Nations Unies S/2004/22

Conseil de sécurité

Distr. générale
13 janvier 2004
Français
Original: anglais

Lettre datée du 7 janvier 2004, adressée au Président du Conseil de sécurité par le Président du Comité du Conseil de sécurité créé par la résolution 1373 (2001) concernant la lutte antiterroriste

Me référant à ma lettre du 9 octobre 2003 (S/2003/1007), j'ai l'honneur de vous faire tenir ci-joint le quatrième rapport que l'Estonie a présenté au Comité contre le terrorisme en application du paragraphe 6 de la résolution 1373 (2001) (voir annexe).

Je vous serais reconnaissant de bien vouloir faire distribuer le texte de la présente lettre et de son annexe comme document du Conseil de sécurité.

Le Président du Comité créé
par la résolution 1373 (2001)
concernant la lutte antiterroriste
(*Signé*) Inocencio F. **Arias**

04-20592 (F) 090204 100204

Annexe

Note verbale datée du 2 janvier 2004, adressée au Président du Comité contre le terrorisme par la Mission permanente de l'Estonie

La Mission permanente de la République d'Estonie auprès de l'Organisation des Nations Unies présente ses compliments au Président du Comité et a l'honneur de lui transmettre le quatrième rapport de l'Estonie sur l'application de la résolution 1373 (2001) (voir la pièce jointe).

Pièce jointe

Estonie

Au nom du Comité contre le terrorisme, je tiens à vous remercier de votre lettre du 6 mars 2003 (S/2003/275), à laquelle était joint le troisième rapport établi par le Gouvernement estonien en réponse à la lettre du JJ MM 200? (*sic*) (S/AC.40/2002/MS/OC.nn) de mon prédécesseur à la présidence du Comité, et présenté en application du paragraphe 6 de la résolution 1373 (2001) du Conseil de sécurité (« la résolution »).

Avec le concours de son groupe d'experts, le Comité a examiné attentivement les rapports précédents ainsi que les autres informations pertinentes communiqués par l'Estonie.

Pour gérer au mieux ses travaux, le Comité a divisé l'application de la résolution en trois grandes phases (les phases A, B et C). Ces phases correspondent en gros aux différents types d'activités menés par les États pour renforcer leurs moyens d'action contre le terrorisme, et chacune de ces phases s'appuie sur les activités de la phase antérieure. Les phases A, B et C sont décrites dans la lettre que le Président du Comité du Conseil de sécurité créé par la résolution 1373 (2001) concernant la lutte antiterroriste a adressée au Président du Conseil de sécurité en date du 16 janvier 2003 (S/2003/72). On trouvera ci-joint copie de cette lettre.

Le Comité invite instamment tous les États à poursuivre l'application de la résolution 1373 (2001) aussi rapidement qu'il leur est possible. Pour aider le Gouvernement estonien dans l'application de cette résolution, le Comité est convenu de lui communiquer les observations et questions ci-après, qui concernent pour l'essentiel la prochaine série de priorités.

Les États doivent veiller à ce que les mesures qu'ils prennent pour lutter contre le terrorisme remplissent toutes les obligations que le droit international leur impose et soient conformes au droit international, et notamment au droit international des droits de l'homme, au droit des réfugiés et au droit humanitaire.

Dans ce contexte, le Comité serait reconnaissant au Gouvernement estonien de lui communiquer de plus amples informations concernant les questions ci-après :

1. Mesures de mise en oeuvre

Efficacité du dispositif de protection du système financier

1.1 Le Comité contre le terrorisme note avec satisfaction, à la section 1.2 de la page 3 du rapport de l'Estonie daté du 6 mars 2003, que les amendements tendant à harmoniser avec les instruments pertinents de l'ONU les dispositions de la loi relative à la prévention du blanchiment d'argent seront soumis prochainement au Parlement afin de mettre l'Estonie en conformité avec l'alinéa a) du paragraphe 1 de la résolution 1373 (2001), qui prescrit aux États de prévenir et réprimer le financement des actes de terrorisme. Le Comité souhaite savoir quel est l'état d'avancement des amendements.

Le projet d'amendements a été présenté au Parlement, qui en a achevé la deuxième lecture le 19 novembre 2003. Les amendements devraient entrer en vigueur le 1er janvier 2004 au plus tard.

Efficacité du dispositif antiterroriste

1.2 Le Comité se félicite de constater que l'Estonie s'est dotée d'une stratégie nationale d'action contre le terrorisme. Il souhaiterait avoir un aperçu de cette stratégie, qui a été adoptée par la Commission nationale pour la sécurité, sans compromettre toutefois le caractère confidentiel des informations qu'elle pourrait contenir.

La stratégie d'action nationale a été formulée juste après les attentats terroristes du 11 septembre 2001 aux États-Unis par la Commission gouvernementale pour la sécurité, qui avait été convoquée à cette fin. Elle visait à renforcer rapidement la coopération et l'échange d'informations entre les différentes administrations pour mieux prévenir les actes de terrorisme, et aussi pour améliorer la coopération et l'échange d'informations entre les trois États baltes. Ce document ne répond cependant plus à la situation actuelle et ne présente par conséquent plus d'intérêt particulier.

1.3 L'application effective de l'alinéa b) du paragraphe 2 de la résolution suppose que les États prennent les mesures voulues pour empêcher que des actes de terrorisme ne soient commis. Le Comité se félicite de constater que, comme elle le mentionne à la page 9 de son premier rapport, l'Estonie a pris des mesures pour renforcer la sécurité aérienne et se conformer aux prescriptions de l'annexe 17 de la Convention relative à l'aviation civile internationale. Il souhaiterait être informé des progrès réalisés par l'Estonie dans ce domaine. Il souhaite également avoir un aperçu des mesures de sécurité maritime et portuaire prises par l'Estonie pour protéger les navires et les installations portuaires contre les actes de terrorisme, en conformité avec le chapitre XI-2 de la Convention de 1974 pour la sauvegarde de la vie humaine en mer, que l'Estonie a signée.

1. Le Parlement estonien a ratifié toutes les conventions internationales en matière de sécurité aérienne. Le cadre juridique de la sécurité aérienne en Estonie se présente comme suit :

Le principal texte relatif à la sécurité aérienne est la loi relative à l'aviation, qui a été adoptée par le Parlement en 1999. Le Règlement No 44 du Gouvernement de la République, intitulé « Procédures de sécurité aérienne », constitue de fait le règlement d'application de la loi relative à l'aviation.

Le 30 mai 2003, le Comité national pour la sécurité de l'aviation civile a adopté un programme national de sécurité pour l'aviation civile.

La loi relative à l'aviation ne comprend actuellement de dispositions détaillées ni sur la répartition des responsabilités entre les divers organismes concernés par la sécurité aérienne ni sur les mesures de sécurité à mettre en place pour protéger l'aviation civile contre les actes illicites visant la sécurité aérienne. C'est pourquoi un groupe de travail a été chargé d'amender la loi relative à l'aviation en y incorporant un nouveau chapitre sur la sécurité aérienne. Ce chapitre tiendra compte de l'ensemble des dispositions de l'annexe 17, de ses amendements les plus récents, et des règlements et recommandations de l'Union européenne et de la Conférence européenne de l'aviation civile. Les amendements à la loi relative à l'aviation devraient être soumis au Gouvernement de la République, pour approbation et transmission au Parlement, au plus tard au début de 2004.

Le Comité national de la sécurité aérienne est chargé de mettre au point une politique de sécurité pour l'aviation estonienne et de coordonner et encourager les initiatives en matière de sécurité aérienne. C'est la Direction nationale de la sécurité qui est chargée d'intervenir en cas d'incident ou de menace concrète (telle qu'une menace d'action terroriste, par exemple).

2. L'Estonie a adhéré le 19 novembre 1991 à la Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer ainsi qu'à son Protocole de 1978. Ces deux instruments sont entrés en vigueur le 16 mars 1992 en ce qui concerne l'Estonie.

L'Estonie suivait déjà les prescriptions du Protocole de 1988 relatif à la Convention internationale pour la sauvegarde de la vie humaine en mer avant même qu'il n'entre en vigueur pour elle le 20 novembre 2003. Du fait que la Convention a souvent été modifiée par l'Organisation maritime internationale et que son Protocole prescrit aux États participants de faire appliquer un certain nombre de règles sur le plan national, l'Estonie devra, pour respecter cette prescription du Protocole, transposer les règles en question dans son droit interne (il en est ainsi, par exemple, des règles édictées par le Code international pour la sûreté des navires et des installations portuaires).

a) Une loi portant amendement de la loi relative à la sécurité maritime (qui devrait être envoyée au *Riigikogu* en avril 2004 et dont les amendements sont partiellement incorporés en conjonction avec la loi portant amendement de la loi relative à la sécurité maritime, laquelle est actuellement examinée par la Commission des finances du *Riigikogu*) a été adoptée dans le cadre des préparatifs susmentionnés et elle permettra de renforcer la sécurité de la navigation maritime et des navires;

b) En ce qui concerne les ports estoniens, de nouveaux règlements inspirés par la loi relative à la sécurité existante sont en cours de rédaction et devraient aider à mettre les activités et la sécurité de ces ports en conformité avec les prescriptions du Protocole de 1988 relatif à la Convention internationale pour la sauvegarde de la vie humaine en mer. Ces nouveaux règlements devraient entrer en vigueur d'ici juillet 2004.

1.4 À l'alinéa e) du paragraphe 2 de la résolution, les États sont requis de veiller à ce que toute personne qui participe au financement, à l'organisation, à la préparation ou à la perpétration d'actes de terrorisme soit traduite en justice. Le Comité souhaiterait avoir un aperçu des programmes de formation que l'Estonie met concrètement à la disposition de ses fonctionnaires, de sa police judiciaire, des membres du parquet et des autorités judiciaires pour les aider à appliquer cet alinéa de la résolution. Cet aperçu pourrait porter, par exemple, sur :

a) Les caractéristiques actuelles et les tendances observées dans les méthodes et les techniques de financement du terrorisme;

b) Les moyens techniques utilisés pour dépister des fonds qui représentent le produit du crime ou qui servent à financer le terrorisme, afin de pouvoir les geler, les saisir ou les confisquer.

Les services d'enquête étudient les tendances suivies par le financement du terrorisme.

Le dépistage des fonds et avoirs financiers terroristes repose sur les services de renseignement ainsi que sur la surveillance et l'analyse des transactions effectuées par l'entremise des établissements de crédit. Étant donné que le financement du terrorisme est par définition une activité illicite et clandestine, il importe au plus haut point de détecter aussi tôt que possible les éventuelles tentatives visant à commettre ce genre de crime. C'est pourquoi l'Estonie attribue un degré de priorité très élevé aux activités de renseignement et a mis en place un dispositif intégré faisant intervenir plusieurs techniques d'enquête.

Les projets d'amendements à la loi relative à la prévention du blanchiment d'argent proposent que les membres des professions visées dans cette loi soient tenus de déclarer au Service de renseignement financier tout soupçon de financement du terrorisme. Ils autorisent le Service de renseignement financier à établir une liste indicative d'indices de financement du terrorisme qui sera affichée sur son site Web.

1.5 Dans la perspective d'une mise en oeuvre effective de l'alinéa e) du paragraphe 2 de la résolution, l'Estonie pourrait-elle donner au Comité un aperçu des mesures qu'elle prend pour faciliter le dépistage, la surveillance et l'arrestation des personnes impliquées dans des activités de financement du terrorisme et pour les traduire en justice? Ainsi, par exemple, a-t-elle mis au point des stratégies ou des dispositifs particuliers pour aider les établissements financiers, les organes de contrôle, les services de police et les services chargés de la surveillance des frontières à joindre leurs efforts dans l'application de l'alinéa e) du paragraphe 2?

En 2002, l'Organisme de contrôle des établissements financiers a publié des directives pour la prévention du blanchiment d'argent qui expliquent en détail les obligations pesant sur les établissements de crédit et autres établissements financiers dans la gestion de leurs relations commerciales avec leurs clients, et notamment celles de vérifier l'identité de leurs clients et de mettre régulièrement à jour les informations relatives au blanchiment d'argent dont elles disposent sur leurs clients. S'agissant du financement du terrorisme, les amendements à la loi relative à la prévention du blanchiment d'argent actuellement envisagés renforceront le contrôle des établissements financiers et soumettront de nouvelles professions à des obligations similaires à celles qui pèsent sur les établissements financiers, et ceci afin de prévenir tant le blanchiment d'argent que le financement du terrorisme. Le début de 2003 a vu l'adoption d'une loi relative aux sanctions internationales qui prescrit la marche à suivre face aux individus visés par des sanctions internationales, notamment pour terrorisme et financement du terrorisme. Bien que cette loi ait probablement besoin d'être amendée, elle offre un cadre juridique pour la recherche de personnes impliquées dans le financement du terrorisme.

En application de la loi relative aux sanctions internationales, le Gouvernement a publié un certain nombre d'arrêtés qui imposent des restrictions aux personnes morales et physiques frappées de sanctions internationales par le Conseil de sécurité des Nations Unies ou le Conseil de l'Europe.

L'Estonie n'a pas adopté de stratégie spéciale pour faciliter la coopération entre ses diverses administrations. Toutefois, un certain nombre de ces dernières ont approuvé un mémorandum d'accord qui les engage à échanger des informations et à créer des groupes de travail et des équipes d'intervention conjointes. On peut par conséquent dire que l'Estonie a mis en place un dispositif de coordination pour

lutter contre le financement du terrorisme. Grâce à ce dispositif, les différents services de police estoniens collaborent étroitement entre eux dans la conduite de leurs enquêtes, et ceci afin d'utiliser plus rationnellement leurs ressources.

1.6 En ce qui concerne la mise en oeuvre de l'alinéa e) du paragraphe 2 de la résolution, le Comité souhaite connaître, pour la période allant du 1er janvier 2001 au 31 décembre 2002 :

b) Combien de poursuites ont été engagées contre des terroristes ou ceux qui les aident :

Aucune;

c) La valeur des fonds et avoirs qui ont été bloqués ou saisis :

Sans objet;

d) Combien d'enquêtes sont en cours et/ou ont été menées à terme :

Aucune;

e) Combien d'enquêtes ont dû être coordonnées sur le plan international :

Aucune.

1.7 En ce qui concerne la mise en oeuvre effective de l'alinéa e) du paragraphe 2 de la résolution, le Comité souhaite avoir un aperçu des lois adoptées pour lutter contre la cybercriminalité et des dispositions qui visent à empêcher les terroristes d'utiliser l'Internet et autres moyens électroniques à leurs propres fins.

Le seul texte législatif estonien sur cette question est le Code pénal, qui sanctionne les cybercrimes ci-après :

Article 178. Production d'articles à caractère de pornographie enfantine ou diffusion de pornographie enfantine

1) Celui qui produit, stocke, distribue, affiche ou diffuse de quelque façon que ce soit des images, écrits ou autres documents, ou des reproductions de documents représentant un mineur de moins de 14 ans dans une situation érotique ou pornographique est passible d'une sanction pécuniaire ou d'une peine d'emprisonnement d'un an.

2) Lorsqu'elles sont commises par une personne morale, les infractions susmentionnées sont passibles d'une sanction pécuniaire.

Article 206. Sabotage d'ordinateur

1) La substitution, la suppression, l'endommagement ou le blocage illicites de données ou de programmes installés dans un ordinateur, s'ils provoquent un préjudice important; ou l'insertion illicite de données ou de programmes dans un ordinateur, si elle crée un préjudice important, sont passibles d'une sanction pécuniaire ou d'une peine d'un an d'emprisonnement.

2) Le même acte, s'il est commis avec l'intention de perturber le fonctionnement d'un ordinateur ou d'un réseau de télécommunication, est passible d'une sanction pécuniaire ou d'une peine d'emprisonnement de trois ans.

Article 207. Le fait de détériorer une connexion à un réseau informatique

Le fait de détériorer ou de bloquer une connexion à un réseau ou à un système informatique est passible d'une sanction pécuniaire.

Article 208. Propagation de virus informatiques

1) La propagation d'un virus informatique est passible d'une sanction pécuniaire ou d'une peine d'emprisonnement d'un an.

2) Le même fait, s'il est commis au moins deux fois ou de manière à provoquer des dommages importants, est passible d'une sanction pécuniaire ou de trois ans d'emprisonnement.

Article 213. Fraude informatique

Celui qui obtient un bénéfice économique par l'introduction, la substitution, l'effacement ou le blocage de programmes ou de données informatiques ou en interférant avec une opération de traitement de données, et influence par conséquent le résultat de cette opération, est passible d'une sanction pécuniaire ou d'une peine d'emprisonnement de cinq ans.

Article 217. Utilisation illicite d'un ordinateur, d'un système informatique ou d'un réseau informatique

1) L'utilisation illicite d'un ordinateur, d'un système informatique ou d'un réseau informatique par contournement d'un code, d'un mot de passe ou de tout autre dispositif de protection est passible d'une sanction pécuniaire.

2) Le même fait, s'il :

1) Provoque des dommages importants ou

2) Est commis en ayant recours à un secret d'État ou à un ordinateur, un système informatique ou un réseau informatique qui contient des informations réservées à un usage officiel, est passible d'une sanction pécuniaire ou d'une peine d'emprisonnement de trois ans.

Articles 219 à 230. Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le chapitre 14 du Code pénal est consacré aux atteintes à la propriété intellectuelle

Article 284. Mise à disposition de codes de sécurité

La mise à disposition illicite des codes de sécurité d'un ordinateur, d'un système informatique ou d'un réseau informatique, si elle est commise avec l'intention d'obtenir un bénéfice économique et si elle entraîne des dommages sérieux ou des conséquences graves, est passible d'une sanction pécuniaire ou d'une peine de trois ans d'emprisonnement.

Article 315. Activités illicites de surveillance spéciale ou exceptionnelle

Le fait, pour une personne officiellement investie de l'autorité nécessaire pour pratiquer la surveillance, de mener des activités illicites de surveillance spéciale ou exceptionnelle est passible d'une sanction pécuniaire ou d'une peine de trois ans d'emprisonnement.

L'interception illégale est punie en tant qu'activité illégale de surveillance.

1.8 S'agissant de la mise en oeuvre effective de l'alinéa e) du paragraphe 2 de la résolution, le Comité souhaite savoir si le droit estonien autorise la mise en place de tribunaux extraordinaires pour juger les affaires de terrorisme, la mise en liberté sous caution de terroristes, le recours aux techniques d'infiltration et la mise sous écoute en vue de prévenir des actes de terrorisme.

Le terrorisme et les infractions qui lui sont liées sont jugés par les tribunaux pénaux ordinaires puisqu'ils constituent, en droit, des infractions pénales.

Tous les moyens extraordinaires mentionnés dans la question du Comité peuvent être employés, à condition qu'un tribunal en autorise l'emploi. Les techniques d'infiltration et la mise sous écoute peuvent également être employées dans le cadre de la lutte contre le trafic de drogues ou contre tout autre type d'activité criminelle.

1) Cependant, pour engager des poursuites judiciaires contre une organisation terroriste, il faut constituer un tribunal extraordinaire car les affaires concernant des organisations criminelles sont jugées par un collège de trois juges. La raison en est qu'une organisation terroriste peut être considérée comme une catégorie d'organisation criminelle.

Code de procédure pénale

Article 23. Tribunaux de première instance

Les articles 255 et 256 du Code pénal disposent que les affaires criminelles sont jugées par un collège de trois juges.

2) Le nouveau Code de procédure pénale, qui entrera en vigueur le 1er juillet 2004, exclut la liberté sous caution pour les terroristes.

Article 135. Cautionnement

2) Par « cautionnement », on entend la somme versée à titre de mesure préventive par un suspect, un prévenu, ou une autre personne agissant pour le compte du suspect ou du prévenu, au compte séquestre du tribunal. La liberté sous caution ne s'applique pas aux suspects ou aux prévenus dans le cas des infractions pénales visées aux articles 89, 90, 96, 114, 214, 237 (terrorisme), 244, 246, 255, 256 et 405 (explosifs) du Code pénal.

3) L'infiltration et la mise sous écoute sont autorisées lorsqu'elles visent à prévenir un acte de terrorisme.

Loi relative à la surveillance

Article 14. Recrutement de personnes disposées à coopérer secrètement à des activités de surveillance

1) Les organismes de surveillance sont habilités à recruter des adultes, avec leur consentement, qui sont disposés à coopérer secrètement et volontairement, de façon temporaire ou permanente, à des activités de surveillance.

Loi relative aux organes de sécurité

Article 23. Création d'une personne physique ou morale fictive

1) Lorsque les activités d'un organe de sécurité lui imposent de créer une personne fictive, le ministre compétent dépose une demande d'inscription au Registre du commerce ou à celui des associations à but non lucratif et des fondations, selon le cas. Lorsque cette personne fictive n'est plus nécessaire, le ministre compétent dépose une demande de radiation en se conformant à la procédure normale.

Article 25. Dérogations au droit à la confidentialité des communications

3) Il peut être dérogé au droit d'une personne à la confidentialité de ses communications par les moyens suivants :

Examen d'envois postaux;

Mise sous écoute, observation ou enregistrement de messages et autres informations transmises par télégraphe, téléphone et autres moyens de communication;

Mise sous écoute, observation ou enregistrement d'informations transmises par tout autre moyen.

Code de procédure pénale

Article 120. Infiltrants

Par « infiltrant », on entend un fonctionnaire qui, agissant sous une identité fictive, recueille des éléments de preuve dans une enquête criminelle. Des documents fictifs, qu'il s'agisse de documents d'identité ou d'autres types de documents, peuvent lui être délivrés afin de lui permettre de changer d'identité.

Un infiltrant est autorisé à entrer dans des relations juridiques sous une identité fictive. Il est astreint aux mêmes obligations que tout fonctionnaire d'un organisme d'enquête, pour autant que ces obligations ne lui imposent pas de compromettre son identité fictive.

Efficacité des services douaniers, des services de contrôle de l'immigration et des contrôles aux frontières

1.9 S'agissant de l'application des alinéas b) et g) du paragraphe 2 de la résolution, qui font obligation aux États de prendre les mesures voulues pour empêcher que des actes de terrorisme ne soient commis et d'instituer des contrôles efficaces aux frontières, l'Estonie pourrait-elle faire savoir au Comité si la liste des personnes soupçonnées de terrorisme qui est distribuée aux gardes frontière estoniens (comme il est dit à la page 11 de son premier rapport) est également communiquée à d'autres administrations ou incorporée dans les bases de données du Service des douanes et des autres organismes de contrôle estoniens? De même, en ce qui concerne les alinéas b) et g) du paragraphe 2, le Comité souhaite être informé de l'état d'avancement du projet du Service des douanes estonien consistant à établir des relations de travail avec certaines entreprises privées et à renforcer ses moyens d'analyse des données pour mieux faire face au terrorisme et autres formes de criminalité.

Les bases de données des gardes frontière estoniens contiennent des informations sur les terroristes et leurs associés qui doivent permettre soit de les appréhender soit de mener une enquête approfondie sur eux. La liste de personnes soupçonnées de terrorisme mentionnée plus haut est révisée et actualisée périodiquement en collaboration avec la Direction générale de la sécurité (*Kaitsepolitsei*).

La Direction des douanes ne dispose pas d'un accès en ligne à la liste de terroristes établie par la Direction des gardes frontière en coopération avec la Direction générale de la sécurité. Elle n'y a accès qu'en cas de besoin : la Direction des gardes frontière répond en effet aux demandes d'information de la Direction des douanes concernant des cas précis de soupçon de terrorisme.

Relations avec des entreprises privées : La Direction des douanes a conclu des mémorandums d'accord avec DHL International Eesti As, Air Cargo Estonia AS, TNT Express Worldwide Eesti AS, Schenker AS et AS Eesti Post (Service estonien des postes). De même, elle a passé des accords de coopération avec les sociétés de services téléphoniques qui lui donnent accès à leurs bases de données. La Direction des douanes a également accès à la base de données passagers d'AS Estonian Air (la compagnie aérienne nationale estonienne).

Renforcement des moyens d'analyse des données : la Direction des douanes a mis en place un dispositif d'échange d'informations avec la Direction des gardes frontière, la Direction de la police et la Direction des impôts, et elle a accès aux bases de données des sociétés de télécommunication (ELION AS, TELE 2). Des analyses de risque sont effectuées tant au niveau des régions qu'au niveau central. Un logiciel spécialisé (Analysts' Notebook) a été retenu à cette fin. L'analyse opérationnelle et tactique fait appel au module de sélectivité MODSEL de ASYCUDA (le principal système de traitement des déclarations) et au module RISK du système national estonien d'informatisation des transports. Tous les fonctionnaires des services de renseignement sont reliés à un réseau de communication à base de courrier électronique qui permet une rapide diffusion des principales informations.

La Direction des douanes dispose d'un agent de liaison chargé de recueillir et d'analyser les informations en provenance des différents postes de douane et de transmettre au Service de renseignement financier les informations pertinentes afin d'obtenir en retour des informations concernant d'éventuelles infractions liées au blanchiment d'argent et au financement du terrorisme. La Direction des douanes ne s'occupe pas directement de blanchiment d'argent et se contente de transmettre les informations pertinentes, pour enquête, à la Direction de la police.

1.10 À la page 13 de son premier rapport, l'Estonie rapporte que, dans le cadre de la mise en oeuvre de l'alinéa g) du paragraphe 2 de la résolution, elle a donné à la Direction des gardes frontière les moyens d'équiper les principaux postes frontière de systèmes VSC-2000 et DIXI-05 de détection des documents de voyage contrefaits ou falsifiés. Le Comité souhaite savoir si l'Estonie prévoit d'équiper ainsi tous les points d'accès à son territoire et, si tel est le cas, à quel horizon ce projet pourrait être mené à terme.

Tous les points de passage de la frontière et tous les postes de gardes frontière assurant des services de contrôle aux frontières seront équipés de systèmes Money Checker (30 unités). L'Estonie n'a pas l'intention d'acquérir de nouveaux DIXI-05

ou VSC-2000. Elle acquerra plutôt des systèmes de type VSC-4C ou DOCUBOX-500 qui seront attribués à ceux des principaux points de passage de la frontière qui n'ont pas reçu de VSC-2000.

Le Centre d'analyse des documents de voyage mis en place au sein de la Direction nationale des gardes frontière doit acquérir un système numérique de type DOCUCENTER 3000, à la suite de quoi le VSC-2000 qu'il utilise actuellement sera transféré à l'important point de passage de Luhamaa sur la frontière avec la Russie.

1.11 À l'alinéa g) du paragraphe 2 de la résolution, les États sont requis d'instituer des contrôles efficaces lors de la délivrance de documents d'identité. L'Estonie pourrait-elle donner au Comité un aperçu des dispositions de sa législation qui régissent l'octroi de la nationalité estonienne ou d'autres droits civiques? Un étranger qui acquiert la nationalité estonienne ou d'autres droits civiques a-t-il le droit de changer de nom? Quelles précautions sont prises pour vérifier l'identité réelle d'une personne avant de lui délivrer de nouveaux documents d'identité?

Le changement de nom ou de prénom d'un citoyen estonien ou d'une personne justifiant d'un permis de séjour qui n'est pas citoyen d'un autre État doit être approuvé par le Ministre de l'intérieur sur la base de la demande formulée par la personne concernée. Les changements de nom ou de prénom accordés à des adultes sont communiqués aux casiers judiciaires tenus par la Direction nationale de la police. Actuellement, les citoyens estoniens et les étrangers justifiant d'un permis de séjour peuvent changer leurs noms sur simple demande. La promulgation de la loi relative aux noms, qui en est encore à l'état de projet, est censée rendre plus strictes les conditions d'attribution des noms.

1.12 S'agissant de l'application de l'alinéa g) du paragraphe 2 de la résolution, quelles mesures l'Estonie a-t-elle prises pour s'assurer que ses documents d'identité, documents de voyage et autres documents officiels (certificats de naissance, certificats de mariage, permis de conduire, cartes du service militaire, etc.) satisfont aux normes de sécurité minimales de l'Organisation internationale de normalisation qui visent à rendre impossible la reproduction, la falsification ou l'obtention de documents frauduleux?

Les cartes d'identité et les documents de voyage satisfont aux normes de l'Organisation internationale de l'aviation civile, qui fait partie du système des Nations Unies et dont l'Estonie est membre. Le niveau de sécurité des cartes d'identité et des nouveaux passeports estoniens est très élevé; un nouveau passeport pour étrangers sera mis en circulation très prochainement. Les anciens passeports, qui sont très faciles à falsifier, sont encore en usage en Estonie. Le niveau de sécurité des documents délivrés entre 1992 et le premier semestre de 1996 est faible, car ces documents ne sont pas lisibles par ordinateur. Leur validité doit cependant expirer très bientôt. L'Estonie compte actuellement cinq types de documents d'état civil, à savoir les certificats de naissance, de mariage, de divorce, de changement de nom et de décès. Les normes de sécurité appliquées qui régissent l'impression de ces documents sont satisfaisantes, puisqu'elles font intervenir trois dispositifs de sécurisation différents.

1.13 À l'alinéa d) du paragraphe 3 de la résolution, il est demandé aux États de devenir parties aux conventions et protocoles internationaux relatifs au terrorisme. À cet égard, le Comité souhaiterait être informé de l'état

d'avancement de la loi de ratification du Protocole pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental.

Les formalités nationales d'adhésion en sont à leur dernière phase, et le *Riigikogu* (Parlement) a ratifié le Protocole le 12 novembre 2003. Nous prévoyons devenir partie au Protocole d'ici à la fin de l'année.

1.14 Pour appliquer effectivement l'alinéa a) du paragraphe 2 de la résolution, les États doivent, entre autres choses, mettre fin à l'approvisionnement en armes des terroristes. À la page 8 de son premier rapport, l'Estonie dit envisager d'élaborer un processus de contrôle des activités de courtage ainsi que des programmes de conformité interne du secteur industriel afin de mieux contrôler l'exportation d'armes et de matériel de guerre. Le Comité souhaiterait être informé de l'état d'avancement de ce projet.

En tenant compte des derniers développements dans ce domaine, le Gouvernement estonien a adopté un projet de loi relative au contrôle des exportations qui, entre autres dispositions, abolirait les contrôles sur les articles à double usage et introduirait, en plus des permis individuels, des autorisations globales et générales. En outre, ce projet définit plus clairement les mesures de contrôle des activités de courtage et crée un registre du courtage. Il est actuellement examiné par le Parlement et devrait être adopté avant la fin de 2003.

1.15 Combien d'enquêtes ont été effectuées et/ou de poursuites judiciaires ont été engagées en 2002 pour des affaires de violation du régime d'exportation d'armes, y compris les produits dangereux? Combien de ces enquêtes et/ou poursuites judiciaires étaient liées au terrorisme?

Trois enquêtes et une action en justice ont été engagées pour des affaires de violation du régime de contrôle des exportations. Ni ces enquêtes ni cette action en justice, qui ont pris place en 2002, n'était liée au terrorisme.

Il n'a pas été ouvert d'enquête ni engagé de poursuite judiciaire liées à des affaires de terrorisme en 2002.