Division de la criminalité économique
Direction Générale des
Droits de l'Homme et des affaire juridiques
Strasbourg, 12 décembre 2007
Final/public

Projet sur la cybercriminalité

Rapport d'avancement

Situation au 30 novembre 2007

Projet financé par le Conseil de l'Europe et Microsoft

Table des matières

Contact

Pour de plus amples renseignements, veuillez contacter:

Division de la criminalité économique
Direction Générale des Droits de l'Homme et des Affaires juridiques
Conseil de l'Europe
Strasbourg (France)

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

1 Contexte

En 2001, la Convention sur la cybercriminalité du Conseil de l'Europe a été adoptée et ouverte à la signature. Ce traité et le Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques aident les sociétés à faire face aux défis de la cybercriminalité en prévoyant :

- l'incrimination des cyber-infractions et, par conséquent, en garantissant un certain niveau d'harmonisation entre les pays
- des mesures procédurales pour permettre des enquêtes efficaces
- une coopération internationale efficace contre la criminalité.

Bien qu'ils aient été élaborés par le Conseil de l'Europe, la convention et son protocole servent de plus en plus dans n'importe quel pays du monde de lignes directrices pour l'élaboration d'une législation nationale et de cadre mondial pour la coopération contre la cybercriminalité.

Le projet contre la cybercriminalité a été conçu pour aider les pays dans leurs efforts visant à ratifier la Convention et son protocole ainsi que d'y adhérer et de les mettre en œuvre. Il a été lancé en septembre 2006 et devrait durer jusqu'en février 2009. L'objectif et les résultats attendus sont les suivants :

Objectif du projet :	promouvoir une large mise en œuvre de la Convention sur la cybercriminalité (STE 185) et son Protocole sur le racisme et la xénophobie (STE 189)
Résultat 1 :	rédiger des lois appliquant les normes de STE 5 et 189 disponibles dans au moins 10 pays européens et cinq pays non-européens
Résultat 2 :	renforcer les capacités d'enquête, de poursuite, et de sanction des systèmes de justice pénale
Résultat 3 :	renforcer les capacités des deux organes de justice pénale à coopérer au niveau international

Bien que ce projet ait disposé au départ d'un budget de 1,7 million d'euros, des contributions volontaires de Microsoft d'un montant de 270 000 euros (350 000 dollars en 2006 et 2007) et l'allocation jusqu'ici de 360 000 euros du budget du Conseil de l'Europe (2006-2008) lui ont permis de commencer à une échelle réduite.

Après un premier rapport d'avancement en mars 2007, le présent rapport résume les activités et les résultats obtenus à la fin novembre 2007 et fournit une liste actualisée des activités pour la période décembre 2007 - juin 2008.

2 Activités

2.1 Liste des activités

Date	*Lieu*	*Description*
Sept. 2006 – Fév. 2007		
31 Août - 1er sept 2006	Genève, Suisse	Participation à la réunion de l'Union Internationale des Télécommunications sur la cybersécurité et le spam: promotion de la Convention sur la cybercriminalité comme ligne directrice pour l'élaboration de législations nationales
17-19 oct. 2006	Rome, Italie	Appui à la 2e conférence de formation du réseau de points de contact 24/7 du G8
27-29 nov. 2006	Pitesti, Roumanie	Appui à la Conférence nationale de formation sur la cybercriminalité en Roumanie
29-30 nov. 2006	Lisbonne, Portugal	Séminaire international pour les pays lusophones sur le thème "Relever le défi de la cybercriminalité - Expérience, bonne pratique et propositions d'amélioration"
13-14 fév. 2007	Le Caire, Égypte	Réunions et avis législatifs pour faciliter l'adhésion à la Convention sur la cybercriminalité. Suivis par un examen du projet de loi sur la cybercriminalité en avril 2007
20-23 fév. 2007	New Delhi, Inde	Réunions et avis législatifs pour faciliter l'adhésion à la Convention sur la cybercriminalité. Suivis par un examen du projet d'amendements législatifs en mars 2007
Février 2007	Strasbourg	Analyse du projet de loi sur la cybercriminalité du Pakistan
6-7 février 2007	Kiev, Ukraine	Conférence régionale pour les pays d'Europe orientale sur la coopération contre la cybercriminalité (financée par le projet UPIC sur la coopération internationale en matière pénale)
27 février – 2 mars 2007	Brasilia, Brésil	Réunions et avis législatifs pour faciliter l'adhésion à la Convention sur la cybercriminalité
Mars – novembre 2007		
19–21 mars 2007	Belgrade, Serbie	Conférence régionale pour les pays de l'Europe du sud-est sur la coopération contre la cybercriminalité (financée par le projet PACO-Serbie sur la criminalité économique)
26-27 mars 2007	Bucarest, Roumanie	Appui à deux séminaires de formation pour les procureurs (Institut national de la magistrature de Roumanie)
18-20 avril 2007	Afrique du Sud	Réunions pour promouvoir la ratification de la Convention sur la cybercriminalité et de son Protocole et participation au "Colloque sur la sécurité en ligne et sûreté et bien-être des citoyens d'Afrique du Sud" organisées par Microsoft

23–24 avril 2007	Philippines/ Asie et Pacifique	Promotion de la législation sur la cybercriminalité conformément à la Convention sur la cybercriminalité – Contribution à l'atelier sur la sécurité des réseaux organisé par la Coopération économique Asie-Pacifique et l'ASEAN à Manille, Philippines
11 mai 2007	Moscou (Fédération de Russie)	Réunion sur la mise en œuvre de la Convention sur la cybercriminalité en Fédération de Russie
14–15 mai 2007	Genève	Atelier sur la Convention sur la cybercriminalité dans le cadre de la série de manifestations liées au suivi du SMSI à l'UIT
Mai 2007	Strasbourg	Analyse du projet de loi sur la cybercriminalité des Philippines
18 juin 2007	Dubaï	Contribution à une réunion régionale des États du Conseil de coopération du Golfe
21 juin	Maroc	Réunions pour discuter de la législation sur la cybercriminalité et de l'adhésion à la Convention sur la cybercriminalité
11–12 juin 2007	Strasbourg	Conférence Octopus Interface sur "a coopération contre la cybercriminalité "
19-20 juin 2007	Casablanca (Maroc)	Formation de procureurs d'Afrique du Nord et du Moyen-Orient– Contribution au projet POGAR du PNUD
10 sept. 2007	New Delhi (Inde)	Conférence nationale sur la cybercriminalité (en coopération avec les ASSOCHAM)
12-14 sept. 200	New Delhi (Inde)	Contribution à la conférence mondiale d'Interpol sur la cybercriminalité
17 sept. 2007	Genève (Suisse)	Atelier de l'UIT
26-28 sept. 2007	Sao Paulo (Brésil)	ICCYBER 2007: Conférence internationale sur la cybercriminalité
28 sept. 2007	Sao Paulo (Brésil)	Réunion avec le Groupe de direction de l'Internet du Brésil
28 sept. 2007	Sao Paulo (Brésil)	Atelier de formation pour les procureurs
Oct. 2007	Strasbourg	Lancement d'études sur la cybercriminalité
1er -2 oct. 2007	Colombie	Atelier national Workshop sur la législation sur la cybercriminalité
2 oct. 2007	Lyon (France)	Groupe de travail européen d'Interpol
5 oct. 2007	Genève (Suisse)	Réunion du Groupe d'experts de haut niveau de l'UIT
9-11 oct. 2007	Washington (États-Unis)	3e atelier conjoint Plan d'Action de Londres/ Réseau de contact européen des autorités spam
12 oct. 2007	Bruxelles	Réunion avec eBay
22 oct. 2007	Paris	Étude sur la coopération entre les autorités de répression et les fournisseurs de services: première réunion du groupe de travail
24-26 oct. 2007	Heerlen (Pays-Bas)	Conférence du réseau européen police scientifique et sécurité

25-26 oct. 2007	Makati City (Philippines)	Ateliers pour législateurs et experts sur la cybercriminalité
26-27 oct. 2007	Vérone (Italie)	Conférence internationale "Criminalité informatique et cybercriminalité: infractions mondiales, réponses mondiales "
29-31 oct. 2007	Jakarta (Indonésie)	Réunions sur la législation sur la cybercriminalité pour l'Indonésie
5-9 nov. 2007	Bangkok (Thaïlande)	Sommet international sur la police du cyberespace
7-9 nov. 2007	Tomar (Portugal)	Contribution à la "Conférence sur la fraude et le vol d'identité " organisée par les autorités portugaises dans le contexte de la Présidence de l'UE
7-9 nov. 2007	La Haye	Réunion des experts d'Europol sur la criminalité de haute technologie
12-16 nov. 2007	Rio de Janeiro (Brésil)	Forum sur la gouvernance d'Internet
15-16 nov. 2007	Bruxelles	Conférence des experts de la Commission européenne sur la cybercriminalité
15-16 nov. 2007	Buenos Aires (Argentine)	Atelier sur la législation sur la cybercriminalité et l'adhésion à la Convention
19-20 nov. 2007	Washington (États-Unis)	Organisation des États Américains
26-27 nov. 2007	Le Caire (Égypte)	Conférence régionale sur la cybercriminalité
30 nov.-2 déc.	Courmayeur (Italie)	Contribution à la Conférence ISPAC des Nations Unies sur le défi croissant de la fraude d''identité

2.2 Coopération avec les pays et les régions

2.2.1 Région arabe

Le Conseil de l'Europe a contribué à un atelier régional sur la cybercriminalité pour les procureurs de la région arabe (Casablanca, Maroc, 19 et 20 juin 2007), organisé par le programme POGAR du Programme des Nations Unies pour le Développement. Il a fourni des informations utiles concernant l'état de la législation sur la cybercriminalité dans cette région (Bahreïn, Égypte, Jordanie, Liban, Maroc, Émirats arabes unis et Yémen) et éveillé l'intérêt pour la Convention.

Un résultat immédiat a été une demande d'examen du projet de législation du Maroc, ; cet examen est en cours.

Une conférence sur la lutte contre la cybercriminalité dans les pays du Conseil de coopération du Golfe (CCG) s'est tenue à Abou Dhabi le 18 juin 2007. Elle était organisée par le Ministère de la justice des Émirats arabes unis en coopération avec Microsoft et avec la participation de responsables de haut niveau. Elle a mis l'accent sur les approches du CCG dans la lutte contre la cybercriminalité. Un consultant du Conseil de l'Europe a présenté la Convention sur la cybercriminalité qui est reproduite dans les conclusions.

Quelque 400 représentants d'institutions des secteurs public et privé de la région arabe et d'autres pays ainsi que d'organisations non-gouvernementales et d'organismes internationaux ont participé à la première conférence régionale sur la cybercriminalité tenue au Caire les 26 et 27 novembre 2007. Cette conférence s'est tenue sous les auspices de Ahmed Fathy Sorour, président du Parlement égyptien, et a été ouverte par Tarek Kamel, Ministre des communications et des technologies de l'information. Elle a été organisée par

l'Association égyptienne pour la prévention de la criminalité informatiques et Internet et soutenue par l'Agence pour le développement de l'industrie de la technologie de l'information (ITIDA), le Conseil de l'Europe, l'Office des Nations Unies contre la drogue et le crime, Microsoft, l'université Aïn, IRIS, EASCIA et d'autres partenaires.

La déclaration adoptée à l'issue de la conférence contenait un appel vigoureux invitant les pays à mettre en œuvre Convention sur la cybercriminalité :

> *Les participants prennent note avec satisfaction des efforts déployés en Égypte et dans d'autres pays de la région arabe concernant le renforcement de la législation sur la cybercriminalité. Ces efforts devraient bénéficier d'un degré élevé de priorité et aboutir dès que possible pour protéger les sociétés de cette région contre la menace de la cybercriminalité.*
> *La convention de Budapest (2001) sur la cybercriminalité est reconnue comme la ligne directrice mondiale pour l'élaboration d'une législation en ce domaine. Les pays de la région arabe sont encouragés à faire usage de ce modèle lors de l'élaboration de règles de fond et de procédure.*

2.2.2 Argentine

Une mission du Conseil de l'Europe s'est rendue à Buenos Aires les 15 et 16 novembre 2007. Elle a participé à une série de réunions bilatérales avec de hauts responsables et des homologues et - le 16 novembre - à un atelier organisé avec le soutien de la faculté de droit de l'université de Buenos Aires. Cette manifestation a réuni environ 40 experts/professionnels (principalement du ministère des affaires étrangères, du ministère public fédéral, des institutions d'application des lois et institutions judiciaires, de juristes pénalistes, de professeurs d'université, du Parlement, de membres de groupes de travail rédigeant la législation et de fournisseurs de services du secteur privé).

Les deux principaux résultats ont été un vif soutien à l'adhésion de l'Argentine à la Convention (que tout le monde estime possible au premier semestre de 2008) et un premier examen systématique (suivi par une discussion) de la législation sur la cybercriminalité tenant compte des dispositions de la Convention.

À la fin de novembre 2007, le Sénat a adopté des amendements à la loi pénale concernant la cybercriminalité.

Conséquence directe, le ministère de la justice enverra prochainement une demande au Conseil de l'Europe pour qu'il fasse une expertise juridique du projet de loi sur la criminalité avec les amendements introduits par le Sénat avant examen et adoption par la Chambre des députés. En ce qui concerne le droit procédural, une proposition d'amendement à la loi sur la procédure pénale de l'Argentine a été préparée par un groupe de travail et peut maintenant être elle aussi examinée.

2.2.3 Brésil

En février 2007, le Conseil de l'Europe a aidé le Sénat fédéral à revoir et améliorer le projet de loi sur la cybercriminalité. En juin 2007, le sénateur Azevedo et ses collaborateurs s'est rendu à Strasbourg et a participé à la conférence Octopus Interface. À ce stade, la loi révisée allait être adoptée par le Sénat. Toutefois, devant les craintes exprimées par les fournisseurs de services d'autres auditions devaient être organisées.

En septembre, le Conseil de l'Europe a participé à une conférence internationale sur les enquêtes sur la cybercriminalité et la police scientifique appliquée aux cyberdélits (ICCYBER, Sao Paulo, 26 -28 septembre). Cette visite a également donné lieu à une table ronde avec le Groupe de direction d'Internet du Brésil qui a été l'occasion d'un dialogue entre fournisseurs de services, le gouvernement et un représentant du Sénat sur le projet de loi.

La visite a également été utilisée pour un séminaire de formation pour les procureurs spécialisés dans la cybercriminalité à Sao Paulo.

2.2.4 Colombie

En Colombie, un groupe de travail interorganisations dirigé par le Ministère des affaires étrangères travaille à un projet de loi sur la cybercriminalité. Les 1er et 2 octobre 2007 un atelier a été organisé à Bogotá pour revoir ce projet de loi avec l'aide d'experts du Conseil de l'Europe. Cet atelier très productif a abouti à des recommandations précises d'amélioration. Le groupe de travail a ensuite préparé une version révisée de la loi (envoyée au Conseil de l'Europe le 23 novembre 2007) et va maintenant engager un dialogue avec le Congrès sur cette question.

À la suite de cette visite, les autorités colombiennes envisagent également d'adhérer à la Convention.

2.2.5 Égypte

En février 2007, une mission du Conseil de l'Europe s'est rendue au Caire et en mai 2007 le Conseil de l'Europe a soumis une analyse écrite sur la conformité du projet de loi de l'Égypte intitulé « Réglementation de la protection des données et des informations électroniques et lutte contre les infractions en matière d'information » avec les prescriptions de la Convention sur la cybercriminalité du Conseil de l'Europe

Toutefois, entre mai et novembre 2007, il semble que peu de progrès aient été accomplis en ce qui concerne cette loi. Afin de lui donner une nouvelle impulsion, le Conseil de l'Europe a soutenu une conférence sur la cybercriminalité tenue au Caire les 26 et 27 novembre 2007 (voir ci-dessus). Le dialogue avec le Ministère des communications et des technologies de l'information sur cette loi devrait se poursuivre.

2.2.6 Inde

À la suite de la mission effectuée à New Delhi du 21 au 23 février 2007, une analyse détaillée des projets d'amendement à la loi sur la technologie de l'information a été envoyée à la Commission permanente sur la technologie de l'information du Parlement en mars. Le Parlement a ensuite organisé d'autres auditions et renvoyé son rapport au gouvernement début septembre. Ce rapport reflète certaines des observations faites par les experts du Conseil de l'Europe et fait référence à la Convention sur la cybercriminalité. Il appartient maintenant au gouvernement d'accepter ou non ces changements et de les incorporer dans une nouvelle version de la loi.

Afin de poursuivre le dialogue sur cette question, le projet a soutenu une conférence nationale sur la cybercriminalité qui s'est tenue à Delhi en septembre 2007 en coopération avec les chambres de commerce et d'industrie associées d'Inde (ASSOCHAM). Microsoft et eBay ont également soutenu cette manifestation.

Pour ce qui est du suivi, le dialogue avec le gouvernement, et particulièrement le Ministère des technologies de l'information et des communications devrait être poursuivi et une assistance directe devrait être proposée aux responsables de la rédaction de la nouvelle version de la loi. Le prochain Forum sur la gouvernance d'Internet qui se tiendra en Inde en décembre 2008 pourra faciliter les progrès vers l'adhésion de l'Inde à la Convention.

2.2.7 Indonésie

Une mission du Conseil de l'Europe s'est rendue à Jakarta du 29 octobre au 1er novembre 2007. Cette visite a été facilitée par Microsoft Indonésie.

Les discussions avec des représentants du Ministère des technologies de l'information et des communications, du Parlement et un certain nombre d'autres parties prenantes ont indiqué que la législation existante (code pénal, droit de la procédure pénale, loi sur les télécommunications et d'autres) ne pouvait être appliquée que dans une mesure limitée pour les enquêtes et les poursuites visant la cybercriminalité. Les efforts en cours pour élaborer un cadre juridique plus cohérent contre la cybercriminalité comprennent en particulier le «

Projet de loi sur l'information et les transactions électroniques », avec un chapitre VII sur les actions interdites et un chapitre XI sur l'interrogation, les poursuites et l'examen pendant la procédure judiciaire.

À la suite de la demande qui lui a été fait pendant la visite, le Conseil de l'Europe a préparé une analyse écrite du projet de loi contre les dispositions de la Convention en novembre 2007.

Le Conseil de l'Europe a également demandé la traduction de la Convention sur la cybercriminalité en bahasa indonesia pour aider les parties prenantes à mieux comprendre les conditions exigées.

2.2.8 Nigeria

Des représentants du Nigeria ont participé à la Conférence Octopus en juin 2007. D'autres contacts ont abouti à une demande d'analyse du projet de loi qui a été initié à la fin de novembre 2007.

2.2.9 Philippines

En avril 2007, le Conseil de l'Europe a participé à une réunion sur la cybercriminalité organisée par la Coopération économique Asie-Pacifique (APEC) et l'ASEAN à Manille Pendant cette réunion il a été prié par les autorités des Philippines d'examiner le projet de loi sur la cybercriminalité.

Au début du mois de juin, une analyse détaillée a été envoyée à Manille, et le même mois les Philippines ont participé à la conférence Octopus sur la cybercriminalité à Strasbourg.

Le résultat a été qu'en septembre 2007 les Philippines ont envoyé une lettre au Secrétaire général du Conseil de l'Europe en vue de leur adhésion à la Convention sur la cybercriminalité. Les consultations prévues par l'article 37 de la Convention sont en cours.

Les 25 et 26 octobre 2007 un atelier a été organisé à Makati City (Manille) par le Ministère de la justice, la Commission pour les technologies de l'information et des communications des Philippines et le Conseil de l'Europe avec l'appui de Microsoft, auquel a participé une soixantaine de représentants d'institutions publiques et privées.

Le projet de loi examiné pendant l'atelier était une version actualisée de celui qui avait été revu par les experts du Conseil de l'Europe en avril/mai 2007, et il constitue déjà une très bonne base. Les discussions ont abouti à un certain nombre de propositions d'améliorations complémentaires. Si ces propositions sont prises en compte, les Philippines auront une loi sur la cybercriminalité qui pourra servir d'exemple à d'autres pays d'Asie.

2.2.10 Roumanie

Appui à la conférence nationale de formation sur la cybercriminalité en Roumanie (Pitesti, 27 29 novembre 2006) : Le projet a fourni un cofinancement limité à une conférence organisée en Roumanie par le ministère de l'intérieur pour les enquêteurs de la police, les procureurs et les juges (Pitesti, Roumanie, 27 29 novembre 2006). Une centaine d'enquêteurs, de procureurs et de juges de différentes régions de la Roumanie ont été formés pour pouvoir mettre en œuvre la législation sur la cybercriminalité adoptée en 2004 lorsque la Roumanie a ratifié la Convention sur la cybercriminalité. Cette conférence a bénéficié d'un fort soutien international comme en témoigne la participation de responsables de l'étranger de l'application des lois (en particulier des États-Unis), des représentants du secteur privé (y compris Microsoft), d'Europol et du Conseil de l'Europe. La Roumanie a pris d'importantes mesures contre la cybercriminalité en adoptant une législation (en 2004) et en créant des services spécialisés au sein du Ministère de l'intérieur et du ministère public. Une formation complémentaire, en particulier des juges, sera nécessaire.

La conférence de formation à l'Institut national de la magistrature (26 27 mai 2007, Bucarest, Roumanie) a fait suite à celle qui s'était tenue en 2006. Les participants étaient des

juges, des procureurs et les experts qui avaient été choisis pour travailler comme formateurs pour des activités de formation complémentaire à la cybercriminalité. La présentation de l'expert du Conseil de l'Europe était en rapport avec la Convention sur la cybercriminalité et mettait l'accent sur les dispositions de droit pénal matériel.

2.2.11 Fédération de Russie

La Fédération de Russie n'a pas encore signé la Convention en raison de préoccupations liées à l'article 32. Une mission du Conseil de l'Europe s'est rendue à Moscou en mai 2007 pour donner des explications sur cet article et des discussions ont eu lieu par la suite à Strasbourg. Ces clarifications ont semblé satisfaisantes et devraient aider les autorités russes à avancer vers la signature et la ratification de la Convention dans l'avenir proche.

2.2.12 Serbie

Le Conseil de l'Europe fournit des soutiens intensifs à la Serbie en vue de l'élaboration d'une législation sur la cybercriminalité, du renforcement des capacités en matière de répression et de justice pénale pour les enquêtes et les poursuites visant la cybercriminalité, promouvoir la coopération internationale et l'adhésion à la Convention sur la cybercriminalité.

Ces activités ne sont pas financées par le projet sur la cybercriminalité mais par le projet PACO-Serbie contre la criminalité économique du Conseil de l'Europe et l'Agence européenne pour la reconstruction. Elles sont néanmoins mises en œuvre comme contribution aux objectifs de ce projet.

Les activités au cours de la période considérée ont compris entre autres l'organisation d'une conférence régionale sur la cybercriminalité (voir ci-dessous), la préparation d'un manuel pour les enquêtes sur la cybercriminalité pour les services d'application des lois et l'appareil judiciaire, une expertise sur l'harmonisation des dispositions du code de pénal et du code de procédure pénale serbe avec les normes internationales dans le domaine de la cybercriminalité, suivie d'une table ronde avec les membres du groupe de travail et les homologues serbes compétents pour présenter et discuter les résultats, la participation d'experts et de praticiens serbes à la conférence Octopus sur la criminalité organisée par le Conseil de l'Europe en juin 2007, deux formations techniques d'une semaine sur la cybercriminalité pour un total de 80 praticiens et la participation de six représentants (des ministères de l'intérieur et de la justice, de la Direction pour la prévention du blanchiment d'argent, du tribunal de district et du ministère public) au séminaire international sur la lutte contre le financement du terrorisme (Suisse, 15 17 octobre 2007).

Dans les mois qui viennent, des séances de formation spécialisées supplémentaires seront organisées pour des praticiens sur des thèmes tels que les enquêtes de police scientifique, l'équipe d'intervention en cas d'urgence informatique (CERTC) et le système de repérage des exploiteurs d'enfants (CETS).

2.2.13 Afrique du Sud

En avril 1007, une mission du Conseil de l'Europe s'est rendue en Afrique du Sud pour examiner l'état de la mise en œuvre de la Convention sur la cybercriminalité et pour contribuer à un colloque sur la sécurité informatique et l'exploitation des enfants organisé par Microsoft.

L'Afrique du Sud a participé à l'élaboration de ces instruments et signé la Convention en novembre 2001. Toutefois le Protocole n'a pas encore été signé et la Convention n'est pas encore ratifiée. La visite a aidé à remettre ces points à l'ordre du jour du Ministère de la justice de manière que la ratification de la Convention et la signature du Protocole puissent intervenir dans l'avenir proche.

Les autorités sud-africaines sont d'avis - confirmé par un certain nombre d'enquêtes couronnées de succès. - que la base légale minimum existe depuis l'adoption de la loi 25 de 2002 sur les communications et les transactions électroniques et de la loi 70 de 2002 sur la

réglementation de l'interception des communications et la fourniture d'informations liées aux communications.

Le chapitre XIII de la loi 25 de 2002 sur les communications et les transactions électroniques incrimine l'accès non autorisé aux données, l'interception des données ou les interventions sur les données - ce qui comprend l'abus de dispositifs (article 86), l'extorsion, la fraude et la falsification informatiques (article 87) ainsi que la tentative, l'aide et la complicité. Bien que la loi 25 définisse ces infractions pénales, nombre de ses autres dispositions ne sont toujours pas appliquées, y compris la désignation cyberinspecteurs (Chapitre XII) disposant de pouvoirs d'enquête étendus. Dans la pratique le Service de police d'Afrique du Sud (SAPS) applique le code de procédure pénale et d'autres lois pour enquêter sur la cybercriminalité. Les principales dispositions manquantes semblent être la possibilité d'une préservation rapide des données.

La pornographie enfantine est couverte par la loi sur les films et publications de 1996. Elle inclut l'impression qu'une personne est un mineur ainsi que les images morphées.

Ces dispositions devraient permettre à l'Afrique du Sud de ratifier la Convention et le Protocole mais avec le temps il sera peut-être nécessaire néanmoins d'améliorer la législation.

Des représentants de l'Afrique du Sud ont participé à la conférence Octopus à Strasbourg en juin et informé que la Convention allait être soumise au Parlement pour qu'il en approuve la ratification ; la signature du Protocole fera l'objet d'une procédure distincte.

2.2.14 Europe du Sud-Est

Une conférence régionale sur la cybercriminalité s'est tenue à Belgrade du 19 au 21 mars 2007 dans le cadre du projet PACO-Serbie sur la criminalité économique.

Y ont participé des représentants de 16 pays et d'organisations internationales ainsi que d'organismes du secteur privé. Les participants ont examiné l'état actuel de la législation sur la cybercriminalité, le fonctionnement de la coopération internationale contre la cybercriminalité, y compris la création de points de contact 24/7, les questions liées aux enquêtes et aux poursuites visant la cybercriminalité, ainsi que les partenariats public-privé.

Ces questions ont été discutées dans le contexte de la Convention sur la cybercriminalité du Conseil de l'Europe (STE 185) et du Protocole additionnel sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE 189). Sur les 19 pays qui étaient alors parties à la Convention, neuf ont participé à la conférence, à savoir l'Albanie, la Bosnie-Herzégovine, la Bulgarie, la Croatie, la France, la Hongrie, la Roumanie, la Slovénie et l'ex-République yougoslave de Macédoine.

En Serbie, des mesures sont prises pour modifier la législation pénale, et le processus de ratification de la Convention devrait être achevé dans l'avenir très proche. Les autres pays qui ont participé ou contribué à la conférence, à savoir l'Allemagne, l'Italie, la Moldova, le Monténégro, la Turquie et le Royaume-Uni, ont été encouragés à ratifier la Convention dès que possible.

Les discussions sur l'état de la législation sur la cybercriminalité ont montré que les pays participants avaient introduit ces dernières années une série de mesures de fond et de procédure qui satisfaisaient à nombre des conditions de la Convention, comme en témoigne l'exemple de la Roumanie. Il est encore nécessaire dans certains pays d'harmoniser la législation nationale avec la Convention. Cela est vrai en particulier pour la coopération internationale et les dispositions du droit procédural. Le Conseil de l'Europe a été prié d'appuyer des ateliers sur la législation sur la cybercriminalité en Albanie, Bosnie-Herzégovine, Bulgarie et dans l'ex-République yougoslave de Macédoine.

En ce qui concerne les enquêtes, les poursuites et les sanctions visant la cybercriminalité, des progrès considérables ont été faits en termes de spécialisation et de compétences. Les bonnes pratiques sont illustrées par les exemples de la France, de l'Italie, de la Roumanie et

du Royaume-Uni. Des efforts importants sont également déployés en Serbie - où un procureur et des sections des tribunaux chargés de la cybercriminalité ont été désignés et où la création d'un service d'enquêtes sur la cybercriminalité est en cours - et d'autres pays de l'Europe du sud-est. Une formation et une spécialisation complémentaires sont nécessaires non seulement pour les enquêteurs mais aussi pour les procureurs et les juges.

La création de points de contact 24/7 a été considérée comme un moyen très utile de faciliter la coopération internationale, comme le montre l'expérience du réseau 24/7 du G8 et comme le demande l'article 35 de la Convention sur la cybercriminalité. De tels points de contact ont été créés dans la plupart des pays participants, dont la Bulgarie, la Croatie, la France, la Hongrie, l'Italie, l'ex République yougoslave de Macédoine, la Roumanie, le Royaume-Uni, et la Slovénie. La Serbie a désigné un point de contact temporaire. La création d'un point de contact est en cours en Albanie. La Bosnie-Herzégovine est encouragée à prendre une décision dans l'avenir très proche.

La nécessité de partenariats public-privé a été clairement reconnue par tous les participants. Des présentations faites par des représentants de l'Association des fournisseurs de services Internet de la Serbie et de Microsoft ont indiqué les possibilités que de tels partenariats peuvent offrir aux institutions publiques et privées.

Pour résumer, les participants ont souligné la nécessité-il d'une base juridique claire et d'une coopération efficace contre la cybercriminalité à tous les niveaux - national, interorganisations, public-privé et international - et l'importance de la Convention sur la cybercriminalité et de son Protocole à cet égard. L'échange d'expériences et les contacts établis pendant la conférence ont aidé à renforcer cette coopération.

2.2.15 Ukraine

Dans le cadre du projet sur la coopération internationale en matière pénale en Ukraine (UPIC) du Conseil de l'Europe et de la Commission européenne, le Conseil de l'Europe a organisé une conférence internationale sur la coopération contre la cybercriminalité à Kiev (Ukraine) les 6 et 7 février. Y ont participé des représentants de l'Estonie, de la France, de l'Italie, de la Lettonie, de la Lituanie, de la Fédération de Russie, des Pays-Bas, de la Roumanie et de l'Ukraine, d'organisations internationales et d'organisme du secteur privé.

En Ukraine, certaines dispositions de fond et de procédure de la législation nationale ne sont pas encore harmonisées avec la Convention. Les droits, les pouvoirs et les obligations des autorités chargées de la répression lois et des fournisseurs de services, y compris la responsabilité des personnes juridiques et les dispositions relatives à la préservation rapide des données devraient être précisés davantage pour faciliter la coopération entre le secteur public et le secteur privé. Ces questions ont été identifiées et devraient être abordées par les autorités ukrainiennes responsables.

En ce qui concerne les enquêtes et les poursuites visant la cybercriminalité, il y a un besoin évident de spécialisation et de création d'unités sur la cybercriminalité ou la criminalité de haute technologie, comme le montrent les exemples de la France, de l'Italie et de la Roumanie présentés pendant la conférence. En Ukraine, divers types de cyberinfractions ont fait l'objet d'enquêtes et ont été déférées au tribunal. Toutefois, les capacités des unités existantes auraient besoin d'être encore renforcées.

La création de points de contact 24/7 est considérée comme un moyen très utile de faciliter la coopération internationale, comme le montre l'expérience du réseau 24/7 du G8 et comme l'exige l'article 35 de la Convention sur la cybercriminalité. L'Ukraine n'a pas encore de tel point de contact, mais devrait en créer un dès que possible pour répondre aux exigences de la Convention.

2.3 Coopération avec d'autres organisations

2.3.1 Au niveau mondial : Conférence Octopus Interface sur la coopération contre la cybercriminalité (Strasbourg, juin 2007)

Plus de 140 experts en cybercriminalité provenant de quelque 55 pays, d'organisations internationales et du secteur privé se sont réunis au Conseil de l'Europe à Strasbourg les 11 et 12 juin 2007 pour :

- analyser la menace de la cybercriminalité
- vérifier l'efficacité de la législation sur la cybercriminalité
- promouvoir la mise en œuvre de la Convention sur la cybercriminalité et de son Protocole comme ligne directrice pour le développement de législations nationales, et encourager la ratification large et rapide et l'adhésion à ces traités
- renforcer la coopération entre différentes initiatives en permettant aux parties prenantes d'exploiter plus efficacement les possibilités qui existent et d'en explorer de nouvelles.

Un ensemble complet de recommandation a été adopté à l'issue de la conférence. Celle-ci a offert une tribune à de nombreuses organisations et initiatives qui ont pu partager leurs expériences et leurs bonnes pratiques, à savoir : le Forum sur la gouvernance d'Internet, Digital Rights Europe, la Commission européenne, ENISA, l'Organisation des États Américains, Interpol, la Coopération économique Asie-Pacifique, InHope, le Centre international pour les enfants disparus et exploités, l'Organisation de la conférence islamique et le Programme des Nations Unies pour le Développement. Les initiatives et les représentants du secteur privé comprenaient Microsoft, le groupe de travail contre le hammeçonnage (Anti-Phishing Working Group), FIRST/CERT USA, le Plan d'action de Londres et d'autres encore.

Un atelier a été organisé conjointement avec le Sous-groupe sur la criminalité de haute technologie du G8, avec la participation des points de contact 24/7 de plus de 25 pays.

L'impact spécifique de la conférence comprend la fusion des registres des points de contact 24/7 du G8 et du Conseil de l'Europe, l'intensification de la coopération avec les Philippines et de nombreux autres pays en vue de leur adhésion, l'octroi du statut d'observateur au Plan d'action de Londres, des études spécifiques sur la législation sur la cybercriminalité, la coopération entre les autorités de répression et les fournisseurs de services, une coopération plus intensive avec la Commission européenne, et d'autres encore.

Pour résumer, cette conférence a donné une nouvelle impulsion importante et un surcroît de crédibilité aux efforts de lutte contre la cybercriminalité du Conseil de l'Europe.

2.3.2 Coopération économique Asie-Pacifique

Le Conseil de l'Europe a été invité à présenter la Convention sur la cybercriminalité à un atelier de l'APEC/ASEAN sur la cybercriminalité lors de la 35e réunion du groupe de travail sur les télécommunications de l'APEC à Manille (Philippines) en avril 2007. Cette présentation a suscité l'intérêt des pays d'Asie du Sud-Est et une demande immédiate d'assistance législative de la part des Philippines, qui ont ensuite fait une demande d'adhésion à la Convention. Ce pourrait également être le point de départ d'une coopération plus poussée avec l'ASEAN.

2.3.3 Conférence du réseau européen police scientifique et sécurité

Le Conseil de l'Europe a été invité à participer avec un orateur principal à cette première conférence organisée par l'université de Zuyd (Pays-Bas) du 24 au 26 octobre 2007, qui a réuni de nombreux experts de l'application des lois, des universitaires, de hauts responsables de sociétés telles que Capgemini ou Symantec et d'autres entreprises de haute technologie.

Dans le prolongement de cette conférence, le Conseil de l'Europe a déjà été invité à participer à la conférence de l'année prochaine qui mettra l'accent sur sa dimension européenne. Selon le financement disponible, des conférences de ce type pourraient être tenues par les organisateurs et le Conseil de l'Europe ailleurs en Europe, par exemple en Europe du sud-est et en Russie où il est nécessaire de faire œuvre de sensibilisation, de constituer des réseaux et d'échanger les meilleures pratiques entre responsables, praticiens des autorités de répression et de l'appareil judiciaire, universitaires, organisations internationales et secteur privé.

2.3.4 Union européenne (présidence portugaise) et Commission européenne

Du 7 au 9 novembre 2007, le Ministère de l'intérieur du Portugal a tenu une conférence sur « la fraude et le vol d'identité – la logistique de la criminalité organisée » à Tomar (Portugal) dans le cadre de la Présidence portugaise de l'Union européenne. Le Conseil de l'Europe a été invité à parrainer un atelier sur « La cybercriminalité et le vol d'identité ». La conférence a montré l'importance de la Convention sur la cybercriminalité pour les enquêtes et les poursuites visant le vol d'identité au moyen de systèmes informatiques. Elle a été l'occasion de rappeler aux États membres de l'Union européenne la nécessité d'accélérer la ratification de la Convention dans la mesure où moins de la moitié d'entre eux l'ont fait jusqu'à présent.

La participation à cette conférence a également été importante compte tenu de la proposition de la Commission européenne d'élaborer une législation sur le vol d'identité (voir Communication sur la cybercriminalité de mai 2007) et des activités de l'Office des Nations Unies contre la drogue et le crime concernant le vol d'identité.

La communication sur la cybercriminalité de la Commission européenne (mai 2007) et les conclusions du Conseil du 8/9 novembre 2007 exprimant le soutien énergique à la Convention sur la cybercriminalité en Europe et ailleurs dans le monde est une bonne base de coopération solide entre le Conseil de l'Europe et la Commission européenne.

> *2127e réunion du Conseil*
> *Justice et Affaires intérieures*
> *Bruxelles, 8 et 9 novembre 2007*
>
> *4) met l'accent sur la confiance placée dans la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, soutient et encourage la mise en œuvre des mesures qui y sont prévues et demande la participation la plus large possible de tous les pays;*
> *5) juge extrêmement important de favoriser la coopération avec des pays tiers dans le cadre de la prévention de la cybercriminalité et de la lutte contre celle-ci, compte tenu notamment du rôle pivot joué par la Convention du Conseil de l'Europe sur la cybercriminalité, par la promotion, en liaison avec le Conseil de l'Europe, de l'introduction de ce cadre juridique à vocation universelle, notamment dans les pays qui reçoivent une aide au développement et une assistance technique;*

Le Conseil de l'Europe a participé à la conférence sur la cybercriminalité organisée par la Commission européenne à Bruxelles les 15 et 16 novembre. La réunion a souligné la nécessité de mettre en œuvre la Convention. Elle a également fait référence à la nécessité d'une coopération entre les autorités de répression et les fournisseurs de services dans les enquêtes sur la cybercriminalité (et à l'étude en cours sous les auspices du Conseil de l'Europe) et au réseau des points de contact 24/7.

2.3.5 Europol

Europol a participé à la conférence Octopus en juin 2007. L'évaluation de la menace de la cybercriminalité qu'il a publiée en août 2007 (« criminalité de haute technologie à l'intérieur de l'Union européenne ») comprend une recommandation concernant la mise en œuvre de la Convention sur la cybercriminalité et reconnaît que les conférences Octopus Interface constituent une plate-forme de coopération entre les différentes parties prenantes.

Le Conseil de l'Europe a participé à la réunion annuelle des experts d'Europol sur la criminalité de haute technologie tenue à la Haye du 6 au 8 novembre 2007, qui a réuni entre autres des experts de la plupart des États membres de l'Union européenne, de la CE, des États-Unis d'Amérique, d'Interpol, de sociétés privées (Microsoft, EBay, Paypal, Skype) et de sociétés spécialisées dans les télécommunications (KPN).

Dans une séance de l'atelier consacrée à la coordination de la formation tenue le 6 novembre, le Conseil de l'Europe a présenté les activités de formation organisées dans le cadre du projet sur la cybercriminalité.

À l'ouverture de la session plénière le 7 novembre, les organisateurs de la réunion ont invité le Conseil de l'Europe à faire une présentation sur l'état de la Convention sur la cybercriminalité et les activités liées à la cybercriminalité. Cette présentation a été suivie de plusieurs questions liées aux dispositions de la Convention et à l'état des signatures et ratifications.

À titre de suivi, Europol le Conseil de l'Europe continueront d'intensifier leurs efforts communs, en particulier pour développer une compréhension commune et la coopération entre les autorités de répression et le secteur privé pendant les enquêtes.

2.3.6 Groupe de travail du G8 sur la criminalité de haute technologie : Réseau des points de contact 24/7

La Convention sur la cybercriminalité prévoit la création de points de contact qui devraient être joignables 24 heures sur 24, sept jours sur sept, afin de faciliter la coopération internationale dans les enquêtes sur la cybercriminalité. La disposition correspondante de la Convention est fondée sur l'expérience du réseau 24/7 du G8 créé en 1997 et comprend actuellement une cinquantaine de pays.

Le projet a soutenu la deuxième conférence de formation du réseau 24/7 du G8 (Rome, 17-19 octobre 2006) et parrainé la participation de représentants de la Bulgarie, de la Roumanie, de la Turquie et de l'Ukraine à cette conférence. Cette dernière a comporté une séance sur la Convention sur la cybercriminalité et a aidé ainsi à promouvoir ce traité dans une cinquantaine de pays européens et non-européens. La réunion a contribué en outre à préciser que les points de contact 24/7 du réseau du G8 devraient être compatibles avec ceux créés en vertu de la Convention. Elle a ainsi renforcé la compréhension commune du G8 et du Conseil de l'Europe sur cette question.

La conférence Octopus Interface de juin 2007 a comporté également un atelier pour les points de contact, organisé conjointement avec le Groupe de travail du G8 sur la criminalité de haute technologie, qui a abouti à une proposition de fusionner les registres des points de contact du Conseil de l'Europe avec ceux du G8. La proposition a été acceptée en novembre 2007. Des détails et des procédures précises doivent maintenant être élaborés pour la tenue du registre.

2.3.7 Union internationale des télécommunications

Le Sommet mondial de la société de l'information a chargé l'UIT, entre autres, de faciliter le suivi des questions liées à la cybersécurité. Le Conseil de l'Europe a ainsi contribué à la réunion de suivi tenue à Genève en mai 2007, qui a comporté un atelier consacré à la Convention sur la cybercriminalité et à la facilitation des discussions en groupe.

Au cours de la même réunion, le Secrétaire général de l'UIT a présenté la stratégie de cybersécurité et appelé notamment à l'élaboration de lois types pour assurer l'interopérabilité en l'absence de cadres juridiques internationaux. La Convention sur la cybercriminalité a été passée sous silence.

En outre, l'UIT a décidé d'organiser de son propre chef une réunion au Vietnam en août 2007, alors qu une réunion conjointe Conseil de l'Europe/ONUDC/UIT était prévue depuis octobre 2006.

D'un autre côté, le conseil de l'Europe a été invité à l'atelier de l'UIT sur les cadres d'action nationale organisé le 17 septembre 2007 à Genève. Les participants étaient des responsables de nombreux pays européens et non-européens (y compris du Moyen-Orient et d'Afrique).

La partie « loi type » de la stratégie de cybersécurité de l'UIT peut donner matière à controverse, mais les discussions sur cette question dans différentes instances (y compris le Forum sur la gouvernance d'Internet) ont aussi eu un effet positif dans ce sens qu'elles ont reconfirmé que la Convention sur la cybercriminalité était la ligne directrice mondiale pour la législation en la matière.

2.3.8 Forum sur la gouvernance d'Internet

Le Conseil de l'Europe a participé activement à la conférence du Forum de 2007 (Rio de Janeiro, 12-16 novembre 2007), où deux réunions ont été spécialement consacrées à la cybercriminalité :

-- un forum concernant les meilleures pratiques sur la Convention
-- un atelier sur les réponses législatives aux cybermenaces actuelles et futures.

Le Conseil de l'Europe a fait appel à des experts renommés d'Europe, d'Asie, d'Amérique du Sud et d'Afrique pour faire des présentations ou participer comme orateurs principaux à des discussions ouvertes. Il en est résulté que la Convention est apparue comme un instrument non seulement « européen » mais aussi mondial soutenu sur tous les continents. Les deux activités ont rassemblé un total d'environ 300 participants du monde entier.

Des officiels du Costa Rica, du Brésil et de l'Argentine ont fait part de leur volonté affirmée d'adhérer bientôt à la Convention, tandis que d'autres participants de pays tels que El Salvador, le Koweït, Israël, le Lesotho et la Tunisie et beaucoup d'autres ont exprimé un vif intérêt pour la Convention et pour un suivi bilatéral direct avec le Conseil de l'Europe.

Des contacts ont été établis par la Secrétaire générale adjointe du Conseil de l'Europe avec les autorités indiennes responsables du prochain Forum sur la gouvernance d'Internet à Delhi en décembre 2008. Cette manifestation pourrait contribuer à promouvoir l'adhésion à la Convention sur la cybercriminalité.

2.3.9 Interpol

Le Conseil de l'Europe et Interpol ont coopéré à plusieurs occasions. Le Conseil de l'Europe a, entre autres, participé à la réunion d'octobre du Groupe de travail européen sur la criminalité de haute technologie à Lyon.

Un événement important a été la 7e conférence internationale sur la cybercriminalité, réunion mondiale organisée par Interpol à New Delhi (Inde) du 12 au 14 septembre, à laquelle le Conseil de l'Europe a contribué. Une série de recommandations y ont été adoptées, dont la première avait trait à la Convention sur la cybercriminalité :

Les délégués à la 7e Conférence internationale sur la cybercriminalité ont recommandé:

- *Que la Convention sur la cybercriminalité du Conseil de l'Europe soit recommandée comme la norme internationale juridique et procédurale pour lutter contre la cybercriminalité. Les pays sont encouragés à y adhérer.*

2.3.10 Plan d'action de Londres (PAL)

Le Conseil de l'Europe a participé au troisième atelier conjoint PAL - CNSA (Réseau de contact européen des autorités spam) organisé à Washington du 9 au 11 octobre 2007. En

particulier, une séance sur la coopération transfrontalière en matière de répression – mobiliser les ressources des réseaux de répression internationaux, animée par la Federal Trade Commission des États-Unis, a permis au Conseil de l'Europe de faire une présentation sur la Convention et de mettre l'accent sur les dispositions de cette dernière visant à faciliter la coopération au niveau international. Etaient également représentés à cette séance le Ministère de la justice des États-Unis, le Commissariat à la protection de la vie privée du Canada, le CNSA et Microsoft.

Le Comité des ministres du Conseil de l'Europe a approuvé le 7 novembre 2007 la demande d'octroi du statut d'observateur du Plan d'action de Londres auprès de l'Organisation. Dans les mois qui viennent, cela permettra au Conseil de l'Europe d'instaurer une coopération et des activités plus étroites avec le Plan d'action de Londres : sensibilisation des sociétés privées et des fournisseurs de services Internet, échanges de bonnes pratiques, formation pour les autorités de répression et le corps judiciaire, mise en œuvre de procédures renforçant la coopération internationale.

2.3.11 Organisation des États Américains

L'OEA appuie la mise en œuvre de la Convention sur la cybercriminalité dans ses 34 États depuis plusieurs années. Le Conseil de l'Europe a participé à la réunion du groupe d'experts sur la criminalité de haute technologie à Washington les 19 et 20 novembre 2007. Cette réunion a donné de claires indications sur les progrès accomplis dans cette région en (dans des pays comme l'Argentine, le Brésil et la Colombie).

La République dominicaine a adopté en 2007 une nouvelle loi sur la cybercriminalité qui s'inspire largement de la Convention et elle pourra demander à adhérer à cette dernière lorsque le Congrès aura approuvé la ratification. Il est envisagé de tenir un atelier en février 2008 afin de donner une impulsion politique à cet égard.

Un certain nombre d'autres pays ont déclaré qu'ils souhaiteraient recevoir un appui du Conseil de l'Europe, notamment les Bahamas, le Mexique, le Nicaragua et le Pérou.

En outre, un accord de base a été conclu pour tenir une réunion conjointe OEA/Conseil de l'Europe sur la législation sur la cybercriminalité pour les 34 pays de l'OEA, si possible en juin 2008 à Carthagène (Colombie)

2.3.12 POLCYB

La société pour la police du cyberespace (POLCYB) a été enregistrée en juin 1999 comme société à but non lucratif. Elle a son siège en Colombie britannique (Canada) et son objectif est de renforcer les partenariats internationaux entre professionnels publics et privés pour prévenir et combattre les infractions dans le cyberespace (voir http://www.polcyb.org).

Le 7^{e} Sommet international annuel de la Société pour la police du cyberespace, qui s'est tenu à Bangkok (Thaïlande) du 5 au 9 novembre 2007, était organisé par POLYB en coopération avec l'Académie internationale pour le respect de la loi (ILEA), Bangkok et le Conseil de l'Europe. Il était également soutenu par le secteur privé.

Le Sommet a réuni plus de 100 participants du secteur public, travaillant tant dans le secteur public, en particulier dans les services de répression, que dans le secteur privé, pour débattre des perspectives internationales de la police et des principes pour lutter contre la cybercriminalité. Les trois premiers jours, les discussions ont porté sur un certain nombre de questions telles que la collaboration internationale, les poursuites sur la base de preuves numériques, l'exploitation des enfants, les enquêtes, les logiciels malveillants et les technologies émergentes. Des discussions sur la formation aux preuves numériques ont eu lieu les deux derniers jours.

L'importance de la Convention sur la cybercriminalité a été reconnue pendant les discussions et il a été convenu qu'il y avait grand besoin d'améliorer les lois et les procédures des États, compte tenu en particulier des normes contenues dans la Convention sur la cybercriminalité.

2.3.13 Office des Nations Unies contre la drogue et le crime

Le Conseil de l'Europe et l'ONUDC ont coopéré de manière constructive. Entre autres choses, le Conseil de l'Europe a facilité la participation de l'ONUDC à la conférence sur le vol d'identité organisée par les autorités portugaises (Tomar, novembre 2007) et contribué à une réunion sur le vol identité tenue à Courmayeur (Italie) fin novembre 2007. À son tour, le Conseil de l'Europe a été invité à participer à un groupe d'experts sur le vol d'identité de l'ONUDC (Courmayeur, Italie, 29 novembre-2 décembre).

Une réunion conjointe du Conseil de l'Europe, de l'ONUDC et de l'UIT, qui avait été prévue pour août 2007 au Vietnam, a été annulée, l'UIT ayant décidé de faire cavalier seul.

Il y a certainement des possibilités d'approfondir encore la coopération avec l'ONUDC dans le domaine de lutte contre la cybercriminalité en 2008.

2.4 Études

En octobre 2007 ont été lancées cinq études dans le cadre du projet sur la cybercriminalité. Elles doivent être terminées à temps pour la conférence Octopus et le Comité de la Convention sur la cybercriminalité la première semaine d'avril 2008 :

1. Rapport sur la situation de la cybercriminalité ("Menaces et tendances actuelles et adéquation de la réponse internationale ")	L'étude devrait fournir aux décideurs une analyse à jour des menaces et tendances actuelles de la cybercriminalité et de la manière dont on peut y répondre en mettant en œuvre les instruments internationaux existants. Elle devrait en outre évaluer si les instruments existants sont suffisants. Elle s'intégrera également au travail du Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe. L'étude, en cours, est menée par des chercheurs de la France et des Pays-Bas..
2. Étude sur la législation sur la cybercriminalité ("Législation mettant en œuvre la Convention sur la cybercriminalité: analyse comparative des bonnes pratiques et de l'efficacité")	L'étude devrait constituer une ressource pour les pays qui sont en train de renforcer leur législation nationale contre la cybercriminalité conformément à la Convention. L'étude, en cours, est menée par l'institut de recherche de Vérone (Italie).
Étude sur le rôle des fournisseurs de services ("Coopération entre les fournisseurs de services et les autorités de répression contre la cybercriminalité: vers des lignes directrices communes?")	L'étude vise à faciliter la coopération entre fournisseurs de services et autorités de répression dans la prévention de la cybercriminalité et les enquêtes. Elle devrait comprendre une proposition de lignes directrices communes à cette fin pour discussion plus approfondie à la conférence sur la cybercriminalité les 1er et 2 avril 2008 et au Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe les 3 et 4 avril 2008. Un groupe de travail a été créé et a tenu sa première réunion à Paris le 22 octobre 2007.
3. Étude sur la coopération internationale ("L'efficacité de la coopération internationale contre la cybercriminalité: exemples de bonne pratique ")	L'étude doit aider les pays à mieux utiliser les dispositions de la Convention sur la cybercriminalité relatives à la coopération internationale, notamment l'article 35 sur les points de contact 24/7. Elle est menée par un expert du Portugal.

4. Étude sur la protection des données ("Les enquêtes sur la cybercriminalité et la protection des données personnelles et de la vie privée")	Ce document aura pour objet de donner des orientations aux pays sur les moyens de rendre les enquêtes sur la cybercriminalité compatibles avec les préoccupations relatives à la protection des données et de la vie privée (en particulier lors de la mise en ouvre des dispositions procédurales de la Convention sur la cybercriminalité). L'étude est menée par un chercheur des Pays- Bas.

3 Résultats

Objectif du projet : *Promouvoir une large mise en œuvre de la Convention sur la cybercriminalité(STE 185) et de son Protocole sur le racisme et la xénophobie (STE 189)*

Depuis son lancement en septembre 2006, le projet sur la cybercriminalité a aidé à faire de la Convention la principale norme de référence pour la législation sur la cybercriminalité au niveau mondial. En témoignent entre autres la reconnaissance dont a bénéficié la Convention au Forum sur la gouvernance d'Internet, à Interpol, Europol, l'Union européenne et la Commission européenne, l'Organisation des États Américains, la Coopération économique Asie-Pacifique, l'Office des Nations Unies contre la drogue et le crime et ailleurs. En témoignent également la coopération de plus en plus étroite avec le secteur privé (en particulier Microsoft) et d'autres initiatives telles que le groupe de travail sur la lutte contre le hammeçonnage, le Plan d'action de Londres, POLCYB ou ICCYBER.

3.1 Résultat 1: Législation

Législation mettant en œuvre la convention sur la cybercriminalité et son Protocole sur le racisme et la xénophobie (projets de lois satisfaisant aux normes de STE 185 et 189 dans au moins 10 pays européens et cinq pays non européens)

Depuis le lancement du projet, la Convention sur la cybercriminalité a été présentée aux représentants de plus de 150 pays du monde à l'occasion de différents types de réunion.

Des conseils spécifiques sur des projets de loi ont été donnés aux pays suivants :

- Argentine (atelier en novembre 2007 et analyse ultérieure du projet de législation)
- Brésil (examen et commentaire sur le projet de législation en février 2007)
- Colombie (atelier examinant le projet de loi en octobre 2007)
- Égypte (réunion avec les autorités publiques en février 2007, analyse écrite du projet de loi en mai 2007 et conférence de suivi et discussion en novembre 2007)
- Inde (réunion avec les autorités publiques en février 2007, analyse écrite du projet de loi en mai 2007 et discussion de suivi en septembre 2007)
- Indonésie (réunion avec les autorités publiques et analyse écrite du projet de loi en novembre 2007)
- Pakistan (analyse du projet de loi en février 2007)
- Philippines (analyse écrite du projet de loi en juin 2007 et atelier de suivi ayant donné lieu à des commentaires supplémentaires en octobre 2007)
- Serbie (série d'ateliers en 2006/2007 et analyse écrite de la législation en octobre 2007).

La coopération avec le Maroc a commencé en juin 2007 et un projet de dispositions de droit pénal est en cours d'analyse.

Les réunions avec des représentants de pays d'Europe centrale, orientale et du sud-est ont également indiqué qu'un travail législatif supplémentaire est nécessaire dans les pays qui ont déjà ratifié la convention, comme l'Albanie, la Bosnie-Herzégovine, « l'ex-République yougoslave de Macédoine » et l'Ukraine. En Bulgarie, des amendements à la législation existante sont en cours et un atelier destiné à les analyser se tiendra en décembre 2007.

Afin de faciliter l'analyse de la législation sur la cybercriminalité par rapport aux dispositions de la Convention, des profils ont été établis pour plus de 40 pays et 22 d'entre eux ont été publiés en juin 2007. Les profils des pays qui ont ratifié la Convention ont été examinés et améliorés en novembre 2007 et serviront de base à des ateliers dans les pays qui doivent être organisés dans les mois à venir et qui auront pour but d'améliorer encore la législation sur la cybercriminalité.

La République dominicaine et Sri Lanka ont adopté une nouvelle législation en 2007, la République dominicaine suivant de très près la Convention et Sri Lanka la suivant dans une certaine mesure. Des travaux législatifs guidés par la Convention sont en outre en cours dans des pays tels que le Liban, le Sénégal et la Thaïlande. De nombreux autres pays du monde ont déclaré qu'ils souhaiteraient recevoir une assistance pour l'examen de leur législation, ce qui pourrait conduire à une coopération spécifique en 2008.

Pour résumer, les processus législatifs que le projet a été en mesure d'appuyer et de lancer en 2006/2007 ont dépassé les attentes, si l'on considère en particulier que, pour beaucoup de pays non-européens, le Conseil de l'Europe avaient eu auparavant peu de contacts. La Convention sert de ligne directrice ou de « loi type » dans de nombreux pays.

Pour ce qui est des nouvelles ratifications par des pays européens, les progrès ont été moins satisfaisants, bien qu'un travail législatif soit en cours dans beaucoup d'entre eux. Alors qu'en 2006 sept pays avaient déposé l'instrument de ratification, en 2007 (en novembre) seulement trois pays supplémentaires étaient devenus parties à la Convention. Dans deux autres pays (Allemagne et Slovaquie) les parlements ont ratifié ce traité au deuxième semestre de 2007 et devraient déposer l'instrument d'ici peu. Néanmoins, la moitié des États membres de l'Union européenne n'ont toujours pas ratifié cette Convention. L'appel à la ratification lancé en novembre 2007 par le Conseil de la Justice et les Affaires intérieures de l'Union européenne contribuera peut-être à accélérer ce processus. Huit états membres du Conseil de l'Europe n'ont pas encore signé la Convention.

Ratification de la Convention sur la cybercriminalité depuis novembre 2001

Année	Année 1	Année 2	Année 3	Année 4	Année 5	Année 6
	2002	2003	2004	2005	2006	2007
Ratif suppl.	+ 2	+2	+4	+3	+7	+3
Total	2	4	8	11	18	21

En ce qui concerne le protocole sur le racisme et la xénophobie, quatre pays supplémentaires ont ratifié cet instrument en 2007, ce qui porte le nombre à 11, et 20 autres pays l'ont signé.

On pourrait avancer que le rythme de mise en œuvre de la Convention est aussi rapide, sinon plus rapide, que celui d'autres conventions du Conseil de l'Europe dans le domaine pénal[1], que la mise en œuvre des mesures de droit procédural (plus nombreuses dans la Convention que dans d'autres traités internationaux) prend du temps, et que les pays sont censés avoir la législation en place et qu'elle soit adoptée par les parlements au moment de la ratification. D'un autre côté, il semble aussi que dans certains pays la question de la cybercriminalité - malgré son importance - ne reçoive pas la priorité nécessaire.

[1] À l'exception de la Convention pénale sur la corruption qui avait 32 ratifications six ans après son ouverture à la signature.

État des signatures et ratifications de la Convention sur la cybercriminalité (novembre 2007)

Ratifiée (21):

- Albanie
- Arménie
- Bosnie-Herzégovine
- Bulgarie
- Chypre
- Croatie
- Danemark
- Estonie
- États-Unis d'Amérique
- Finlande
- France
- Hongrie
- Islande
- Lettonie
- Lituanie
- Norvège
- Pays-Bas
- L'„ex-République yougoslave de Macédoine"
- Roumanie
- Slovénie
- Ukraine

Signée (22):

- Afrique du Sud
- Allemagne
- Autriche
- Belgique
- Canada
- Espagne
- Grèce
- Irlande
- Italie
- Japon
- Luxembourg
- Malte
- Moldova
- Monténégro
- Pologne
- Portugal
- République tchèque
- Royaume-Uni Serbie
- Slovaquie
- Suède
- Suisse

Non signée (8 États membres du CdE:

- Andorre
- Azerbaïdjan
- Fédération de Russie
- Géorgie
- Liechtenstein
- Monaco
- Saint-Marin
- Turquie

Invités à adhérer (2):

- Costa Rica
- Mexique

Demande d'adhésion (1):

- Philippines

3.2 Résultat 2 : Capacités de la justice pénale

Renforcement des capacités d'enquête, de poursuite et de sanctions de la cybercriminalité

En ce qui concerne le renforcement des capacités pour des enquêtes, des poursuites et des sanctions plus efficaces, le projet a mis l'accent sur la création de la base juridique en accord avec les dispositions de droit procédural de la Convention.

Plusieurs centaines de policiers et de procureurs ont participé à des activités dans le monde entier où les dispositions procédurales de la Convention ont été expliquées. Le projet a contribué à un certain nombre de formations destinées spécifiquement aux enquêteurs de la police scientifique et à d'autres formations destinées aux procureurs.

Un problème particulier identifié dans différents pays est lié à la nécessité pour les autorités de répression de coopérer avec les fournisseurs de services dans les enquêtes sur les cyberinfractions. Une étude a été lancée et un groupe de travail a été créé pour élaborer des lignes directrices à cet égard qui pourrait être appliquées dans n'importe quel pays.

Bien que le personnel des services de répression de nombreux pays ait fait beaucoup de progrès sur le plan du développement des compétences dans ce domaine et bien que cela soit vrai également en partie des procureurs, le corps judiciaire est manifestement en retard. Des mesures ont donc été prises par le projet pour élaborer des modules de formation à l'intention des juges. Une première formation aura lieu en Bulgarie à la mi-décembre 2007.

3.3 Résultat 3 : Coopération internationale

Renforcement des capacités des organes de justice pénale à coopérer au niveau international

La capacité des pays à coopérer au niveau international sera fortement renforcée lorsqu'ils deviendront partie à la Convention.

Les conférences régionales organisées en Serbie et en Ukraine, la conférence mondiale Octopus tenue à Strasbourg en juin 2007 ont fortement mis l'accent sur la coopération internationale contre la cybercriminalité. La participation du Conseil de l'Europe à de nombreuses manifestations organisées par d'autres organisations ont aidé à expliquer les dispositions pertinentes de la Convention.

En octobre 2007 a été lancée une étude qui doit documenter les bonnes pratiques dans la mise en œuvre des dispositions de la Convention relative à la coopération internationale. Ses résultats devraient être disponibles en avril 2008.

Le projet a contribué au renforcement des points de contact 24/7 conformément à l'article 35 de la Convention et à l'expérience du sous-groupe du G8 sur la criminalité de haute technologie.

Le risque de réseaux concurrents ou de multiplication des points de contact et des réseaux a été réduit grâce à un accord conclu en novembre 2007 avec le sous-groupe du G8 visant à regrouper les registres des points de contact du Conseil de l'Europe et du G8.

4 L'avenir

Outre le comité de la Convention sur la cybercriminalité (T-CY), le Projet contre la cybercriminalité est la ressource la plus importante dont dispose le Conseil de l'Europe pour appuyer la mise en œuvre de la Convention.

Les résultats obtenus jusqu'à présent montrent que le projet a été très efficace et pragmatique, et que beaucoup a été accompli avec des ressources limitées.

L'impulsion donnée par le projet offre maintenant des possibilités uniques d'exercer un impact dans le monde entier entre décembre 2007 et la fin prévue du projet en février 2009.

À la fin de 2008, le projet devrait être évalué et des propositions devraient être élaborées concernant les activités futures de coopération technique du Conseil de l'Europe dans le domaine de la cybercriminalité.

4.1 Priorités en 2008[2]

D'une façon générale, l'approche couronnée de succès choisie par le projet restera la même :

- La coopération se poursuivra avec de nombreuses organisations (telles que les Nations Unies, l'Organisation des États Américains, Interpol, Europol et beaucoup d'autres) comme moyen économique d'atteindre une portée et un impact maximaux. Cela facilitera également la participation aux discussions sur l'élaboration de normes internationales et européennes supplémentaires, par exemple sur la question du vol d'identité, les attaques contre les infrastructures critiques ou la question de la vie privée qui prendront de l'importante dans l'avenir proche.
- Une coopération étroite avec le secteur privé sera recherchée. L'élaboration des lignes directrices sur la coopération en les autorités de répression et les fournisseurs de services devrait être utile à cet égard.

Une conférence Octopus mondiale se tiendra à Strasbourg les 1er et 2 avril 2007 et donnera un nouvel élan aux objectifs et aux résultats escomptés du projet. Elle sera suivie par les troisièmes consultations des parties à la Convention (le T-CY) les 3 et 4 avril.

4.1.1 Appui au renforcement de la législation en vue de mettre en œuvre la Convention et de permettre l'adhésion à la Convention

Comme en 2006/2007, la Convention sera promue comme étant la ligne directrice ou une « loi type »pour l'élaboration de législations sur la cybercriminalité dans le monde entier.

Une étude analysant la mise en œuvre des dispositions de la Convention sur la criminalité sera finalisée en avril 2008.

La promotion de la ratification et de l'adhésion à la Convention restera essentielle, mais l'accent sera mis davantage sur la mise en œuvre effective des dispositions de la Convention. En plus des études qui sont en cours, d'autres outils pratiques devront être mis au point.

La préparation de profils de pays sur la législation sur la cybercriminalité sera étendue à de nouveaux pays, et ceux qui existent seront améliorés. Cela permettra de partager les bonnes pratiques et des exemples de législation sur la cybercriminalité et servira de point de départ à l'analyse de la législation par rapport aux dispositions de la Convention.

[2] Bien qu'il y ait suffisamment de fonds pour couvrir les activités jusqu'en avril 2000, la mise en oeuvre du projet après cette date dépendra de la disponibilité de contribution complémentaire (voir ci-après la section pertinente).

On insistera davantage sur la mise en œuvre du Protocole sur le racisme et la xénophobie.

Des activités spécifiques seront menées en rapport avec l'article 9 (pornographie enfantine) en liaison avec la nouvelle Convention pour la protection des enfants contre l'exploitation et les abus sexuels (STCE 201).

En Europe, les activités seront axées sur la promotion de la ratification par les pays qui ne sont pas encore parties (États membres de l'Union européenne, Moldova, Monténégro, Russie, Turquie et d'autres). Dans les pays européens qui sont déjà parties, des ateliers seront organisés pour renforcer l'efficacité de la législation sur la cybercriminalité, par exemple en Albanie, Bosnie-Herzégovine, Bulgarie et dans l'ex-République yougoslave de Macédoine).

En Afrique, la coopération avec l'Égypte, le Maroc et l'Afrique du Sud se poursuivra. D'autres pays comme le Nigeria et le Sénégal seront soutenus.

Les possibilités avec d'autres pays de la région arabe seront explorées.

Dans les Amériques, la coopération se poursuivra avec l'Argentine, le Brésil, la Colombie, le Costa Rica, la République dominicaine et le Mexique en vue de l'adhésion. Un atelier avec les 34 états membres de l'Organisation des États Américains aidera à promouvoir le renforcement de la législation dans toute cette région.

En Asie et dans le Pacifique, les travaux se poursuivront avec l'Inde, l'Indonésie et les Philippines. L'adhésion de pays où existe déjà une législation pertinente sera promue (par exemple Australie, Nouvelle-Zélande, Singapour et Sri Lanka). La coopération avec l'ASEAN sera recherchée en vue de réformes législatives dans toute cette région.

Le projet apportera une contribution au Forum sur la gouvernance d'Internet en Inde en décembre 2008.

4.1.2 Le renforcement des capacités d'enquête, de poursuite et de sanctions dans le domaine de la cybercriminalité

Les lignes directrices pour la coopération entre les autorités de répression et les fournisseurs de services devront être finalisées et diffusées dans le monde entier. Elles appuieront la mise en œuvre des dispositions procédurales de la Convention.

Une étude sur la question de la protection des données/ de la vie privée dans les enquêtes sur la cybercriminalité sera achevée en avril et pourra déboucher sur d'autres activités dans ce domaine.

Le Conseil de l'Europe contribuera à la formation d'enquêteurs et de procureurs par l'intermédiaire de ce projet et aux activités organisées par d'autres organisations.

Le projet mènera une série d'activités visant à la formation du corps judiciaire. La première se tiendra en Bulgarie les 17 et 18 décembre 2007 et aidera à mettre au point un module de formation qui pourra ensuite être exécutée dans d'autres pays. D'autres activités suivront au second semestre de 2008 si des fonds sont disponibles.

4.1.3 Coopération internationale

Une étude sur les bonnes pratiques dans la mise en œuvre des dispositions de la Convention relatives à la coopération internationale sera achevée en avril 2008.

En coopération avec le Sous-groupe sur la criminalité de haute technologie du G8, le projet aidera à tenir le registre des points de contact.

Des activités spécifiques de formation seront menées pour renforcer l'efficacité des points de contact existants.

Dans les pays qui ont ratifié la Convention et n'ont pas encore de tels points de contact, la création de ces derniers sera promue.

4.2 Activités proposées (décembre 2007 – juin 2008)

Date	Lieu	Description
Oct. 2007 – avril 2008	Strasbourg et ailleurs	Études sur la législation sur la cybercriminalité, rapport de situation, coopération autorités de répression – fournisseurs de services, coopération internationale, vie privée
13-14 déc. 2007	La Haye (Pays-Bas)	Réunion de la Commission de droit international sur la coopération secteur public- secteur privé
17-18 déc. 2007	Bulgarie	Atelier de formation pour les juges (Bulgarie, Roumanie, Serbie et "l'ex-République yougoslave de Macédoine", et examen de la législation sur la cybercriminalité
Déc. 2007	Strasbourg	Analyse de la législation sur la cybercriminalité du Nigeria
Janv. 2008	Kosovo	Atelier sur l'assistance législative
Janv. 2008	Géorgie	Atelier sur l'assistance législative
	Albanie	Atelier sur la législation et les enquêtes sur la cybercriminalité
Fév. 2008 (à confirmer)	Sénégal	Atelier sur l'assistance législative
Fév. 2008	Maroc	Atelier sur la législation et les enquêtes sur la cybercriminalité
7 fév. 2008	Düsseldorf, Allemagne	Étude sur la coopération autorités de répression – fournisseurs de services: 2e réunion du groupe de travail
Mars 2008	République Dominicaine	Atelier pour examiner la législation et promouvoir l'adhésion à la Convention
Fév. 2008	Monténégro	Atelier sur l'assistance législative
20-21 fév. 2008	Londres	Réunion McAfee sur la cybersécurité
Mars 2008	"l'ex-Republiq ue yougoslave de Macédoine "	Atelier sur la législation et les enquêtes sur la cybercriminalité
Mars 2008	Bosnie – Herzégovine	Atelier sur l'assistance législative
1er-2 avril 2008	Strasbourg	Conférence Octopus Interface sur la cybercriminalité (sera suivie par une réunion du Comité de la Convention sur la cybercriminalité les 3 et 4 avril)
Mai 2008	Europe (lieu à confirmer)	Atelier pour les points de contact 24 des pays européens
Avril-– juin 2008	Afrique	Jusqu'à 2 ateliers sur l'assistance législative
Avril – juin 2008	Asie et Pacifique	Jusqu'à 3 ateliers sur l'assistance législative
Avril – juin 2008	Région arabe	Jusqu'à 2 ateliers sur l'assistance législative
Avril– juin 2008	Amériques	Jusqu'à 2 ateliers sur l'assistance législative
18 – 23 mai 2008	Australie	Conférence annuelle AusCERT Asie-Pacifique sur la sécurité de l'information
Juin 2008	Colombie (à confirmer)	Conférence régionale OEA/CdE sur la législation sur la cybercriminalité pour les 34 États membres de l'OEA
Déc. 2007 – juin 2008	Monde	Participation à des manifestations organisées par d'autres organisations

4.3 Coopération avec Microsoft

Les activités du projet en 2006 et 2007 ont été financés par des contributions volontaires de Microsoft et par le budget du Conseil de l'Europe (Projet 143 sur la criminalité économique). La coopération de Microsoft est allée au-delà de la fourniture d'un financement :

- Des représentants des bureaux de Microsoft dans le monde entier ont facilité le contact avec les parties prenantes et fourni des informations concernant le cadre législatif et institutionnel
- Dans un certain nombre de cas, ils ont apporté un appui supplémentaire localement aux réunions organisées par les autorités publiques et le Conseil de l'Europe
- Ils ont promu la mise en œuvre de la Convention par des manifestations organisées par Microsoft ; et le Conseil de l'Europe a été invité à participer à un certain nombre d'entre elles
- Ils ont utilisé la Convention pour analyser le cadre juridique de pays d'Asie et du Pacifique
- Ils ont mené un certain nombre d'activités liées à la protection des enfants et promu la mise en œuvre de l'article 9 sur la pornographie enfantine de la Convention sur la cybercriminalité et tiennent compte aussi maintenant de la nouvelle Convention sur l'exploitation et les abus sexuels des enfants (STCE 201)
- Microsoft appuie l'étude sur la coopération entre les autorités de répression et les fournisseurs de services et a facilité la participation d'autres fournisseurs de services au groupe de travail créé par le Conseil de l'Europe pour élaborer des projets de lignes directrices pour cette coopération[3].

La coopération entre Microsoft et le Conseil de l'Europe a été très pragmatique et axée sur les résultats. Une poursuite de ce partenariat en 2008/2009 irait dans le sens des intérêts des deux parties. En même temps, il faudrait chercher un financement auprès d'autres institutions des secteurs public et privé.

[3] Outre Microsoft, eBay, British Telecom, Telefonica et différentes associations de fournisseurs de services participent également à ce groupe de travail.