COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 22.5.2007
COM(2007) 267 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL ET AU COMITÉ DES RÉGIONS

Vers une politique générale en matière de lutte contre la cybercriminalité

{SEC(2007) 641}
{SEC(2007) 642}

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL ET AU COMITÉ DES RÉGIONS

Vers une politique générale en matière de lutte contre la cybercriminalité

1. INTRODUCTION

1.1. Qu'est-ce que la cybercriminalité?

La sécurité des systèmes d'information, de plus en plus importants dans nos sociétés, recouvre de nombreux aspects, dont la lutte contre la cybercriminalité, qui en est un élément fondamental. Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes «cybercriminalité», «criminalité informatique» ou «criminalité liée à la haute technologie» sont souvent utilisés indifféremment. Aux fins de la présente communication, «cybercriminalité» s'entend des «infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'information ou contre ces réseaux et systèmes».

Dans la pratique, le terme «cybercriminalité» englobe trois catégories d'activités criminelles. La première comprend les **formes traditionnelles de criminalité**, telles que la fraude ou la falsification, même si, dans le contexte de la criminalité dans le cyberespace, elle concerne en particulier les infractions commises par l'intermédiaire de réseaux de communications électroniques et de systèmes d'information (ci-après: «réseaux électroniques)». La deuxième concerne la publication de **contenus illicites** par voie électronique (par exemple, ceux ayant trait à la violence sexuelle exercée contre des enfants ou à l'incitation à la haine raciale). La troisième vise les **infractions propres aux réseaux électroniques**, c'est-à-dire les attaques visant les systèmes d'information, le déni de service et le piratage. Ces atteintes peuvent aussi être portées contre des infrastructures critiques fondamentales en Europe et toucher des dispositifs d'alerte rapide dans de nombreux domaines, ce qui pourrait avoir des conséquences désastreuses pour l'ensemble de la société. Le point commun de ces catégories d'infractions est que celles-ci peuvent être commises à grande échelle et que la distance géographique entre le lieu de commission de l'acte délictueux et ses effets peut être considérable. Cela explique que les aspects techniques des méthodes d'investigation appliquées sont souvent identiques. Par conséquent, la présente communication sera axée sur ces points communs.

1.2. Dernières évolutions en matière de cybercriminalité

1.2.1. Généralités

En raison d'une évolution constante des activités criminelles associée à un manque d'informations fiables, il est difficile de se faire une idée exacte de la situation actuelle. Quelques tendances générales se dégagent toutefois:

- Le nombre de délits informatiques augmente et les activités criminelles se sophistiquent et s'internationalisent de plus en plus[1].

- Il apparaît clairement que des groupes criminels organisés sont de plus en plus impliqués dans la cybercriminalité.

- Cependant, le nombre des poursuites engagées en Europe dans le cadre de la coopération transfrontalière entre les services répressifs n'augmente pas.

1.2.2. Criminalité traditionnelle dans le cadre de réseaux électroniques

La plupart des infractions sont commises à l'aide de réseaux électroniques et différents types de fraude ou de tentative de fraude constituent des formes de criminalité particulièrement courantes et croissantes sur les réseaux électroniques. Des outils tels que le vol d'identité, le hameçonnage («phishing»)[2], les pourriels («spams») et les programmes malveillants peuvent être utilisés pour commettre des fraudes à grande échelle. Le commerce illicite sur Internet, national et international, est également un problème qui se pose de manière de plus en plus aiguë. Il inclut le trafic de stupéfiants, d'espèces menacées et d'armes.

1.2.3. Contenus illicites

Un nombre croissant de sites au contenu illicite sont accessibles en Europe. Ils montrent des images de violence sexuelle exercée contre des enfants, incitent à la commission d'actes terroristes, font l'apologie de la violence, du terrorisme, du racisme et de la xénophobie. L'action répressive contre ces sites est très difficile à mettre en œuvre car les propriétaires et gestionnaires de site se trouvent souvent dans d'autres pays que le pays visé, et souvent en dehors de l'Union. Ces sites peuvent être déplacés très rapidement, également en dehors du territoire de l'UE et la définition de l'illégalité varie considérablement d'un État à l'autre.

1.2.4. Criminalité propre aux réseaux électroniques

Les attaques de grande envergure dirigées contre des systèmes d'information, des organisations ou des particuliers (souvent à l'aide de «botnets»[3]) semblent de plus en plus fréquentes. De même, des incidents sous la forme d'attaques directes de caractère systématique, bien coordonnées et de grande envergure perpétrées contre les infrastructures d'information critiques d'un État ont récemment été observés. Ce phénomène a été aggravé par la fusion des technologies et l'interconnexion accélérée des systèmes d'information, qui ont rendu ces derniers plus vulnérables. Les attaques sont souvent bien organisées et perpétrées à des fins d'extorsion. L'on peut supposer que le nombre des attaques rapportées est minimisé, notamment en raison du préjudice commercial susceptible de résulter de la révélation de problèmes de sécurité.

---

1 La plupart des observations relatives aux tendances actuelles figurant dans la présente communication sont extraites de l'étude relative à l'incidence d'une communication sur la cybercriminalité, commandée par la Commission en 2006 (contrat n° JLS/2006/A1/003).

2 Le hameçonnage désigne la pratique frauduleuse qui consiste à tenter d'obtenir des informations sensibles, telles que des mots de passe ou des coordonnées de cartes de crédit, en se faisant passer pour une personne de confiance dans le cadre d'une communication électronique.

3 Par «botnet» (réseau de machines zombies), on entend un groupe d'ordinateurs compromis qui, sous un contrôle commun, exécutent des programmes.

1.3. Objectifs

Compte tenu de cet environnement en mutation, il est urgent de prendre des mesures – aux niveaux national et européen – contre toutes les formes de cybercriminalité qui constituent des menaces de plus en plus lourdes pour les infrastructures critiques, la société, les entreprises et les citoyens. La protection des personnes contre la cybercriminalité est souvent compliquée par des problèmes relatifs à la détermination de la juridiction compétente, au droit applicable, à la répression transfrontalière ou à la reconnaissance et l'utilisation de preuves électroniques. La nature essentiellement transfrontalière de la cybercriminalité accentue ces difficultés. Pour faire face à ces menaces, la Commission lance une initiative en faveur d'une politique générale visant à améliorer la coordination de la lutte contre la cybercriminalité à l'échelle européenne et internationale.

L'objectif est de renforcer la lutte contre ce phénomène aux niveaux national, européen et international. Les États membres et la Commission estiment depuis longtemps que la poursuite de l'élaboration d'une politique de l'UE à part entière constitue une priorité. L'initiative sera axée sur deux dimensions de cette lutte, a répression et le droit pénal. La politique qui en résultera viendra compléter d'autres mesures prises par l'Union pour améliorer la sécurité dans le cyberespace en général. Elle portera sur les éléments suivants: l'amélioration de la coopération opérationnelle entre les services répressifs, l'amélioration de la coopération et de la coordination politiques entre les États membres, la coopération politique et juridique avec les pays tiers, la sensibilisation, la formation, la recherche, le renforcement du dialogue avec l'industrie et d'éventuelles mesures législatives.

La politique relative à la lutte contre la cybercriminalité et aux poursuites engagées contre celle-ci sera définie et mise en œuvre dans le plein respect des droits fondamentaux, notamment de la liberté d'expression, du respect de la vie privée et familiale et de la protection des données à caractère personnel. Toute mesure législative prise dans le cadre de cette politique sera tout d'abord examinée au regard de sa compatibilité avec ces droits, notamment ceux consacrés par la charte des droits fondamentaux de l'UE. Il convient de noter que toutes les initiatives de cette nature seront menées en tenant dûment compte des articles 12 à 15 de la directive sur le commerce électronique[4], pour autant que cet instrument juridique soit applicable.

L'objectif de la présente communication peut être scindé en trois grands volets opérationnels, synthétisés comme suit:

- Améliorer et faciliter la coordination et la coopération entre les unités spécialisées dans la cybercriminalité, d'autres autorités compétentes et d'autres experts dans l'Union européenne.

- Élaborer, grâce à une collaboration avec les États membres, les organisations et parties concernées compétentes au niveau international et de l'Union, un cadre politique cohérent pour l'Union en matière de lutte contre la cybercriminalité.

- Sensibiliser aux coûts et aux dangers que comporte la cybercriminalité.

---

[4] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (JO L 178 du 17.7.2000, p. 1).

2. INSTRUMENTS JURIDIQUES EN VIGUEUR EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE

2.1. Instruments et mesures adoptés au niveau de l'UE

La présente communication relative à la politique en matière de cybercriminalité consolide et développe la communication de 2001 intitulée «Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité»[5] (ci-après: «la communication de 2001»). Celle-ci proposait des dispositions législatives pertinentes, de fond et de procédure, pour réprimer les activités criminelles nationales et transnationales. Plusieurs propositions importantes en ont résulté, notamment celle qui a donné lieu à la décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information[6]. Dans ce contexte, il convient également de noter que d'autres instruments législatifs, plus généraux, ont été adoptés qui portent aussi sur des aspects de la lutte contre la cybercriminalité, tels que la décision-cadre 2001/413/JAI concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[7].

La décision-cadre 2004/68/JAI relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie[8] illustre bien l'attention particulière accordée par la Commission à la **protection des enfants**, notamment contre toutes les formes de contenus illicites ayant trait à la violence sexuelle exercée contre les enfants qui sont publiés par l'intermédiaire de systèmes d'information, une priorité horizontale qui sera maintenue à l'avenir.

Pour relever les défis de sécurité qui se posent à la société de l'information, la Communauté européenne a élaboré une triple approche à l'égard de la sécurité des réseaux et de l'information: des mesures spécifiques relatives à la sécurité des réseaux et de l'information, le cadre réglementaire pour les communications électroniques et la lutte contre la cybercriminalité. Bien que ces trois volets puissent, dans une certaine mesure, être élaborés séparément, leurs nombreuses interdépendances plaident pour une coordination étroite. Dans le domaine connexe de la sécurité des réseaux et de l'information, une communication de la Commission, intitulée «Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne»[9], a été adoptée en 2001, parallèlement à celle consacrée à la cybercriminalité la même année. La directive 2002/58/CE «Vie privée et communications électroniques» fait obligation aux fournisseurs de services de communications électroniques accessibles au public de garantir la sécurité de leurs services. Elle contient aussi des dispositions contre le pourriel («spam») et les espiogiciels («spyware»). La politique relative à la sécurité des réseaux et de l'information a été complétée depuis par plusieurs mesures, tout récemment dans la communication intitulée «Une stratégie pour une société de l'information sûre»[10], qui expose une stratégie revitalisée et définit le cadre permettant d'approfondir et de préciser une approche cohérente en matière de sécurité des réseaux et de l'information, ainsi que dans la communication sur la lutte contre le pourriel, les espiogiciels et les logiciels malveillants[11], et par la création en 2004 de l'Agence européenne chargée de la sécurité des

---

5 COM(2000) 890 du 26.1.2001.
6 JO L 69du 16.3.2005, p. 67.
7 JO L 149 du 2.6.2001, p. 1.
8 JO L 13 du 20.1.2004, p. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.

réseaux et de l'information[12]. L'Agence a pour principal objectif d'acquérir des compétences spécialisées pour encourager la coopération entre les acteurs des secteurs public et privé, ainsi que de prêter assistance à la Commission et aux États membres. Les **résultats des recherches** menées dans le domaine technologique pour sécuriser les systèmes d'information joueront également un rôle majeur dans la lutte contre la cybercriminalité. Par conséquent, les technologies de l'information et de la communication ainsi que la sécurité figurent parmi les objectifs du septième programme-cadre de recherche de l'UE (7ème PC), qui sera opérationnel de 2007 à 2013[13]. La révision du cadre réglementaire pour les communications électroniques pourrait donner lieu à des modifications destinées à renforcer l'efficacité des dispositions relatives à la sécurité figurant dans la directive «Vie privée et communications électroniques» et la directive 2002/22/CE «Service universel»[14].

2.2. Instruments internationaux en vigueur

En raison de la nature mondiale des réseaux d'information, aucune politique de lutte contre la cybercriminalité ne peut être efficace si les efforts sont confinés à l'UE. Les auteurs d'infractions peuvent non seulement porter atteinte aux systèmes d'information ou commettre leurs délits d'un État membre à l'autre, mais ils peuvent aussi aisément le faire en dehors du ressort de l'Union. Par conséquent, la Commission participe activement à des débats et des structures de coopération internationaux, notamment au groupe de Lyon/Rome du G8 sur la criminalité de haute technologie et aux projets gérés par Interpol. Elle suit en particulier attentivement les travaux du réseau de contacts joignables 24 heures sur 24 dans le domaine de la criminalité de haute technologie internationale (le réseau 24/7)[15], auquel de nombreux pays ont adhéré, dont la plupart des États membres de l'Union. Le réseau du G8 est un mécanisme permettant d'accélérer les contacts entre les États participants, des points de contact joignables en permanence ayant été établis pour les affaires impliquant la production de preuves électroniques et celles qui requièrent d'urgence l'assistance de services répressifs étrangers.

Le principal instrument européen et international dans ce domaine est sans doute la convention de 2001 du Conseil de l'Europe sur la cybercriminalité[16]. Adoptée puis entrée en vigueur en 2004, celle-ci contient des définitions communes de différents types de cybercriminalité et jette les bases d'une coopération judiciaire opérationnelle entre les États parties. De nombreux États l'ont signée, y compris les États-Unis d'Amérique et d'autres États non européens, ainsi que tous les États membres. Un certain nombre d'États membres n'ont toutefois pas encore ratifié la convention ou son protocole additionnel relatif aux actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Vu l'importance communément accordée à la convention, la Commission encouragera les États membres et les pays tiers concernés à la ratifier et examinera la possibilité pour la Communauté européenne de devenir partie à celle-ci.

---

12 Règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

13 Dans le contexte du 6ème programme–cadre de recherche et de développement technologique, l'Union a déjà soutenu plusieurs projets de recherche pertinents et fructueux.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

15 Voir l'article 35 de la convention sur la cybercriminalité du Conseil de l'Europe.

16 http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

3. APPROFONDISSEMENT D'INSTRUMENTS SPECIFIQUES DE LUTTE CONTRE LA CYBERCRIMINALITE

3.1. Renforcer la coopération opérationnelle entre les services répressifs et les efforts de formation au niveau de l'UE

L'absence ou la sous-utilisation de structures immédiates pour la **coopération opérationnelle transfrontalière** demeure une faiblesse importante du domaine de la justice, de la liberté et de la sécurité. Dans les affaires urgentes de cybercriminalité, l'entraide traditionnelle s'avère lente et inefficace et la mise en place de nouvelles structures de coopération n'est pas encore satisfaisante. Si les services judiciaires et répressifs nationaux coopèrent étroitement en Europe par l'intermédiaire d'Europol, d'Eurojust et d'autres structures, il y a manifestement lieu de renforcer et de clarifier les responsabilités. Les consultations lancées par la Commission indiquent que l'utilisation de ces canaux fondamentaux n'est pas optimale. L'approche européenne, davantage coordonnée, doit être tant opérationnelle que stratégique et englober aussi l'échange d'informations et de bonnes pratiques.

Dans un avenir proche, la Commission insistera particulièrement sur les besoins de **formation**. Il est avéré que les évolutions technologiques requièrent une formation continue des services répressifs et judiciaires aux questions touchant à la cybercriminalité. Un soutien financier renforcé et mieux coordonné de l'UE est donc envisagé en faveur de programmes de formation multinationaux. En outre, dans le cadre d'une coopération étroite avec les États membres et d'autres organes compétents tels qu'Europol, Eurojust, le collège européen de police (CEPOL) et le réseau européen de formation judiciaire (REFJ), la Commission s'efforcera de coordonner et de relier au niveau de l'Union tous les programmes de formation pertinents.

Elle organisera en 2007 une **réunion** d'experts en matière de répression, provenant des États membres mais aussi d'Europol, du CEPOL et du REFJ, pour qu'ils débattent de la manière d'améliorer la coopération stratégique et opérationnelle, ainsi que de la formation dans le domaine de la cybercriminalité en Europe. Parmi les questions qui seront envisagées figurent l'établissement d'un point de contact permanent pour l'échange d'informations et la création d'une plate-forme de formation en matière de cybercriminalité, tous deux à l'échelon de l'UE. La réunion de 2007 sera la première d'une série de rencontres programmées dans un avenir proche.

3.2. Renforcer le dialogue avec l'industrie

Les secteurs privé et public ont tous deux intérêt à élaborer conjointement des méthodes de détection et de prévention des dommages causés par les activités criminelles. Une participation commune des secteurs privé et public, fondée sur la confiance mutuelle et un même objectif, celui de réduire les dommages, promet d'être un moyen efficace pour accroître la sécurité, également dans le cadre de la lutte contre la cybercriminalité. Les dimensions publique et privée de la politique de la Commission en matière de cybercriminalité seront, en temps utile, intégrées dans une politique globale planifiée de l'UE relative au dialogue entre les deux secteurs, englobant l'intégralité du domaine de la sécurité européenne. Cette politique sera notamment portée par le forum européen pour la sécurité, la recherche et l'innovation, que la Commission entend créer prochainement et qui regroupera les parties concernées des secteurs public et privé.

Des opérateurs privés contrôlent en grande partie l'évolution des technologies de l'information et des systèmes de communications électroniques modernes. Des entreprises privées évaluent les menaces, définissent des programmes de lutte contre la criminalité et élaborent des solutions techniques pour prévenir celle-ci. L'industrie s'est montrée très encline à aider les pouvoirs publics à combattre la cybercriminalité, notamment en ce qui concerne la lutte contre la pédopornographie[17] et d'autres types de contenus illicites sur Internet.

Une autre question concerne le manque apparent d'échanges d'informations, de compétences spécialisées et de bonnes pratiques entre les secteurs public et privé. Pour protéger des modèles et des secrets d'entreprise, les opérateurs privés rechignent souvent - la loi ne les y obligeant pas clairement - à communiquer aux services répressifs des informations pertinentes relatives à la fréquence des délits. Or, ces informations peuvent être indispensables pour que les pouvoirs publics puissent élaborer une politique de lutte contre la criminalité qui soit efficace et appropriée. Les moyens d'améliorer les échanges d'information intersectoriels seront envisagés également au regard des règles en vigueur en matière de protection des données à caractère personnel.

La Commission joue déjà un rôle important dans diverses structures, associant les secteurs public et privé, qui luttent contre la cybercriminalité, telles que le groupe d'experts en matière de prévention de la fraude[18]. Elle est persuadée qu'une politique générale efficace pour combattre la cybercriminalité doit également comprendre une stratégie de coopération entre les acteurs des secteurs public et privé, y compris les organisations de la société civile.

Pour élargir la coopération public-privé dans ce domaine, la Commission organisera en 2007 une conférence destinée aux spécialistes de la répression et aux représentants du secteur privé, notamment les fournisseurs de services Internet, pour débattre de la manière d'améliorer la coopération opérationnelle entre les deux secteurs en Europe[19]. La conférence abordera tous les thèmes jugés porteurs de valeur ajoutée pour les deux secteurs, mais surtout les questions suivantes:

- Améliorer la coopération en faveur de la lutte contre les activités et les contenus illicites sur Internet, notamment dans le domaine du terrorisme et de l'exploitation sexuelle des enfants, et contre d'autres activités illégales particulièrement sensibles du point de vue de la protection de l'enfance.

- Ébaucher des accords entre les secteurs public et privé à l'échelle de l'Union, pour bloquer les sites comportant des contenus illicites, notamment des images de violence sexuelle exercée contre des enfants.

- Concevoir un modèle européen pour le partage d'informations nécessaires et pertinentes entre les secteurs privé et public, tout en cultivant un climat de confiance mutuelle et en tenant compte des intérêts de toutes les parties.

---

17 Un exemple récent de coopération dans ce domaine est la collaboration entre des services répressifs et des sociétés émettrices de cartes de crédit, dans le cadre de laquelle celles-ci ont aidé les services de police à localiser des acheteurs de pédopornographie en ligne.

18 Voir le site http://ec.europa.eu/internal_market/payments/fraud/index_fr.htm

19 La conférence pourrait être envisagée comme le prolongement du forum de l'UE présenté au point 6.4 de la communication relative à la cybercriminalité.

- Constituer un réseau de points de contact pour la répression désignés tant dans le secteur privé et que dans le secteur public.

3.3. Législation

Une harmonisation générale des définitions des infractions et des droits pénaux nationaux dans le domaine de la cybercriminalité n'est pas encore opportune, en raison de la diversité des types d'infraction couverts par cette notion. Étant donné que l'efficacité de la coopération entre les organes répressifs dépend souvent du fait qu'ils disposent de définitions au moins partiellement harmonisées des infractions, la poursuite du rapprochement des législations des États membres reste un objectif à long terme[20]. En ce qui concerne certaines définitions d'infractions fondamentales, une étape importante a déjà été franchie avec la décision-cadre relative aux attaques visant les systèmes d'information. Comme expliqué ci-dessus, de nouvelles menaces sont ensuite apparues et la Commission suit attentivement cette évolution, compte tenu de l'importance d'une évaluation continue des besoins en matière législative. La surveillance de ces menaces évolutives fait l'objet d'une coordination étroite avec le programme européen de protection des infrastructures critiques.

Il convient toutefois d'envisager dès maintenant l'adoption d'instruments législatifs ciblés pour lutter contre la cybercriminalité. Un problème particulier susceptible de nécessiter l'adoption d'une réglementation concerne les délits informatiques commis dans le cadre d'un **vol d'identité**. Généralement, par «vol d'identité» on entend l'utilisation de données d'identification personnelles, par exemple un numéro de carte de crédit, pour commettre d'autres infractions. Dans la plupart des États membres, l'auteur sera très probablement poursuivi pour fraude, ou un éventuel autre délit, plutôt que pour l'usurpation d'identité, la fraude étant considérée comme une infraction plus grave. Le vol d'identité en tant que tel n'a pas fait l'objet d'une criminalisation dans tous les États membres. Il est souvent plus aisé de prouver ce délit que celui de fraude, de sorte que la coopération européenne en matière de répression bénéficierait du fait que l'usurpation d'identité soit érigée en infraction pénale dans tous les États membres. En 2007, la Commission engagera des consultations pour déterminer s'il est judicieux de légiférer.

3.4. Élaboration de statistiques

Il est communément admis que l'information relative à la fréquence des délits est nettement insuffisante et qu'il convient notamment de l'améliorer sensiblement pour permettre une comparaison des données entre les États membres. La communication de la Commission intitulée *Élaboration d'une stratégie globale et cohérente de l'UE en vue de l'établissement de statistiques sur la criminalité et la justice pénale: Plan d'action de l'UE 2006–2010*[21], exposait un plan quinquennal ambitieux visant à résoudre à ce problème. Le groupe d'experts institué dans le cadre de ce plan d'action devait constituer un forum adéquat pour élaborer des indicateurs pertinents permettant d'apprécier l'ampleur de la cybercriminalité.

4. LA VOIE A SUIVRE

La Commission entend désormais approfondir la politique générale de lutte contre la cybercriminalité. Vu les pouvoirs limités dont l'institution dispose dans le domaine du droit

---

[20] Cet objectif à long terme était déjà mentionné à la page 3 de la communication de 2001.

[21] COM(2006) 437 du 7.8.2006.

pénal, cette politique ne peut que compléter les mesures prises par les États membres et d'autres instances. Les mesures les plus importantes – chacune impliquera le recours à l'un ou plusieurs des instruments présentés au chapitre 3, voire tous – seront également soutenues par le programme financier «Prévenir et combattre la criminalité».

4.1. La lutte contre la cybercriminalité en général

- Établir une coopération opérationnelle renforcée entre les instances répressives et judiciaires des États membres. Cette action débutera par l'organisation d'une réunion spécialisée d'experts en 2007 et pourrait comporter l'instauration d'un point de contact central de l'UE en matière de cybercriminalité.

- Accroître le soutien financier accordé aux initiatives destinées à améliorer la formation des services répressifs et judiciaires en matière de traitement des affaires de cybercriminalité et prendre des mesures pour coordonner tous les efforts de formation multinationaux dans ce domaine en créant une plate-forme de formation de l'UE.

- Encourager les États membres et tous les pouvoirs publics à s'engager plus résolument à prendre des mesures efficaces contre la cybercriminalité et à allouer suffisamment de ressources à la lutte contre ce phénomène.

- Soutenir la recherche contribuant à la lutte contre la délinquance dans le cyberespace.

- Organiser au moins une grande conférence (en 2007), rassemblant des organes répressifs et des opérateurs privés, notamment pour lancer une coopération dans la lutte contre les activités illicites menées sur Internet par l'intermédiaire de réseaux électroniques et contre de tels réseaux, pour promouvoir un échange plus efficace de données à caractère non personnel et pour envisager des projets concrets de coopération entre le public et le privé afin de donner suite aux conclusions de cette conférence de 2007.

- Prendre l'initiative d'actions associant les secteurs public et privé et y participer, afin de sensibiliser le public, notamment les consommateurs, aux coûts et aux dangers que représente la cybercriminalité, tout en évitant de saper la confiance des consommateurs et utilisateurs en ne se concentrant que sur les aspects négatifs de la sécurité.

- Participer activement à une coopération internationale globale en matière de lutte contre la cybercriminalité et promouvoir celle-ci.

- Mettre en place et soutenir des projets internationaux conformes à la politique de la Commission dans ce domaine, par exemple ceux dirigés par le G8, ainsi que des projets compatibles avec les documents de stratégie régionale ou nationale (en matière de coopération avec les pays tiers) et y contribuer.

- Prendre des mesures concrètes pour encourager tous les États membres et pays tiers concernés à ratifier la convention du Conseil de l'Europe sur la cybercriminalité et son protocole additionnel, et examiner la possibilité pour la Communauté de devenir partie à celle-ci.

- Prendre des mesures en vue d'examiner, avec les États membres, le phénomène d'attaques coordonnées et à grande envergure perpétrées contre les infrastructures de l'information

des États membres et de proposer des mesures visant à les prévenir et les combattre, incluant la coordination des réponses et l'échange d'informations et de bonnes pratiques.

4.2. La lutte contre la criminalité traditionnelle dans le cadre des réseaux électroniques

- Entreprendre une analyse approfondie dans la perspective de l'élaboration d'une proposition de réglementation spécifique de l'UE pour lutter contre le vol d'identité.

- Promouvoir l'élaboration de techniques et de procédures pour combattre la fraude et le commerce illicite sur Internet, également dans le cadre de projets de coopération associant les secteurs public et privé.

- Poursuivre et approfondir les travaux réalisés dans des domaines spécifiques ciblés, tels que ceux que le groupe d'experts en matière de prévention de la fraude consacre à la lutte contre la fraude portant sur des moyens de paiement autres que les espèces et commise dans le cadre de réseaux électroniques.

4.3. Contenus illicites

- Continuer à élaborer des mesures de lutte contre des contenus illicites spécifiques, en particulier ceux qui ont trait à la violence sexuelle exercée contre les enfants ou qui font l'apologie du terrorisme, et notamment en assurant le suivi de la mise en œuvre de la décision-cadre relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie.

- Inviter les États membres à allouer suffisamment de moyens financiers pour intensifier le travail des organes répressifs, en accordant une attention particulière à l'identification des victimes de violence sexuelle apparaissant sur des images diffusées en ligne.

- Lancer et soutenir des actions de lutte contre les contenus illicites susceptibles d'inciter des mineurs à adopter des comportements violents ou des comportements illicites graves, notamment certains types de jeux vidéo extrêmement violents accessibles en ligne.

- Engager et promouvoir le dialogue entre les États membres et avec des pays tiers concernant les techniques de lutte contre les contenus illicites ainsi que les procédures de fermeture de sites web illégaux, également en vue de la possible conclusion d'accords formels avec des pays voisins et d'autres pays sur cette question.

- Conclure des accords volontaires et des conventions au niveau de l'UE, entre les pouvoirs publics et les opérateurs privés, notamment les fournisseurs de services Internet, portant sur les procédures de blocage et de fermeture des sites Internet illégaux.

4.4. Suivi

La présente communication décrit, en guise de prochaines étapes, un certain nombre de mesures visant à améliorer les structures de coopération dans l'UE. La Commission donnera suite à ces mesures, elle évaluera les progrès accomplis dans la mise en œuvre des actions envisagées et elle fera rapport au Conseil et au Parlement.