exercices conjoints. Ceci semble pouvoir constituer un exemple des meilleures pratiques, éventuellement reproductible ailleurs sur la base d'un voisinage régional. (Belgique)
- Des accords bilatéraux ou des protocoles d'accord existent avec tous les pays voisins en vue d'une coopération en situation de crise. (Bulgarie)

- Des accords de coopération et d'assistance en matière de prévention et de gestion des conséquences d'incidents majeurs (y compris des attaques terroristes) existent avec tous les pays voisins. (Lituanie)
- La coopération semble être particulièrement poussée entre les pays du Benelux, qui échangent des informations sur les analyses de risque, la gestion des situations d'urgence et la mise en place d'exercices conjoints. Ceci semble pouvoir constituer un exemple des meilleures pratiques, éventuellement reproductible ailleurs sur la base d'un voisinage régional. (Luxembourg).
- Le dispositif slovaque de réaction aux crises et de redressement après une crise se caractérise par la coopération régionale au sein du groupe de Visegrad. Cette coopération se traduit par une très forte coordination en matière de formation et d'exercices des différents acteurs, conformément aux accords gouvernementaux bilatéraux conclus entre la Pologne, la République tchèque, la Hongrie et la Slovaquie. Le groupe de Visegrad est connu pour les réunions annuelles de ses États parties qui examinent des plans de travail, procèdent à des échanges d'informations et d'experts et organisent formations et exercices. (République slovaque)
- De nombreux exercices sont réalisés, tant pour les services nationaux ou locaux qu'avec les pays voisins. Les comptes rendus de ces exercices permettent de souligner les points qui doivent être améliorés et ceux sur lesquels des précisions doivent être apportées dans les plans d'intervention. (Slovénie)
- Des accords de coopération et d'assistance ont été conclus avec tous les pays voisins en matière de prévention et de gestion des conséquences d'incidents majeurs (y compris des attaques terroristes). (Slovénie)
- En ce qui concerne la coopération transfrontalière, le centre opérationnel de communication de *Vrata Megvarje* peut être cité comme un bon exemple de coopération avec les pays voisins. Ce centre, déjà opérationnel, regroupe des forces de police italiennes, autrichiennes et slovènes. Il fonctionne 24 h/24, tous les jours de la semaine, dispose de ses propres locaux et d'un personnel permanent composé d'agents de ces trois pays. (Slovénie)

1.3. Réseaux de communication et systèmes informatiques

- Toutes les forces de sécurité (police, pompiers, ambulances) peuvent communiquer sur le même réseau numérique (ASTRID). Ceci garantit la cohérence des efforts de secours à tous les niveaux. (Belgique)
- La gestion et la maintenance du réseau radio de la police chypriote sont assurées par un service de police spécial qui gère et entretient l'ensemble du système. De plus, le fait de disposer d'un réseau de téléphone privé et de conclure un contrat de maintenance spécial avec les prestataires qui le gèrent est considéré comme relevant des meilleures pratiques. (Chypre)
- Le développement du réseau national de communications renforcera la coordination et la coopération entre les régions. (République tchèque)
- L'un des objectifs du plan d'action national vise à aborder la question relative à l'obligation, pour les fournisseurs de services Internet et de messagerie électronique, de conserver les données pertinentes et de les communiquer aux autorités compétentes (ne concerne pas le contenu des communications mais des données telles que l'expéditeur, le destinataire et l'heure de la transmission du message). En vertu de la législation en vigueur et conformément au cadre réglementaire de l'UE concernant les communications électroniques, ces fournisseurs ne sont pas des fournisseurs de services de communications électroniques (c'est-à-dire des fournisseurs de services de transmission) mais plutôt des fournisseurs de services de la société de l'information (c'est-à-dire des fournisseurs de services de contenu). (République tchèque)
- Un exemple de bonnes pratiques dans le domaine des communications a pu être observé avec KRISEINFO.DK, un site Internet solide et de grande portée qui publie des informations simples et pertinentes à destination du public. Il est hébergé sur des serveurs situés hors des frontières du Danemark, capables de résister en cas de crise et restant opérationnels même si le système central de communication au Danemark rencontre des difficultés. (Danemark)

- Un site Internet doté d'une structure similaire à celle de KRISEINFO.DK serait un modèle de bonne pratique pour d'autres États membres de l'UE ne disposant pas d'une telle structure. La capacité avérée du site KRISEINFO.DK à communiquer au public des données basiques et vitales en situation de crise doit être soulignée. (Danemark)

- Maintenance du réseau radio assurée par le service technique de l'état-major de la police grecque, responsable de la vérification et de la surveillance de tous les réseaux de communication vocale. Le département Technologies de l'information de l'état-major de la police grecque est chargé de vérifier et surveiller tous les réseaux de communication de données.
Les forces de police grecques sont autonomes en ce qui concerne les modes de transmission. Elles n'ont dans ce domaine aucun besoin de ressources techniques ou humaines extérieures. (Grèce)

- Un organe efficace de lutte contre les cyberattaques: la CERT (Équipe d'intervention en cas d'urgence informatique). La CERT remplit les fonctions suivantes:
 - elle est le centre de gestion des crises liées à la cybercriminalité;
 - elle est responsable de la protection des infrastructures d'information critiques des institutions publiques et du secteur privé;
 - elle propose des formations à la direction et au personnel de sociétés privées;
 - elle propose un service de base de données personnalisé répondant à des besoins individuels;
 - elle fournit des informations périodiques (quotidiennes/hebdomadaires), sur la base d'un abonnement. (Hongrie)

- Un réseau de communication efficace: TETRA. Ce réseau est numérique et crypté. Il est nécessaire d'étendre ce réseau à tout le territoire hongrois. (Hongrie)

- La base de donnée "informatique, communications, commandement, contrôle pour l'information" (C4I), mise au point par la *Guardia di Finanza* et qui associe une sorte de système de suivi des navires (VTS) à des fonctionnalités supplémentaires en termes d'analyse, pourrait présenter un intérêt pour d'autres États membres, notamment ceux qui disposent d'une longue zone côtière. Tous les partenaires de la *Guardia di Finanza* ont accès à cette base de données et peuvent ajouter des données. Le système peut également être utilisé comme outil de planification des opérations. (Italie)
- Définition claire des rôles entre institutions. La répartition claire des tâches entre les structures en place traitant du terrorisme est l'un des plus grands avantages du système letton. Cette répartition claire, renforcée par le plan national de lutte contre le terrorisme, permet une meilleure et plus efficace prévention des attaques terroristes et la gestion de leurs répercussions. (Lettonie)
- Malte est bien équipée pour contrer toute attaque informatique sur les systèmes de communication utilisés par les forces de sécurité. L'existence des services maltais pour les technologies de l'information et la formation (MITTS) et le rôle central qu'ils jouent reflètent l'importance que les autorités maltaises attachent à ce risque. (Malte)
- Le numéro d'urgence 112 est utilisé dans tous le pays. La police, les services de la protection civile et les forces armées sont mutuellement en charge du fonctionnement du système. Les numéros d'urgence utilisés par le passé sont toujours valables mais les appels sont automatiquement transférés vers le 112. (Malte)
- Un accent très net est également mis sur le bon fonctionnement d'une infrastructure TI et de communication comprenant des lignes en surnombre pour une communication plus sûre et des systèmes de sauvegarde en cas de défaillance du système. Des exercices sont également organisés en vue de garantir la sécurité des communications. Le service spécial de télécommunications, qui fait partie du système de défense, prévoit des lignes de communication spécifiques fonctionnant indépendamment des réseaux publics. (Roumanie)
- Le ministère de l'économie utilise EPSIS, une application logicielle permettant de soutenir la mobilisation de l'économie en situation de crise. Il a été proposé de déployer le système EPSIS (via une connexion Internet sécurisée) aux autorités régionales (agence locale de gestion des situations d'urgence), ce qui devrait accroître la prise de conscience de la situation et l'efficacité de la réaction en cas de crise. (République slovaque)

- WIS: Il s'agit d'un système d'information national reposant sur Internet (web-based information system - WIS) qui a été élaboré pour faciliter l'échange d'informations entre les différents acteurs, à tous les niveaux, dans le système suédois de gestion des situations d'urgence, avant, pendant, et après une crise. WIS permet une prise de conscience efficace et partagée de la situation en cas de crise. Le public et les médias disposent également d'un libre accès à ce site Internet, ce qui leur permet d'avoir une vue globale du cours des événements en cas de crise. (Suède)
- Le système du 112 suédois, exploité par SOS alarm, une entreprise publique, offre un bon niveau de réponse aux appels d'urgence et une norme uniforme de traitement de ces appels dans tout le pays. (Suède)

2. FORMATION/EXERCICES

- Les séminaires mis en place par le BVT (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung - Office fédéral pour la protection de la constitution et la lutte contre le terrorisme) portent principalement sur les enjeux de la toute première réaction en cas d'attaque terroriste. Ces séminaires permettent de regrouper efficacement toute l'expertise requise pour gérer les toutes premières heures qui suivent un incident. Des échanges de vues et un débat ouvert favorisent les interactions entre les différentes organisations engagées dans la gestion des crises. Les programmes des séminaires traitent aussi bien d'informations générales concernant le terrorisme que de l'évaluation de la menace, d'études de cas ou de l'identification des victimes et du travail des médias. Le dernier de ces séminaires a eu lieu en mars 2009. (Autriche)
- De nombreux cours de formation sont organisés à tous les niveaux concernés (depuis le sommet de la hiérarchie politique jusqu'aux premiers intervenants dans les régions et les municipalités). Les résultats et les enseignements tirés des formations sont intégrés dans les plans de gestion de crise. (Bulgarie)
- Formation continue des forces de police chypriotes, y compris de la police des ports et de la police maritime et des autres autorités de la république en prévision d'une attaque terroriste. Les forces spéciales de la police chypriote devraient être citées comme bon exemple de cet effort. (Chypre)

- Coopération des services du matériel: Le pays dispose de deux forces de déminage: l'une intervient dans les situations d'urgence (c'est la plus importante; activités quotidiennes, campagnes auprès du public, etc.); l'autre a un caractère militaire (souvent à l'étranger). Ces deux forces s'entraînent ensemble et les exercices provoquant des détonations sont également pratiqués sur terrain militaire. (Estonie)
- Coopération des unités SWAT. Il existe dans le pays quatre forces qui participent néanmoins à des activités d'entraînement conjointes et, en fonction de la situation, à des interventions conjointes: une équipe militaire (qui intervient de façon autonome dans le cadre de situations à caractère purement militaire, souvent à l'étranger), les K-Kommando de la police criminelle (équipe la plus nombreuse et la mieux équipée au sein du ministère de l'intérieur, possède ses propres plongeurs), l'équipe de police répressive (qui agit de manière indépendante en cas d'émeutes), l'équipe du service des prisons (chargée d'apaiser les tensions dans les prisons) et l'équipe KAPO (qui intervient de façon autonome dans les cas nécessitant un niveau de confidentialité absolue). Lors de leurs entraînements, les équipes sont mises face à des situations diverses. (Estonie)
- Des "situations éprouvantes" se présentent fréquemment. Dès lors, la nature et l'efficacité des forces spéciales sont régulièrement mises à l'épreuve dans des conditions réelles. Ceci permet une mise à jour permanente des procédures et des ressources nécessaires. Grâce à cette dynamique, une coopération performante et efficace est possible entre les instances concernées par la gestion de crise. (Finlande)
- L'exploitant du métro berlinois met à disposition de la police et des pompiers, dans l'une de ses stations, un dispositif d'exercice comportant tous les équipements nécessaires, y compris des rails et des wagons. Il est possible de s'exercer sur cet équipement toutes les semaines. (Allemagne)
- Les exercices stratégiques "LÜKEX". Ces exercices sont organisés tous les deux ans, leur préparation s'étendant sur une période de 12 à 16 mois lorsque les différents acteurs (au niveau fédéral comme au niveau des Länder, acteurs publics et privés, autorités civiles et militaires) participent déjà activement et sont entraînés à l'exercice en tant que tel. De cette manière, l'exercice permet non seulement de tester les structures, les processus et la coordination en place mais également de contribuer au développement des capacités des instances concernées. (Allemagne)

- Exercices réguliers de lutte contre le terrorisme. L'importance attachée en permanence à la mise à l'épreuve du système de gestion de crise de la police et les moyens financiers qui y sont consacrés peuvent être considérés comme un exemple des meilleures pratiques. Tous les services et bureaux concernés participent aux exercices. Pour ces exercices, la question budgétaire ne semble pas poser problème. (Grèce)
- Système intéressant d'évaluation des incidents. La Grèce dispose d'un système permettant d'évaluer tous les incidents qui surviennent. La performance de tous les niveaux de commandement est évaluée. On s'attache tout particulièrement à tenter d'identifier l'accumulation d'erreurs. Le matériel collecté et évalué est ensuite utilisé à des fins de formation, selon une approche pratique consistant à tirer des enseignements. (Grèce)
- Résultat des exercices et adoption de mesures très concrètes. Les autorités italiennes ont évité de conclure que les exercices avaient nécessairement débouché sur les résultats positifs escomptés et ont plutôt insisté sur les "améliorations nécessaires", ce qui leur a permis d'améliorer les mécanismes et de clarifier le rôle de chacune des institutions concernées par la gestion de la situation. (Italie)
- De nombreux exercices sont réalisés, tant pour les services nationaux ou locaux qu'avec les pays voisins. Grâce à ces exercices, il est possible, lors de comptes rendus, de recenser les points devant être améliorés et de revoir les plans d'action. (Lituanie)
- Aux fins de toute poursuite judiciaire ultérieure, l'armée et les membres des services de la protection civile reçoivent une formation spéciale sur la manière d'éviter la destruction des preuves au cas où ils seraient appelés sur les lieux d'une attaque. (Malte)
- L'Université de Leyde a créé une chaire de terrorisme. L'université contribue ainsi à développer l'expertise dans le domaine de la lutte contre le terrorisme, ce qui pourrait aussi se refléter dans une analyse comme la DTN (évaluation de la menace terroriste). L'existence de cette discipline au sein de l'université permet non seulement un aperçu historique des événements qui sont à l'origine de toutes les politiques de sécurité actuelles mais également une approche globale du problème du terrorisme. (Pays-Bas)

- Les exercices pratiqués au niveau régional (voïvodies) sont toujours observés et évalués par les représentants d'autres voïvodies ainsi que, dans la mesure du possible, par les autorités centrales. Ceci garantit un haut niveau d'objectivité et donc des échanges de vues sur les problèmes rencontrés et sur les meilleures pratiques. De plus, les acteurs clés des différentes voïvodies se connaissent personnellement, ce qui constitue une valeur ajoutée pour la coopération en situation réelle. (Pologne)

- Approche consistant à intégrer dans les programmes scolaires des connaissances de base sur la protection civile et les situations de crise: Le ministère de l'intérieur, en coopération avec le ministère de l'éducation, a intégré de nouveaux éléments aux programmes scolaires, centrés sur les jeunes enfants, et dont les trois principaux objectifs sont:
 - a) de sensibiliser les plus jeunes aux éventuelles menaces et de leur apprendre à réagir, le cas échéant, de manière appropriée;
 - b) de motiver les jeunes afin qu'ils s'intéressent au travail des services de la protection civile et des premiers intervenants, et de les inciter à participer;
 - c) de faire en sorte que les jeunes jouent le rôle de messagers pour les générations plus âgées, en transmettant l'information collectée et les enseignements tirés.
 (République slovaque)

- De nombreux exercices sont réalisés, tant pour les services nationaux ou locaux qu'avec les pays voisins. Les comptes rendus de ces exercices sont l'occasion de souligner les points qui doivent être améliorés et ceux sur lesquels des précisions doivent être apportées dans les plans d'intervention. (Slovénie) L'utilisation du réseau Malla B dans les opérations quotidiennes contribue à renforcer la connaissance que les utilisateurs ont du système et rend son usage simple et efficace en cas de crise ou de situation d'urgence. (Espagne)

- Des exercices réguliers à différents niveaux (national, régional, local) réalisés dans différentes régions selon différents scénarios et avec la participation d'autres pays, ainsi que les comptes rendus établis à l'issue des exercices en fonction de la procédure retenue, permettent de renforcer en permanence les capacités de réaction. (Royaume-Uni)

- Un programme national d'exercices de lutte contre le terrorisme a été adopté par les décideurs politiques concernés; il couvre la période 2008-2012. (Royaume-Uni)

3. CIBLES FACILES

- Bonne approche concernant la meilleure façon de protéger les "cibles faciles". Les autorités grecques considèrent que le meilleur moyen de protection des "cibles faciles" est une évaluation fiable de la menace. (Grèce)
- Les instances gouvernementales et les sociétés privées (commerciales et industrielles) coopèrent étroitement à l'élaboration de technologies pour la protection des zones sensibles (lieux de rassemblements, infrastructures critiques). (Royaume-Uni)

4. AUTRES

- Le ministère de l'intérieur dispose d'un institut supérieur de planification d'urgence qui joue le rôle de centre de connaissances et élabore des instruments et un savoir-faire, met en place des réseaux avec des universitaires, des experts et d'autres centres au niveau européen et international, propose des formations, un environnement de formation ainsi qu'un forum de discussion. Cet organe centralisé et spécialisé, qui entretient des relations transfrontalières, semble être un excellent instrument d'échange des connaissances et des meilleures pratiques. (Belgique)
- Les pompiers sont des acteurs polyvalents extrêmement bien formés qui sont également capables d'apporter les premiers soins médicaux. S'agissant de la réaction des civils, le fait que des instructions de base concernant la réaction de la population civile en cas d'urgence soient communiquées via les annuaires est incontestablement une bonne pratique. (Finlande)
- Il existe un réel partenariat public-privé dont les principaux opérateurs (télécommunications, transports et énergie) sont vraiment partie prenante. Au stade de la planification des exercices comme à celui de leur mise en oeuvre, le partenariat repose sur une communication constante. (France)
- L'Office fédéral de la sécurité de l'information (BSI), dont les responsabilités sont multiples (autorités publiques, entreprises privées et citoyens), est un excellent exemple de regroupement, au sein d'un même organisme, de tout ce qui touche aux questions de sécurité des communications. Le BSI semble jouir d'une solide autorité en tant que prestataire de services et n'est pas perçu comme le "chien de garde" de la surveillance des données. (Allemagne)

- L'action de l'Agence fédérale pour l'aide technique (THW), basée sur le volontariat, est un exemple intéressant. L'agence fournit (sur demande) un soutien technique concret dans le domaine de la protection civile dans les cas de catastrophes, de situations d'urgence à grande échelle et d'accidents. Environ 80 000 de ses membres sont des volontaires et 800 sont des professionnels à temps plein, organisés du niveau local au niveau national. Bien que la prédominance du volontariat puisse poser certains problèmes (en termes par exemple de professionnalisme, de disponibilité des volontaires, de diversité des compétences disponibles), jusqu'à présent, ce système a fait ses preuves en Allemagne. Dans le même temps, la large base de ce volontariat garantit une couverture considérable de la population et un certain niveau de sensibilisation et de compétence en matière de gestion de crise réparti sur l'ensemble des structures de la société. (Allemagne)
- Structure et travail du centre national des opérations de santé. Ce centre est un exemple de coordination efficace de l'aide médicale apportée en cas de crise. La création même d'un centre général de coordination et de veille comme celui-ci dans le secteur de la santé peut être considérée comme relevant des meilleures pratiques. (Grèce)
- Dans le cadre d'une enquête, la population a exprimé ses attentes à l'égard du gouvernement et des autorités publiques en ce qui concerne la préparation à la gestion de crise. L'un des principaux constats est que la population souhaite savoir qu'un plan d'action a été élaboré par le gouvernement et les autorités publiques. Les détails de ce plan ne présentent pas un intérêt majeur pour la population. Conséquence de l'enquête, chaque foyer a reçu des explications sur "la préparation aux risques majeurs", en anglais et en irlandais. (Irlande)
- Les locaux de réunion du centre national de crise sont bien conçus et bien situés, notamment les trois pièces différentes: l'une pour la prise de décision politique, l'autre pour le personnel opérationnel et la troisième réservée aux médias. (Luxembourg)

- Nous avons été frappés de constater que le Luxembourg est particulièrement au fait des meilleures pratiques dans d'autres pays, notamment les pays voisins. Tirant parti de son expérience, le Luxembourg a su concevoir des solutions individuelles basées sur les particularités du pays, notamment sa taille. (Luxembourg)
 - L'installation de portiques de détection des radiations dans les entreprises de traitement des ferrailles métalliques recyclées et sur le site national de recyclage des déchets pourraient devenir la norme au niveau européen. (Luxembourg)
-