CONSEIL DE L'UNION
EUROPÉENNE

FR

Conclusions du Conseil relatives à une stratégie de travail concertée et à des mesures concrètes de lutte contre la cybercriminalité

2908ème session du Conseil JUSTICE et AFFAIRES INTERIEURES
Bruxelles, les 27 et 28 novembre 2008

Le Conseil a adopté les conclusions suivantes:

"RAPPELANT QUE:

- l'un des objectifs de l'Union européenne est la mise en place progressive d'un espace de justice, de liberté et de sécurité par l'élaboration d'actions communes entre les États membres dans le domaine de la coopération policière et judiciaire;

- la protection des Européens est une des missions essentielles de l'Europe. L'Union doit donc être en mesure de détecter les formes émergentes de criminalité et d'adapter son action afin que des ripostes efficaces soient mises en place rapidement;

- les infractions relevées sur internet sont en augmentation constante ces dernières années et sont de plus en plus transnationales, internet abolissant les frontières;

P R E S S E

Rue de la Loi 175 B – 1048 BRUXELLES Tél.: +32 (0)2 281 8239/ 6319 Fax: +32 (0)2 281 8026
press.office@consilium.europa.eu http://www.consilium.europa.eu./Newsroom

- la priorité donnée à une stratégie visant à lutter contre la criminalité organisée et la criminalité informatique a été établie lors du Conseil européen de Tampere en octobre 1999. Elle a depuis été confirmée au travers de nombreux travaux menés par les institutions européennes, notamment la communication de la Commission au Parlement européen, au Conseil et au Comité des régions intitulée: "vers une politique générale en matière de lutte contre la cybercriminalité" du 22 mai 2007 et la décision−cadre 2005/222/JAI du 24 février 2005 relative aux attaques visant les systèmes d'information[1], que la Commission a l'intention de mettre à jour en 2009;

- la Commission effectuera, au plus tard le 15 septembre 2010, une évaluation de l'application de la directive 2006/24/CE du Parlement Européen et du Conseil du 15 mars 2006 relative à la conservation des données;
- la Commission et le Conseil de l'Europe ont déjà œuvré pour renforcer les partenariats entre autorités publiques et secteur privé en vue de lutter contre la cybercriminalité;

- la Commission présentera une communication sur les priorités futures dans le domaine de liberté, de sécurité et de justice en Europe qui préfigurera le prochain programme pluriannuel (2010-2014) et qui devrait aborder la lutte contre la cybercriminalité;

- l'adoption par le Conseil des conclusions relatives à l'établissement de dispositifs nationaux permettant d'alimenter une plate-forme européenne de signalement des infractions relevées sur internet[1] traduit cette volonté de renforcer la coopération policière en dotant les services de police de moyens efficaces et ambitieux;

- enfin, la mise au point d'un plan d'ensemble contre la cybercriminalité apparaît comme la méthode de travail la plus appropriée au niveau de l'Union pour trouver des solutions à toutes les questions qui se posent ou qui sont susceptibles de se poser dans un avenir proche en la matière et pour assurer le suivi de leur mise en œuvre;

LE CONSEIL:

1) ESTIME qu'il est important de lutter contre la cybercriminalité dans ses différents composants et invite les États membres et la Commission à définir une stratégie de travail concertée, en prenant en considération le contenu de la Convention du Conseil de l'Europe sur la cybercriminalité.

   La finalité de cette stratégie devrait être de permettre de faire face encore plus efficacement aux multiples activités criminelles commises à l'aide de réseaux électroniques qui prennent des formes aussi préoccupantes que la pédopornographie, toute forme de violence sexuelle, et tout acte terroriste, tel que défini par la décision−cadre 2002/475/JAI du 13 juin 2002. Elle devrait également contribuer à répondre aux menaces spécifiques qui pèsent sur les réseaux électroniques (attaques de grande envergure dirigées contre les systèmes d'information).

   Enfin, cette stratégie devrait aborder les moyens de lutter contre les formes traditionnelles d'activités criminelles commises via internet, comme la fraude à l'identité, le vol d'identité, les ventes frauduleuses, les infractions financières, le commerce illicite sur internet, notamment le trafic de stupéfiants et d'armes;

---

[1] JO L 69 du 16.3.2005, p. 67.

[1] Doc. 13243/08 ENFOPOL 162 CRIMORG 140.

2) CONSIDÈRE que la recherche d'une réponse efficace à ces différentes menaces liées aux réseaux électroniques doit se traduire par des mesures horizontales telles que:

a) le renforcement du partenariat entre autorités publiques et secteur privé en vue de l'élaboration conjointe de méthodes de détection et de prévention des dommages causés par les activités criminelles et de la communication des informations pertinentes relatives à la fréquence des délits par les sociétés victimes aux services répressifs. En particulier, il est recommandé que la Commission travaille à la déclinaison des lignes directrices adoptées par la Conférence sur la coopération globale contre la cybercriminalité, réunie sous les auspices du Conseil de l'Europe les 1er et 2 avril 2008, visant à améliorer le partenariat entre autorités publiques et secteur privé dans le cadre de la lutte contre la cybercriminalité. Dans ce contexte, le Conseil prend note des recommandations faites à l'issue de la réunion d'experts organisée par la Commission les 25 et 26 septembre de cette année, figurant en annexe;

b) l'amélioration de la connaissance et de la formation parmi les acteurs engagés dans la lutte contre la cybercriminalité en Europe. Plus particulièrement, il s'agirait de mettre en place un réseau des chefs de service de lutte contre la cybercriminalité. Cette initiative viendrait en effet compléter utilement les travaux engagés par les groupes d'experts actifs dans ce domaine, qui ne tiendra pas seulement compte des risques futurs, mais aussi des procédures en cas d'actions urgentes relatives à des incidents graves, à l'image du groupe constitué sous l'égide d'Europol, ou par les centres communs de recherche, mis en place par la Commission.

c) le renforcement de la coopération technique internationale avec les pays tiers, confrontés de plus en plus souvent à ce fléau criminel, ainsi que de l'assistance technique;

3) INVITE, dans cette perspective, les États membres et la Commission à présenter des mesures se fondant sur des études de cas tenant notamment compte des évolutions technologiques, afin de préparer, à court et à moyen terme, des outils à vocation opérationnelle, tels que:

a) à court terme:

- la création d'une plate−forme européenne de signalement des faits de nature délictuelle et criminelle commis sur internet;
- l'élaboration, en consultation avec les opérateurs privés, d'un modèle d'accord européen en matière de coopération entre les services répressifs et les opérateurs privés;
- la formulation d'une description de ce que signifie l'usurpation d'identité sur internet, dans le respect des législations nationales;
- la création de cadres nationaux et la mise en place d'échanges de bonnes pratiques telles que les cyberpatrouilles, outil moderne de lutte contre la criminalité sur internet, permettant le partage de l'information sur les pseudonymes au niveau européen conformément aux lois nationales en matière d'échange des données;
- le recours aux équipes communes d'enquêtes et d'investigations;
- une solution aux problèmes posés par l'itinérance dans les réseaux électroniques et par l'anonymisation des produits de télécommunication prépayés;

b) à moyen terme:

- la mise en place d'échanges de bonnes pratiques sur les dispositifs de blocage et / ou de fermeture des sites pédopornographiques dans les États membres. Les prestataires de services devraient être encouragés à adopter ces mesures. La plate−forme européenne pourrait être, si nécessaire, l'outil permettant d'établir une liste noire commune;
- la facilitation des perquisitions à distance, si cela est prévu en vertu du droit national, permettant aux services d'enquête d'accéder rapidement aux informations, avec l'accord du pays hôte;
- le développement de définitions provisoires de catégories d'infractions et d'indicateurs statistiques afin de promouvoir la collecte de statistiques comparables sur les différentes formes de cybercriminalité, en tenant compte des travaux actuels de l'Union européenne dans ce domaine;

4) INVITE la Commission à évaluer les progrès accomplis dans la préparation de la mise en œuvre des actions visées aux points 2 et 3 ci-dessus, et demande aux États membres de l'informer de leurs contributions;

5) APPELLE à la mise en place de mesures complémentaires à plus long terme dans le cadre du prochain programme multiannuel JLS (2010-2014).

ANNEXE

1. Les autorités répressives et le secteur privé[1] devraient être encouragés à s'engager dans des échanges de données opérationnels et stratégiques afin de renforcer leur capacité d'identification et de lutte contre les catégories de cybercriminalité émergentes. Les autorités répressives devraient être encouragées à informer les fournisseurs d'accès des tendances cybercriminelles.

2. En particulier, les États membres sont encouragés à mettre en place un système standard d'échanges des données opérationnelles et stratégiques entre les services répressifs et le secteur privé. Parmi les composantes essentielles de ce système, l'on compte les structures et les procédures suivantes:

3. Des points de contact permanents: des points de contact policiers permanents – et des équivalents dans le secteur privé – devraient être mis en place afin d'améliorer la clarté et l'efficacité des processus de requête et de réponse. L'homologue du secteur privé devrait également fournir un service "en dehors des heures ouvrées" afin de répondre aux demandes urgentes des services répressifs. La qualification "urgent" devrait faire l'objet d'un accord entre les services répressifs et le secteur privé.

---

[1] Le terme "secteur privé" n'inclut pas seulement les entreprises du secteur privé, mais également les autres acteurs concernés de l'industrie des technologies de l'information et de la communication (TIC), y compris les équipes de réponse à une urgence informatique (CERT).

4. Les services répressifs et le secteur privé sont encouragés à s'assister mutuellement par le biais de formations, d'un soutien pédagogique et d'un soutien des services et opérations effectués.

5. Formulaire de requête standard: au niveau national, et si possible aux côtés des pays tiers, les services de police devraient standardiser et structurer le formulaire d'émission et de réponse aux requêtes. Le secteur privé devrait utiliser ledit formulaire lors de ses réponses à des requêtes de la police. Les requêtes policières devraient être au moins écrites, de préférence au format électronique, et contenir les informations suivantes:
   - numéro de référence,
   - référence à une base juridique,
   - les données spécifiques demandées,
   - le délai,
   - les informations permettant de vérifier la source de la requête.

6. Niveaux de priorité de la requête: le secteur privé et les services répressifs devraient convenir d'un système établissant les priorités parmi les requêtes policières transmises au secteur privé.

7. Les services répressifs et le secteur privé devraient garder à l'esprit les coûts occasionnés par la création de requêtes et la réponse à celles-ci. Des procédures devraient être mises en place afin de tenir compte de l'impact financier de ces activités. Un défraiement des coûts ou un dédommagement des Parties concernées devrait être envisagé.

8. La Commission européenne, les États membres et les acteurs du secteur privé sont appelés à faciliter les échanges de bonne pratiques, en vertu des points 1-7 ci-dessus, afin de rapprocher les dispositifs nationaux et, à terme, de créer un système d'échanges des données opérationnelles et stratégiques au niveau européen. "