Conférence Octopus Interface sur

Coopération contre la Cybercriminalité

11 et 12 juin 2007
Conseil de l'Europe, Strasbourg, France

Compte rendu de la conférence

Plus de 140 experts en cybercriminalité provenant de quelque 55 pays, d'organisations internationales et du secteur privé, se sont rencontrés 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 ainsi que l'accession larges et rapides 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.

Ci-après, les résultats des débats qui se sont tenus en séances plénières et en ateliers :

1 CYBERCRIMINALITE : ANALYSE DE LA SITUATION ET IDENTIFICATION DES NOUVELLES MENACES

Le défi à relever

Une présentation du représentant d'Europol, suivie d'un débat avec des représentants de France, de Microsoft, de l'INHOPE et de l'ICMEC, ainsi que les interventions d'autres participants ont mené aux constats suivants :

- Les sociétés du monde entier dépendent des technologies de l'information et de la communication. L'augmentation de la cybercriminalité rend les sociétés hautement vulnérables.
- Les programmes malveillants — codes et logiciels malicieux, dont les virus, les vers, les chevaux de Troie, les logiciels espions, les robots et les réseaux zombies — évoluent et se répandent rapidement. Ils sont utilisés, entre autres, pour les attaques en déni de service, les vols d'identité (hameçonnage et autres techniques d'ingénierie sociale), les fraudes, le blanchiment d'argent et d'autres crimes économiques.
- Les spams, qui représenteraient la grande majorité du trafic de courrier électronique, sont non seulement source de désagrément mais contribuent également à la diffusion croissante de programmes malveillants.
- Les auteurs d'infractions s'organisent de plus en plus pour commettre des infractions visant à générer des profits illicites.
- Les réseaux zombies constituent l'un des outils majeurs de ces activités criminelles, non seulement pour commettre des attaques en déni de service et des extorsions, mais également pour diffuser des logiciels publicitaires et des logiciels espions.
- Une économie de services clandestine se développe. Des réseaux zombies sont, par exemple, loués à des criminels organisés.

- Le changement de visage de la menace est également confirmé par les analystes du secteur : les attaques à objectifs multiples, de masse, menées à grande échelle, voire au niveau mondial, par des virus, des vers et des spams qui attirent l'attention sont remplacées par des attaques plus ciblées et plus petites qui visent des utilisateurs, des groupes, des organisations ou des secteurs spécifiques et qui évitent d'attirer l'attention. Ces attaques relèvent de plus en plus de la criminalité économique.
- Les petites et moyennes entreprises sont particulièrement vulnérables dans la mesure où, souvent, elles n'investissent pas les ressources nécessaires à la protection de leurs systèmes.
- Les systèmes de paiement en ligne deviennent un sujet de préoccupation majeur aux Etats-Unis.
- L'usage abusif d'Internet se développe pour l'exploitation et l'abus sexuels des enfants ainsi que pour le trafic d'êtres humains. Une grande partie des sites de pornographie enfantine et des images d'abus subis par des enfants s'avèrent désormais de nature commerciale et génèrent des produits importants.
- Le risque de cyber-attaques contre des infrastructures critiques (cyber-terrorisme) augmente.
- Le stockage de données à distance pose des problèmes pour les investigations dans le domaine de la cybercriminalité.
- Les technologies et techniques mises en œuvre dans le domaine de la cybercriminalité se développent rapidement et deviennent plus sophistiquées. Les réseaux de prochaine génération (NGN), y compris les services tels que la voix sur IP, poseront de nouveaux défis aux autorités chargés de l'application de la loi.

Les mesures à prendre

Les propositions suivantes ont été présentées :

- Une coopération est requise à l'échelle mondiale pour lutter contre la cybercriminalité. Les pays du monde entier devraient adhérer à des normes mondiales pour le partage des informations. L'application la plus large possible de la Convention sur la Cybercriminalité constituera une étape importante à cet égard.
- Les partenariats entre les secteurs public et privé représentent la pierre angulaire d'une telle coopération mondiale. L'industrie se doit de coopérer avec les organismes chargés de l'application de la loi. La difficulté consiste à trouver l'équilibre entre les droits au respect de la vie privée et les besoins en matière de sécurité.
- Encourager les victimes de la cybercriminalité à signaler les infractions ; faciliter leurs démarches en ce sens et prendre des mesures pour assurer la protection des témoins.
- Améliorer la qualité et la cohérence des données sur la cybercriminalité, par exemple, grâce à des systèmes de communication centralisés, aux recherches sur les cybercriminels et autres.
- Les institutions publiques, mais aussi l'industrie et d'autres organisations du secteur privé, doivent continuer à mener leur travail d'analyse et à réaliser leurs évaluations des menaces qui s'avèrent particulièrement utiles. Par exemple, le prochain rapport de tendance de l'association INHOPE sur la pornographie enfantine et les contenus illicites fournira de précieuses informations.
- Eriger en infraction pénale la pornographie enfantine et les abus d'enfants sur Internet en mettant pleinement en application l'article 9 de la

Convention sur la Cybercriminalité sans aucune restriction, sauf lorsque cela s'avère absolument nécessaire.
- Appliquer également les autres traités et réglementations protégeant les enfants des abus.
- Améliorer, à tous les niveaux, la sensibilisation à l'utilisation en toute sécurité des technologies de l'information et de la communication, par exemple à l'aide de programmes adaptés ou par l'intermédiaire d'institutions spécialisées. Les utilisateurs eux-mêmes (les utilisateurs individuels mais également les entreprises et les institutions publiques) sont directement responsables de leur protection.
- Mettre en œuvre des mesures de protection des infrastructures critiques.
- Prendre des mesures afin de trouver des solutions aux problèmes posés par les développements technologiques tels que les réseaux NGN, y compris la voix sur IP.

2 MISE EN ŒUVRE DE LA CONVENTION SUR LA CYBERCRIMINALITE ET DE SON PROTOCOLE SUR LA XENOPHOBIE ET LE RACISME

Le défi à relever

La cybercriminalité est un phénomène de grande envergure, qui se développe rapidement, devient de plus en plus dangereux et dépasse les frontières sans aucune difficulté. Il est évident qu'il est nécessaire et possible de lutter contre la cybercriminalité à l'échelle mondiale. Pour ce faire, les pays doivent non seulement disposer d'un droit pénal matériel et procédural compatible et, dans la mesure du possible, harmonisé, mais également collaborer plus étroitement afin de garantir une coopération internationale efficace.

La Convention sur la Cybercriminalité donne des lignes directrices exploitables, qui ont été positivement accueillies, pour développer des législations nationales. Elle définit en outre un cadre de coopération internationale. A ce jour, la Convention a été ratifiée par 21 Etats et signée par 22 autres. Le Protocole additionnel sur le racisme et la xénophobie a été ratifié par 11 Etats et signé par 20 autres.

Les défis à relever sont les suivants :

- Augmenter le nombre de Parties à la Convention et au Protocole additionnel. Les Etats ayant déjà signé ces traités devraient tout particulièrement accélérer le processus de ratification.
- Promouvoir la Convention au niveau mondial. Outre les six Etats non européens ayant signé ou ratifié le traité, ou ayant été invités à y adhérer, d'autres Etats devraient être encouragés à viser l'accession à ces instruments.
- Garantir et promouvoir l'efficacité de la Convention et de son Protocole additionnel entre les Parties.

Les bonnes pratiques à partager

Du fait de son importance, la Convention, qui est le seul instrument en matière de cybercriminalité ayant un caractère obligatoire dans le monde, a été fréquemment prise comme modèle lors de l'élaboration de projets de loi. Suite au large soutien apporté à la Convention dans les différentes régions du monde, pratiquement toutes les nouvelles législations et tous les nouveaux projets de loi s'inspirent très largement des dispositions de la Convention. De telles réformes sont actuellement menées dans des pays tels que l'Argentine, le Brésil, l'Egypte, l'Inde, le Nigeria, le Pakistan et les Philippines.

Cette démarche garantit la compatibilité des législations au niveau mondial et offre une base efficace et solide à la coopération entre les pays.

Les mesures à prendre

- Les pays ayant déjà signé la Convention ou le Protocole, ou ayant été invités à y adhérer, devraient mener le processus de ratification à bien dès que possible.
- Les pays ayant mis en œuvre la Convention devraient partager leur expérience. Les « Profils des pays en matière de législation sur la cybercriminalité » préparés par le Conseil de l'Europe, dans le cadre du Projet sur la cybercriminalité, peuvent s'avérer utiles à cet égard.[1]
- Le Conseil de l'Europe et d'autres partenaires sont prêts à apporter leur aide aux pays intéressés et à les conseiller en matière de législation sur la cybercriminalité.
- La consultation des Parties, par l'intermédiaire du Comité de la Convention sur la Cybercriminalité T-CY, apportera des conseils et une assistance dans la mise en œuvre de la Convention et de son Protocole.

3 L'EFFICACITE DE LA LEGISLATION SUR LA CYBERCRIMINALITE

Le défi à relever

Les pays doivent ériger en infraction pénale certaines conduites (droit pénal matériel) et donner aux autorités chargées de l'application de la loi et à la justice pénale des moyens efficaces de mener des investigations, d'engager des poursuites et de juger des actes de cybercriminalité (droit procédural), en leur permettant notamment d'agir rapidement afin de préserver les preuves volatiles. Ils doivent en outre définir des dispositions en faveur d'une coopération internationale efficace. A cet égard, tout pays est encouragé à utiliser la Convention en tant que ligne directrice. Certains pays, déjà Parties à la Convention, devront éventuellement prendre des mesures supplémentaires afin de mettre leur législation en parfaite conformité avec ce traité.

Le principal défi consiste à amener les pays à adopter une législation nationale en matière de droit pénal matériel et procédural, et à mettre en œuvre une coopération internationale dans le respect de la Convention sur la Cybercriminalité.

Par ailleurs, la question de la juridiction continue de poser des problèmes majeurs pour l'application de la loi à travers le monde.

Les bonnes pratiques à partager

Les représentants des Etats ci-dessous, tous membres du Conseil de l'Europe, ont présenté leur législation nationale sur la cybercriminalité et les questions connexes : l'Italie, la Roumanie, la Russie, la Norvège, les Pays-Bas, le Portugal et l'Azerbaïdjan.
L'Inde, l'Argentine, le Brésil, le Mexique, l'Egypte et l'Afrique du Sud ont également fait une présentation. Microsoft a en outre donné une vue d'ensemble de la législation et des initiatives législatives en matière de cybercriminalité actuellement en place dans des Etats de la région Asie-Pacifique.

[1] Voir www.coe.int/cybercrime

L'intérêt de la Convention sur la Cybercriminalité et de son premier Protocole additionnel a été généralement reconnu et jouit d'un large soutien.

La majorité des intervenants ont donné une vue d'ensemble des dispositions de leur législation nationale sur la cybercriminalité en vigueur. Les Etats signataires et les Etats qui s'emploient à adhérer à la Convention ont souligné les projets de loi en instance et les efforts législatifs supplémentaires à déployer. En conclusion, la mise en œuvre de la Convention semble avoir entraîné, dans la plupart des cas, une vaste révision des dispositions juridiques en place et l'adoption de nouvelles lois. Les informations fournies laissent prévoir un nombre considérable de ratifications et de demandes d'adhésion en 2007.

Certaines difficultés rencontrées par les législateurs nationaux lors de la mise en œuvre du texte de la Convention ont été mentionnées, par exemple en ce qui concerne l'article 2 (accès illégal), l'article 3 (interception illégale), l'article 9 (pornographie enfantine), l'article 32 (accès transfrontière) et l'article 35 (réseau 24/7). Par ailleurs, plusieurs intervenants, dont ceux ayant déjà signé ou ratifié la Convention, ont fait référence à des formes spécifiques de cybercriminalité que leur législation nationale érige en infraction pénale mais qui ne sont pas (explicitement) définies par la Convention comme un vol d'identité, un acte de cyberharcèlement ou un acte de cyberdiffamation. Il conviendrait également d'étudier la nécessité d'ériger en infraction pénale l'usage abusif d'autres fonctionnalités des technologies de l'information et de la communication (telles que le Wifi, l'identification biométrique et l'identification par radiofréquence).

Plusieurs problèmes relatifs aux investigations et en rapport avec la collecte des preuves électroniques ont été évoqués, en particulier au sujet des preuves se trouvant en dehors du territoire national. La Convention prévoit à cet égard une assistance mutuelle accélérée afin de protéger les preuves électroniques trouvées dans un autre Etat partie à la Convention.
Des difficultés ont été rencontrées dans la coopération entre des Etats membres du Conseil de l'Europe et des Etats non membres. Par exemple, les procédures d'entraide judiciaire classiques à suivre pour le transfert des éléments demandés sont en général relativement longues, ce qui peut mettre en danger l'investigation et les poursuites engagées dans le cadre d'un crime. En outre, la difficulté éventuelle à déterminer la localisation physique d'un serveur informatique, qui empêche les autorités chargées de l'application de la loi de demander une assistance mutuelle, a également été mise en avant.

Un bref débat s'est tenu sur la nécessité de mettre en place un pouvoir coercitif pour ordonner aux fournisseurs de services Internet de bloquer le trafic Internet provenant de certaines sources, en raison de son contenu. Ce pouvoir est déjà en place dans certains pays. Dans d'autres cas, le blocage du trafic est réalisé en collaboration avec les fournisseurs de services Internet.

La plupart des représentants ont insisté sur la nécessité de créer des organismes de coordination et d'investigation spécialisés au niveau national, et de prendre des mesures de formation continue, en particulier pour le ministère public et le corps judiciaire.

Certains représentants ont souligné le fait que leurs économies en développement ne disposent pas toujours de moyens financiers suffisants pour apporter l'expertise et l'équipement nécessaires aux autorités chargées de l'application de la loi ainsi qu'au pouvoir judiciaire. Le soutien d'autres Etats et du secteur privé est donc indispensable.

Des détails sur la procédure et les conditions d'adhésion puis de ratification ont conclu la session.

Les mesures à prendre

- Une évaluation plus rigoureuse de l'efficacité de la législation sur la cybercriminalité pourrait s'avérer nécessaire et des exemples de bonnes pratiques devraient être échangés. Les « Profils des pays en matière de législation sur la cybercriminalité » préparés par le Conseil de l'Europe peuvent s'avérer utiles à cet effet.
- Les pays qui élaborent actuellement des projets de loi en matière de cybercriminalité peuvent demander au Conseil de l'Europe, aux autorités des Etats parties à la Convention ou au secteur privé de leur apporter une aide pour l'élaboration de leur législation sur la cybercriminalité.
- Les capacités de la justice pénale et des autorités chargées de l'application de la loi à mettre en œuvre les lois en matière de cybercriminalité doivent être consolidées.
- La question de la juridiction peut être étudiée de façon plus approfondie par des instances compétentes, dont le Comité de la Convention sur la Cybercriminalité (T-CY).

4 COOPERATION INTERNATIONALE ET FONCTIONNEMENT DU RESEAU DE POINTS DE CONTACT 24/7

Le défi à relever

La cybercriminalité a une dimension internationale qui nécessite une coopération internationale efficace et immédiate afin de préserver les preuves volatiles au-delà des frontières. Le réseau de points de contact joignables vingt-quatre heures sur vingt-quatre, sept jours sur sept, est un outil important à cet égard. L'établissement de ces points de contact est encouragé par le Sous-groupe sur la criminalité de haute technologie du G8 depuis 1997 et est également prévu dans l'article 35 de la Convention sur la Cybercriminalité.

Les défis à relever sont les suivants :

- Toutes les Parties à la Convention n'ont pas établi de points de contact opérationnels.
- Il risque d'exister plusieurs réseaux de points de contact différents, tels qu'un réseau pour le G8 et un réseau pour le Conseil de l'Europe.
- Le fondement juridique permettant aux points de contact d'agir n'est pas pleinement établi dans plusieurs pays (par exemple, en ce qui concerne la conservation rapide des données).
- La coopération doit reposer sur plusieurs points de contact dans le cadre d'une coopération judiciaire efficace.

Les bonnes pratiques à partager

Le réseau du Sous-groupe sur la criminalité de haute technologie du G8 a acquis une vaste expérience au cours de ses dix années d'existence. Des principes directeurs et d'autres documents ont été élaborés. Le protocole peut aider les pays à établir des points de contact. La « Check-list d'utilisation du réseau 24/7 du G8 » peut aider les points de contact à formuler leurs demandes dans un format qui contient toutes les informations requises, afin que le point de contact requis puisse agir.

Les exemples des points de contact opérationnels en Italie, aux Etats-Unis, en France et en Roumanie ont été examinés.

Les mesures à prendre

- Tous les pays qui ont ratifié la Convention devraient mettre en place des points de contact opérationnels, comme établi dans l'article 35. Les membres du réseau G8 et du Conseil de l'Europe devraient apporter leur aide à cet effet, si nécessaire.
- Les points de contact mis en place en vertu de la Convention sont encouragés à adhérer également au réseau du Sous-groupe sur la criminalité de haute technologie du G8.
- Le Sous-groupe sur la criminalité de haute technologie du G8 et le Conseil de l'Europe devraient coopérer afin d'établir un registre combiné des points de contact et de le tenir à jour (uniquement à des fins d'application de la loi). Cette proposition devrait être examinée à la prochaine réunion du sous-groupe G8.
- Des formats standardisés de demandes, tels que la « Check-list d'utilisation du réseau 24/7 du G8 » peuvent s'avérer utiles, afin de faciliter la coopération entre points de contact.
- L'Italie prévoit, si les moyens disponibles le permettent, de mettre en place un portail sécurisé réservé au réseau des points de contact. Cette solution pourrait faciliter la tenue à jour du registre et contribuer au partage d'autres informations, telles que les modèles de demandes.
- Après les conférences de formation des points de contact organisées par le sous-groupe du G8 à Rome (Italie) en 2004 et en 2006, une nouvelle conférence de formation pourrait être envisagée pour 2009. Afin de maintenir la dynamique, le Conseil de l'Europe devrait envisager l'organisation d'un atelier de formation pour les points de contact dès 2008.
- Des tests du réseau ou tests de Ping pourraient être réalisés afin de vérifier si les points de contact sont opérationnels.
- Des efforts devraient être déployés afin de poursuivre l'extension du réseau. Il conviendrait, à cet effet, d'examiner la composition, les méthodes de travail et les compétences de réseaux déjà en place dans ce domaine, comme celui d'Interpol, par exemple.

5 INITIATIVES D'AUTRES ORGANISATIONS ET PARTIES PRENANTES : POSSIBILITES DE COOPERATION ET DE SYNERGIES

Le défi à relever

Au cours de ces dernières années, les organisations internationales, les Etats, ainsi que les parties prenantes publiques et privées ont multiplié les initiatives témoignant de l'engagement pris à l'échelle mondiale pour traiter le problème de la cybercriminalité et trouver des solutions adaptées. Par conséquent, la dynamique autour de cette question est très forte, mais le risque d'activités redondantes (la tendance naturelle privilégiant un travail isolé et une coordination limitée avec les autres) présente une difficulté majeure. Tous les acteurs suivent un seul et même objectif, qui exige une harmonisation et une centralisation plus fortes des efforts et des actions, notamment à l'échelle internationale. Cette coordination devrait fonctionner comme Internet : des cellules interconnectées les unes aux autres en fonction des besoins, créant ainsi des synergies et une nouvelle dynamique. Les réunions telles que la Conférence Octopus, combinées à une coordination officielle entre parties prenantes, peuvent servir d'interface afin de faciliter ce type de coopération.

Les bonnes pratiques à partager

Des actions et programmes divers qui représentent des bonnes pratiques à échanger et à développer davantage ont été présentés, comme la coopération entre les autorités chargées de l'application de la loi et le secteur privé sous forme de plateforme commune pour échanger des informations et définir les rôles et attentes des différents acteurs, le rôle de coordination de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) avec l'industrie, les organisations internationales, les pays tiers et les universités, et son projet de créer un système paneuropéen d'information sur la sécurité informatique (EISAS) s'adressant aux citoyens ainsi qu'aux petites et moyennes entreprises, le kit d'outils anti-spam créé par l'OCDE, le groupe consultatif international créé dans le cadre du programme PDNU sur la Gouvernance dans la région arabe (POGAR) afin de soutenir les actions visant à former la justice pénale afin qu'elle puisse faire face à la criminalité de haute technologie, la création de services d'assistance en ligne supplémentaires en Afrique et en Asie dans le cadre de l'association INHOPE qui facilite et coordonne le travail des services d'assistance en ligne en réponse à l'utilisation illégale et au contenu illicite sur Internet, la mise en place de campagnes mondiales contre la pornographie enfantine, telles que celle lancée par le Centre international pour les enfants disparus et exploités.

Les mesures à prendre

Ci-après, plusieurs propositions d'efforts collectifs et d'améliorations de la coopération à l'échelle internationale :

- Forum sur la gouvernance d'Internet : le Conseil de l'Europe participera à la prochaine réunion programmée à Rio en novembre 2007 où il soulignera la nécessité de s'assurer qu'Internet ne présente aucun danger et que les droits de l'homme ainsi que la primauté du droit sont également respectés dans le cyberespace.
- Des organisations telles que European Digital Rights continueront de vérifier si les lois sur la cybercriminalité portent indûment atteinte à des droits au respect de la vie privée et à la liberté d'expression sur Internet.
- Commission européenne : la communication de la Commission de mai 2007 peut servir de base solide à toute coopération supplémentaire. La Commission a exprimé sa détermination à promouvoir la Convention et son Protocole, à encourager les pays tiers à adhérer à la Convention et à envisager l'adhésion des Communautés européennes à la Convention. Le Conseil de l'Europe est prêt à participer aux activités mentionnées dans la Communication.
- Organisation des Etats américains (OEA) : elle continuera à encourager ses Etats membres à adhérer à la Convention et est prête à examiner des possibilités supplémentaires de coopération avec des organisations internationales. Le Conseil de l'Europe poursuivra sa coopération fructueuse avec l'OAE et envisagera la possibilité d'une formation conjointe pour soutenir les Etats membres de l'OAE dans l'élaboration d'une législation sur la cybercriminalité.
- Interpol : cette organisation encourage l'ensemble de ses Etats membres à utiliser les outils (réseau 24/7, bases de données) qu'elle propose dans le domaine de la criminalité de haute technologie. Le Conseil de l'Europe est prêt à soutenir l'organisation des réunions du groupe de travail Proche et Moyen Orient ainsi que du groupe de travail Afrique, dans le courant de l'année 2007.
- Coopération économique pour l'Asie-Pacifique et ANASE : ces organisations continueront à promouvoir la Convention auprès de leurs Etats membres et

le renforcement de la législation sur la cybercriminalité. Le Conseil de l'Europe est prêt à travailler avec des pays de la région Asie-Pacifique, par l'intermédiaire de la CEAP et de l'ANASE, afin d'atteindre cet objectif. Il est prêt, le cas échéant, à participer à la prochaine réunion du groupe de travail sur les télécommunications (TEL) de la CEAP qui aura lieu au Chili.

- Organisation de la conférence islamique (OCI) : elle continuera à agir contre la diffamation religieuse sur Internet. Le Conseil de l'Europe devrait coopérer avec l'OCI pour lutter contre l'intolérance et la discrimination en vertu de la Convention sur la Cybercriminalité et de son Protocole additionnel sur l'incrimination des actes de nature raciste et xénophobe.
- Programme PDNU sur la Gouvernance dans la région arabe (POGAR) : le Conseil de l'Europe participera à la prochaine conférence de formation sur la cybercriminalité organisée par le Programme PDNU sur la Gouvernance dans la région arabe, les 19 et 20 juin 2007 à Casablanca, à l'intention des procureurs de la région arabe. La possibilité d'une coopération plus étroite entre le Conseil de l'Europe et le Programme PDNU sur la Gouvernance dans la région arabe pourrait être envisagée.

6 PARTENARIATS PUBLIC-PRIVE

Le défi à relever

Les investigations dans le cadre de crimes sur Internet nécessitent le plus souvent une étroite coopération entre les entreprises privées (telles que les fournisseurs de services Internet) et les organismes chargés de l'application de la loi. Cette coopération concerne notamment :

- l'identification des suspects sur la base d'une adresse IP ou de coordonnées bancaires,
- la communication d'informations sur les abonnés,
- l'identification de contenus illégaux stockés et l'accès à ces contenus.

Pour le secteur privé, la coopération avec les organismes chargés de l'application de la loi peut être source de conflits dans les cas où la coopération ne repose pas sur un cadre juridique établi. Le partenariat entre les secteurs public et privé joue donc un rôle particulièrement important par rapport à deux aspects :

- l'amélioration de la coopération dans les limites du cadre juridique en place,
- le développement de principes pour la mise en œuvre ou l'amélioration des procédures de partenariats entre les secteurs public et privé.

Les partenariats entre les secteurs public et privé, dans le cadre d'investigations sur Internet, ne peuvent être étendus à l'infini. Les limites résultent, par exemple, du fait que certains éléments clés des investigations pénales doivent, tout au moins dans la plupart des juridictions, rester sous le contrôle absolu des organismes compétents chargés de l'application de la loi.

Les bonnes pratiques à partager

L'importance des partenariats entre les secteurs public et privé a motivé et continue de motiver la mise en œuvre de plusieurs initiatives. Compte tenu du fait que de nombreux acteurs mondiaux du secteur de l'Internet ont leur siège aux Etats-Unis, ces entreprises jouent un rôle important. Ci-après, plusieurs des bonnes pratiques présentées au cours de la Conférence :

- Le partenariat entre le Conseil de l'Europe et Microsoft, qui soutient le Projet sur la cybercriminalité et contribue ainsi à promouvoir la Convention sur la Cybercriminalité à travers le monde.
- Le système de surveillance de l'exploitation des enfants, développé par Microsoft en partenariat avec les autorités chargées de l'application de la loi au Canada, qui est actuellement mis en place dans plusieurs pays.
- Le Plan d'Action de Londres qui vise à promouvoir l'établissement d'une coopération internationale de lutte contre le spam.
- Le groupe de travail de lutte contre le hameçonnage APWG (Anti-Phishing Working Group). Cette association mondiale de coopération entre l'industrie et les autorités chargées de l'application de la loi vise à remédier à la fraude et au vol d'identité suite à des hameçonnages, des pharmings ou des usurpations d'adresses Emails de tous types. Elle compte désormais plusieurs milliers de membres, organismes et entreprises à travers le monde.
- Le Sous-groupe sur la criminalité de haute technologie du G8 a encouragé les pays à rejoindre le Réseau de points de contact de haute technologie 24/7 et à tirer profit du travail du sous-groupe en matière de coopération entre le secteur privé et les autorités chargées de l'application de la loi, de protection des infrastructures d'informations critiques, de conservation des données et autres questions connexes. Les documents et meilleures pratiques dans ces domaines peuvent être consultés sur le site www.coe.int/economiccrime.
- La coopération entre les organismes chargés de l'application de la loi et les entreprises du secteur privé en Serbie.

Les mesures à prendre

- Il conviendrait de continuer à développer et étendre les partenariats entre les secteurs public et privé.
- Dans le même temps, les limites des partenariats entre les secteurs public et privé devraient être évaluées de manière plus approfondie.
- Les acteurs régionaux devraient être identifiés et intégrés en plus des acteurs mondiaux.
- Des lignes directrices ou des règles en matière de partenariats public-privé devraient être définies sur la base de bonnes pratiques.

7 LE ROLE DES FOURNISSEURS DE SERVICES

Le défi à relever

Les fournisseurs de services jouent un rôle important dans le succès futur du réseau. Sans les services proposés par les fournisseurs d'accès, il serait impossible d'atteindre l'objectif visant à assurer à un maximum de personnes un accès aux sources Internet. Sans les capacités de stockage mises à disposition par les hébergeurs, souvent à titre supplémentaire sans frais, les utilisateurs d'Internet dans les pays en développement perdraient un instrument d'échange important avec les autres utilisateurs. Si ces intérêts des utilisateurs doivent être protégés et défendus, la législation doit prendre en considération la protection du travail des fournisseurs d'accès. Il conviendra notamment d'examiner la limitation de leur responsabilité pénale pour les infractions commises par leurs clients.

En plus de sécuriser les connexions Internet, les fournisseurs de services jouent un rôle majeur dans les investigations sur Internet. Ils peuvent tout particulièrement aider la police et les organismes chargés de l'application de la loi à :

- bloquer l'accès à des sites Internet,
- identifier et supprimer des contenus illicites,
- identifier les auteurs d'infractions,
- installer des outils d'investigation,
- collecter des données (conservation des données),
- prévenir les infractions (violation des droits d'auteur, spam).

Les bonnes pratiques à partager

- Le débat sur l'ajustement des obligations et des droits des fournisseurs de services vient de reprendre.
- La Directive de l'UE sur le e-commerce énonce des principes de base.
- La Convention sur la Cybercriminalité, eu égard à l'obligation des fournisseurs de services d'apporter leur aide aux organismes chargés de l'application de la loi.

Les mesures à prendre

- Le débat ouvert sur le rôle des fournisseurs de services et le cadre juridique correspondant devrait se poursuivre. Les bonnes pratiques devraient être recueillies afin de définir des normes ou lignes directrices communes.

En bref :

1. Améliorer l'analyse de la cybercriminalité, faciliter la déclaration des infractions par les victimes, renforcer la sensibilisation et promouvoir des mesures visant à protéger les individus, les utilisateurs des secteurs public et privé ainsi que les infrastructures critiques.
2. Mettre en œuvre la Convention sur la Cybercriminalité et son Protocole, et apporter tout le soutien nécessaire à cet égard.
3. Partager les informations relatives à la législation sur la cybercriminalité et analyser son efficacité.
4. Prendre des mesures afin d'améliorer le fonctionnement des points de contact du réseau 24/7.
5. Adopter une approche pragmatique de la mise en œuvre de coopérations entre différentes initiatives et organisations ; créer des réseaux et exploiter les possibilités qui existent.
6. Prendre des mesures pour renforcer les partenariats public-privé.
7. En ce qui concerne le rôle des fournisseurs de services : recueillir les bonnes pratiques et envisager de définir des lignes directrices communes en veillant au bon équilibre entre les besoins en matière de sécurité et les droits au respect de la vie privée.

En résumé : Coopérer.

Strasbourg, le 12 juin 2007