COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-CY (2008) 04

Strasbourg, le 08 avril 2008

COMITE DE LA CONVENTION SUR LA CYBERCRIMINALITE (T-CY)

3e concertation multilatérale des Etats parties à la Convention sur la cybercriminalité [STE n°185]

Strasbourg, 3 - 4 avril 2008

RAPPORT DE REUNION[1]

AVANT-PROPOS

Le T-CY se félicite du soutien international croissant apporté à la Convention sur la cybercriminalité et invite les Etats qui ne l'ont pas encore fait à devenir parties dès que possible.

Il relève les réalisations importantes du Projet sur la cybercriminalité et prend note en particulier des lignes directrices non contraignantes sur la coopération entre les organes de répression et les fournisseurs de services internet dans les enquêtes sur la cybercriminalité, adoptées par la Conférence Octopus Interface « Coopération contre la cybercriminalité ».

Le T-CY fait plusieurs propositions pour faciliter la mise en œuvre de la Convention et invite en particulier les Etats qui ne l'ont pas encore fait à fournir des informations sur leurs points de contact pour le réseau 24/7, à transmettre leurs profils ainsi que des traductions de la Convention.

Le T-CY prend également note de plusieurs instruments internationaux présentant un intérêt dans le domaine de la cybercriminalité, des travaux de certains comités et du Forum sur la gouvernance de l'internet (IGF).

[1] Pour plus d'informations sur le T-CY et le Projet sur la cybercriminalité, voir : www.coe.int/cybercrime

TABLE DES MATIERES

RAPPORT

I. INTRODUCTION

1. Le Comité de la Convention sur la cybercriminalité (T-CY) s'est réuni dans le bâtiment G du Conseil de l'Europe les 3 et 4 avril 2008 ; cette réunion s'est tenue en application de l'article 46 de la Convention sur la cybercriminalité [STE n°185] (ci-après « la Convention »), qui prévoit que « les Parties se concertent périodiquement, au besoin, […] ».

2. Mme Margaret KILLERBY (Secrétaire p. i. du T-CY) ouvre la réunion et souhaite la bienvenue aux participants à la 3e concertation des parties.

3. La liste des participants et l'ordre du jour, qui mentionne les documents de référence pour chaque point, figurent respectivement **aux annexes I et II**.

4. Le T-CY remercie chaleureusement le président sortant, M. Henrik KASPERSEN (Pays-Bas), pour sa contribution majeure aux activités du Conseil de l'Europe dans le domaine de la cybercriminalité et, en particulier, pour sa présidence du T-CY et du Comité d'experts ayant préparé la Convention.

5. Les Etats parties à la Convention élisent Mme Betty SHAVE (Etats-Unis) en tant que présidente et Mme Cristina SCHULMAN (Roumanie) en tant que vice-présidente.

6. Le T-CY souhaite la bienvenue à Mme Brigitte MABANDLA, ministre de la Justice et du développement constitutionnel de la République d'Afrique du Sud, qui informe le T-CY de la situation actuelle de la législation relative à la cybercriminalité en Afrique du Sud.

II. ECHANGE DE VUES SUR LA SITUATION ACTUELLE CONCERNANT LA CONVENTION SUR LA CYBERCRIMINALITE [STE N°185] ET SON PROTOCOLE ADDITIONNEL [STE N°189]

a. Etats des signatures, ratifications et adhésions

i. Questions générales

7. Le T-CY prend note de l'état actuel des signatures et ratifications de la Convention sur la cybercriminalité **(voir annexe III)**. Il souligne le fait que de nombreux Etats non européens s'intéressent vivement à la Convention et qu'au niveau mondial, la quasi-totalité des nouveaux lois et projets de loi sont calqués sur ses dispositions.

8. Le T-CY, en particulier :

- se félicite du soutien international croissant à la Convention sur la cybercriminalité ;

- note que les Etats qui ne sont pas encore parties à la Convention en examinent attentivement les dispositions et que la plupart d'entre eux envisagent de devenir parties dès que possible, notamment pour pouvoir faire pleinement usage des dispositions procédurales de la Convention en matière de coopération internationale. Il est probable que l'Autriche, l'Allemagne, l'Irlande, l'Italie, l'Espagne et le Royaume-Uni deviennent parties à la Convention en 2008 ;

- note que depuis sa précédente réunion, la Slovaquie est devenue partie à la Convention, que la Géorgie l'a signée le 1er avril et que l'Azerbaïdjan envisage de la signer au premier semestre 2008 ;

- prend note des mesures législatives et autres prises par les Etats en vue de devenir parties à la Convention, constate que les délais de ratification s'expliquent principalement par la longueur quelquefois excessive des processus législatifs, et encourage les Etats à accélérer le processus de ratification ;

- note que le Costa Rica et le Mexique ont été invités à adhérer à la Convention, que les Philippines seront invitées à y adhérer et que la République dominicaine a demandé à être invitée à y adhérer ;

9. Le T-CY prend note de l'état actuel des signatures et ratifications du Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques [STE n°189] (ci-après « le protocole ») (**voir annexe IV**) et se félicite de la signature de ce protocole par le ministre sud-africain de la Justice et du développement constitutionnel ;

10. Le T-CY accueille avec satisfaction les informations relatives aux contacts et à la coopération avec les pays non Européens suivants dans le domaine de la cybercriminalité : Argentine, Australie, Bahreïn, Botswana, Brésil, Colombie, Chili, Chine, Costa Rica, République dominicaine, Egypte, Inde, Indonésie, Laos, Malaisie, Maroc, Nigéria, Pérou, Philippines, Singapour, Sri Lanka, Trinité et Tobago, Vietnam, ainsi qu'avec des organisations régionales telles que l'Organisation des Etats américains (OEA).

11. Le T-CY encourage les Etats et les organisations internationales ou autres instances à promouvoir la Convention, notamment dans les Etats avec lesquels ils entretiennent des relations historiques ou privilégiées, ou encore avec les Etats de leur région.

ii. Points de contact

12. Le T-CY rappelle aux Etats de fournir, avant ou au moment de devenir parties à la Convention, toutes les informations requises par les dispositions de la Convention et en particulier celles concernant leur point de contact pour le réseau 24/7 créé en vertu de l'article 35.

13. Le T-CY invite l'Arménie, la Bosnie-Herzégovine et l'Ukraine, qui sont parties à la Convention, à établir d'urgence de tels points de contact. Il invite également les Etats à informer le Conseil de l'Europe de tout changement concernant les points de contact.

14. Le T-CY décide de fusionner le Répertoire des points de contact du Sous-groupe du G8 sur la criminalité de haute technologie (sous groupe « Lyon-Rome ») et la liste de contacts établie en vertu de la Convention.

15. Le T-CY souligne également qu'il importe d'améliorer l'efficacité du fonctionnement des points de contact et d'examiner les besoins en termes d'autorités judiciaires et de procureurs spécialisés. Il demande au Conseil consultatif de procureurs européens (CCPE) et à EUROJUST d'étudier cette question de manière plus approfondie.

16. Le T-CY demande au Projet sur la cybercriminalité de préparer, en coopération avec le Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC) et le réseau du G8 :

- un rapport traitant en particulier de la nature, du rôle, des pouvoirs, du fondement juridique et des adresses de messagerie institutionnelles des points de contact, et de le lui remettre à la prochaine réunion du T-CY.

iii. Traductions de la Convention

17. Outre les langues d'origine (anglais et français), le site Web consacré à la cybercriminalité contient actuellement des traductions de la Convention en 12 langues (arabe, néerlandais, allemand, hongrois, italien, indonésien, portugais, roumain, russe, slovaque, espagnol et turc – voir le site Web).

18. The T-CY invite les participants à envoyer au Secrétariat des traductions de la Convention dans d'autres langues afin qu'elles puissent être intégrées sur le site Web et aider les personnes et les Etats qui en ont besoin.

b. Mise en œuvre de la Convention dans la législation nationale – Examen de l'article 1.d concernant la définition des données relatives au trafic et de l'article 3 concernant l'accès illégal aux systèmes informatiques

i. Données relatives au trafic

19. Le T-CY convient qu'il faut faire une distinction entre les données relatives au trafic telles que définies à l'article 1.d de la Convention et les données relatives au contenu.

ii. Accès illégal

20. Le représentant de la Commission européenne informe le T-CY que la Commission européenne publiera en mai ou en juin de cette année un rapport détaillé sur la mise en œuvre de la Décision-cadre 2005/222/JHA du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information. Ce rapport comportera des informations sur la façon dont les Etats membres de l'UE ont mis en pratique les dispositions relatives à l'accès illégal.

c. Examen des réponses des parties au questionnaire sur la mise en œuvre de la Convention

21. Le T-CY prend note des réponses à ce questionnaire transmises par les pays suivants : Bulgarie, Allemagne, Hongrie, Roumanie, Russie, Slovaquie, Etats-Unis. Le comité demande aux parties qui ne l'ont pas encore fait ou à celles qui souhaitent les mettre à jour, d'envoyer leurs réponses dès que possible au Secrétariat.

22. Le T-CY décide d'examiner ces réponses à sa prochaine réunion.

d. Examen de problèmes spécifiques découlant de la coopération internationale entre les parties / entre les parties et d'autres Etats

23. L'un des problèmes particuliers mis en évidence par le T-CY concerne la rigueur de l'établissement de demandes officielles d'entraide judiciaire pour faire suite aux demandes de conservation rapide et autres mesures préliminaires. Il a été proposé, entre autres, que les points de contact 24/7 et les autorités compétentes chargées de l'entraide judiciaire renforcent leur coopération mutuelle.

e. Entraide judiciaire dans les affaires informatiques

24. Le T-CY remercie le PC-OC pour les informations qu'il apporte en matière d'entraide judiciaire dans les affaires informatiques concernant les Etats suivants : Arménie, Bosnie-Herzégovine, Bulgarie, Canada, Grèce, Hongrie, Lettonie, Luxembourg, Malte, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suisse et Suède. Le T-CY est informé que le PC-OC obtiendra d'autres réponses encore, que le T-CY décide d'examiner à sa prochaine réunion.

25. Le T-CY fait observer que le 2e Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale [STE n°182] est très important pour la coopération dans le domaine de la cybercriminalité, car il permet l'établissement de contacts directs entre les pouvoirs publics des Parties.

26. En outre, le T-CY estime que les points de contact du PC-OC, EUROJUST et le Réseau judiciaire européen peuvent également apporter une aide utile.

27. Le T-CY prend note d'une proposition faite par la Roumanie concernant la préparation par le T-CY d'un aide-mémoire dont les points de contact 24/7 pourraient se servir pour leurs demandes de conservation rapide de données informatiques, et demande au Projet sur la cybercriminalité d'en présenter un projet pour examen par le T-CY à sa prochaine réunion.

f. Difficultés à déterminer la localisation des serveurs et des propriétaires

28. Le T-CY fait remarquer qu'il peut quelquefois être très difficile de localiser les serveurs et d'en identifier les propriétaires ; en outre, les retards dans la localisation des serveurs peuvent empêcher les services de répression d'intervenir à temps. M. Gareth Sansom (Canada) fait une présentation PowerPoint sur le problème de la localisation : cyberespace contre espace géographique, qui apporte de nombreuses informations utiles sur cette question.

29. Le T-CY reconnaît que de nombreuses difficultés juridictionnelles se posent du fait de la facilité avec laquelle les serveurs peuvent changer rapidement de pays ou du fait de l'utilisation de zombies. Il convient de la nécessité d'examiner plus avant les questions de compétence au vu des évolutions technologiques et invite le Projet sur la cybercriminalité à soumettre un rapport sur cette question à la prochaine réunion du T-CY.

g. Examen de l'établissement de règles communes pour les FSI et leurs relations avec les services de répression

30. Voir IIIb. ci-dessous.

h. Formations proposées (par les instances internationales ou les Etats)

31. Le T-CY reconnaît que, bien que la Convention offre à tous les Etats une solution juridique complète, les problèmes techniques graves doivent également être examinés et que la formation (police, procureurs, juges et législateur) revêt une importance particulière dans la lutte contre la cybercriminalité.

32. Le T-CY regrette l'absence d'une base de données globale concernant les formations proposées au niveau international, mais note que l'Office européen de police (EUROPOL) et le Collège européen de police (CEPOL) travaillent en étroite collaboration pour apporter une formation aux Etats de l'Union européenne.

33. Le T-CY insiste sur la nécessité de proposer aux policiers, aux juges et aux procureurs une formation en criminalistique appliquée à la cybercriminalité. Il invite le Conseil consultatif de procureurs européens (CCPE) et le Conseil consultatif de juges européens (CCJE) d'examiner cette question.

i. Exemples de partenariats publics et privés pour le blocage de sites Web, à la lumière des travaux récents menés par le Conseil de l'Europe (Recommandation CM/Rec(2007)16 et Recommandation CM/Rec(2008)6)

34. Le T-CY prend note de la Recommandation CM/Rec(2007)16 du Comité des Ministres sur des mesures visant à promouvoir la valeur de service public de l'Internet (voir en particulier la partie V de l'annexe à la recommandation, relative à la sécurité, qui énonce que « les Etats

membres devraient s'engager à une coopération juridique internationale afin de développer et de renforcer la sécurité et le respect du droit international sur Internet. Ils devraient notamment prendre les mesures suivantes : […] promouvoir un usage plus sûr de l'Internet et des TIC, en particulier pour les enfants, en luttant contre les contenus illégaux et en s'attaquant aux contenus préjudiciables et, le cas échéant, non sollicités grâce à la régulation, l'encouragement de l'autorégulation, y compris l'élaboration de codes de conduite, et le développement de systèmes et de normes techniques adéquates »).

35. Le T-CY prend également connaissance de la Recommandation CM/Rec(2008)6 du Comité des Ministres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet. Il note en particulier l'annexe à la recommandation qui contient les lignes directrices suivantes :

- utilisation et contrôle des filtres internet pour exercer et jouir pleinement de la liberté d'expression et d'information;

- mise en place d'un filtrage approprié pour les enfants et les jeunes ;
- utilisation et mise en œuvre de filtres internet par les secteurs public et privé.

j. Statistiques concernant l'étendue de la cybercriminalité et rapports des instances internationales ou des Etats

36. Le T-CY reconnaît qu'il importe d'évaluer l'étendue de la cybercriminalité et les domaines dans lesquels elle est susceptible de se développer. De telles informations permettent aux Etats de planifier l'avenir, notamment sur le plan des besoins en ressources humaines et financières. Elles sont indispensables pour pouvoir prendre des mesures suffisantes de lutte contre la criminalité grave sur internet.

37. Le T-CY est informé que la France a proposé à l'Union européenne de recueillir des données statistiques sur les différents types d'infractions.

III INFORMATIONS CONCERNANT LE PROJET SUR LA CYBERCRIMINALITE

a. Activités à ce jour et programme de travail

38. Le T-CY prend connaissance des progrès réalisés dans le cadre du Projet sur la cybercriminalité, qui a été lancé en septembre 2006 et a permis de faire de la Convention une ligne directrice globale pour l'élaboration de la législation relative à la cybercriminalité et un cadre pour la coopération internationale. Il a accompagné de nombreux autres pays – en plus des pays européens – dans leur travail législatif et a fourni des analyses détaillées pour l'Argentine, le Brésil, la Colombie, l'Egypte, l'Inde, l'Indonésie, le Nigéria et les Philippines.

39. Le financement du projet est actuellement assuré par le budget du Conseil de l'Europe et par des contributions volontaires de l'Estonie et de Microsoft. Le T-CY invite d'autres Etats et instances à apporter de nouvelles contributions de manière à assurer la mise en œuvre pleine et entière du projet.

b. Conférence Octopus Interface « Coopération contre la cybercriminalité » (1er et 2 avril 2008) et lignes directrices pour la coopération entre les organes de répression et les fournisseurs de services internet dans les enquêtes sur la cybercriminalité

40. De nombreux participants du T-CY ont assisté à cette conférence, qui s'est déroulée à Strasbourg les 1er et 2 avril 2008 dans le cadre du projet sur la cybercriminalité. Pour les conclusions de la conférence, on se référera à **l'annexe VI**.

41. Le T-CY se félicite des conclusions de cette conférence internationale et prend connaissance des rapports préparés dans le cadre du projet. Il note avec satisfaction que la conférence internationale du projet s'est tenue immédiatement avant la réunion du T-CY et recommande la poursuite de cette pratique à l'avenir si cela est possible.

42. Le T-CY se félicite de l'adoption par la Conférence de lignes directrices non contraignantes sur la coopération entre les organes de répression et les fournisseurs de services Internet dans les enquêtes sur la cybercriminalité (**voir annexe V au présent rapport**) ; le T-CY reconnaît leur utilité pour la promotion de la coopération dans ce domaine.

c. Profils des Etats

43. Le T-CY se félicite de l'intégration sur le site Web des 27 profils suivants en matière de législation sur la cybercriminalité : Albanie, Argentine, Arménie, Autriche, Brésil, Bulgarie, Italie, Chine, Croatie, Chypre, République tchèque, République dominicaine, France, Allemagne, Hongrie, Lituanie, Maroc, Mexique, Moldova, Portugal, Roumanie, République slovaque, ex-République yougoslave de Macédoine, Philippines, Turquie, Ukraine, Etats-Unis d'Amérique.

44. Le T-CY souligne l'utilité des profils des Etats, à la fois pour l'analyse de la mise en œuvre de la Convention dans le droit interne et pour les échanges de bonnes pratiques et d'expériences.

45. Le T-CY encourage les participants à contribuer à la préparation des profils de leurs Etats et, au besoin, à leur mise à jour.

IV. ECHANGE DE VUES SUR LA COOPERATION ENTRE LES ETATS, LES ORGANISATIONS INTERNATIONALES, LE MILIEU DE LA RECHERCHE ET LE SECTEUR PRIVE

46. Le T-CY insiste sur la nécessité de promouvoir des partenariats publics et privés afin de lutter contre la cybercriminalité, et note que de tels partenariats pourraient jouer un rôle important dans la prévention de l'utilisation de l'internet à des fins criminelles.

47. L'utilité d'une coopération étroite entre le T-CY et le Sous-groupe du G8 sur la criminalité de haute technologie (sous groupe « Lyon-Rome ») est mise en évidence, en particulier pour veiller à une coordination adéquate entre les points de contact du réseau 24/7.

V. AUTRES TRAVAUX MENES PAR LE CONSEIL DE L'EUROPE SUR DES SUJETS SPECIFIQUES RELATIFS A LA CYBERCRIMINALITE

a. Deuxième réunion du Forum sur la gouvernance de l'Internet (IGF) (Rio de Janeiro, 12 – 15 novembre 2007) et préparation de la troisième réunion de l'IGF (Hyderabad, Inde, 3 – 6 décembre 2008)

48. Le Secrétariat donne des informations sur la réunion 2007 de l'IGF ; il ajoute que le Conseil de l'Europe a été la plus active et la plus visible des organisations intergouvernementales présentes et le principal protagoniste des débats relatifs à la cybercriminalité, à la protection des enfants, au droit au respect de la vie privée et à la participation démocratique sur l'internet.

49. Le Conseil de l'Europe a organisé 15 manifestations sur l'ouverture, la sécurité, l'accès, la diversité et les ressources internet critiques, dont deux événements spécifiquement liés à la Convention sur la cybercriminalité, qui a de ce fait gagné en visibilité. Un certain nombre de pays d'Amérique du Sud ont indiqué qu'ils souhaitaient adhérer à la Convention, et des pays d'autres régions ont porté un grand intérêt à la Convention et à un suivi bilatéral direct avec le Conseil de l'Europe.

50. Le T-CY est informé que le Conseil de l'Europe prépare maintenant sa participation à la prochaine réunion de l'IGF, qui se tiendra à Hyderabad (Inde), du 3 au 6 décembre 2008. L'Inde et plusieurs autres pays pourraient adhérer à la Convention sur la cybercriminalité lors de cette réunion.

51. Le Secrétariat invite :

- les participants au T-CY à lui transmettre toute proposition de questions à examiner au prochain IGF ;
- les personnes qui représenteront les Etats ou organisations à l'IGF de prendre contact avec lui afin d'assurer une coordination et une efficacité optimales dans le domaine de la cybercriminalité.

b. Ouverture à la signature de la Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (SCTE n°: 201)

52. Le T-CY prend connaissance de cette convention, qui a été signée par 27 Etats.

53. L'information au T-CY relevait en particulier les articles suivants de la convention :

- l'article 6, qui traite de l'éducation des enfants, et demande aux Etats parties de donner des informations aux enfants sur les situations à risque d'exploitation et d'abus sexuels, notamment celles résultant de l'utilisation des nouvelles technologies de l'information et de la communication ;
- l'article 20, consacré aux infractions se rapportant à la pornographie enfantine, qui présente de nombreuses similitudes avec l'article 9 de la Convention sur la cybercriminalité mais, contrairement à ce dernier, ne se limite pas aux infractions commises au moyen d'un système informatique. L'article 20 demande également aux parties, à moins qu'ils aient émis une réserve à ce propos, à ériger en infraction pénale « le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine » ;
- l'article 30, qui contient des principes relatifs aux enquêtes, aux poursuites et au droit procédural, et demande aux parties de prendre des mesures pour identifier les victimes « notamment grâce à l'analyse des matériels de pornographie enfantine, tels que les photographies et les enregistrements audiovisuels, accessibles, diffusés ou transmis par le biais des technologies de communication et d'information. »

c. Information concernant les travaux du Groupe de spécialistes sur les produits pharmaceutiques contrefaits (PC-S-CP)

54. Le T-CY est informé que, pour faire face à la circulation de médicaments contrefaits, devenue courante, et à l'absence de sanctions pénales efficaces dans de nombreux pays, le PC-S-CP prépare actuellement des textes visant, entre autres, à ce que ces actes soient érigés en infraction. Sous réserve d'acceptation par les organes compétents du Conseil de l'Europe, ces textes feront l'objet une convention, qui tiendra pleinement compte de la Convention sur la cybercriminalité.

55. Toute nouvelle Convention dans ce domaine devrait être ouverte à tous les Etats, et la participation d'Etats non européens devrait être encouragée.

d. Avis du CODEXTER sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes

56. Le T-CY prend note de cet avis du CODEXTER qui lui a été transmis par le Comité des Ministres.

57. L'avis du CODEXTER encourageait en particulier les Etats à devenir parties à la Convention sur la cybercriminalité et indiquait : « la mise en œuvre effective de la Convention sur la cybercriminalité permettrait de s'assurer que les législations nationales prévoient des sanctions appropriées en cas d'attaques graves, et notamment à caractère terroriste, dirigées contre des infrastructures informatiques ou générales. »

58. Le T-CY prend note des différents points de vue sur la nécessité d'un instrument spécifique dans ce domaine.

VII DIVERS

59. Le T-CY prend connaissance des décisions adoptées par le Comité européen pour les problèmes criminels (CDPC) à sa 56e réunion, sur des questions relatives à la cybercriminalité.

VIII. PROCHAINE REUNION DU COMITE DE LA CONVENTION SUR LA CYBERCRIMINALITE (T-CY)

60. Le T-CY décide de tenir sa prochaine réunion en mars 2009, si possible immédiatement après la Conférence Octopus Interface sur la cybercriminalité.

61. Il décide de faire figurer les points suivants à l'ordre du jour :

    a. états des signatures, ratifications et adhésions à la Convention et à son Protocole (y compris l'avancement et le calendrier prévisionnel)
    b. rapport concernant les points de contact (à préparer par le Projet sur la cybercriminalité)
    c. réponses des Etats parties concernant la mise en œuvre de la Convention
    d. entraide judiciaire dans les affaires liées à l'informatique
    e. aide-mémoire à l'usage des points de contact 24/7 pour les demandes de conservation rapide des données informatiques (à préparer par le projet sur la cybercriminalité)
    f. rapport sur les questions de compétence à la lumière des évolutions techniques qui permettent un changement rapide de serveur d'un pays à un autre (à préparer par le projet sur la cybercriminalité)

62. Le T-CY décide d'inviter à sa prochaine réunion toutes les catégories de participants invités à la présente réunion. Il estime en outre qu'il serait intéressant d'y inviter les Etats qui souhaitent adhérer la Convention ainsi que d'autres organisations intergouvernementales internationales.

63. Le T-CY demande donc à tous les participants à la présente réunion de faire parvenir au Secrétariat des propositions concernant d'éventuelles autres catégories de participants à inviter à sa prochaine réunion. Les propositions devront être transmises au Secrétariat (DG1.cybercrime@coe.int) pour le 1er septembre 2008 au plus tard.

ANNEXE I

LISTE DE PARTICIPANTS

PARTIES PARTICIPANT A LA CONVENTION SUR LA CYBERCRIMINALITE

BULGARIA / BULGARIE

M. Krassimir BOJANOV, Adjoint au Représentant permanent de la Bulgarie auprès du Conseil de l'Europe, STRASBOURG, France

CROATIA / CROATIE

Mr Ivan MIJATOVIC, Chief inspector, Ministry of the Interior, ZAGREB, Croatia

ESTONIA / ESTONIE

Mr Markko KÜNNAPU, Adviser, Criminal Police Department, Ministry of Justice, TALLINN, Estonia

FINLAND / FINLANDE

Mr Antti PIHLAJAMÄKI, Chief District Prosecutor, Prosecutor's Office of South-West Finland, TURKU, Finland

FRANCE

M. Fabien LANG, Commissaire de Police, Adjoint au Chef de l'OCLCTIC, Direction centrale de la Police Judiciaire, NANTERRE, France

Mme Setareh Marie AGHA BABAEI, Stagiaire, Direction Centrale de la police judiciaire (OCLCTIC), NANTERRE, France

HUNGARY / HONGRIE

Mr Zsolt SZABOLCSI, Senior detective, National Bureau of Investigation, High-tech Crime Department, BUDAPEST, Hungary

Ms Eszter VICZKO, Legal Adviser, Ministry of Justice, BUDAPEST, Hungary

ICELAND / ISLANDE

Ms Ragna ÁRNADÓTTIR, Director of Legal Affairs, Ministry of Justice and Ecclesiastical Affairs, REYKJAVÍK, Iceland; *Apologised / Excusé*

Mr Gunnar Narfi GUNNARSSON, Legal Expert, Directorate of Legal Affairs, Ministry of Justice and Ecclesiastical Affairs, REYKJAVÍK, Iceland; *Apologised / Excusé*

NETHERLANDS / PAYS-BAS

Mr Henrik W. K. KASPERSEN, Director Computer/Law Institute, Vrije Universiteit, De Boelelaan AMSTERDAM, The Netherlands

NORWAY / NORVEGE

Mr Erik MOESTUE, Police Prosecutor, National Criminal Investigation Service (NCIS), OSLO, Norway

ROMANIA / ROUMANIE

Ms Cristina SCHULMAN, Vice Chair of the Committee, Legal adviser – Department for International Law and Treaties Ministry of Justice, BUCHAREST, Romania

Ms Ioana Bogdana ALBANI, Chief Prosecutor, Head of the Cybercrime Unit, Prosecutor's Office attached to the High Court of Cassation and Justice, Directorate for the Investigation of Organised Crime and Terrorism, BUCHAREST, Romania

SLOVAKIA / SLOVAQUIE

Mr Miroslav TIZA, Prosecutor, The General's Prosecutors Office of the Slovak Republic, International Department, BRATISLAVA, Slovak Republic

UKRAINE

Mr Andrii FIALKOVSKYI, Advisor, National Security Council, KIEV, Ukraine

UNITED STATES OF AMERICA / ETATS-UNIS D'AMÉRIQUE

Ms Betty SHAVE, Chair of the Committee, Assistant Deputy Chief for International Computer Crime, Computer Crime and Intellectual property Section, US Department of Justice, WASHINGTON, DC

Mr Thomas DUKES, Trial Attorney, US Department of Justice, Computer Crime and Intellectual Property Section, WASHINGTON DC

OTHER PARTICIPANTS / AUTRES PARTICIPANTS

AZERBAÏJAN / AZERBAIDJAN

Mr Bakhtiyar N. MAMMADOV, Head of Legal and Human Resources Department, Ministry of Communications and Information Technologies, BAKU, Republic of Azerbaijan

CANADA

Mr Gareth SANSOM, Director, Technology & Analysis, Ministry of Justice, OTTAWA, Canada

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Mr Tomáš HUDEČEK, Ministry of Justice, International Section, PRAGUE 2, Czech Republic

GEORGIA / GEORGIE

Mr Levan JANIKASHVILI, Deputy Head of Operative, Technical Department, Ministry of Internal Affairs of Georgia, TBILISI, Georgia

Ms Natia GVAZAVA, Head of International Cooperation Unit, Ministry of Internal Affairs of Georgia, TBILISI, Georgia

GERMANY / ALLEMAGNE

Mr Alexander DÖRRBECKER, Deputy Head of Division, Federal Ministry of Justice, BERLIN, Germany

Ms Ivonne SCHWINDT, Assistant, Federal Ministry of Justice, BERLIN, Germany

GREECE / GRECE

Mr Theodoros MITRAKOS, Solicitor, Ministry of Justice, ATHEN, Greece; Apologised / Excusé

HOLY SEE / SAINT SIEGE

Apologised / Excusé

JAPAN / JAPON

Mr Shoichi ITO, Senior Superintendent, Cybercrime Division, Community Safety Bureau, National Police Agency, 2TOKYO, Japan

Mr Hiroyuki OSHIMA, Official, International Organized Crime Division, Foreign Policy Bureau, Ministry of Foreign Affairs, TOKYO, Japan

Mr Akira TAKANO, Consul (Attorney), Consulate General of Japan, STRASBOURG, France

MEXICO / MEXIQUE

Mr Rodrigo LABARDINI FLORES, Deputy Legal Adviser “B”, Ministry of Foreign Affairs, MEXICO CITY, Mexico

Mr Guillermo VALLS ESPONDA, Agregado Legal para la Unión Europea y Suiza, Procuraduría General de la República / Embajada de México en España, MADRID, Spain

Mr J. Iván FLORES CONTRERAS, Liaison Office for EU of Ministry of Public Safety of Mexico, Mexico Embassy in Spain, ,MADRID, Spain

MOLDOVA

Mr Valentin COLIBAN, Deputy Chief of Informatization Directorate, Ministry of Informational Development, Chisinau, Republic of Moldova

PORTUGAL

Mr Pedro VERDELHO, Docente, Centre for Judiciary Studies, LISBOA, Portugal

RUSSIAN FEDERATION / FEDERATION DE RUSSIE

Mr Boris MIROSHNIKOV, Head of Department “K”, Ministry of Interior, MOSCOW, Russian Federation

Mr Mikhail SHURGALIN, Head of Section, Department of New Challenges and Threats, Ministry of Foreign Affairs, MOSCOW, Russian Federation

SPAIN / ESPAGNE

Mr Antonio ROMA VALDES, Public Prosecutor, Fiscalia SCI, Fiscalia de Santiago, SANTIAGO, Spain

Mr Luis Maria URIARTE VALIENTE, Prosecutor, Fiscalia General Del Estado, Fiscalia Provincial de Pontevedra, PONTEVEDRA, Spain

SWITZERLAND / SUISSE

Mme Christine MAGNIN, Unité Droit pénal international, Office fédéral de la Justice, BERNE, Switzerland

M. Nicolas BOTTINELLI, Unité entraide judiciaire, Office fédéral de la Justice, BERNE, Suisse

M. Mauro VIGNATI, Analyste Cybercrime, Federal Office of Police, BERN, Switzerland

Mr Adrian KOSTER, Juriste, Federal Office of Police, BERN, Switzerland;

TURKEY / TURQUIE

Mr Osman NIHAT SEN, Head of the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Mr Erol AKTAY, Communications Expert at the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Mr Dogan KILINC, Communications Expert at the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Ms Özlem ALLIOĞLU, Lawyer, Radio and Television Supreme Council, ANKARA, Turkey

Mr Soner BASLI, System Analyst, Radio and Television Supreme Council, ANKARA, Turkey

Mr Nihat ÇAYLAK, Expert, Radio and Television Supreme Council, ANKARA, Turkey

UNITED KINGDOM / ROYAUME-UNI

Apologised / Excusé

EUROPEAN COMMITTEE ON CRIME PROBLEMS / COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS (CDPC)

Mr Branislav BOHÁČIK, Head of Division for Judicial Co-operation in Criminal Matters, Ministry of Justice, BRATISLAVA, Slovak Republic

STEERING COMMITTEE ON THE MEDIA AND NEW COMMUNICATION SERVICES / COMITE DIRECTEUR SUR LES MEDIAS ET LES NOUVEAUX SERVICES DE COMMUNICATION (CDMC)

M. Thomas SCHNEIDER, Service des Affaires internationales, Office fédéral de la communication, BIENNE, Suisse

INTERNATIONAL TELECOMMUNICATION UNION (ITU) / UNION INTERNATIONALE DES TELECOMMUNICATIONS (UTI)

Mr Alexander NTOKO, Head, Corporate Strategy Division, International Telecommunication Union GENEVA, Switzerland

ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE) ACTION AGAINST TERRORISM UNIT (ATU) / ORGANISATION POUR LA SECURITE ET LA COOPERATION EN EUROPE (OSCE) UNITE D'ACTION CONTRE LE TERRORISME (UAT)

Mr Nemanja MALISEVIC, CTN Co-ordinator, Assistant Programme Officer, Organization for Security and Co-operation in Europe, VIENNA, Austria

Mr Joseph MANGAN, Information Management Officer, Strategic Police Matters Unit, Organization for Security and Co-operation in Europe, OSCE VIENNA, Austria

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC) / OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC)

Mr Gillian MURRAY, Focal Point for Cybercrime, Division for Treaty Affairs, United Nations Office on Drugs and Crime, VIENNA, Austria

Mr Chang SOO LEE, Division for Treaty Affairs(DTA), Treaty and Legal Assistance Branch(TLAB/OCS), United Nations Office on Drugs and Crime, VIENNA, Austria

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

Mr Michael CARLIN, European Commission, Head of Sector, BRUSSELS, Belgium

EUROPOL

Mr Nicola DILEONE, First Officer, Europol, OC Groups Unit/ High Tech Crime Centre, THE HAGUE, The Netherlands

SECRETARIAT OF THE COUNCIL OF EUROPE
SECRETARIAT DU CONSEIL DE L'EUROPE

Council of Europe - Directorate General of Human Rights and Legal affairs
DG-HL
Conseil de l'Europe - Direction des droits de l'Homme et des affaires juridiques

T-CY – Contacts
Website: www.coe.int/cybercrime
Telephone of the Secretariat: +33 3 90 21 50 35

Ms Margaret KILLERBY, Secretary a.i. to the T-CY, Head of Law Reform Department a.i., Director of Co-operation

Mr Alexander SEGER, Head of Economic Crime Division, Technical Co-operation Department, Directorate of Co-operation

Mr Carlo CHIAROMONTE, Head of Criminal Law Division, Law Reform Department

Mr Lee HIBBARD, Coordinator of International Information Society, Media and Information Society Division

Mr David DOLIDZE, Administrator, Gender Equality and Anti-Trafficking Division

Ms Dominique WULFRAN, Assistant, Law Reform Department

INTERPRETERS / INTERPRETES

Mme Isabelle MARCHINI
Mme Pascale MICHLIN

ANNEXE II

ORDRE DU JOUR

1. **Opening of the meeting / *Ouverture de la réunion***

   Working documents / *Documents de travail*:

   - Information document concerning the T-CY /
     Document d'information concernant le T-CY T-CY(2008) INF 01
   - Report of the second meeting of the Cybercrime Convention Committee /
     Rapport de la deuxième réunion du Comité de la Convention sur la cybercriminalité
     T-CY(2007)03

2. **Election of the Chair and Vice-Chair by representatives of States Party to the Convention / Election du président et du vice-président par les représentants des Etats parties à la Convention**

3. **Adoption of the agenda / Adoption de l'ordre du jour**

4. **Exchange of views on the present situation concerning the Convention on Cybercrime (CETS No.:185) and its Additional Protocol (CETS No.:189) / *Echange de vues sur la situation actuelle concernant la Convention sur la cybercriminalité (STCE no. :185) et son Protocole additionel (STCE no. :189)***

   a. State of signatures, ratifications and accession to the Convention and its additional Protocol (including progress made and likely future timetable) / *Etat des signatures, ratifications, adhésions à la Convention et à son protocole additionnel (y compris l'état d'avancement et le calendrier prévisionnel);*

   b. Implementation of the Convention in national legislation – Consideration of the implementation of Article 1.d concerning the definition of traffic data and of Article 2 concerning illegal access to computer systems / *Mise en œuvre de la Convention dans la législation nationale – examen de l'article 1.d concernant la définition des données relatives au trafic et de l'article 2 concernant l'accès illégal aux systèmes informatiques ;*

   c. Consideration of the replies of the Parties to questions on the practical implementation of the Convention / *Examen des réponses des parties aux questions concernant la mise en œuvre pratique de la Convention*;

   d. Consideration of specific difficulties arising out of international co-operation / *Examen de problèmes spécifiques découlant de la coopération internationale:*

      - between the Parties / *entre les Parties*
      - between Parties and other States / *entre les Parties et d'autres Etats*;

   e. Mutual legal assistance in computer related cases in particular in urgent cases in the light of information provided by the CDPC and the PC-OC, and consideration of the implementation of Articles 16 and 17 on expedited preservation of the Convention on Cybercrime (see paragraphs 21 – 25 of T-CY (2007)03) / *Entraide judiciaire dans les affaires informatiques, notamment en cas d'urgence, à la lumière des informations fournies par le CDPC et le PC-OC, et examen de la mise en œuvre des articles 16 et 17 sur la conservation rapide de la Convention sur la cybercriminalité (voir paragraphes 21 - 25 du document T-CY (2007)03)*;

f. Difficulties to ascertain the location of servers and owners (see paragraph 34 of T-CY (2007)03) / *Difficultés à déterminer la localisation des serveurs et des propriétaires (voir paragraphe 34 de T-CY (2007)03)*;

g. Consideration of establishing common rules for ISPs and their relations with law enforcement, in the light of the Study prepared under the Project on Cybercrime (see also paragraph 16 of T-CY (2007)03) / *Examen de l'établissement de règles communes pour les FAI et leurs relations avec les services de répression à la lumière d'une étude préparée dans le cadre du Projet sur la Cybercriminalité (voir aussi paragraphe 16 du document T-CY (2007)03)*;

h. Available training (by international bodies or by States) (see paragraph 14 of T-CY (2007)03) / *Formations proposées (par les instances internationales ou les Etats) (voir paragraphe 14 du document T-CY (2007)03)*;

i. Examples of public and private partnerships for the purpose of blocking of websites in the light of the recent relevant work carried out by the Council of Europe (Recommendation CM/Rec(2007)16 and Recommendation CM/Rec(2008)6) (see paragraph 29 of T-CY (2007)03) / *Exemples de partenariats publics et privés pour le blocage de sites Web, à la lumière des travaux récents menés par le Conseil de l'Europe (Recommandation CM/Rec(2007)16 et Recommandation CM/Rec(2008)6) (voir paragraphe 29 du document T-CY (2007)03)* ;

j. Statistics concerning the extent of cybercrime and reports from international bodies or States (see paragraphs 40 and 41 of T-CY (2007)03) / *Statistiques concernant l'étendue de la cybercriminalité et rapports des instances internationales ou des Etats (voir paragraphes 40 et 41 du document T-CY (2007)03)*.

Working documents / *Documents de travail*:

- Information document concerning the T-CY /
  Document d'information concernant le T-CY (item/*point* 4.a) T-CY(2008) INF 01

- Report of the second meeting of the Cybercrime Convention Committee /
  Rapport de la deuxième réunion du Comité de la Convention sur la cybercriminalité
  (items/*points* 4. b, c, d, e, f, g, h, I, j, k)
  T-CY(2007)03

- The Convention on Cybercrime (CETS No.:185) and its explanatory report
  La Convention sur la cybercriminalité (STCE no. :185) et son rapport explicatif
  (items/*points* 4.a, b, c, d, e, f, g)*;*

- The Protocol to the Convention (CETS No.:189) and its explanatory report
  Le Protocole à la Convention (STCE no. :189) et son rapport explicatif
  (items/*points* 4.a, b, c, d, e, f, g) *;*

- Replies of the Parties to questionnaire concerning
  the practical implementation of the Convention /
  Réponses des états Parties au questionnaire
  sur la mise en œuvre de la Convention (item/*point* 4.c) T-CY (2008)01

- Replies to the questionnaire of the PC-OC concerning mutual legal assistance in computer related cases /
  Réponses au questionnaire du PC-OC sur l'entraide judiciaire dans les affaires liées à l'informatique (item/*point* 4.e) PC-OC (2007) 15 PROV

- Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet / *Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet* (item/*point* 4.i)

- Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters / *Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet* (item/*point* 4.i)

- "National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices" (la mise en œuvre de la Convention sur la cybercriminalité dans les législations nationales – analyse comparative et bonnes pratiques), préparé par Prof. Dr. Lorenzo Picotti, Université de droit de Vérone (Italie) – En anglais (point 4.b)

- "The effectiveness of international co-operation against cybercrime: examples of good practice" (l'efficacité de la coopération internationale contre la cybercriminalité : exemples de bonnes pratiques), préparé par Pedro Verdelho (Portugal)– En anglais (point 4.e)

- "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime" (Lignes directrices pour la coopération entre les organes de répression et les fournisseurs de services internet contre la cybercriminalité), préparé par Cormac Callanan (Irlande), Marco Gercke (Allemagne) – En anglais (point 4.g)

5. Information concerning the Project on Cybercrime / *Informations concernant le Projet sur la cybercriminalité*

a. Activities to date and workplan 2008 / *Activités à ce jour et programme des travaux 2008*

Working documents / *Documents de travail*:

- Progress Report of the Project on Cybercrime / *Rapport intermédiaire du Projet sur la cybercriminalité*
- Report of the second meeting of the Cybercrime Convention Committee /
  Rapport de la deuxième réunion du Comité de la Convention sur la cybercriminalité
  , T-CY(2007)3
- *Studies prepared under the Project on Cybercrime / Etudes préparées dans le cadre du Projet sur la cybercriminalité*

b. Octopus Interface Conference « Co-operation Against Cybercrime », 1-2 April 2008 / *la Conférence Octopus Interface « Coopération contre la Cybercriminalité », 1-2 avril 2008 ;*

c. Country Profiles / Profils des Etats

6. **Exchange of views on co-operation between States, international organisations, academia and the private sector / *Echange de vues sur la coopération entre les Etats, les organisations internationales, le milieu de la recherche et le secteur privé***

Working documents / *Documents de travail*:

- Report of the second meeting of the Cybercrime Convention Committee / *Rapport de la deuxième réunion du Comité de la Convention sur la cybercriminalité* T-CY(2007)3
- Cybercrime and the European Union / *La cybercriminalité et l'Union Européenne* T-CY(2007)02

7. **Other work carried out in the Council of Europe concerning specific matters relating to cybercrime */ Autres travaux menés par le Conseil de l'Europe sur des sujets spécifiques relatifs à la cybercriminalité***

a. Information concerning the Second Meeting of the Internet Governance Forum (IGF), Rio de Janeiro, 12 - 15 November 2007 and preparations for the Third IGF meeting in New Delhi, December 2008 / *Informations sur le "Internet Governance Forum", Rio de Janeiro, 12-15 novembre 2007 et préparation de la troisième réunion a New Delhi, décembre 2008*

Working documents / *Documents de travail:*

- Summary of the Chairman of the Second Meeting of the IGF / *Résumé par le Président de la deuxième réunion de l'IGF*

b. Opening for signature of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.: 201) / *Ouverture à la signature de la Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (STCE n°201)*

Working documents / *Documents de travail:*

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and its Explanatory Report / *Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels et son rapport explicatif ;*

c. Information concerning the work of the Group of Specialists on Counterfeit Pharmaceutical Products (PC-S-CP) / *Information concernant les travaux du Groupe de spécialistes sur les produits pharmaceutiques contrefaits (PC-S-CP)*

Working documents / *Documents de travail:*

- Final Report of the PC-S-CP / *Rapport Final du PC-S-CP*

d. Opinion of CODEXTER on cyberterrorism and use of the Internet for terrorist purposes / *Avis du CODEXTER sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes*

Working documents / *Documents de travail:*

- Information Document concerning the Opinion of CODEXTER on cyberterrorism and use of Internet for terrorist purposes /

Document d'information concernant l'avis du CODEXTER
sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes
T-CY (2008) INF 02

8. Any other business / *Divers*

9. Next meeting of the Cybercrime Convention Committee (T-CY) / *Prochaine réunion du Comité de la Convention sur la cybercriminalité (T-CY)*

10. Adoption of the abridged meeting report / *Adoption du rapport abrégé de la réunion*

ANNEXE III

Convention sur la cybercriminalité
STCE no. : 185

Traité ouvert à la signature des Etats membres et des Etats non membres qui ont participé à son élaboration et à l'adhésion des autres Etats non membres

Ouverture à la signature

Lieu : Budapest
Date : 23/11/2001

Entrée en vigueur

Conditions : 5 Ratifications incluant au moins 3 Etats membres du Conseil de l'Europe
Date : 1/7/2004

Situation au : 8/4/2008

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	23/11/2001	20/6/2002	1/7/2004				X			
Andorre										
Arménie	23/11/2001	12/10/2006	1/2/2007							
Autriche	23/11/2001									
Azerbaïdjan										
Belgique	23/11/2001									
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006				X			
Bulgarie	23/11/2001	7/4/2005	1/8/2005		X	X				
Croatie	23/11/2001	17/10/2002	1/7/2004							
Chypre	23/11/2001	19/1/2005	1/5/2005							
République tchèque	9/2/2005									
Danemark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonie	23/11/2001	12/5/2003	1/7/2004				X			
Finlande	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Géorgie	1/4/2008									
Allemagne	23/11/2001									
Grèce	23/11/2001									
Hongrie	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Islande	30/11/2001	29/1/2007	1/5/2007		X		X			
Irlande	28/2/2002									
Italie	23/11/2001									
Lettonie	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein										
Lituanie	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malte	17/1/2002									
Moldova	23/11/2001									
Monaco										

Monténégro	7/4/2005			55						
Pays-Bas	23/11/2001	16/11/2006	1/3/2007				X	X		
Norvège	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Pologne	23/11/2001									
Portugal	23/11/2001									
Roumanie	23/11/2001	12/5/2004	1/9/2004				X			
Russie										
San Marin										
Serbie	7/4/2005			55						
Slovaquie	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovénie	24/7/2002	8/9/2004	1/1/2005				X			
Espagne	23/11/2001 r									
Suède	23/11/2001									
Suisse	23/11/2001									
Ex-République yougoslave de Macédoine	23/11/2001	15/9/2004	1/1/2005				X			
Turquie										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
Royaume-Uni	23/11/2001									

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Canada	23/11/2001									
Costa Rica										
Japon	23/11/2001									
Mexique										
Afrique du Sud	23/11/2001									
Etats-Unis	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Nombre total de signatures non suivies de ratifications :	22
Nombre total de ratifications/adhésions :	22

ANNEXE IV

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques
STCE no. : 189

Traité ouvert à la signature des Etats qui ont signé le Traité STE 185

Ouverture à la signature
Lieu : Strasbourg
Date : 28/1/2003

Entrée en vigueur
Conditions : 5 Ratifications.
Date : 1/3/2006

Situation au : 8/4/2008

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	26/5/2003	26/11/2004	1/3/2006							
Andorre										
Arménie	28/1/2003	12/10/2006	1/2/2007							
Autriche	30/1/2003									
Azerbaïdjan										
Belgique	28/1/2003									
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006							
Bulgarie										
Croatie	26/3/2003									
Chypre	19/1/2005	23/6/2005	1/3/2006							
République tchèque										
Danemark	11/2/2004	21/6/2005	1/3/2006		X			X		
Estonie	28/1/2003									
Finlande	28/1/2003									
France	28/1/2003	10/1/2006	1/5/2006			X				
Géorgie										
Allemagne	28/1/2003									
Grèce	28/1/2003									
Hongrie										
Islande	9/10/2003									
Irlande										
Italie										
Lettonie	5/5/2004	14/2/2007	1/6/2007							
Liechtenstein										
Lituanie	7/4/2005	12/10/2006	1/2/2007			X				
Luxembourg	28/1/2003									
Malte	28/1/2003									
Moldova	25/4/2003									
Monaco										

Monténégro	7/4/2005			55						
Pays-Bas	28/1/2003									
Norvège										
Pologne	21/7/2003									
Portugal	17/3/2003									
Roumanie	9/10/2003									
Russie										
San Marin										
Serbie	7/4/2005			55						
Slovaquie										
Slovénie	26/2/2004	8/9/2004	1/3/2006							
Espagne										
Suède	28/1/2003									
Suisse	9/10/2003									
Ex-République yougoslave de Macédoine	14/11/2005	14/11/2005	1/3/2006							
Turquie										
Ukraine	8/4/2005	21/12/2006	1/4/2007			X				
Royaume-Uni										

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Canada	8/7/2005									
Japon										
Afrique du Sud	4/4/2008									
Etats-Unis										

Nombre total de signatures non suivies de ratifications :	21
Nombre total de ratifications/adhésions :	11

ANNEXE V

LIGNES DIRECTRICES POUR LA COOPERATION ENTRE ORGANES DE REPRESSION ET FOURNISSEURS DE SERVICES INTERNET CONTRE LA CYBERCRIMINALITE

Ces lignes directrices sont le résultat de plusieurs débats entre les représentants du secteur et les organes de répression (forces de l'ordre), qui se sont rencontrés entre octobre 2007 et février 2008 sous les auspices du projet sur la cybercriminalité du Conseil de l'Europe. Il est complété par une étude détaillée.

Ce projet a fait l'objet de discussions complémentaires et a été adopté pendant la Conférence « Coopération contre la cybercriminalité (Conseil de l'Europe, Strasbourg, France) des 1er-2 avril 2008.

Il s'agit d'un outil non contraignant sur le plan juridique. Il pourra être diffusé et exploité pour aider les forces de l'ordre et les fournisseurs de services de tous les pays du monde à organiser leur coopération contre la cybercriminalité en respectant leurs rôles et responsabilités respectifs, ainsi que les droits des utilisateurs de l'internet.

Ce texte sera également soumis à l'examen du Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe.

Lignes directrices pour la coopération entre organes de répression et fournisseurs de services internet contre la cybercriminalité[2]

Introduction

1. La construction de la société de l'information fait appel au renforcement de la confiance envers les technologies de l'information et de la communication (TIC), à la protection des données à caractère personnel et à la confidentialité, ainsi qu'à la promotion d'une culture globale de cyber-sécurité dans un contexte mondial au sein duquel les sociétés deviennent de plus en plus dépendantes des TIC et donc, vulnérables à la cybercriminalité.

[2] Ce document ne reflète pas nécessairement les positions officielles du Conseil de l'Europe. Pour de plus amples informations, contacter Alexander.seger@coe.int

2. Les première et deuxième phases du Sommet mondial sur la société de l'information (Genève 2003 – Tunis 2005) ont pris l'engagement – entre autres – de construire une société de l'information inclusive au sein de laquelle chacun pourra créer, obtenir, utiliser et partager l'information et le savoir, mettre en œuvre ses potentialités et améliorer sa qualité de vie conformément aux buts et aux principes de la Charte des Nations Unies, et en respectant pleinement et mettant en œuvre la Déclaration universelle des Droits de l'Homme. Cette société de l'information fait appel à de nouvelles formes de partenariat et de coopération entre les États, le secteur privé, la société civile et les organisations internationales.

3. Les fournisseurs de services internet (FSI) et les organes de répression, ou forces de l'ordre, jouent un rôle crucial dans la réalisation de cette vision.

4. Des lois nationales conformes à la Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest) permettront aux États de créer une base juridique cohérente pour la coopération entre les secteurs public et privé, pour l'exercice des pouvoirs d'investigation ainsi que pour la coopération internationale.

5. Ces lignes directrices n'ont pas pour objectif de se substituer aux instruments juridiques existants ; elles présupposent que ceux-ci sont à même de fournir un système d'instruments d'investigation bien équilibrés ainsi que les clauses de sauvegarde et la protection des droits fondamentaux de l'être humain tels que la liberté d'expression, le droit au respect de la vie, du foyer et de la correspondance privés et le droit à la protection des données. Par conséquent, nous recommandons que les États adoptent ces dispositions dans leurs lois nationales afin de mettre en œuvre les dispositions de procédure de la Convention sur la cybercriminalité et de définir les obligations des autorités d'investigation et des forces de l'ordre tout en mettant en place les conditions et les sauvegardes prévues à l'article 15 de la Convention. Cela aura pour effet :

- d'assurer l'efficacité des activités des forces de l'ordre ;
- de protéger l'aptitude des fournisseurs de services internet à fournir des services ;
- de faire en sorte que les lois nationales soient conformes aux normes mondiales ;
- de promouvoir les normes mondiales au lieu de solutions nationales isolées ;
- de contribuer au bon fonctionnement du droit et notamment à l'application des principes de légalité, de proportionnalité et de nécessité.

6. Ces lignes directrices utilisent la définition du « fournisseur de services » de la Convention sur la cybercriminalité dans son article 1, qui en donne une acception large :

i toute entité publique ou privée offrant aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

7. Afin d'optimiser la cybersécurité, réduire l'utilisation des services à des fins illicites et renforcer la confiance envers les TIC, il est fondamental que les fournisseurs de services internet et les forces de l'ordre coopèrent efficacement avec toute la considération due à leurs rôles respectifs, aux coûts de cette coopération et aux droits des citoyens.

8. L'objectif de ces lignes directrices est d'aider les forces de l'ordre et les fournisseurs de services internet à structurer leurs interactions en lien avec les questions de cybercriminalité. Elles reposent sur des bonnes pratiques existantes et devraient être applicables dans tous les pays du monde en accord avec les lois nationales et dans le respect de la liberté d'expression, du droit au respect de la vie privée, à la protection des données personnelles et des autres droits fondamentaux des citoyens.

9. Par conséquent, nous recommandons aux États, aux forces de l'ordre et aux fournisseurs de services internet de prendre les mesures suivantes au niveau national :

Lignes directrices communes

10. Il conviendrait d'encourager les forces de l'ordre et les fournisseurs de services internet à s'engager dans des échanges d'information visant à renforcer leur capacité à identifier et combattre les types de cybercriminalité émergents. Les forces de l'ordre devraient tenir les fournisseurs de services informés sur les tendances de la cybercriminalité.

11. Les forces de l'ordre et les fournisseurs de services internet devraient développer une culture de la coopération – plutôt que de la confrontation – incluant le partage de bonnes pratiques. Il conviendrait d'encourager la tenue de réunions régulières en vue de l'échange des expériences et de la résolution des problèmes.

12. Les forces de l'ordre et les fournisseurs de services devraient développer conjointement des procédures de coopération écrites. Lorsque c'est possible, les deux parties devraient être invitées à se transmettre des retours d'information structurés sur le fonctionnement de ces procédures.

13. Il conviendrait d'envisager des partenariats formels entre les forces de l'ordre et les fournisseurs de services afin d'établir des relations à long terme avec les garanties réciproques appropriées, de façon à ce que le partenariat n'enfreigne pas les droits des acteurs du secteur ou qu'il n'interfère pas avec les pouvoirs d'application de la loi du côté des forces de l'ordre.

14. Tant les forces de l'ordre que les fournisseurs de services internet devraient protéger les droits fondamentaux des citoyens conformément aux normes des Nations Unies et aux autres normes européennes et internationales applicables, telles que la Convention des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe, le Pacte international de 1966 des Nations Unies, relatif aux droits civils et politiques, la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ainsi que les lois nationales. Cela place des limites raisonnables au niveau de coopération envisageable.

15. Il conviendrait d'encourager les forces de l'ordre et les fournisseurs de services internet à coopérer en vue de faire appliquer les normes de respect de la vie privée et de la protection des données au niveau national, mais également par rapport aux flux de données transfrontaliers. Les travaux du Conseil de l'Europe et de l'OCDE apportent des lignes de conduite à cet égard.

16. Les deux parties devraient être conscientes des coûts afférents à la génération de requêtes et aux réponses à apporter. Il conviendrait de développer des procédures tenant compte de l'impact financier de ces activités, ainsi que des questions de remboursement des coûts ou de juste compensation pour les parties concernées.

Mesures à prendre par les forces de l'ordre

17. Une coopération élargie et stratégique – encourager les forces de l'ordre à apporter leur assistance aux fournisseurs de services dans le cadre d'une coopération élargie et stratégique avec le secteur privé, ce qui impliquerait de conduire régulièrement des séminaires de formation juridique, ainsi que de faire remonter les informations collectées à l'occasion des plaintes enregistrées ou des renseignements obtenus par les fournisseurs de services sur des activités criminelles connues.

18. Procédures pour les requêtes pénales – encourager les forces de l'ordre à élaborer des procédures écrites, incluant les mesures appropriées d'application, pour l'émission et le traitement des requêtes pénales, et pour s'assurer que ces requêtes soient prises en charge dans le respect des procédures agréées.

19. Formation – encourager les forces de l'ordre à proposer des formations à une équipe désignée au sein de leur personnel sur la manière de mettre ces procédures en œuvre, y compris sur la manière d'obtenir les enregistrements auprès des fournisseurs de services et de traiter les informations reçues, mais également sur les technologies internet et leur impact en général ainsi que sur la manière de respecter les principes du droit et les droits fondamentaux des individus.

20. Ressources techniques – les personnels des forces de l'ordre responsables de la coopération avec les fournisseurs de services devraient s'équiper des ressources techniques nécessaires, et notamment d'un accès à internet, d'une adresse de messagerie qui mette en évidence l'identité du service, et d'autres ressources techniques leur permettant de recevoir, de la part des fournisseurs de services, des informations en toute sécurité par voie électronique.

21. Personnel et points de contact désignés – les interactions entre les forces de l'ordre et les fournisseurs de services devraient se limiter aux personnels dûment formés. Il conviendrait d'encourager les forces de l'ordre à désigner des points de contact pour la coopération avec les fournisseurs de services.

22. Autorité pour les requêtes – encourager les forces de l'ordre à définir clairement dans leurs procédures écrites quel personnel interne peut autoriser quel type de mesure et de requête auprès des fournisseurs de services internet et comment ces requêtes peuvent être validées/autorisées par ces derniers.

23. Encourager les forces de l'ordre à mettre à la disposition des fournisseurs de services internet des informations relatives à leurs procédures et, chaque fois que c'est possible, à indiquer quel personnel ou quel poste de travail désigné est responsable de la coopération avec les fournisseurs de services internet.

24. Vérification de la source de la requête – la source d'une requête émanant des forces de l'ordre doit être vérifiable par les fournisseurs de services :

- toute correspondance devrait inclure un nom de contact, un numéro de téléphone et une adresse de messagerie correspondant à celle de l'agent des forces de l'ordre sollicitant les enregistrements, de façon à ce que le fournisseur de services puisse contacter la personne à l'origine de la requête le cas échéant ;
- les fournisseurs de services ne devraient pas se voir demander de correspondre avec un agent au travers de son adresse de messagerie personnelle, mais plutôt par un compte de messagerie approprié, mis en place par le service ;
- toute correspondance devrait porter l'en-tête du service concerné et le numéro du central téléphonique principal du service, ainsi que son adresse web, de façon à ce que les fournisseurs de services puissent prendre les mesures nécessaires pour vérifier l'authenticité des requêtes s'ils estiment devoir le faire.

25. Requêtes – les requêtes des forces de l'ordre aux fournisseurs de services devraient être faites par écrit (ou par tout autre méthode électronique juridiquement acceptable) et être dûment consignées à des fins de traçabilité. Dans les cas d'extrême urgence, ou lorsque les requêtes orales sont acceptables, elles doivent être immédiatement suivies d'une confirmation écrite (ou autre méthode électronique juridiquement acceptable).

26. Format de requête standard – au niveau national, et international si c'est possible, il conviendrait d'encourager les forces de l'ordre à standardiser et à structurer le format employé pour envoyer des requêtes et y répondre. Au minimum, les requêtes devraient contenir les informations suivantes :

- un numéro d'enregistrement
- la référence aux textes juridiques de base
- les données spécifiques sollicitées
- les informations permettant de vérifier la source de la requête

27. Spécificité et précision des requêtes – encourager les forces de l'ordre : à s'assurer que les requêtes envoyées sont spécifiques, complètes et claires, et qu'elles sont suffisamment détaillées pour permettre aux fournisseurs de services d'identifier les données pertinentes ; à faire en sorte que les requêtes sont envoyées au fournisseur de services qui possède les enregistrements ; à éviter les requêtes concernant des données multiples et non spécifiées.

28. Encourager les forces de l'ordre à fournir autant de faits que possible quant aux investigations, sans mettre en danger l'enquête conduite ni des droits fondamentaux, afin de permettre aux fournisseurs de services d'identifier les données pertinentes.

29. Encourager les forces de l'ordre à fournir des explications et de l'assistance aux fournisseurs de services en matière de techniques d'investigation générales afin qu'ils puissent mieux comprendre comment leur coopération pourra déboucher sur des investigations plus efficaces pour lutter contre le crime et assurer une meilleure protection des citoyens.

30. Définition des priorités – encourager les forces de l'ordre à définir des priorités dans leurs requêtes, notamment pour celles concernant les gros volumes de données, afin de permettre aux fournisseurs de services de traiter d'abord les plus importantes. La définition des priorités sera meilleure si elle est cohérente sur l'ensemble des forces de l'ordre au niveau national et si possible, au niveau international.

31. Justification des requêtes – encourager les forces de l'ordre à être conscientes des coûts que les requêtes impliquent pour les fournisseurs de services et d'accorder à ces derniers des délais de réponse suffisants. Les forces de l'ordre devraient être conscientes du fait que les fournisseurs de services pourront avoir à répondre à des requêtes provenant d'autres autorités publiques ; elles devraient être encouragées à surveiller les volumes sollicités.

32. Confidentialité des données – Il conviendrait que les forces de l'ordre assurent la confidentialité des données réceptionnées.

33. Éviter les coûts inutiles et de perturber le bon déroulement des activités – encourager les forces de l'ordre à éviter de susciter des coûts inutiles et de perturber le bon fonctionnement des activités des fournisseurs de services et autres.

34. Encourager les forces de l'ordre à limiter le recours aux points de contact d'urgence aux cas extrêmement urgents de façon à éviter un recours abusif à ce service.

35. Encourager les forces de l'ordre à faire en sorte que les mesures conservatoires et autres mesures provisoires soient suivies, dans les temps, de mesures de divulgation, ou que le fournisseur de services internet soit informé à temps du fait que les données conservées ne sont plus requises.

36. Requêtes internationales – encourager les forces de l'ordre nationales à ne pas adresser de requêtes directes aux fournisseurs de services internet non nationaux, mais de faire appel aux procédures décrites dans les traités internationaux, comme la Convention sur la cybercriminalité et le réseau 24/7 des points de contact d'application de la loi pour les mesures urgentes, et ce notamment pour les mesures conservatoires.

37. Requêtes d'assistance juridique mutuelle internationale – encourager les forces de l'ordre et l'administration de la justice à prendre les mesures nécessaires pour que les requêtes de mesures conservatoires soient suivies de procédures internationales en vue d'une assistance juridique mutuelle, ou d'informer le fournisseur de services internet à temps de la caducité des mesures de conservation des données.

38. Coordination entre forces de l'ordre – encourager les forces de l'ordre à coordonner leur coopération avec les fournisseurs de services internet et à échanger leurs bonnes pratiques au niveau national et international. Au niveau international, elles devraient faire appel aux organes représentatifs internationaux chargés de ces aspects.

39. Programmes de conformité juridique – encourager les forces de l'ordre à organiser les interactions susmentionnées avec les fournisseurs de services sous forme de programme de conformité juridique et à fournir une description de ce programme aux fournisseurs de services, avec les éléments suivants :

- les informations nécessaires pour contacter le personnel des forces de l'ordre désigné pour prendre en charge le programme de conformité juridique, ainsi que les horaires auxquels ce personnel peut être contacté ;
- les informations nécessaires pour que le fournisseur de services soit en mesure de fournir des documents aux responsables du programme de conformité juridique ;

-
- les autres informations spécifiquement destinées aux responsables de ce programme (comme par exemple, les modalités de coopération internationale d'un organe de répression, les documents à traduire dans des langues données, etc.).

40. Audit du système de conformité – encourager les forces de l'ordre à suivre et à auditer le système de traitement des requêtes à des fins statistiques, de manière à identifier les forces et les faiblesses du système et à en publier, le cas échéant, les conclusions.

Mesures à prendre par les fournisseurs de services

41. Coopération visant à réduire l'utilisation des services à des fins illicites – dans le respect des droits et des libertés, tels que la liberté d'expression, le respect de la vie privée et des autres lois nationales et internationales, ainsi que dans le respect des accords d'utilisation, il conviendrait d'encourager les fournisseurs de services à coopérer avec les forces de l'ordre afin de contribuer à la réduction de l'utilisation des services pour des activités criminelles telles que les définit le droit.

42. Encourager les fournisseurs de services à rendre compte aux forces de l'ordre des incidents illicites qui l'affectent et dont ils ont connaissance, sans que cela les oblige à rechercher activement les faits ou les circonstances indiquant l'existence d'activités illicites.

43. Encourager les fournisseurs de services à assister les forces de l'ordre en matière de formation et d'autres types de soutien portant sur leurs services et leur fonctionnement.

44. Suivi des requêtes émanant des forces de l'ordre – encourager les fournisseurs de services à réaliser tous les efforts raisonnables pour assister les forces de l'ordre dans l'exécution de leurs requêtes.

45. Procédures de réponse aux requêtes - encourager les fournisseurs de services à élaborer des procédures écrites, incluant les mesures appropriées d'application, pour le traitement des requêtes, et à faire en sorte que les requêtes font l'objet d'un suivi dans le respect des procédures agréées.

46. Formation – encourager les fournisseurs de services à s'assurer qu'ils ont apporté la formation appropriée à leur personnel responsable de la mise en œuvre de ces procédures.

47. Personnel et points de contact désignés – encourager les fournisseurs de services à désigner un personnel dûment formé pour faire office de point de contact pour la coopération avec les forces de l'ordre.

48. Assistance d'urgence – encourager les fournisseurs de services à mettre en œuvre les moyens permettant aux forces de l'ordre de contacter le personnel en charge de la conformité juridique en dehors des heures normales de travail, afin de répondre aux situations d'urgence ; encourager les fournisseurs de services à fournir aux forces de l'ordre les informations pertinentes en vue de l'assistance d'urgence.

49. Ressources – encourager les fournisseurs de services à fournir des points de contact ou du personnel responsable de la coopération avec les forces de l'ordre, dotés des ressources nécessaires pour répondre aux requêtes des forces de l'ordre.

50. Programmes de conformité juridique – encourager les fournisseurs de services à organiser leur coopération avec les forces de l'ordre sous forme de programmes généraux de conformité juridique, et à fournir une description de ces programmes aux forces de l'ordre, avec les éléments suivants :

- les informations permettant aux forces de l'ordre de contacter les responsables du programme de conformité juridique, ainsi que les horaires auxquels ils peuvent être contactés ;
- les informations permettant aux forces de l'ordre de fournir des documents aux responsables du programme de conformité juridique ;
- les autres informations spécifiquement destinées aux responsables du programme (par exemple, comment un fournisseur de services conduit ses activités dans plusieurs pays, les documents à traduire dans des langues données, etc.) ;
- afin que les forces de l'ordre puissent leur adresser des requêtes spécifiques et appropriées, encourager les fournisseurs de services à fournir des informations sur le type de service proposé aux utilisateurs, et notamment les liens vers les services et les informations complémentaires, ainsi que les détails de contact pour de plus amples informations ;
- encourager les fournisseurs de services internet à fournir la liste, lorsque c'est possible et sur demande des forces de l'ordre, des types de données pouvant être mis à disposition pour chaque service à la réception d'une requête de divulgation valide émanant des forces de l'ordre et acceptant que l'ensemble des données ne soit pas disponible pour toutes les enquêtes criminelles.

51. Vérification de la source des requêtes – encourager les fournisseurs de services à prendre les mesures nécessaires, dans la mesure du possible, pour vérifier l'authenticité des requêtes reçues des forces de l'ordre et lorsque c'est nécessaire, faire en sorte que les enregistrements de données relatives aux clients ne soient pas divulguées à des personnes non autorisées.

52. Réponse – encourager les fournisseurs de services à répondre sous forme écrite (ou tout autre moyen électronique juridiquement acceptable) aux requêtes émanant des forces de l'ordre, à faire en sorte que les requêtes et les réponses soient dûment archivées, et tout en acceptant que ce traçage ne contienne aucune donnée personnelle.

53. Format de requête standard – encourager les fournisseurs de services à standardiser le format d'envoi d'informations aux forces de l'ordre, en tenant compte du format des requêtes employé par les forces de l'ordre.

54. Encourager les fournisseurs de services à traiter les requêtes dans un délai raisonnable, conformément aux procédures écrites définies par leurs soins, et de tenir les forces de l'ordre informées des délais moyens de réponse aux requêtes.

55. Validation des informations envoyées – encourager les fournisseurs de services à ce que les informations transmises aux forces de l'ordre soient complètes, précises et protégées.

56. Confidentialité des requêtes – il conviendrait que les fournisseurs de services assurent la confidentialité des requêtes reçues.

57. Explications pour les informations non fournies – encourager les fournisseurs de services à fournir aux forces de l'ordre émettrices d'une requête des explications dans les cas de rejet ou d'impossibilité de fournir des informations.

58. Audit du système de conformité – encourager les fournisseurs de services à suivre et à auditer le système de traitement des requêtes à des fins statistiques, de manière à identifier les forces et les faiblesses du système et d'en publier, le cas échéant, les conclusions.

59. Coordination entre fournisseurs de services – tout en gardant à l'esprit les lois antitrust et de la concurrence, il conviendrait d'encourager les fournisseurs de services à coordonner leur coopération avec les forces de l'ordre et à partager entre eux les bonnes pratiques, en faisant appel dans ce but, aux associations professionnelles de fournisseurs de services.

ANNEXE VI

Conférence Octopus Interface sur la coopération contre la cybercriminalité

Conseil de l'Europe, Strasbourg, France, 1-2 avril 2008

CONCLUSIONS DE LA CONFÉRENCE

La Conférence qui s'est tenue au Conseil de l'Europe à Strasbourg les 1er et 2 avril 2008 a réuni plus de 210 experts de la cybercriminalité, venant de 65 pays, organisations internationales et du secteur privé.

La Conférence :

- a examiné les menaces actuelles et prévues dans le domaine de la cybercriminalité, telles que les logiciels malveillants, le vol d'identité et autres formes de fraude, les réseaux de zombies (*botnets*) et attaques de déni de service, la pornographie mettant en scène des enfants et les abus sur les enfants, ainsi que les incidences des réseaux sociaux et des technologies telles que la voix sur réseau IP et les réseaux de nouvelle génération. La Convention sur la cybercriminalité, particulièrement pertinente ici, aborde de manière globale les défis liés à la cybercriminalité. Ce phénomène, en constante évolution, doit faire l'objet d'une surveillance attentive afin que les initiatives législatives et autres puissent être ajustées au niveau national et international, ainsi que dans le secteur privé ;

- a examiné l'efficacité de la législation sur la cybercriminalité. A ce propos, une nette tendance globale au renforcement de la législation, en suivant les grandes lignes de la Convention sur la cybercriminalité, a été observée dans tous les pays. Les pays qui ont signé ce traité ont été invités à en accélérer la ratification, et d'autres pays ont été encouragés à demander l'adhésion. Durant la Conférence, la Géorgie a signé la Convention sur la cybercriminalité, la République dominicaine a remis une demande d'adhésion et il a été annoncé que les Philippines étaient invitées à y adhérer. La Conférence a insisté sur le rôle du Comité de la Convention sur la cybercriminalité (T-CY) dans le suivi de la mise en œuvre de la Convention et de son protocole sur la xénophobie et le racisme ;

- a examiné les mesures de renforcement de la coopération internationale, notamment les points de contact 24/7, et d'amélioration de la coordination au niveau national. Les pays ont été encouragés à adhérer à la Convention et à l'utiliser en tant que cadre pour la coopération internationale. Il a été décidé que le Conseil de l'Europe et le Sous-groupe sur la criminalité de haute technologie du G8 tiendraient un répertoire commun des points de contact ;

- a adopté des lignes directrices sur la coopération entre les organes de répression et les fournisseurs de services internet dans les enquêtes relatives à la cybercriminalité. Ces lignes directrices peuvent maintenant être diffusées dans le monde entier afin

d'aider les organes de répression et les fournisseurs de services internet à structurer leur coopération. Il a été décidé que ces lignes directrices seraient soumises au Comité de la Convention sur la cybercriminalité pour examen ;

- a fait remarquer qu'il importe de trouver un juste équilibre entre la nécessité de renforcer la sécurité des technologies de l'information et de la communication d'une part, et la nécessité de renforcer la protection de la vie privée, des données à caractère personnel, de la liberté d'expression et des droits fondamentaux d'autre part.