ANNEXE III

DOCUMENTS DE FOND SUR DES DÉVELOPPEMENTS SUR LE DÉLIT CYBERNÉTIQUE DANS LE CADRE DU REMJAS ET DE L'OEA

INDEX THÉMATIQUE

1. CONCLUSIONS ET RECOMMANDATIONS DE LA DEUXIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE. (Lima, Pérou. 1er- 3 mars 1999)

2. QUESTIONNAIRE ÉLABORÉ LORS DE LA PREMIERE REUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE (Washington, DC. LES Etats-Unis. Mars 12, 1999)

3. RAPPORT FINAL DE LA DEUXIÈME RÉUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE (Washington, DC. LES Etats-Unis. 14 et 15 octobre 1999)

4. RECOMMANDATIONS DE LA DEUXIÈME RÉUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE. (Washington, DC. LES Etats-Unis. 14 et 15 octobre 1999)

5. CONCLUSIONS ET RECOMMANDATIONS DE LA TROISIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE. (San José, Costa Rica. 1er- 3 mars 2000)

6. CONCLUSIONS ET RECOMMANDATIONS DE LA QUATRIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE. (Port of Spain, Trinité-et-Tobago. 10- 13 mars 2002)

7. RÉSOLUTIONS RÉCENTES DE L'ASSEMBLÉE GÉNÉRALE LIÉES AU DÉLIT CYBERNÉTIQUE

   AG/RES 1849 (XXXII-0/02)
   AG/RES 1924 (XXXIII-0/03

CONCLUSIONS ET RECOMMANDATIONS DE LA DEUXIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE

(Lima, Pérou. 1er- 3 mars 1999)

CHAPITRE IV
CONCLUSIONS ET RECOMMANDATIONS

III. RENFORCEMENT ET DÉVELOPPEMENT DE LA COOPÉRATION INTERAMÉRICAINE

A. Renforcer et développer la coopération internationale dans les domaines les plus préoccupants tels que la lutte contre le terrorisme, la lutte contre la corruption, le blanchiment de l'argent, le trafic des stupéfiants, le trafic illicite d'armes, le crime organisé et la délinquance transnationale.

B. Délit Cybernétique

En raison de l'importance et de la difficulté des questions que soulèvent les délits cybernétiques, et vu l'étendue et l'envergure potentielle des problèmes qu'ils posent à nos pays, il est recommandé que soit créé un groupe gouvernemental d'experts dans le cadre de l'OEA, ayant pour mandat :

1. Établir le diagnostic des activités délictueuses liées aux ordinateurs et à l'information, ou qui sont accomplies au moyen d'ordinateurs utilisés pour commettre une infraction;
2. Établir un diagnostic des lois, politiques et pratiques nationales relatives à ces activités;
3. Identifier les organismes nationaux et internationaux dotés de la spécialisation pertinente,
4. Identifier des mécanismes de coopération au sein du Système interaméricain pour combattre le délit cybernétique.

Le groupe gouvernemental d'experts devrait présenter un rapport à la Troisième Réunion des ministres de la justice, ministres, *Attorneys General* et *Procuradores Generales* des Amériques.

QUESTIONNAIRE
ÉLABORÉ LORS DE LA PREMIERE REUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE

1. Quelles sont les entités de votre pays qui, chargées des enquêtes et des poursuites judiciaires, disposent d'une expertise en matière de délit cybernétique (activités criminelles ciblant les ordinateurs et les systèmes d'information, ou utilisant les ordinateurs pour commettre un délit)?

2. Votre pays a-t-il été victime d'un cas quelconque ou d'un nombre élevé de délits cybernétiques, tels que:

1. L'utilisation d'équipement informatique par des criminels en vue d'emmagasiner des informations concernant la perpétration d'un délit?

2. L'utilisation d'équipement informatique par des criminels en vue de communiquer avec d'autres criminels, des victimes, ou d'autres personnes?

3. Des activités criminelles qui font de l'usage des ordinateurs une composante substantielle de la perpétration du délit?

4. Des activités criminelles visant les ordinateurs et les systèmes d'information électronique, comme par exemple l'accès non autorisé aux réseaux informatisés?

3. Avez-vous jamais demandé ou reçu une assistance juridique internationale dans un cas de délit cybernétique? Quels ont été les mécanismes mis en œuvre pour fournir cette assistance et dans quels délais ont-ils été engagés?

4. La législation de votre pays définit-elle un réseau informatique? Le cas échéant, veuillez fournir la définition et la référence aux paragraphes /articles de votre code.

5. La législation de votre pays définit-elle les données informatisées? Cette définition inclut-elle des programmes ou codage similaire? Si vous disposez d'une définition, veuillez la fournir assortie de la référence aux paragraphes/articles de votre code.

6. La législation pénale de votre pays sanctionne-t-elle la destruction, la modification, l'altération, l'accès et l'usage non autorisés, ou autre interférence similaire, information ou donnée provenant de votre réseau informatique ou programme?

7. La législation pénale de votre pays sanctionne-t-elle l'effacement, l'altération, l'inaccessibilité, l'acquisition non autorisés, ou d'autre interférence similaire, information ou donnée provenant d'un réseau informatisé ou programme?

8. La législation pénale de votre pays sanctionne-t-elle l'interception non autorisée de la transmission par n'importe quel moyen ou dans n'importe quel mode, de données informatisées ou de programmes?

9. Faut-il un motif exprès en relation avec la perpétration des délits énoncés aux questions 6, 7 et 8?

10. Les délits énumérés aux questions 6, 7 et 8 sont-ils passibles d'une mise en accusation?

11. Les délits énumérés aux questions 6, 7 et 8 sont-ils passibles d'extradition?
12. Vote pays aurait-il juridiction sur le comportement d'un individu qui serait considéré comme un délit informatique selon les termes décrits dans les questions ci-dessus,

a. si l'acte est commis uniquement sur le territoire de votre pays,
b. si un ou plusieurs des composantes de l'acte se sont produits à l'intérieur du territoire national
c. si le délit a provoqué des dommages sur votre territoire?

13. La législation de certains pays peut autoriser seulement la saisie de matériel tangible par les autorités chargées de l'enquête. Celle de votre pays autorise-t-elle la saisie de données informatisées intangibles (i.e. par impression ou par copie de données sur papier ou sur disquette, qui sont ensuite saisies), ou bien le support physique sur lequel est sauvegardée l'information (par exemple une disquette ou l'ordinateur lui-même) doit–il être saisi?

14. La législation autorise-t-elle la perquisition en ligne des réseaux informatisés nationaux. Dans l'affirmative, pour quel type de délits?

15. Un transporteur de télécommunications ou un fournisseur de service Internet peut-il volontairement fournir des renseignements concernant l'utilisation d'un téléphone ou de services informatisés (i.e. facturation ou autres dossiers d'usage, ou données relatives à l'identité de l'abonné) aux autorités chargées de l'enquête?

16. La législation de votre pays permet-elle de forcer les transporteurs de télécommunications ou les fournisseurs du service Internet à fournir les informations dont fait état la question 15?

17. La législation de votre pays oblige-t-elle *a*. un suspect ou *b*. une tierce personne, à fournir l'accès (y compris le dévoilement du mot de passe) à un réseau informatisé ou à des données qui font l'objet d'une perquisition légale?

18. Étant donné que les réseaux informatisés peuvent contenir un large volume de données, la législation de votre pays autorise-t-elle les autorités chargées de l'enquête et qui mènent une perquisition d'un réseau informatisé à saisir:

a. des données qui sont pertinentes pour l'enquête, mais ne sont pas couvertes par la portée du mandat judiciaire ou autre pièce autorisant la perquisition,
b. des données qui sont pertinentes pour un délit différent de celui qui fait l'objet de l'enquête et est spécifié dans le mandat ou autre pièce autorisant la perquisition,
c. sans mandant judiciaire ou autre, des données lorsque qu'il existe un risque d'effacement ou de destruction des données?

19. En ce qui concerne la question 18, les autorités chargées de l'enquête peuvent-elles saisir de telles données sans obtenir un autre mandat judiciaire?

20. La législation de votre pays autorise-t-elle les autorités chargées de l'enquête à effectuer des perquisitions pour recueillir ou intercepter (ou autrement obtenir) *a*. un système de télécommunications ou *b*. un réseau informatisé, ou des données au sujet de la source ou de la destination d'une communication téléphonique ou par ordinateur à un moment simultané avec la création de cette communication dans le présent et dans le futur?

21. La législation de votre pays autorise-t-elle l'interception par les autorités chargées de l'enquête de communications téléphoniq ues ou par ordinateur pour que celles-ci puissent être saisies de leur contenu?

22. La législation octroie-t-elle aux transporteurs de télécommunications ou aux fournisseurs de service Internet l'autorité légale ou leur fait-elle obligation de procéder ou d'aider à l'interception ou à l'obtention de données mentionnées aux questions 20 et 21?

23. La législation permet-elle aux transporteurs de télécommunications ou aux fournisseurs de service Internet de surveiller le contenu des communications? Dans l'affirmative, ces communications peuvent-elles être volontairement transmises aux autorités chargées de l'enquête?

24. La législation oblige-t-elle les transporteurs de télécommunications ou les fournisseurs de service Internet à conserver les données concernant l'identité de l'abonné et des informations relatives aux communications transactionnelles (i.e. la date, l'heure, le numéro de téléphone ou l'adresse Internet qui avait été contacté)?

25. Les autorités chargées de l'enquête peuvent-elles obliger un transporteur de télécommunications ou un fournisseur de service Internet à conserver des données concernant l'identité de l'abonné et des informations relatives aux communications transactionnelles (i.e. la date, l'heure, le numéro de téléphone ou l'adresse Internet qui avait été contactée) lorsque ces données ont été précédemment recueillies par un transporteur ou un fournisseur?

26. Des données statistiques sont-elles tenues sur le nombre de cas de délits informatisés

a. rapportés par les victimes?
b. rapportés à la police?
c. portés devant les tribunaux?

27. Votre pays offre-t-il des programmes de formation aux délits informatisés:

a. à la police?
b. au parquet?
c. à la branche judiciaire?

28. Énumérez les mécanismes de coopération technique dans le domaine du délit cybernétique.

29. Quelles mesures sont en voie d'adoption en ce qui concerne la révision d'instruments interaméricains se rapportant à la coopération juridique et judiciaire?

RAPPORT FINAL DE LA DEUXIÈME RÉUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE

(Washington, DC. LES Etats-Unis. 14 et 15 octobre 1999)

NOTE EXPLICATIVE

Conformément aux recommandations émanées de la Deuxième Réunion des ministres de la justice des Amériques tenue à Lima (Pérou) en mars 1999, l'Assemblée générale a adopté la résolution AG/RES. 1615 (XXIX-O/99), par laquelle elle a décidé tenir des réunions d'experts gouvernementaux sur le délit cybernétique.

Pour donner suite à ce mandat, le Conseil a tenu, par l'intermédiaire de son Groupe spécial de la justice, deux réunions d'experts gouvernementaux sur le délit cybernétique les 12 mai et 14 et 15 octobre 1999.

La Deuxième Réunion d'experts gouvernementaux a adopté plusieurs recommandations en vue de leur examen par la Troisième Réunion des ministres de la justice des Amériques.

Le 20 octobre 1999 le Conseil permanent de l'OEA a pris note des informations fournies par la Présidente du Groupe spécial de la justice, l'Ambassadrice Beatriz M. Ramacciotti, Représentante permanente du Pérou, et a décidé de soumettre à la Troisième Réunion des ministres de la justice des Amériques les recommandations relatives au délit cybernétique, approuvées à la Deuxième Réunion d'experts gouvernementaux.

10 février 2000

RAPPORT FINAL
DE LA DEUXIÈME RÉUNION D'EXPERTS GOUVERNEMENTAUX
SUR LE DÉLIT CYBERNÉTIQUE

I. INTRODUCTION

En mars 1999, les Ministres de la justice des Amériques ont recommandé la création d'un Groupe d'experts intergouvernementaux sur le délit cybernétique ayant pour mandat (1) d'établir le diagnostic des activités délictueuses liées aux ordinateurs et à l'information dans les États membres; (2) d'établir un diagnostic des lois, politiques et pratiques nationales relatives à ces activités; (3) d'identifier les organismes nationaux et internationaux dotés de la spécialisation pertinente; (4) d'identifier les mécanismes de coopération du Système interaméricain pour combattre le délit cybernétique.

II. ANTÉCÉDENTS

À cette fin, la Première réunion d'experts gouvernementaux sur le délit cybernétique a été convoquée en mai 1999 dans le but de réaliser les buts fixés par les ministres de la justice. Pour faciliter l'exécution de ses mandats, la Première Réunion du Groupe d'experts a élaboré un questionnaire qui sollicite de tous les États membres des informations au sujet de leurs expériences en ce qui concerne différents types de délit cybernétique, les lois essentielles, les principes en matière de juridiction et d'extradition qui les régissent, les lois régissant la préservation et la collecte de preuves dans ces cas et, enfin, l'existence de programmes de formation spécialisée ou d'organismes chargés d'appliquer la loi et/ou d'experts dans la lutte contre le délit cybernétique.

Par la suite, le Groupe spécial de la justice a décidé de tenir la Deuxième Réunion d'experts gouvernementaux sur le délit cybernétique les 14 et 15 octobre 19991/. Cette réunion a été convoquée pour analyser les réponses des gouvernements des États membres au questionnaire élaboré en la matière, examiner les mécanismes de coopération qui existent dans le Système interaméricain sur le délit cybernétique et écouter les exposés faits par les experts : M. Rodolfo Ojales, Avocat du Ministère de la justice des États-Unis; M. Joe DiAngelo, de *CitiGroup*; M. John Ryan, de *America Online*; M. Don Cavendar, de *Computer Analysis and Response Team*; Mme Ketherine Fithen, de *Computer Emergency Response Team*, Université Carnegie-Mellon; M. Steve Branigan, de *Bell Labs* et M. Raùl Sanguineti, Chef d'Unité du Département des systèmes de gestion de l'information. La synthèse de ces exposés figure en annexe au présent rapport.

Sur la base des réponses présentées par les gouvernements des États membres au questionnaire établi par la Première Réunion d'experts gouvernementaux sur le délit cybernétique (GE/REMJA/doc.15/99)2/, la réunion a disposé d'un document rédigé par le Sous-secrétariat aux questions juridiques du Secrétariat général (GE/REMJA/doc.47/99) qui compile et compare les réponses au questionnaire. Ce document est annexé au présent rapport.

---

[1] Le document contenant la liste des participants à la Réunion d'experts est publié sous la cote GE/REMJA/doc. /99.

[2] À ce jour, des réponses ont été envoyées par le Mexique (GE/REMJA/doc.15/99 add. 1); les États-Unis (GE/REMJA/doc.15/99 add. 2); l'Équateur (GE/REMJA/doc.15/99 add. 3); le Brésil (GE/REMJA/doc.15/99 add. 4); El Salvador (GE/REMJA/doc.15/99 add. 5); le Costa Rica (GE/REMJA/doc.15/99 add. 6); le Pérou (GE/REMJA/doc.15/99 add. 7); l'Argentine (GE/REMJA/doc.15/99 add. 8); la Trinité et Tobago (GE/REMJA/doc.15/99 add. 9); le Panama (GE/REMJA/doc.15/99 add. 10) et le Venezuela GE/REMJA/doc.15/99 add. 11).

Il convient de souligner que le diagnostic demandé est fondé sur les réponses au questionnaire présentées par onze États membres jusqu'au 14 octobre 1999, ainsi que sur les délibérations de la Réunion d'experts qui ont eu lieu durant leurs séances de travail. Cependant, la réunion d'experts a estimé que les réponses reflétaient la situation générale des Amériques, même si elles étaient peu nombreuses. En outre, le présent rapport comporte des recommandations destinées à renforcer la capacité des États membres à affronter les principales préoccupations en matière de sécurité publique et les défis créés par les nouvelles technologies et à poursuivre la mise en place de mécanismes interaméricains pour étudier et combattre le délit cybernétique.

III. DIAGNOSTIC

Aux fins de ce diagnostic, la Réunion d'experts entend par "délit cybernétique" une activité délictueuse dont l'objet matériel ou l'instrument d'exécution fait appel à des systèmes de technologie de l'information (notamment les systèmes de télécommunications et d'informatique).

Sept (7) des États membres qui ont répondu au questionnaire n'ont pas dit avoir subi un préjudice grave par suite d'un délit cybernétique. Le délit cybernétique est encore perçu comme quelque chose de rare qui souvent n'est pas puni spécifiquement par la loi. Cependant, dans quelques États membres, on sanctionne des comportements dictés par l'utilisation de technologies de l'information, lorsque ceux-ci constituent en soi des délits, par exemple la fraude, le non-paiement d'impôts, la diffamation ou la distribution du matériel pornographique prenant pour acteurs des enfants.

Vu ce qui précède, il est manifestement nécessaire de mettre en place, d'adapter et d'harmoniser les lois, procédures et institutions nécessaires pour combattre dans les États membres l'abus croissant et l'utilisation frauduleuse des ordinateurs.

S'agissant de la législation concernant la collecte de preuves, il est indispensable de disposer du droit de dépister, de faire la collecte, d'assurer la préservation et la divulgation des informations sur le trafic des communications électroniques et des données informatiques pour mener des enquêtes sur les délits commis au moyen des ordinateurs. Vu la nouveauté du délit cybernétique et la difficulté de le détecter, il est probable que quelques États membres n'ont pas encore fait face aux problèmes particuliers liés à la collecte de preuves sur ce type de délit. A ce sujet, neuf (9) États ont fait savoir que leurs lois permettent de saisir des biens tangibles conformément aux procédures, et d'obliger les fournisseurs d'accès à l'Internet et aux sociétés de télécommunications à présenter des informations relatives aux abonnés et à la facturation. Toutefois, il semble que dans certains cas il ne serait pas permis aux enquêteurs de prendre d'autres mesures pertinentes pour mener une enquête sur le délit cybernétique, par exemple l'obtention d'information sur la source et la destination des communications en même temps que la transmission de ces communications, ce qui peut être nécessaire pour suivre la trace d'une *intrusion* informatique.

Il se peut que la plus grosse difficulté à laquelle sont confrontés les États membres soit de ne pas avoir des organismes disposant de l'expertise nécessaire pour mener les investigations, et poursuivre en justice les auteurs des délits cybernétiques. De même, ils ne disposent pas de la formation nécessaire. Cependant, les délits cybernétiques font souvent l'objet d'enquêtes par d'autres unités (par exemple celles s'occupant du crime organisé, du trafic des stupéfiants) qui ne sont pas spécialisées dans le délit cybernétique. À cause du manque d'organismes adéquats, ce qui pourrait porter atteinte à l'investigation nationale et internationale en matière de délit cybernétique, une des priorités dans ce domaine devrait être la mise en place de mécanismes de formation appropriés.

Très peu d'États membres (les États-Unis parmi ceux qui ont répondu à l'enquête) ont affronté des problèmes liés au caractère transnational du délit cybernétique, ou ont introduit ou reçu des demandes d'aide internationale en la matière. Mais, en dépit de l'absence de demandes reçues à ce jour, il n'est pas inhabituel de dépister un délit cybernétique à travers des réseaux d'ordinateurs situés dans une multitude de pays n'ayant pas de rapport avec l'auteur du délit ou la victime. Ainsi, la capacité de demander et de fournir une aide internationale revêt une importance critique et doit faire l'objet d'un examen plus approfondi par les États.

Il ne s'avère pas évident cependant, selon les résultats du sondage, que les questions liées à la juridiction, à l'extradition et à la coopération internationale soient adéquatement régies par des lois spécifiques ou générales des États membres ainsi que par les accords multilatéraux ou bilatéraux existants.

Finalement, en dépit de l'absence apparente de préjudice causé à la région par les délits cybernétiques, les exposés faits devant le Groupe par des représentants d'autres institutions internationales, de gouvernements, d'entités du secteur privé et d'organisations consacrées à la sécurité informatique, indiquent que le problème des délits cybernétiques prendra certainement plus d'ampleur. Par conséquent, il est important de veiller à ce que les Etats membres soient prêts à mener des enquêtes et à entamer des poursuites contre les délits lorsqu'ils sont perpétrés sur leur territoire.

IV. IDENTIFICATION DES ENTITÉS NATIONALES ET INTERNATIONALES DOTÉES DE L'EXPERTISE PERTINENTE

Les réponses à la première question dans le document ci-joint (GT/REMJA/doc.47/99) identifient les entités nationales dotées de l'expertise pertinente. De surcroît, le Groupe d'experts a relevé les institutions internationales suivantes dotées d'expertise en matière de délits cybernétiques: le Conseil de l'Europe, le Groupe des Huit, l'Union européenne, l'Organisation pour la coopération économique et le développement, les Nations Unies (y compris l'UNAFEI) et l'Interpol. Finalement, plusieurs entités universitaires et du secteur privé détiennent une expertise d'importance critique, notamment les sociétés de télécommunications et les "équipes d'intervention" connexes comme l'Equipe d'intervention d'urgence en informatique de l'Université *Carnegie-Mellon* des Etats-Unis.

V. IDENTIFICATION DE MÉCANISMES DE COOPÉRATION AU SEIN DU SYSTÈME INTERAMÉRICAIN

Un certain nombre d'accords existants peuvent être utilisés pour faciliter la coopération dans la lutte contre le délit cybernétique, notamment les traités bilatéraux et multilatéraux d'entraide judiciaire en vigueur, l'Interpol, les commissions rogatoires et les mécanismes informels de coopération. En outre, quelques pays des Amériques ont adhéré, ou sont sur le point d'adhérer, au Groupe de liaison en service 24 heures par jour et 7 jours par semaine.

VI. RECOMMANDATIONS

Dans le cadre des dispositions de la résolution AG/RES.1615/99 (XXIX-O/99) et reconnaissant la menace globale que posent les délits cybernétiques et le besoin d'une intervention rapide et adéquate par des fonctionnaires nationaux bien entraînés, la Réunion d'experts formule les recommandations suivantes qui seront soumises, par l'intermédiaire du Conseil permanent, à la Troisième Réunion des Ministres de la justice des Amériques:

1. Prier instamment les États membres de créer une ou plusieurs entités publiques dotées de l'autorité et d'une fonction spécifiques pour mener les enquêtes sur les délits cybernétiques et les poursuites judiciaires qui s'imposent.

2. Que les États qui ne disposent pas encore de lois sur les délits cybernétiques prennent les mesures requises dans ce sens.

3. Demander au États membres de déployer tous les efforts nécessaires pour harmoniser leurs lois en matière de délit cybernétique, afin de faciliter la coopération internationale pour la prévention de ces activités illégales et la lutte contre elles.

4. Que les États membres déterminent leurs besoins de formation en matière de délit cybernétique en facilitant les mécanismes de coopération bilatérale, régionale et multilatérale dans ce domaine.

5. Encourager la formulation de directives générales pour orienter les efforts législatifs en matière de délit cybernétique.

6. Envisager des mesures, notamment la création d'un Fonds spécifique volontaire, pour appuyer le développement de la coopération dans le Continent en la matière.

7. Encourager entre les États membres l'échange d'informations en matière de délit cybernétique.

8. Appuyer la diffusion d'informations sur les activités menées à ce sujet dans le cadre de l'OEA y compris le site sur le Web consacré à cette question.

9. Que les États membres envisagent la possibilité d'adhérer à des mécanismes de coopération ou d'échange d'informations déjà existants, par exemple le 'Groupe de contact de 24 heures par jour/7 jours par semaine' afin de communiquer ou de recevoir des informations.

10. Que les États membres prennent des mesures pour sensibiliser le public, notamment les usagers du système éducatif, du système judiciaire et d'administration de la justice, sur la nécessité de prévenir et de combattre le délit cybernétique.

VII. CONCLUSIONS

En conclusion, la Réunion d'experts gouvernementaux sur le délit cybernétique tenue dans le cadre du Groupe spécial de la justice du Conseil permanent, se permet de transmettre à cet organe le présent rapport qui résume les activités réalisées durant la réunion d'experts et énonce des recommandations pour qu'elles soient soumises à la considération de la Troisième réunion des Ministres de la justice des Amériques.

RECOMMANDATIONS DE LA DEUXIÈME RÉUNION D'EXPERTS GOUVERNEMENTAUX SUR LE DÉLIT CYBERNÉTIQUE

(Washington, DC. LES Etats-Unis. 14 et 15 octobre 1999)

VI. RECOMMANDATIONS

Dans le cadre des dispositions de la résolution AG/RES.1615/99 (XXIX-O/99) et reconnaissant la menace globale que posent les délits cybernétiques et le besoin d'une intervention rapide et adéquate par des fonctionnaires nationaux bien entraînés, la Réunion d'experts formule les recommandations suivantes qui seront soumises, par l'intermédiaire du Conseil permanent, à la Troisième Réunion des Ministres de la justice des Amériques:

1. Prier instamment les États membres de créer une ou plusieurs entités publiques dotées de l'autorité et d'une fonction spécifiques pour mener les enquêtes sur les délits cybernétiques et les poursuites judiciaires qui s'imposent.

2. Que les États qui ne disposent pas encore de lois sur les délits cybernétiques prennent les mesures requises dans ce sens.

3. Demander au États membres de déployer tous les efforts nécessaires pour harmoniser leurs lois en matière de délit cybernétique, afin de faciliter la coopération internationale pour la prévention de ces activités illégales et la lutte contre elles.

4. Que les États membres déterminent leurs besoins de formation en matière de délit cybernétique en facilitant les mécanismes de coopération bilatérale, régionale et multilatérale dans ce domaine.

5. Encourager la formulation de directives générales pour orienter les efforts législatifs en matière de délit cybernétique.

6. Envisager des mesures, notamment la création d'un Fonds spécifique volontaire, pour appuyer le développement de la coopération dans le Continent en la matière.

7. Encourager entre les États membres l'échange d'informations en matière de délit cybernétique.

8. Appuyer la diffusion d'informations sur les activités menées à ce sujet dans le cadre de l'OEA y compris le site sur le Web consacré à cette question.

9. Que les États membres envisagent la possibilité d'adhérer à des mécanismes de coopération ou d'échange d'informations déjà existants, par exemple le 'Groupe de contact de 24 heures par jour/7 jours par semaine' afin de communiquer ou de recevoir des informations.

10. Que les États membres prennent des mesures pour sensibiliser le public, notamment les usagers du système éducatif, du système judiciaire et d'administration de la justice, sur la nécessité de prévenir et de combattre le délit cybernétique.

RECOMMANDATIONS DE LA TROISIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE

(San José, Costa Rica. 1er- 3 mars 2000)

CHAPITRE IV
CONCLUSIONS ET RECOMMANDATIONS

À l'issue des débats engagés sur les différents points de son ordre du jour, la Troisième réunion des ministres de la justice des Amériques convoquée dans le cadre de l'OEA, en vertu de la résolution AG/RES. 1615 (XXIX-O/99), a adopté les conclusions et recommandations suivantes pour qu'elles soient soumises, par l'intermédiaire du Conseil permanent de l'OEA, à l'Assemblée générale lors de sa trentième Session ordinaire.

1. Délit cybernétique

La Troisième Réunion de la REMJA, se fondant sur les recommandations du Groupe d'experts gouvernementaux sur le délit cybernétique réuni au siège de l'OEA en mai et octobre 1999, exhorte les Etats membres de l'OEA:

1.1. à créer une ou plusieurs entités publiques dotées de l'autorité et d'une fonction spécifique pour mener des enquêtes sur les délits cybernétiques et entamer les poursuites y afférentes;

1.2. à adopter les mesures qui s'imposent pour mettre en œuvre une législation traitant du délit cybernétique, s'ils n'en disposent pas encore;

1.3. à déployer tous les efforts nécessaires pour harmoniser leurs lois en matière de délit cybernétique, afin de faciliter la coopération internationale pour la prévention de ces activités illégales et la lutte contre elles;

1.4. à identifier leurs besoins de formation en matière de délit cybernétique en facilitant les mécanismes de coopération bilatérale, régionale et multilatérale dans ce domaine;

1.5. à envisager la possibilité d'adhérer à des mécanismes de coopération ou d'échange d'informations déjà existants, par exemple le «Groupe de contact de 24 heures par jour/7 jours par semaine» afin de communiquer ou de recevoir des informations;

1.6. à prendre des mesures pour sensibiliser le public, notamment les usagers du système éducatif, du système judiciaire et d'administration de la justice, sur la nécessité de prévenir et de combattre le délit cybernétique;

1.7. à envisager diverses mesures, notamment la création d'un Fonds spécifique volontaire, pour épauler le développement de la coopération dans le Continent en la matière;

1.8. à encourager dans le cadre de l'OEA l'échange d'informations en matière de délit cybernétique et la diffusion d'informations sur les activités menées à ce sujet, y compris le site sur le Web consacré à cette question;

1.9. à assurer le suivi des recommandations du Groupe d'experts gouvernementaux dans le cadre de l'OEA, en tenant compte de la nécessité d'élaborer des grandes lignes destinées à orienter les efforts déployés à l'échelle nationale en matière de délit cybernétique, grâce par exemple à l'élaboration d'une législation type ou d'autres instruments juridiques pertinents et à la conception de programmes de formation.

CONCLUSIONS ET RECOMMANDATIONS DE LA QUATRIÈME RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES SUR LE DÉLIT CYBERNÉTIQUE

(Port of Spain, Trinité-et-Tobago. 10- 13 mars 2002)

CHAPITRE IV
CONCLUSIONS ET RECOMMANDATIONS

Au terme des discussions sur les divers points de l'ordre du jour, la Quatrième Réunion des ministres de la justice des Amériques, convoquée dans le cadre de l'OEA par la résolution AG/RES. 1781 (XXXI-O/01), a adopté les recommandations suivantes pour acheminement, à travers le Conseil permanent de l'OEA, à la XXXII^{ème} Session ordinaire de l'Assemblée générale.

[…]

IV. DÉLIT CYBERNÉTIQUE

La REMJA-IV recommande:

1. Que les États membres répondent au questionnaire élaboré par le Secrétariat général de l'OEA en vue de faciliter l'évaluation des progrès réalisés et la mise en œuvre, dans les plus brefs délais, des recommandations formulées par la REMJA-III dans le cadre de la lutte contre le délit cybernétique.

2. Que, dans le cadre des travaux du Groupe de travail de l'OEA chargé de donner suite aux recommandations de la REMJA-IV, il soit convoqué un nouveau groupe d'experts gouvernementaux en matière de délit cybernétique. Ce groupe aurait pour mandat:

   a. d'assurer le suivi de la mise en œuvre des recommandations formulées par ce Groupe et adoptées par la REMJA-III;

   b. d'envisager l'élaboration des instruments juridiques interaméricains pertinents ainsi que de la législation-type visant à renforcer la coopération continentale pour la lutte contre le délit cybernétique, en envisageant des normes relatives à la confidentialité, à la protection de l'information, aux aspects de procédure et à la prévention du délit.

RÉSOLUTIONS RÉCENTES DE L'ASSEMBLÉE GÉNÉRALE LIÉES AU DÉLIT CYBERNÉTIQUE

RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES

(Bridgetown, Barbade. Juin De 2002)
AG/RES 1849 (XXXII-O/02)

(Résolution adoptée à la quatrième séance plénière tenue le 4 juin 2002)

L'ASSEMBLÉE GÉNÉRALE,

VU le rapport final de la Quatrième réunion des Ministres de la justice des Amériques (REMJA-IV/doc.24/02 rev. 2), tenue à Trinité-et-Tobago du 10 au 13 mars 2002;

RAPPELANT:

Que, dans le Plan d'action du Troisième Sommet des Amériques, les chefs d'État et de gouvernement ont décidé ce qui suit:

"Continuer à appuyer les travaux réalisés dans le cadre des réunions des ministres de la Justice et des procureurs généraux des Amériques… et la mise en œuvre de leurs conclusions et recommandations";

"Mettre en œuvre des stratégies collectives, dont celles se dégageant des réunions des Ministres de la justice des Amériques, afin de renforcer la capacité institutionnelle des États d'échanger des informations et des éléments de preuve" et de renforcer la coopération "en vue de lutter conjointement contre les formes naissantes d'activités criminelles transnationales";

"Élaborer, par le biais de réunions des ministres de la Justice… un échange de pratiques exemplaires et de recommandations" visant à "améliorer les conditions dans les prisons de tout le Continent";

"Créer, au sein de l'OEA, un réseau d'information sur Internet réunissant les autorités juridiques compétentes en matière d'extradition et d'assistance juridique mutuelle";

CONSIDÉRANT:

Que la REMJA-IV, convoquée dans le cadre de l'OEA, a adopté notamment les recommandations suivantes:

Mettre en route "un processus visant à aboutir à l'adoption d'un Plan d'action continental en matière de coopération juridique et judiciaire mutuelle, en vue de lutter conjointement contre les diverses manifestations de la criminalité transnationale organisée et le terrorisme, en vertu de l'engagement pris par les chefs d'État et de gouvernement lors du Troisième Sommet des Amériques";

Que "dans le cadre des travaux du Groupe spécial du Conseil permanent de l'OEA chargé de donner suite aux recommandations des REMJA, il soit convoqué le plus tôt possible, un groupe d'experts gouvernementaux" qui aura pour mandat d'élaborer la proposition de ce Plan d'action continental, qui sera soumise à la REMJA-V "pour examen et approbation";

Que “le Groupe de travail composé de l’Argentine, des Bahamas, du Canada et d’El Salvador, avec l’appui du Secrétariat général de l’OEA, poursuive ses activités” afin que le Réseau d’échange d’information pour l’entraide judiciaire en matière pénale soit étendu à tous les États des Amériques et avance progressivement sur la voie du perfectionnement;

Que “dans le cadre de l’OEA, il soit convoqué une réunion d’autorités centrales chargées des politiques pénitentiaires et carcérales des États membres de l’OEA, dans le but, entre autres, de promouvoir l’échange d’information et de données d’expériences entre elles…, notamment la proposition relative à la mise en place d’un réseau permanent d’échange d’information dans ce domaine”;

Que “dans le cadre des travaux du Groupe de travail de l’OEA chargé de donner suite aux recommandations de la REMJA, il soit convoqué un nouveau groupe d’experts gouvernementaux en matière de délit cybernétique. Ce groupe aurait pour mandat: a) d’assurer le suivi de la mise en œuvre des recommandations formulées par ce Groupe et adoptées par la REMJA-III, et b) d’envisager l’élaboration des instruments juridiques interaméricains pertinents ainsi que de la législation-type”,

DÉCIDE:

1. D’exprimer sa reconnaissance au gouvernement de la République de Trinité-et-Tobago pour avoir accueilli la Quatrième Réunion des Ministres de la justice des Amériques et pour l’organisation efficace de cette réunion qui a contribué au succès de ses travaux.
2. De demander au Conseil permanent:

    a. D’assurer le suivi des recommandations adoptées par la REMJA-IV;

    b. De convoquer, dès que possible, un groupe d’experts gouvernementaux dans le domaine de l’entraide juridique et judiciaire en matière pénale, notamment les autorités centrales dont font état les traités interaméricains de coopération juridique et judiciaire dans ce domaine, lequel groupe aura pour mandat d’élaborer la proposition de Plan d’action continental à laquelle se réfèrent les recommandations de la REMJA-IV, en vue de la présenter à la REMJA-V pour examen.

    c. De convoquer à nouveau le Groupe d’experts gouvernementaux en matière de délit cybernétique afin de donner suite aux mandats auxquels se réfèrent les recommandations de la REMJA-IV.

    d. De convoquer une réunion d’autorités centrales chargées des politiques pénitentiaires et carcérales des États membres de l’OEA, conformément à la recommandation de la REMJA-IV.

3. D’appuyer la tenue d’une réunion technique des autorités centrales et d’autres experts en matière d’entraide judiciaire en matière pénale et d’accepter l’offre du Gouvernement canadien d’accueillir cette réunion.
4. De demander au Secrétariat général de fournir tout le soutien technique nécessaire à la mise en œuvre des recommandations de la REMJA-IV ainsi que des dispositions de la présente résolution.
5. De demander au Conseil permanent d’effectuer le suivi de cette résolution, qui sera exécutée en fonction des ressources allouées dans le Programme-budget ainsi que d’autres ressources, et lui demander de soumettre rapport sur sa mise en œuvre à l’Assemblée générale lors de sa trente-troisième Session ordinaire.

RÉUNION DES MINISTRES DE LA JUSTICE DES AMÉRIQUES

Santiago, Chili. Juin 2003
AG/RES 1924 (XXXIII-O/03)

(Résolution adoptée à la quatrième séance plénière, tenue le 10 juin 2003)

L'ASSEMBLÉE GÉNÉRALE,

VU le Rapport annuel que lui a adressé le Conseil permanent (AG/doc.4156/03 add. 3), notamment la section qui traite de la mise en œuvre de la résolution AG/RES. 1844 (XXXII-O/02) "Réunion des Ministres de la justice des Amériques",

RAPPELANT que dans le Plan d'action du Troisième Sommet des Amériques, les chefs d'État et de gouvernement ont décidé de continuer d'appuyer les travaux réalisés dans le cadre des Réunions des ministres de la justice des Amériques (REMJA) et de mettre en œuvre leurs conclusions et recommandations;

RAPPELANT ÉGALEMENT que la REMJA-IV, organisée dans le cadre de l'OEA, a recommandé que soit convoquée une réunion des autorités centrales et d'autres experts en entraide judiciaire en matière pénale afin de mettre en route un processus qui déboucherait sur l'adoption d'un Plan d'action continental, et de développer un réseau d'échange des informations dans ce domaine; que soit convoquée une réunion d'autorités chargées des politiques pénitentiaires et carcérales des États membres de l'OEA, dans le but, entre autres, de promouvoir l'échange des informations et des données d'expériences entre elles; que soit convoqué de nouveau le Groupe d'experts gouvernementaux en matière de délit cybernétique pour qu'il assure le suivi de la mise en œuvre des recommandations formulées par ce Groupe et adoptées par la REMJA-III;

CONSIDÉRANT la nécessité et l'importance de la convocation de la Cinquième Réunion des ministres de la justice des Amériques (REMJA-V), dans le but, notamment, d'examiner les résultats des réunions techniques tenues conformément aux recommandations de la REMJA-IV et de continuer le processus de renforcement de la coopération entre les autorités dans leurs sphères de compétences respectives,

DÉCIDE:

1. De demander au Conseil permanent d'assurer un suivi, le cas échéant, des recommandations émanées de la réunion des autorités centrales et d'autres experts en entraide judiciaire en matière pénale tenue à Ottawa (Canada) du 30 avril au 2 mai 2003, ainsi que les recommandations des premières réunions du Groupe d'experts gouvernementaux en matière de délit cybernétique, et des autorités pénitentiaires et carcérales qui auront lieu les 23 et 24 juin, et les 16 et 17 octobre 2003 respectivement, conformément aux dispositions de la résolution du Conseil permanent CP/RES. 839 (1359/03).

2. De convoquer la Cinquième Réunion des ministres de la justice des Amériques qui aura lieu pendant le premier semestre de 2004 en fonction des ressources allouées à ce titre dans le Programme-budget de l'Organisation ainsi que d'autres ressources, et de charger le Conseil permanent d'effectuer les travaux préparatoires et de fixer la date de cette réunion, avec l'appui technique du Secrétariat général.

3. De demander au Conseil permanent de présenter un rapport sur la mise en œuvre de la présente résolution à l'Assemblée générale lors de sa trente-quatrième Session ordinaire.