COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 22.5.2007
SEC(2007) 641

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

Document accompagnant la

**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

Résumé de l'analyse d'impact

{COM(2007) 267 final}
{SEC(2007) 642}

RÉSUMÉ

1. INTRODUCTION

L'utilisation d'Internet a explosé ces dernières années et l'apparition de nouveaux phénomènes et de nouvelles techniques a instauré un climat d'insécurité accrue.

Dans son **programme législatif et de travail pour 2007**, la Commission a estimé qu'une révision globale de sa politique en matière de cybercriminalité était devenue nécessaire et a donc envisagé l'élaboration d'une communication sur une politique européenne de lutte contre la cybercriminalité.

Durant la phase initiale de consultations, il est apparu que les données et les statistiques étaient insuffisantes, une des raisons principales pour lesquelles la Commission a commandé en 2006 une **étude externe**[1] qui constitue la principale base de la présente analyse d'impact.

Durant l'étape préparatoire, la Commission a également analysé un certain nombre de mesures législatives et non législatives, notamment sous l'angle d'éventuelles «lacunes» dans le cadre réglementaire existant. Il convient de souligner qu'elle a ainsi accordé une attention particulière à la **convention du Conseil de l'Europe relative à la cybercriminalité**[2] et à la **décision-cadre relative aux attaques visant les systèmes d'information**[3], car elle considérait que celles-ci étaient les instruments les plus complets en termes de dispositions de fond et de procédure.

Sur cette base, la Commission prépare une nouvelle initiative relative à une politique générale, comprenant une communication sur la lutte contre la cybercriminalité au niveau de l'UE. La présente analyse d'impact sera donc essentiellement axée sur des questions stratégiques.

Dans ce contexte, la Commission tient à souligner qu'elle s'engage à veiller à ce que la politique relative à la lutte contre la cybercriminalité et aux poursuites engagées contre celle-ci soit définie et mise en œuvre dans le plein respect des droits fondamentaux, notamment de la liberté d'expression, du droit au respect de la vie privée et familiale et de la protection des données à caractère personnel. Elle procédera conformément à sa communication intitulée «Le respect de la Charte des droits fondamentaux dans les propositions législatives de la Commission», adoptée en 2005 - COM(2005) 172.

2. PROBLEMES ET OBJECTIFS

Le développement rapide d'Internet et d'autres systèmes d'information a donné naissance à un secteur économique totalement nouveau et à de nouveaux flux d'informations, de produits et de services franchissant rapidement les frontières intérieures et extérieures de l'Union. Les

---

[1] Study to Assess the Impact of a Communication on Cyber Crime (étude relative à l'incidence d'une communication sur la cybercriminalité), élaborée par Yellow Window Management Consulting (contrat n° DG 2006/JLS D 2/03).

[2] Convention du Conseil de l'Europe de 2001 relative à la cybercriminalité: http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

[3] Décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information.

consommateurs et les citoyens en tirent manifestement de nombreux avantages. Cependant, ce même développement offre de nombreuses nouvelles possibilités aux délinquants. On perçoit clairement de nouvelles formes de criminalité s'attaquant à Internet ou instrumentalisant des systèmes d'information à des fins délictueuses. Ces activités criminelles évoluent sans cesse et la législation ainsi que la répression opérationnelle éprouvent d'évidentes difficultés à suivre le rythme. La nature transfrontalière intrinsèque de cette nouvelle criminalité requiert également une meilleure coopération transfrontalière en matière de répression.

Afin de l'analyser plus en détail, le problème général a été scindé en huit aspects stratégiques à savoir:

- La vulnérabilité croissante de la société, des entreprises et des citoyens aux risques de la cybercriminalité.
- La plus grande fréquence et sophistication des infractions dans le cyberespace.
- L'absence de politique et de législation cohérentes au niveau de l'UE en matière de lutte contre la cybercriminalité.
- Les difficultés spécifiques rencontrées dans la coopération opérationnelle pour la répression de la cybercriminalité.
- La nécessité d'accroître les compétences et de perfectionner les outils techniques: la formation et la recherche.
- L'absence de structure fonctionnelle de coopération entre les acteurs importants des secteurs public et privé.
- La définition imprécise des responsabilités.
- La sensibilisation insuffisante aux risques que comporte la cybercriminalité.

Il convient de noter que les consultations lancées aux fins du présent état des lieux ont révélé une saisissante convergence de vues de toutes les parties intéressées – qu'il s'agisse d'organes répressifs ou d'entreprises privées – en ce qui concerne les problèmes auxquels l'Union est actuellement confrontée dans ce domaine.

2.1. Qui est concerné?

La cybercriminalité touche tous les secteurs de la société et la politique de lutte contre ce phénomène sera aussi visible pratiquement partout. Étant donné le nombre très élevé d'utilisateurs d'ordinateurs personnels, la plupart des citoyens – déjà en leur qualité de victime potentielle - sont aussi susceptibles d'être concernés par les initiatives prises dans le domaine de la lutte contre la cybercriminalité.

Certains éléments clairs soulignent toutefois également une augmentation des activités criminelles qui visent des groupes de victimes particuliers. Une politique de lutte efficace pourrait donc présenter des avantages manifestes pour ces groupes. L'industrie liée à la société de l'information ainsi que la société de l'information en général pourraient aussi jouer un rôle majeur dans ce cadre, vu les importantes retombées économiques positives qu'entraînerait un renforcement de la sécurité ou l'instauration d'un climat de sécurité accrue.

2.2. L'Union a-t-elle le droit de prendre des mesures?

Vu la portée et l'ampleur des menaces pour la sécurité, il est et sera de plus en plus nécessaire de répondre aux dangers que représente la cybercriminalité. Les questions de sécurité liées à ce phénomène sont d'envergure mondiale et ne sauraient donc être traitées au seul niveau national. La menace est internationale: telle doit donc être la réponse, au moins en partie. C'est incontestablement au niveau national que la lutte contre la cybercriminalité continuera à se déployer essentiellement et avec le plus d'efficacité, mais il est de toute évidence nécessaire de relier les efforts nationaux et, éventuellement, de les compléter au niveau européen.

2.3. Objectifs

Eu égard aux problèmes décrits ci-dessus, l'objectif stratégique global de la politique proposée peut se résumer comme suit:

Renforcer et mieux coordonner la lutte contre la cybercriminalité aux niveaux national, européen et international.

Cet objectif stratégique global peut être scindé en cinq sous-objectifs stratégiques, présentés ci-après selon un ordre de priorité provisoire:

- Améliorer les actions transfrontalières opérationnelles de répression de la cybercriminalité en général et de certaines infractions graves en particulier, et améliorer les échanges d'informations, de renseignements et de bonnes pratiques entres les organes répressifs des États membres et des pays tiers.

- Définir et créer des instruments opérationnels permettant aux secteurs public et privé de coopérer et de se fixer des objectifs communs, ainsi qu'améliorer les échanges d'informations, de renseignements et de bonnes pratiques entre ces deux secteurs, aux fins de la lutte contre la cybercriminalité au niveau de l'Union.

- Établir une plate-forme et des structures politiques en vue de l'élaboration d'une politique cohérente de l'Union en matière de lutte contre la cybercriminalité, en collaboration avec les États membres et les organisations communautaires et internationales compétentes, et améliorer l'efficacité des cadres juridiques et institutionnels en place, également en clarifiant les responsabilités de tous les acteurs concernés.

- Faire face à la menace croissante que représentent certaines formes graves de cybercriminalité en encourageant l'acquisition de compétences, de connaissances et d'outils techniques, y compris en menant des actions destinées à approfondir les formations et les travaux de recherche pertinents.

- Sensibiliser le grand public à la menace que représente la cybercriminalité, notamment les consommateurs et d'autres groupes vulnérables de victimes potentielles.

3. OPTIONS DE POLITIQUE STRATEGIQUE

Toute politique de lutte contre la cybercriminalité, vu la nature de son objet, doit présenter de multiples facettes. Pour être véritablement efficace, elle doit associer des mesures répressives

traditionnelles à d'autres instruments, tels que des éléments autonomes, et inclure la mise en place de structures de coopération entre les différentes parties concernées. Un certain nombre d'aspects du problème et d'objectifs stratégiques pour la présente initiative sont présentés ci-dessus. Pour atteindre ces objectifs, il y a lieu de combiner différentes mesures. Sur la base des larges consultations qu'elle a lancées, la Commission a formulé quatre options de politique générale qui comportent chacune plusieurs actions spécifiques.

3.1. Option de politique générale n° 1: statu quo – aucune nouvelle mesure importante

Cette option signifierait que la Commission ne prendrait actuellement aucune mesure horizontale générale dans ce domaine. Elle impliquerait que la Commission:

- évalue en permanence la nécessité d'adopter une réglementation ciblée ou des mesures de politique générale, et prenne les mesures adéquates le cas échéant;
- assure le suivi des projets actuels de l'Union et des structures internationales en matière de lutte contre la cybercriminalité;
- continue à lancer de nouveaux projets dans des domaines ciblés présentant un intérêt sous l'angle de la lutte contre la cybercriminalité, mais sans prendre d'initiative de politique horizontale.

3.2. Option de politique générale n° 2: législation générale

Cette option entraînerait l'adoption d'une politique visant à proposer par étapes un cadre réglementaire général pour combattre la cybercriminalité. Une politique de cette nature impliquerait que:

- la Commission propose systématiquement des définitions harmonisées des infractions, notamment pour l'Union mais aussi au niveau international;
- la Commission propose des normes minimales communes en matière de criminalisation et de sanctions dans l'Union;
- des plates-formes formelles soient créées pour la coopération entre le public et le privé mais aussi dans le domaine de la formation et de la recherche;
- soit constitué un réseau formel pour la répression.

3.3. Option de politique générale n° 3: création de réseaux informels dans le domaine de la cybercriminalité et de réseaux associant le public et le privé

Cette option signifierait que la Commission, seule ou avec d'autres institutions, établirait officiellement des réseaux ou des groupes d'experts de la cybercriminalité, et associerait cette mesure à l'instauration d'un régime de certification volontaire de la sécurité à l'intention des opérateurs, producteurs et consommateurs. Cela impliquerait:

- de créer une instance informelle regroupant des experts de la répression de la cybercriminalité;

- d'établir une plate-forme ou un réseau informel regroupant des experts de la cybercriminalité provenant des secteurs public et privé.

3.4. Option de politique générale n° 4: une approche stratégique cohérente

Cette option entraînerait l'adoption au niveau de l'Union d'une stratégie cohérente de lutte contre la cybercriminalité. Son élément principal serait la mise en place d'un cadre stratégique pour une politique européenne de lutte contre la cybercriminalité, dans le but principal de formuler de meilleures orientations en vue d'actions concrètes et d'optimiser les ressources existantes. D'autres volets opérationnels importants de cette stratégie consisteraient à:

- améliorer la coopération en matière de répression au niveau de l'Union;
- établir une structure stratégique pour la coopération entre le public et le privé dans le domaine de la lutte contre la cybercriminalité;
- promouvoir l'établissement d'un cadre favorable à une coopération internationale globale dans le domaine concerné;
- adopter des mesures législatives ciblées le cas échéant.

4. ÉVALUATION DES OPTIONS POLITIQUES ET CHOIX DE L'UNE D'ENTRE ELLES

4.1. Évaluation

Les options de politique générale ont été évaluées au regard des critères suivants:

- répercussions sociales
- répercussions économiques
- coûts pour les administrations publiques
- degré de cohérence avec les objectifs politiques
- valeur ajoutée et respect du principe de subsidiarité
- faisabilité

Les conclusions de l'évaluation sont résumées ci-après.

4.1.1. Option de politique générale n° 1

Cette option a été jugée manifestement insuffisante par rapport aux défis existants. Les répercussions de l'option «aucune nouvelle mesure» sont en principe limitées, mais il est difficile de déterminer si celle-ci risque d'avoir d'importants effets car les types de criminalité à venir sont, par définition, inconnus. L'incidence négative potentielle de ce scénario est très forte à long terme, compte tenu de l'importance actuelle et croissante de ce type de criminalité.

4.1.2. Option de politique générale n° 2

La conclusion était que cette option ne pouvait faire l'objet que d'une mise en œuvre très minutieuse et de longue haleine. Il y aurait lieu de procéder à des études de faisabilité juridique approfondies et de mener de longues négociations politiques. Cette option pourrait avoir des répercussions très importantes, mais vu la faible probabilité que de réels progrès soient accomplis à court terme, elle est aléatoire à court terme. L'on peut également se demander si les objectifs de la politique générale seraient atteints aussi efficacement au stade de la mise en œuvre concrète des mesures qu'ils le sont aux niveaux politique et théorique. Si cette option était retenue, le risque serait que le volet opérationnel de la lutte contre la cybercriminalité ne soit pas suffisamment associé aux choix et décisions politiques stratégiques. Vu l'importance des répercussions connexes, il conviendrait également de clarifier le rôle de la Commission à cet égard. Sans doute aussi des résultats semblables pourraient-ils être obtenus avec des mesures moins interventionnistes.

4.1.3. Option de politique générale n° 3

Cette option a été jugée très intéressante d'un point de vue stratégique, même si sa valeur ajoutée et ses répercussions concrètes sont difficiles à prévoir. Le risque qu'elle comporte est que les nouvelles structures de réseau obtiennent peu de résultats tangibles. La Commission serait l'acteur idéal pour coordonner les mesures autonomes dans le domaine concerné mais, dans le cadre de cette option, elle jouerait davantage un rôle de coordination et de médiation que de direction stratégique.

4.1.4. Option de politique générale n° 4

Il a été estimé que cette option comportait plusieurs mesures stratégiques très pertinentes. Très peu de répercussions négatives ou d'obstacles majeurs apparaissent. Un des inconvénients de cette politique est qu'elle aura des retombées directes plutôt modestes. Cela n'est toutefois vrai qu'à court terme; l'adoption de mesures de mise en œuvre adéquates pourrait avoir une très forte incidence. Les répercussions concrètes restent toutefois difficiles à prévoir en détail, car le volet stratégique devra faire l'objet d'une mise en œuvre opérationnelle ultérieurement. Toutes les retombées seront évaluées alors.

Il convient une fois de plus de souligner que les effets directs des stratégies proposées sont limités et que les mesures spécifiques adoptées plus tard dans le cadre de l'une de ces stratégies seront évaluées séparément à ce stade. Cela signifie que la présente évaluation revêt un caractère préliminaire.

4.2. Choix de l'option politique

L'analyse a clairement révélé que l'option n° 4 était la meilleure. Celle-ci répond aussi le mieux aux objectifs généraux décrits au point 2.4 ci-dessus.

L'option consistant à n'adopter aucune mesure dans le domaine concerné ne semble pas viable. Une attitude passive entraînerait probablement le maintien de nombreux projets de coopération bilatérale pour lutter contre la cybercriminalité, sans qu'il soit possible de tirer profit de l'échange horizontal de bonnes pratiques ou d'effets de synergie. Une législation générale visant à créer de nouveaux organes au niveau de l'Union, à harmoniser les définitions des infractions et à clarifier les responsabilités de toutes les parties concernées pourrait s'avérer intéressante, mais une analyse de la situation politique a clairement montré que toute

proposition de réglementation générale et horizontale aurait très peu de chances d'être adoptée. En outre, très peu de parties consultées ont indiqué qu'elles estimaient qu'il s'agissait actuellement de la première priorité. Une législation générale peut cependant présenter de l'intérêt à longue échéance. La création de nouvelles structures informelles pour la coopération entre les services répressifs ou entre le public et le privé au niveau de l'Union pourrait être une bonne idée à long terme, mais toutes les parties intéressées semblent d'avis que les structures actuelles suffisent, même s'il est urgent d'en accroître l'efficacité. Suite à cette analyse, l'option n° 4 «une stratégie cohérente» a donc été privilégiée. Il convient d'observer que celle-ci n'exclut pas la création d'une structure formelle (option 3) ni l'adoption ultérieure d'une législation générale (option 2). L'option privilégiée signifie en réalité que la porte reste ouverte à de nouvelles mesures.

L'analyse préparatoire et les débats organisés indiquent clairement que la «stratégie cohérente» est l'option la plus susceptible d'atteindre les objectifs stratégiques assignés à la politique. Cette stratégie aura probablement d'importantes répercussions positives pour la lutte contre la cybercriminalité transfrontalière, car les compétences et les rôles de toutes les parties participant à ce combat seront clarifiés et renforcés. Elle contribuerait également à l'amélioration du dialogue entre les secteurs public et privé et à leur meilleure compréhension mutuelle, ce qui pourrait avoir de nombreux effets connexes positifs. D'un point de vue économique, l'option privilégiée pourrait entraîner d'importants effets de synergie, une réduction des dommages causés par les activités criminelles et une diminution des coûts supportés par les différents programmes de sécurité.

Il est toutefois probable que quelques années soient nécessaires pour que les effets de l'option retenue se matérialisent. Il est donc difficile d'apprécier à ce stade l'ensemble de ses éventuelles répercussions, d'autant plus que les détails concrets de la politique doivent encore être décidés. Il y aura donc lieu d'évaluer ultérieurement l'incidence particulière des éléments concrets de cette politique.