

18 mai 2011  
Français  
Original: anglais

---

**Neuvième Réunion des chefs des services  
chargés au plan national de la lutte contre  
le trafic illicite des drogues, Europe**

Vienne, 28 juin-1<sup>er</sup> juillet 2011

Point 4 de l'ordre du jour provisoire\*

**Application des recommandations adoptées  
à la huitième Réunion des chefs des services  
chargés au plan national de la lutte contre  
le trafic illicite des drogues, Europe**

**Application des recommandations adoptées à la huitième  
Réunion des chefs des services chargés au plan national de  
la lutte contre le trafic illicite des drogues, Europe\*\***

**I. Introduction**

1. La huitième Réunion des chefs des services chargés au plan national de la lutte contre le trafic illicite des drogues (HONLEA), Europe, tenue à Vienne du 16 au 19 juin 2009, a adopté un ensemble de recommandations après examen par ses groupes de travail des thèmes indiqués ci-après.
2. Conformément à la pratique établie, le rapport de la huitième Réunion a été transmis aux gouvernements représentés à la Réunion. Un questionnaire sur l'application des recommandations adoptées lors de cette réunion a été envoyé aux gouvernements le 18 mars 2011, avec des informations concernant la neuvième Réunion des HONLEA, Europe.
3. Le présent rapport a été établi à partir des informations communiquées à l'Office des Nations Unies contre la drogue et le crime (UNODC) par les gouvernements dans leurs réponses au questionnaire précité. Au 17 mai 2011, il avait été reçu des réponses des Gouvernements des pays suivants: Allemagne, Chypre, Croatie, Espagne, Estonie, Israël, Luxembourg, Malte, Suisse et Turquie.

---

\* UNODC/HONEURO/9/1

\*\* Traduction d'un document non revu par les services d'édition.



## II. Application des recommandations adoptées à la huitième Réunion

### Thème 1. L'influence d'Internet et d'autres médias électroniques sur le trafic de drogues

#### *Recommandation a)*

4. Pour pouvoir exploiter et extraire efficacement des éléments de preuve numériques, la huitième Réunion a recommandé que les gouvernements encouragent dans un premier temps leurs services de détection et de répression à mettre au point une stratégie en la matière.

5. La Croatie a indiqué qu'un décret sur les éléments de preuve numériques avait été adopté afin d'inclure une définition de la preuve numérique dans la loi sur la procédure pénale du pays. Cette loi réglementait les conditions dans lesquelles des données pouvaient être légitimement confisquées, conservées et utilisées dans le cadre d'affaires et posait l'obligation de restituer les données informatiques (loi sur la procédure pénale, articles 183, 184, 262 et 263). Sous réserve de ces dispositions, les enregistrements, documents et objets obtenus par des méthodes spéciales de collecte de preuves, notamment par l'interception, la collecte et l'enregistrement de données informatiques, pourraient être utilisés comme preuves devant les tribunaux (loi sur la procédure pénale, articles 332 et 333).

6. L'Estonie a signalé que la police estonienne avait accès à toutes les options juridiques pour la collecte et l'utilisation de preuves issues de moyens de communication ou d'Internet.

7. L'Allemagne a indiqué que la troisième version des lignes directrices pour l'identification, le rassemblement, l'acquisition et la conservation des preuves numériques (norme ISO/CEI 27037) avait été publiée et que la mise en œuvre de cette norme était prévue pour l'année en cours.

8. Israël a noté que sa législation s'appliquait aussi bien aux infractions visant les systèmes informatiques qu'aux infractions commises à l'aide de moyens informatiques (loi sur l'informatique n° 5755, 1995), et comprenait des dispositions sur les preuves (ordonnance sur les preuves, nouvelle version, n° 5731, 1971). Des cours de formation spécifiques, notamment des modules sur la criminalité liée à l'informatique et la conservation des preuves, étaient proposés aux fonctionnaires de police pour qu'ils se spécialisent en enquêtes informatiques.

9. Chypre, le Luxembourg, Malte et la Suisse n'avaient pris aucune mesure pour appliquer cette recommandation. Alors que Malte a indiqué qu'aucune stratégie nationale officielle concernant les éléments de preuve numériques n'était applicable actuellement, de telles stratégies avaient été mises en œuvre et développées depuis plusieurs années par les forces de police cantonales et fédérales suisses.

10. L'Espagne a mentionné sa législation sur la conservation des données électroniques (loi 25/2007 du 18 octobre 2007 sur la "conservation des données concernant les communications électroniques et les réseaux publics de communication"), en vertu de laquelle les opérateurs de télécommunications étaient obligés de conserver les données en vue de leur utilisation par des agents compétents des services de détection et de répression. La police nationale et la

Garde civile comprenaient des équipes spéciales d'enquête sur le trafic de drogues au moyen d'Internet.

11. La Turquie a signalé que le Département de la lutte contre la contrebande et la criminalité organisée de la police nationale avait mis en place une unité spécialisée dans la lutte contre la cybercriminalité et une stratégie concernant les éléments de preuve numériques, ce qui permettait une certaine homogénéité des enquêtes sur la cybercriminalité qu'il avait menées contre des groupes criminels organisés.

*Recommandation b)*

12. Comme il est urgent d'apporter à la cybercriminalité une réponse concertée à l'échelle mondiale, il a été recommandé que les gouvernements soient encouragés à envisager l'élaboration d'une convention des Nations Unies en la matière, qui donnerait aux États Membres des orientations et des lignes directrices et les aiderait à lutter ensemble contre ce fléau.

13. La Croatie et l'Allemagne avaient ratifié la Convention sur la cybercriminalité<sup>1</sup> du Conseil de l'Europe. Malte était signataire de la Convention et prenait des dispositions pour la ratifier au plus vite.

14. La Croatie a signalé qu'avant même de signer et de ratifier la Convention sur la cybercriminalité et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques<sup>2</sup> elle avait, en 2004, modifié son Code pénal pour créer ou modifier un certain nombre d'infractions pénales ayant trait à la pédopornographie et commises au moyen d'un système ou d'un réseau informatique, à la discrimination raciale ou autre et commises au moyen d'un système informatique, à l'atteinte à la confidentialité, l'intégrité et la disponibilité des données, des programmes et des systèmes informatiques, à la falsification informatique et à l'utilisation frauduleuse de l'informatique.

15. La Croatie et l'Espagne ont mentionné la réunion du groupe intergouvernemental d'experts à composition non limitée sur l'étude approfondie du phénomène de la cybercriminalité, qui s'était tenue à Vienne du 17 au 21 janvier 2011.

16. Chypre, le Luxembourg et la Suisse n'avaient pas pris de mesures comme suite à cette recommandation. La Suisse a indiqué que ses autorités avaient coopéré efficacement à plusieurs reprises avec différents pays sur des affaires de cybercriminalité.

17. L'Allemagne était s'opposée à l'adoption d'une convention des Nations Unies sur la cybercriminalité. À l'inverse, Israël et la Turquie y étaient favorables. Israël soutenait tous les efforts internationaux qui étaient faits dans ce domaine et la Turquie proposait de fournir des services d'expert pour l'élaboration d'une telle convention.

18. L'Espagne a déclaré que la cybercriminalité était une question prioritaire pour les États membres de l'Union européenne et a mentionné les moyens d'action et les

<sup>1</sup> Conseil de l'Europe, *Série des Traités européens*, n° 185.

<sup>2</sup> Conseil de l'Europe, *Série des Traités européens*, n° 189.

instruments juridiques disponibles pour lutter contre ce phénomène, notamment le Programme de Stockholm du Conseil européen et la stratégie de sécurité intérieure de l'Union européenne, ainsi que la Convention sur la cybercriminalité et la directive de l'Union européenne sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications<sup>3</sup>.

*Recommandation c)*

19. Pour lutter contre les infractions facilitées par le recours à la cybertechnologie, les gouvernements ont été encouragés à s'assurer que leur législation nationale permettait d'enquêter efficacement sur ces infractions et d'en poursuivre les auteurs sur le territoire national.

20. La Croatie a signalé que sa nouvelle loi sur la procédure pénale, qui remplacerait en septembre 2011 la loi sur la procédure pénale de 1997, attribuerait le contrôle et la direction des enquêtes criminelles au procureur de l'État et non plus au juge, laissant à ce dernier les décisions concernant la détention, le statut et les droits du défendeur. Un nouveau Code pénal avait également été adopté, qui tenait compte des normes et pratiques juridiques de l'Allemagne, de l'Autriche et de la Suisse. Le Code comprenait l'obligation d'appliquer les normes internationales, notamment celles des Nations Unies, du Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme, de l'Office européen de lutte antifraude et du Comité européen pour la prévention de la torture.

21. Chypre, le Luxembourg et la Suisse n'avaient pas pris de mesures comme suite à cette recommandation. Chypre a noté que sa législation nationale interdisait la présentation des stupéfiants sous un jour favorable dans l'intention d'en fournir à autrui. Le Luxembourg a indiqué que, selon sa législation nationale (loi modifiée du 19 février 1973 sur la revente de substances médicales et la lutte contre la toxicomanie), les infractions liées à l'usage illicite de substances pouvaient donner lieu à des poursuites indépendamment des moyens utilisés pour les commettre, notamment de l'utilisation de cybertechnologies. La Suisse considérait sa législation nationale comme suffisante.

22. L'Estonie a déclaré que sa législation autorisait l'utilisation de données collectées comme preuves, si cela était nécessaire pour résoudre des affaires pénales. L'Allemagne a noté que, en tant que partie à la Convention sur la cybercriminalité, elle avait adopté une législation nationale conforme à cette dernière. Israël a déclaré que, bien que sa législation (loi sur l'informatique, 1995) englobe les infractions liées à la cybertechnologie, elle n'était pas toujours suffisante pour traiter les affaires dans lesquelles il avait été fait appel à des technologies plus avancées, notamment celles liées à Internet et aux communications.

23. Malte a indiqué que sa législation sur la criminalité liée à l'informatique (Délits liés à l'informatique, chapitre 9 des lois de Malte) était constamment mise à jour pour faire face aux menaces émergentes et donner suite aux évaluations des risques. Étant donné que sa législation actuelle ne faisait référence à aucune

---

<sup>3</sup> 2006/24/EC.

technologie spécifique, il n'était pas nécessaire de légiférer à nouveau lorsque de nouvelles terminologies apparaissaient sur le marché. Les services de détection et de répression étaient en contact permanent avec les représentants de différents secteurs, notamment les milieux d'affaires, les prestataires de services électroniques et des autorités, afin de pouvoir réagir aux menaces qui se faisaient jour.

24. L'Espagne a signalé que sa législation sur la conservation des données électroniques stipulait que ces données devaient être conservées de manière à permettre de déterminer le type, la date et l'heure, la durée, l'origine et la destination des communications électroniques, le moyen de communication utilisé et sa localisation, ainsi que l'identité des utilisateurs du service de communication.

25. La Turquie a mentionné sa législation nationale sur la cybercriminalité (article 134 de la loi sur la procédure pénale) et a indiqué qu'elle était mise en œuvre au moyen d'un décret général publié par le directeur du Département de lutte contre la contrebande et la criminalité organisée de la police nationale turque.

*Recommandation d)*

26. La huitième Réunion a recommandé que les gouvernements soient encouragés à définir des normes en matière de preuve numérique afin de préserver l'intégrité et la qualité des éléments de preuve fournis par la cybertechnologie.

27. La Croatie a fait état des normes en vigueur depuis 2009, qui prévoyaient les conditions techniques à remplir pour les enregistrements audiovisuels des interrogatoires de défendeurs et des auditions de témoins et pour leur reproduction, pour les procédures d'administration de la preuve, et notamment des éléments de preuve obtenus par l'interception, le rassemblement et l'enregistrement de données informatiques, ainsi que pour les procès-verbaux et le traitement des enregistrements.

28. Chypre, le Luxembourg, Malte et la Suisse n'avaient pas pris de mesures pour appliquer cette recommandation. Malte a signalé que, malgré l'absence de stratégie nationale officielle, ses services de détection et de répression avaient adapté la majeure partie du "Guide de bonnes pratiques concernant les preuves électroniques liées à l'informatique" publié par l'Association des préfets de police du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord. Des cours de formation annuels étaient dispensés aux agents des services de détection et de répression afin de faire en sorte que les agents chargés des enquêtes informatiques soient familiarisés avec l'évolution de la technologie et qu'ils connaissent les mesures à prendre pour conserver les éléments de preuve numériques. La Suisse a jugé qu'aucune mesure additionnelle n'était nécessaire étant donné que c'était la pratique et les décisions des tribunaux qui définissaient des normes de qualité dans ce domaine.

29. L'Estonie a noté que la conservation de la preuve était réglementée par sa loi sur la procédure pénale.

30. L'Allemagne a mentionné le projet de norme ISO/CEI 27037 et a encouragé les autres pays à appliquer les normes ISO pertinentes.

31. Israël a signalé que, lorsque les agents chargés des enquêtes informatiques déposaient en justice, leurs témoignages étaient acceptés au même titre que les preuves collectées à partir de différentes sources, telles que l'ordinateur du suspect, ou des entreprises publiques et privées.

32. L'Espagne a signalé que, selon sa législation sur la conservation des données électroniques, celles-ci ne pouvaient être transférées par voie électronique aux agents compétents des services de détection et de répression qu'aux fins prévues par la loi et sur autorisation judiciaire. Ces données pouvaient être conservées pendant 12 mois, avec la possibilité de réduire cette période à 6 mois ou de l'étendre à 24 mois en concertation avec l'opérateur de télécommunications.

33. La Turquie a signalé que le Département de lutte contre la contrebande et la criminalité organisée de la police nationale avait mis en place une stratégie concernant les éléments de preuve numérique qui servait de schéma directeur pour ses enquêtes.

## **Thème 2. L'importance de l'information pour démanteler les groupes de trafiquants**

### *Recommandation a)*

34. Pour favoriser une action concertée et efficace des services de détection et de répression contre les réseaux de trafiquants et les groupes criminels organisés opérant au niveau international, il a été recommandé que les gouvernements veillent à ce que leurs services tirent pleinement parti des plates-formes sécurisées de communication, des bases de données et d'autres sources d'information dont elles disposent dans le cadre de leur participation au Centre régional d'information et de coordination pour l'Asie centrale, à l'Office européen de police (Europol), à l'Organisation internationale de police criminelle (INTERPOL), à l'Organisation mondiale des douanes et à d'autres organisations de confiance créées à des fins de coordination.

35. La Croatie a fait état de sa législation nationale sur les douanes, qui offrait la possibilité de faire les déclarations en douane par voie électronique, et de son appartenance à des organismes internationaux compétents dans ce domaine. Parmi ses bonnes pratiques en matière d'échange d'informations par voie électronique figuraient notamment le recours au Réseau douanier de lutte contre la fraude de l'Organisation mondiale des douanes (OMD) et aux systèmes utilisés par INTERPOL, ainsi que l'accord conclu en 2010 avec Europol, qui avait permis la mise en place d'une ligne de communication sécurisée entre les points de contact nationaux et le siège d'Europol. La Croatie a également mentionné les activités qu'elle menait dans le cadre du Comité de coopération mixte du Centre régional de l'Initiative de coopération en Europe du Sud-Est pour la lutte contre la criminalité transfrontière, et de son groupe de travail sur la prévention de la fraude commerciale.

36. Chypre détachait des fonctionnaires de police auprès d'Europol et d'INTERPOL, mais ne participait pas au Centre régional d'information et de coordination pour l'Asie centrale. L'Estonie avait trois agents de liaison détachés auprès d'Europol afin d'échanger des informations sur des questions internationales l'intéressant.

37. L'Allemagne a mentionné le soutien qu'elle apportait de longue date aux plates-formes de communication sécurisées, aux bases de données et aux autres sources d'information pertinentes, notamment celles d'Europol et d'INTERPOL, et les échanges d'informations réalisés par ces intermédiaires.

38. L'Autorité fiscale israélienne était membre du Réseau douanier de lutte contre la fraude et du réseau des Bureaux régionaux de liaison chargés du renseignement pour l'Europe occidentale de l'OMD.

39. Le Luxembourg a déclaré que sa police participait à des échanges d'informations et à des opérations et enquêtes concertées régulières avec INTERPOL et Europol. Malte a signalé qu'elle utilisait les plates-formes de communication mentionnées dans la recommandation pour échanger des renseignements ainsi que pour faciliter la coordination des enquêtes en cours.

40. Les agents des services de détection et de répression espagnols avaient accès aux bases de données d'INTERPOL, d'Europol et de SIRENE au moyen d'un bureau national central par lequel transitaient toutes les demandes adressées à ces institutions. L'Espagne avait détaché un certain nombre d'agents de liaison aux sièges de ces organisations et utilisait les plates-formes de liaison destinées aux échanges d'informations que l'Union européenne avait créées à Dakar et à Accra.

41. La Suisse a indiqué qu'elle avait intensifié sa participation à différents groupes de travail, opérations et conférences d'Europol, d'INTERPOL et d'autres.

42. La Turquie a signalé que, bien que ses services de détection et de répression aient accès à la base de données d'INTERPOL, ils n'avaient pas accès à celle d'Europol, le pays n'étant pas membre de l'Union européenne. Des échanges d'informations avaient eu lieu via le Réseau douanier de lutte contre la fraude de l'OMD, le système de collecte et de diffusion de données concernant la route des Balkans (coordonné par l'Office allemand de répression des infractions douanières) et l'Initiative de coopération pour l'Europe du Sud-Est. Au niveau bilatéral, les autorités nationales turques disposaient de canaux de communication avec leurs homologues étrangers.

*Recommandation b)*

43. Il a également été recommandé que les gouvernements prennent des mesures pour s'assurer qu'ils avaient établi le cadre juridique nécessaire pour faciliter les opérations d'agents infiltrés étrangers sur leur territoire lorsque ces opérations avaient fait l'objet d'un accord mutuel.

44. La Croatie a mentionné les obligations qu'elle avait contractées en vertu des traités internationaux relatifs au contrôle des drogues et ses dispositions législatives et administratives définissant les droits et les obligations en matière d'opérations conjointes avec des enquêteurs infiltrés étrangers. À la fin de l'année 2010, la Croatie avait signé 33 accords bilatéraux internationaux concernant des activités conjointes de détection et de répression. Les services de détection et de répression croates coopéraient au niveau opérationnel avec leurs homologues étrangers, à la fois sur le territoire croate et à l'étranger, principalement dans le domaine du contrôle des drogues.

45. Chypre, Israël et la Turquie ont indiqué qu'ils n'avaient pas pris de mesures comme suite à cette recommandation. Chypre avait l'obligation de coopérer avec les États membres de l'Union européenne conformément à la Convention européenne d'entraide judiciaire en matière pénale. Israël et la Turquie n'avaient pas de cadre juridique concernant les opérations d'agents infiltrés étrangers sur leur territoire.

Israël a déclaré que ses services de détection et de répression évaluaient chaque affaire individuellement et prenaient des mesures en conséquence.

46. L'Allemagne, l'Estonie, le Luxembourg, Malte et la Suisse ont indiqué qu'ils avaient mis en place le cadre juridique nécessaire. Les opérations d'agents infiltrés étrangers en Estonie étaient réglementées par la loi sur la procédure pénale. Au Luxembourg, la législation pertinente (loi du 3 décembre 2009, loi du 21 mars 2006) autorisait également la réalisation de telles opérations par des équipes d'enquête conjointes. À Malte, ces opérations étaient autorisées par la loi depuis l'année 2003, aux termes de l'article 435E du Code pénal, chapitre 9 des lois de Malte.

47. L'Espagne a mentionné le cadre juridique national et international applicable aux opérations d'agents infiltrés étrangers sur son territoire (Convention d'application de l'Accord de Schengen, loi organique 19/94, loi 11/2003 et loi organique 3/2003). Le terme "police judiciaire" était interprété de telle sorte que ces opérations soient possibles, à condition qu'elles visent un acte de criminalité organisée, tel que défini par la loi, et qu'elles obtiennent l'autorisation expresse des autorités judiciaires espagnoles. La police espagnole contrôlait et supervisait les agents infiltrés étrangers, qui étaient entièrement soumis à la législation espagnole tant qu'ils étaient sur le territoire national.

*Recommandation c)*

48. Pour améliorer, resserrer et maintenir une coopération étroite entre les services de détection et de répression chargés d'enquêter sur les réseaux criminels de trafic de drogues illicites, il a été recommandé que les gouvernements encouragent leurs services à répondre en temps voulu aux demandes d'informations et d'assistance qu'ils recevaient de leurs homologues étrangers.

49. La Croatie a mentionné ses obligations internationales et sa législation nationale concernant l'entraide judiciaire et a signalé que ses services de détection et de répression échangeaient des informations avec les services compétents à l'étranger, directement ou par l'intermédiaire du Bureau d'INTERPOL, d'Europol ou du Groupe Egmont des cellules de renseignements financiers, et qu'il y avait eu un certain nombre de cas d'entraide en matière de lutte contre la criminalité internationale liée à la drogue. Pour faciliter les échanges d'informations, la police avait également des agents de liaison en Autriche, en Serbie, en Israël et au siège d'INTERPOL (et auparavant au siège d'Europol), ainsi qu'au sein du Réseau CAMDEN regroupant les autorités compétentes en matière de recouvrement d'avoirs.

50. Chypre a indiqué que le Service national de la répression antidrogue coopérait et répondait à toutes les demandes en temps voulu. L'Estonie échangeait des informations par l'intermédiaire de ses agents de liaison à Europol et disposait d'un bureau SIRENE auprès duquel des informations pertinentes pouvaient être obtenues.

51. L'Allemagne a noté que, dans la majorité des cas, ses services de détection et de répression répondaient rapidement aux demandes d'informations et d'assistance. Israël a signalé que les accords conclus entre ses services et leurs homologues garantissaient la rapidité de l'échange d'informations et de l'assistance, notamment en matière de livraisons surveillées. Le Luxembourg continuait à recevoir de telles demandes, essentiellement de la part des pays voisins, et échangeait des

informations au moyen des canaux fournis par INTERPOL, Europol et le centre de coopération entre la police et les douanes. Malte a déclaré que ces demandes étaient traitées en priorité et qu'une assistance complète était fournie, conformément à la législation maltaise et aux conventions internationales.

52. En Espagne, des bureaux de liaison mis en place par d'autres États permettaient un échange direct d'informations entre services de police. La Suisse a indiqué qu'elle avait envoyé des agents de liaison supplémentaires dans des pays clefs, et qu'elle n'avait reçu aucune plainte concernant les délais de réponse aux demandes d'assistance internationale.

53. La Turquie a noté qu'en 2010 sa police avait répondu à plus de 1 400 demandes d'informations de la part d'homologues étrangers et qu'elle continuerait à répondre à ces demandes dans les meilleurs délais. La gendarmerie et les services des douanes turcs participaient également à des opérations conjointes et à des échanges d'informations avec leurs homologues.

### **Thème 3. Le trafic de drogues en Europe: tendances, stratégies et mesures efficaces**

#### *Recommandation a)*

54. Face à la menace que le trafic transatlantique de cocaïne auquel se livraient des groupes criminels bien organisés et disposant d'importantes ressources posait actuellement aux États d'Afrique de l'Ouest et d'Europe, la huitième Réunion a recommandé que les gouvernements encouragent leurs services à apporter leur contribution et leur soutien au Centre opérationnel d'analyse du renseignement maritime pour les stupéfiants (MAOC-N).

55. La Croatie a signalé que sa police entretenait des contacts et coopérait au niveau opérationnel avec le MAOC-N au Portugal et le Centre de coordination pour la lutte antidrogue en Méditerranée (CeCLAD-M) à Toulon, y compris dans le cadre d'actions opérationnelles conjointes faisant intervenir des services étrangers afin de lutter contre la contrebande internationale de cocaïne en Méditerranée.

56. Chypre, l'Estonie, le Luxembourg et la Suisse n'avaient pas pris de mesures pour appliquer cette recommandation. Chypre a noté qu'en raison de sa situation géographique elle n'entretenait aucune forme de coopération avec le MAOC-N.

57. L'Allemagne disposait du statut d'observateur auprès du MAOC-N, tandis que l'Espagne en était l'un des membres fondateurs.

58. Israël ne participait pas à l'initiative du MAOC-N mais espérait bien y prendre part à l'avenir. La Turquie était prête à soutenir le MAOC-N, qui s'intéressait de très près au trafic transatlantique de cocaïne. Malte a signalé que le MAOC-N n'avait jamais fait directement appel à ses services, mais qu'il avait participé, ainsi que le CeCLAD-M, à une livraison surveillée de cocaïne menée en collaboration avec d'autres États membres.

#### *Recommandation b)*

59. Compte tenu du recours accru à des aéronefs non commerciaux pour acheminer des drogues de l'Amérique latine vers l'Afrique de l'Ouest et de l'Afrique du Nord vers l'Europe, il a également été recommandé que les

gouvernements prennent des mesures immédiates pour renforcer la coopération entre les services de détection et de répression et le secteur de l'aviation dans son ensemble, ainsi que pour aider les services à recueillir les informations nécessaires et à mettre en œuvre les procédures indispensables pour réagir plus efficacement à la menace grandissante que représentait ce trafic.

60. La Croatie a noté que le cadre juridique nécessaire pour la coopération entre les services nationaux de poursuite et le secteur privé, en particulier l'aviation civile, était en place et que les services de détection et de répression coopéraient pleinement au quotidien. Faisant référence à un exemple de coopération fructueuse avec d'autres services de détection et de répression européens concernant une affaire de contrebande de cocaïne depuis les îles des Caraïbes jusqu'en Europe au moyen de petits avions privés, la Croatie a signalé que des activités étaient en cours, qui traduisaient sur le plan opérationnel sa réglementation interne concernant la coopération entre le Ministère de l'intérieur et l'administration des douanes, notamment en matière de lutte contre la contrebande internationale de drogues par voie aérienne.

61. Alors que l'Estonie n'avait pas pris de mesures pour appliquer cette recommandation, Chypre a déclaré qu'il existait une coopération étroite avec le secteur de l'aviation dans son ensemble. Malte a également indiqué que ses services de détection et de répression avaient d'excellents contacts avec les autorités de l'aviation dans le pays.

62. L'Allemagne a cité le projet de communication aéroportuaire AIRCOP, élaboré par l'UNODC et financé par l'Union européenne et le Canada, comme exemple d'initiative propre à améliorer la coopération entre les services de détection et de répression et le secteur de l'aviation dans son ensemble. Destiné à améliorer les capacités des services de détection et de répression et des services judiciaires en matière de coopération internationale, ce projet serait axé sur le renforcement des capacités antidrogue des pays bénéficiaires dans des aéroports sélectionnés, en Afrique de l'Ouest d'abord puis en Amérique latine et aux Caraïbes dans un deuxième temps. Il aurait pour but de créer des liens et de favoriser des synergies entre les différentes mesures mises en œuvre dans ces régions.

63. En Israël, des aéronefs non commerciaux en provenance d'Afrique faisaient l'objet de contrôles aléatoires effectués en collaboration avec les autorités de l'aviation civile, en particulier en cas de doutes sur leur itinéraire ou sur d'autres questions. Les vols en provenance d'Amérique du Sud faisaient l'objet de contrôles plus fréquents.

64. Le Luxembourg a fait état de la mise en œuvre d'un système mettant à la disposition des autorités policières et douanières, en temps réel, des informations de vol concernant les appareils d'aviation sportive et générale. Les services nationaux de détection et de répression coopéraient avec le secteur de l'aviation civile. Les mécanismes de coopération et les procédures d'échange d'informations internationaux ont également été mentionnés, notamment les travaux menés par le Groupe européen de coopération en matière de lutte contre l'abus et le trafic illicite des stupéfiants (Groupe Pompidou) concernant les aéroports, l'assistance mutuelle ou les annuaires des responsables des services de contrôle des stupéfiants dans les aéroports européens et des agents de contact nationaux dans le secteur de l'aviation générale.

65. L'Espagne a fait état de plusieurs mesures adoptées dans le domaine de l'aviation. Un accord conclu en 2003 entre l'armée de l'air et la police concernant le contrôle des appareils d'aviation légère et sportive a fixé des procédures opérationnelles d'échange de communications pour le contrôle des appareils détectés par l'armée de l'air qui entraient sur le territoire national sans autorisation ou dans les cas où une activité illicite, notamment de trafic de drogues, était suspectée. Un accord conclu en 2006 entre le Ministère de la défense et le Ministère de l'intérieur sur la lutte contre le trafic illicite de drogues prévoyait, entre autres mesures, une vigilance accrue de la part de l'armée de l'air et des forces de sécurité concernant tout vol suspect. Les conclusions de 2010 du Conseil de l'Union européenne sur le thème "Trafic de drogue – évaluation de la menace que représentent les aéroports et les avions légers" ont également été mentionnées.

66. La Suisse a signalé que, alors que les douanes et la police nationales menaient des opérations de contrôle visant de petits avions et pistes d'atterrissage, la contrebande par ce moyen ne semblait pas être une voie d'entrée majeure de la drogue dans le pays.

67. En tant que pays de destination du trafic de cocaïne, la Turquie attachait une grande importance au partage d'informations dans ce domaine, et elle a indiqué que l'administration nationale des douanes partageait des informations concernant les saisies de drogues dans les pays européens par l'intermédiaire du Groupe Pompidou, ainsi que des mécanismes du Réseau douanier de lutte contre la fraude de l'OMD et de l'Initiative de coopération pour l'Europe du Sud-Est.

### III. Conclusions

68. La plupart des gouvernements ayant répondu au questionnaire avaient pris des mesures pour appliquer les recommandations relatives à l'influence d'Internet et d'autres médias électroniques sur le trafic de drogues, ou considéré que leur législation nationale ou leur pratique étaient déjà suffisamment conformes à ces recommandations. Des avis divergents ont été exprimés quant à savoir si une convention des Nations Unies contre la cybercriminalité devait être élaborée.

69. Tous les gouvernements ayant répondu avaient pris des mesures pour appliquer les recommandations relatives à l'importance de l'information pour démanteler les groupes de trafiquants, à ceci près que la mise en place d'un cadre juridique pour faciliter les opérations d'agents infiltrés étrangers sur leur territoire lorsque ces opérations avaient fait l'objet d'un accord mutuel restait difficile pour les États Membres qui n'étaient pas liés par les dispositions juridiques sur le sujet en vigueur dans l'Union européenne.

70. Les réponses des gouvernements divergeaient concernant l'application des recommandations sur les tendances du trafic de drogues en Europe. Parmi les nombreux gouvernements qui ne coopéraient pas avec le MAOC-N, certains ont exprimé leur souhait de le soutenir, tandis que d'autres n'avaient pas pris de mesure à ce sujet. La plupart des gouvernements ont fait état de formes de coopération entre leurs services de détection et de répression respectifs dans le domaine de l'aviation ou ont décrit la coopération que ces services entretenaient avec le secteur de l'aviation générale.

71. Le présent rapport ne donne qu'un aperçu partiel de l'application des recommandations, puisque seuls 10 gouvernements sur les 56 membres de la Réunion ont renvoyé les questionnaires au Secrétariat. Étant donné qu'un volume minimum d'informations est nécessaire pour que la Réunion puisse utilement évaluer la suite donnée à ses recommandations, il est important que les gouvernements remplissent et renvoient les questionnaires en temps voulu.

---