COMMISSION EUROPÉENNE

Bruxelles, le 28.3.2012
COM(2012) 140 final

COMMUNICATION DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité

COMMUNICATION DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité

1. INTRODUCTION: LA RÉPONSE EUROPÉENE AUX ACTIVITÉS CRIMINELLES SANS FRONTIÈRES

L'internet est désormais un constituant à part entière et indispensable de notre société et de notre économie. Quatre-vingts pour cent des jeunes européens se connectent entre eux et au monde par le biais des réseaux sociaux en ligne[1], et environ 8 billions USD changent de mains chaque année dans le monde du fait du commerce électronique[2]. Mais plus nous passons de temps en ligne au quotidien et pour nos transactions, plus l'activité criminelle s'y développe elle aussi. Plus d'un million de personnes sont victimes chaque jour de la cybercriminalité[3]. Cela va de la vente de cartes de crédit volées, parfois pour la somme d'un euro seulement, à l'usurpation d'identité et l'exploitation sexuelle des enfants ou à de graves attaques informatiques à l'encontre d'institutions et d'infrastructures.

La cybercriminalité coûte extrêmement cher à la société. Un rapport récent estime qu'à l'échelle mondiale, elle rapporte environ 388 milliards USD par an à ses auteurs, ce qui la rend plus lucrative que le marché mondial du cannabis, de la cocaïne et de l'héroïne confondues[4]. Bien qu'il faille nuancer ces chiffres, l'estimation des coûts pouvant varier selon la définition que l'on donne de la cybercriminalité, il est admis qu'elle constitue une forme de criminalité à faible risque et très rentable, de plus en plus présente et préjudiciable. À l'heure où il est primordial de stimuler la croissance économique, la lutte contre la cybercriminalité doit impérativement s'intensifier afin de préserver la confiance que les citoyens et les entreprises placent dans la communication et le commerce en ligne. Cette lutte renforcée aidera aussi à atteindre les objectifs de croissance fixés par la stratégie Europe 2020[5] et la stratégie numérique pour l'Europe[6].

La liberté de l'internet est l'élément clé qui explique la révolution numérique de ces dernières années. Notre internet sans limites ne connaît ni frontières nationales, ni structure de gouvernance mondiale. Cependant, tout en promouvant et en protégeant cette liberté en ligne conformément à la charte des droits fondamentaux de l'UE, il est de notre devoir de protéger les citoyens contre les groupes criminels organisés qui tentent d'exploiter à leurs fins cette liberté. Aucune autre forme de criminalité n'accorde aussi peu d'importance aux frontières: la cybercriminalité oblige donc les autorités répressives à adopter une approche transnationale

---

1 Eurostat, Accès et utilisation d'internet, 14 décembre 2010.

2 Institut McKinsey, «*Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity*». Rapport de mai 2011, consulté le 8 février 2012.

3 Rapport de Norton sur la cybercriminalité 2011, Symantec, 7 septembre 2011, consulté le 6 janvier 2012.

4 Ibid.

5 Europe 2020 – Une stratégie pour une croissance intelligente, durable et inclusive, COM(2010) 2020 du 3 mars 2010.

6 Une stratégie numérique pour l'Europe, COM(2010) 245 final du 26 août 2010.

basée sur la coordination et la coopération avec des partenaires tant publics que privés. C'est sur ce point que l'Union européenne peut apporter, et apporte effectivement, une valeur ajoutée non négligeable.

L'Union européenne a pris diverses initiatives pour lutter contre la cybercriminalité, notamment la directive de 2011 relative à l'exploitation sexuelle des enfants en ligne et à la pédopornographie, et une directive relative aux attaques contre les systèmes d'information, qui a pour objectif principal de pénaliser l'usage d'outils propres au milieu de la cybercriminalité, plus particulièrement les réseaux de zombies («botnets»)[7], et qui devrait être adoptée en 2012. Europol a multiplié ses activités à l'encontre de la cybercriminalité, jouant un rôle de premier plan dans la récente opération «*Rescue*» qui a permis l'arrestation de 184 pédophiles présumés et l'identification de plus de 200 enfants victimes d'abus à la suite d'une des enquêtes les plus importantes du genre menée par des forces de l'ordre du monde entier. Grâce au travail des analystes d'Europol, qui sont parvenus à passer outre les dispositifs de sécurité d'un serveur clé au centre du réseau, l'identité et les activités des auteurs présumés ont pu être démasquées.

La lutte contre la cybercriminalité, dont le principal instrument juridique est la Convention sur la cybercriminalité du Conseil de l'Europe[8], demeure une priorité absolue. Elle est reprise dans le cycle politique de l'Union européenne pour lutter contre la grande criminalité internationale organisée[9] et fait partie intégrante des initiatives visant à développer une stratégie européenne globale en vue de renforcer la cybersécurité. L'UE a également entamé un dialogue avec des partenaires internationaux, par exemple au sein du groupe de travail UE-États-Unis existant sur la cybersécurité et la cybercriminalité.

De tels progrès mis à part, plusieurs entraves empêchent toujours d'enquêter sur la cybercriminalité et de poursuivre ses auteurs de manière efficace au niveau européen. Il s'agit notamment des limites de juridiction, de l'insuffisance des structures de partage des renseignements, de la difficulté technique de remonter jusqu'aux criminels informatiques, de la disparité des capacités d'enquête et d'analyse, du manque de personnel formé, et de l'absence de coopération régulière avec les parties prenantes chargées de la cybersécurité. Par le biais de l'instrument de stabilité, l'Union européenne traite également les menaces transnationales en rapide évolution liées à la cybercriminalité dans les pays en développement et en transition, lesquels sont généralement dépourvus des capacités nécessaires à la lutte contre cette forme de criminalité organisée.

En réponse à ces défis, la Commission a indiqué que l'une des priorités de la stratégie de sécurité intérieure[10] était de créer un Centre européen de lutte contre la cybercriminalité.

---

7 Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information, COM (2010) 517 final, 30 septembre 2010. Les réseaux de zombies sont des réseaux d'ordinateurs compromis infectés par des logiciels malveillants qui peuvent être commandés à distance dans le but de réaliser des actions spécifiques, y compris des attaques informatiques.

8 Convention sur la cybercriminalité du Conseil de l'Europe, Budapest, 23 novembre 2001, également connue sous le nom de Convention de Budapest. La Convention est accompagnée d'un *protocole additionnel à la Convention sur la cybercriminalité* relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

9 Le cycle politique de l'UE pour lutter contre la criminalité organisée et la grande criminalité internationale, qui couvre la période 2011/2013, a huit priorités, dont l'une est d'«intensifier la lutte contre la cybercriminalité et l'utilisation de l'internet à des fins délictueuses par des groupes criminels organisés».

10 «D'ici à 2013, l'Union entend créer … un centre européen de la cybercriminalité, qui permettra aux États membres et aux institutions de l'UE de développer des moyens opérationnels et d'analyse aux fins

Après avoir réalisé une étude de faisabilité sur la création d'un tel centre[11] à la demande du Conseil[12], la Commission propose un Centre européen de lutte contre la cybercriminalité (EC3), qui fera partie d'Europol et servira de point focal dans la lutte contre la cybercriminalité au sein de l'UE. La présente communication, en s'appuyant sur l'étude de faisabilité, décrit dans leurs grandes lignes les fonctions essentielles envisagées pour ce centre, explique pourquoi celui-ci devrait être installé dans les locaux d'Europol et comment il peut être mis sur pied. Les conséquences en termes de ressources devront toutefois être examinées plus en détail et les dispositions nécessaires prises avant que l'EC3 ne puisse devenir pleinement opérationnel. La mise en place de ce centre sera prise en considération comme il convient dans la prochaine révision de la base juridique d'Europol.

2. PROPOSITION DE CREATION D'UN CENTRE EUROPEEN DE LUTTE CONTRE LA CYBERCRIMINALITE

Afin que le Centre européen de lutte contre la cybercriminalité (EC3) apporte une valeur ajoutée tout en respectant le principe de subsidiarité, il devrait se concentrer sur les grands aspects suivants:

(i) les cybercrimes commis par des groupes criminels organisés, notamment ceux qui génèrent de grands bénéfices, tels que la fraude en ligne;

(ii) les cybercrimes lourds de conséquences pour leurs victimes, tels que l'exploitation sexuelle des enfants en ligne; et

(iii) les cybercrimes (y compris les attaques informatiques) à l'encontre des infrastructures et systèmes d'information critiques de l'Union[13].

Compte tenu de la nature changeante de la cybercriminalité, l'EC3 devrait également être en mesure d'agir pour répondre à des demandes des États membres ou pour faire face à l'apparition de nouvelles menaces informatiques auxquelles l'Union serait exposée.

2.1. Fonctions essentielles et tâches du centre européen de lutte contre la cybercriminalité

L'EC3 devrait remplir quatre fonctions essentielles:

(a) Servir de point de convergence européen des informations relatives à la cybercriminalité

Une fonction de fusion des informations assurerait un rassemblement des renseignements relatifs à la cybercriminalité provenant d'un grand nombre de sources publiques, privées et libres, enrichissant ainsi les données dont disposent les services de police. Ceci devrait progressivement combler les lacunes actuelles dans les renseignements fournis par les

---

des enquêtes et de la coopération avec les partenaires internationaux», dans La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre, COM(2010) 673 final du 22 novembre 2010.

11 Feasibility study for a European Cybercrime Centre, rapport final, février 2012.

12 Conclusions du Conseil concernant un plan d'action visant à mettre en œuvre la stratégie concertée de lutte contre la cybercriminalité, 3010e réunion du Conseil «Affaires générales» du 26 avril 2010.

13 Comme définis dans la directive 2008/114/CE du Conseil du 8 décembre 2008. Cette directive étant actuellement en cours de révision, l'EC3 tiendrait compte de toute mise à jour.

communautés chargées de la cybersécurité et de la lutte contre la cybercriminalité. Les informations recueillies concerneraient les activités et méthodes de la cybercriminalité et les personnes suspectées. Une telle fonction a pour objectif d'améliorer la connaissance et la prévention de la cybercriminalité, sa détection ainsi que la poursuite en justice des faits qui y sont liés. Elle sert également à encourager la création de liens utiles entre les autorités répressives, le réseau des équipes d'intervention en cas d'urgence informatique («réseau des CERT»), et les spécialistes de la sécurité des technologies de l'information et de la communication appartenant au secteur privé. Le partage d'informations doit respecter les règles et accords de confidentialité entre les différentes parties.

La fonction de fusion d'informations servirait également à améliorer le compte rendu des actes de cybercriminalité et le partage des informations en la matière. La Commission souhaiterait que les États membres exigent que les actes graves de cybercriminalité soient signalés aux autorités répressives nationales[14]. Les services de police nationaux pourraient ainsi fournir des informations sur ces faits graves de manière plus régulière à l'EC3, qui, à son tour, diffuserait ces informations, de telle sorte que les collègues dans d'autres États membres sauraient s'ils poursuivent le même objectif et bénéficieraient des informations recueillies par d'autres dans leurs enquêtes.

Le but est de brosser un tableau plus précis de la cybercriminalité en Europe avec le temps, de façon à produire des rapports stratégiques de haute qualité sur les tendances et les menaces, à acquérir des connaissances solides sur la base de chiffres complets concernant la criminalité et à améliorer les renseignements opérationnels qui résultent d'une base de données s'appuyant sur un large éventail de sources.

(b) Mettre en commun l'expertise européenne en matière de cybercriminalité pour soutenir les États membres dans le renforcement de leurs capacités

L'EC3 devrait aider les États membres à réprimer la cybercriminalité grâce à son savoir-faire et à l'organisation de formations. L'objectif principal est de faire respecter la loi, mais des formations devraient également être proposées à la magistrature. Les initiatives existantes d'Europol, du CEPOL et des États membres seraient rationalisées après une analyse approfondie des besoins en vue d'améliorer la coordination et la complémentarité. L'éventail proposé devrait aller de formations techniques spécifiques à des actions plus larges de développement des capacités donnant la possibilité aux fonctionnaires de police, aux procureurs et aux juges de traiter les affaires liées à la cybercriminalité.

Un service «cybercriminalité» devrait être créé pour échanger les meilleures pratiques et les connaissances en la matière ainsi que pour prendre contact avec les États membres, les autorités répressives internationales, les autorités judiciaires, le secteur privé et les organisations de la société civile et pour répondre à leurs questions, par exemple en cas d'attaque informatique ou d'apparition de nouvelles formes d'escroquerie en ligne.

Ce service prodiguerait un soutien et des conseils aux groupes d'experts en cybercriminalité, y compris à la Task Force «cybercriminalité» de l'Union européenne (ci-après dénommée «EUCTF») et aux experts dans leur lutte contre l'exploitation sexuelle des enfants en ligne. Il devrait également instaurer une coopération avec le réseau en pleine expansion des centres

[14] Tels que ceux énumérés dans les articles 3 à 7 de la proposition de directive relative aux attaques visant les systèmes d'information, COM(2010) 517 final du 30 septembre 2010.

d'excellence de lutte contre la cybercriminalité, tels que le «2Centre», et avec la communauté des chercheurs.

L'EC3 devrait également aider les États membres dans l'élaboration et le déploiement d'une application en ligne de notification des cybercrimes, basée sur des normes reconnues, afin d'acheminer les flux de notifications émanant des divers acteurs (entreprises, équipes gouvernementales ou nationales d'intervention en cas d'urgence informatique (CERT), citoyens, etc.) vers les autorités répressives nationales, et des autorités répressives nationales vers l'EC3.

Enfin, l'EC3 devrait faciliter l'échange de bonnes pratiques en matière de justice pénale et d'application de la loi. Une participation efficace de la magistrature dans la lutte contre la cybercriminalité est d'une importance capitale pour améliorer la poursuite des criminels informatiques dangereux dans les États membres.

(c) Apporter un soutien aux enquêtes des États membres sur la cybercriminalité

L'EC3 devrait fournir un soutien opérationnel aux enquêtes sur la cybercriminalité, par exemple en encourageant la mise en place d'équipes communes d'enquête sur la cybercriminalité et l'échange d'informations opérationnelles dans les enquêtes en cours.

Il devrait également fournir une assistance de haute qualité en termes d'analyse (installations, stockage, outils), ainsi qu'une expertise en matière de cryptage pour les enquêtes sur la cybercriminalité.

(d) Se faire le porte-voix des enquêteurs européens sur la cybercriminalité

Au fil du temps, l'EC3 pourrait assumer le rôle de point de ralliement des enquêteurs européens sur la cybercriminalité, les dotant d'une voix collective dans les discussions avec le secteur des TIC, d'autres sociétés du secteur privé, la communauté des chercheurs, les associations d'utilisateurs et les organisations de la société civile sur les moyens d'améliorer la prévention de la cybercriminalité et de coordonner des activités de recherche ciblée.

L'EC3 serait l'interface naturelle avec les activités d'Interpol sur la cybercriminalité et d'autres unités internationales de police combattant la cybercriminalité. Il pourrait également se charger de coordonner les contributions aux initiatives existantes sur la gouvernance de l'internet et au groupe intergouvernemental d'experts à composition non limitée des Nations unies sur l'étude approfondie du phénomène de la cybercriminalité.

L'EC3 devrait également collaborer avec des organisations telles que le réseau INSAFE[15] dans le cadre de la réalisation de campagnes de sensibilisation de la population, adaptant celles-ci aux changements de la cybercriminalité observés dans ses analyses en vue d'encourager les comportements en ligne prudents et sûrs.

2.2. Lieu d'établissement

Comme l'a démontré l'étude de faisabilité, le Centre européen de lutte contre la cybercriminalité devrait faire partie d'Europol et être situé dans ses bâtiments.

---

[15] Réseau européen de centres de sensibilisation promouvant une utilisation sûre et responsable de l'internet et des périphériques mobiles auprès des jeunes.

Cette situation comporte des avantages considérables. Le rôle d'Europol est reconnu parmi les États membres et d'autres partenaires, y compris Interpol et les autorités répressives internationales. De plus, Europol dispose déjà d'un mandat l'autorisant à prendre des mesures à l'égard de la cybercriminalité[16]. La mission essentielle d'Europol est de promouvoir une Europe plus sûre dans l'intérêt de tous les citoyens, en soutenant les autorités répressives de l'UE par l'intermédiaire de l'échange et de l'analyse de renseignements de nature judiciaire.

2.3. Incidences de la création de l'EC3 en termes de ressources

L'étude de faisabilité a passé en revue plusieurs scénarios concernant les conséquences en termes de ressources. Cette incidence de la création du Centre devra être évaluée de manière plus approfondie[17], en tenant compte notamment d'autres tâches qui pourraient à l'avenir incomber à Europol, et dans le contexte plus général de la dotation en personnel des agences de l'Union européenne. Plus particulièrement, cette évaluation sera menée dans le cadre de la révision de la base juridique d'Europol et de la discussion en cours sur la proposition de la Commission relative à la création d'un fonds pour la sécurité intérieure. Il apparaît toutefois déjà clairement que des détachements des États membres seront nécessaires.

Lors de l'évaluation des besoins de ressources, la Commission sera guidée par trois considérations. Premièrement, il est supposé qu'il y aura une augmentation modérée du nombre total d'affaires à traiter liées à la cybercriminalité, et non pas une augmentation massive. Deuxièmement, les États membres renforceront leur propre capacité de lutte contre la cybercriminalité. Et troisièmement, l'EC3 ne s'occupera que de certains types de criminalité informatique.

2.4. Gouvernance

En cas d'établissement de l'EC3 au sein d'Europol, il importerait d'assurer la participation d'autres partenaires de premier plan à la direction stratégique du Centre. Par conséquent, la Commission propose de mettre en place un comité de direction de l'EC3 au sein de la structure de gouvernance d'Europol. Ce comité serait présidé par le directeur de l'EC3. Cet instrument offrirait la possibilité aux autres parties prenantes (Eurojust, le CEPOL, les États membres – par l'intermédiaire de la Task Force «cybercriminalité» de l'UE (EUCTF) –, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et la Commission) d'apporter leur savoir-faire sans générer de charges administratives additionnelles superflues. Le comité pourrait renforcer la responsabilisation de l'EC3 dans l'exercice de ses activités liées à la cybercriminalité, et assurer ce faisant qu'elles sont menées en partenariat, eu égard à l'expertise additionnelle et aux mandats de toutes les parties prenantes.

2.5. Coopération avec des acteurs clés

L'EC3 devrait fournir une réponse coordonnée à la cybercriminalité, non seulement en permettant la collaboration entre différentes agences de l'Union européenne, mais également en servant de point de contact européen unique dans ce domaine.

(a) États membres

---

[16] Décision 2009/371/JAI du Conseil datant du 6 avril 2009 portant création de l'Office européen de police, article 4(1) en liaison avec l'annexe.

[17] L'évaluation doit être cohérente avec les exigences globales pour les agences en matière de budget et de personnel dans le budget de 2013 et dans le prochain cadre financier pluriannuel.

L'objectif principal est d'aider les États membres à lutter contre la cybercriminalité. Le service d'assistance («helpdesk») ainsi que les prestations à fournir par l'EC3, tels qu'une analyse plus ciblée des menaces et un soutien opérationnel mieux informé, serviront aux enquêteurs sur la cybercriminalité dans toute l'Europe. L'EUCTF garantirait la prise en compte des préoccupations des États membres au comité de direction de l'EC3. En outre, les États membres devront continuer de réaliser les investissements nécessaires dans leurs structures nationales de lutte contre la cybercriminalité afin de disposer d'interfaces appropriées pour l'interaction avec l'EC3.

(b) Agences européennes et autres acteurs

Les agences compétentes, notamment EUROJUST, le CEPOL, et l'ENISA, ainsi que la CERT-EU, seraient directement impliquées dans les activités de l'EC3, non seulement par leur participation au comité de direction, mais également par leur coopération opérationnelle, le cas échéant, et en tenant compte de leurs mandats respectifs.

(c) Partenaires internationaux

De par ses efforts pour se situer au centre des informations sur la cybercriminalité en Europe, l'EC3 devrait devenir un interlocuteur précieux pour les partenaires internationaux sur les questions de lutte contre la cybercriminalité. L'EC3 devrait, en partenariat avec Interpol et nos partenaires stratégiques dans le monde, s'efforcer d'améliorer la coordination des réponses à la cybercriminalité et veiller à ce que les besoins de l'application de la loi soient pris en compte dans le développement futur du cyberespace.

(d) Secteur privé, communautés de chercheurs et organisations de la société civile

La création d'un climat de confiance entre le secteur privé et les autorités répressives revêt une importance capitale dans le cadre de la lutte contre la cybercriminalité. En consolidant le travail d'Europol avec des partenaires existants et nouveaux, l'EC3 devrait développer des réseaux de confiance et des plates-formes d'échange d'informations avec l'industrie et d'autres acteurs tels que la communauté des chercheurs et les organisations de la société civile. Ces réseaux et plates-formes devraient faciliter le partage des informations sur une série de questions, y compris l'alerte rapide en cas de menaces informatiques, ainsi que les réponses collaboratives de type «Task Force» aux attaques informatiques et autres formes de cybercriminalité.

L'EC3 devrait également participer aux actions plus larges des entreprises du secteur privé possédant d'importants actifs numériques, telles que les banques et les commerces en ligne, qui visent à lutter contre la cybercriminalité, à s'en protéger plus efficacement et à réduire au maximum les points de vulnérabilité dans les technologies en cours de développement.

Il est de l'intérêt commun des autorités répressives et du secteur privé de parvenir à une vision plus claire de la cybercriminalité en temps réel et d'œuvrer à un démantèlement plus efficace de ses réseaux grâce à une détection plus efficace de leurs nouveaux modes opératoires et à l'arrestation rapide des criminels informatiques.

3. FEUILLE DE ROUTE POUR LA MISE EN PLACE DU CENTRE EUROPEEN DE LUTTE CONTRE LA CYBERCRIMINALITE

3.1. Activités jusqu'à la fin de l'année 2013

Aux fins de la mise en place de la capacité opérationnelle initiale du Centre, la Commission étudiera, en étroite coopération avec Europol, les besoins en termes de ressources humaines et financières nécessaires à la constitution d'une équipe chargée de l'établissement de l'EC3 jusqu'à la fin de l'actuel cadre financier de l'UE. Cette équipe aurait pour tâche par exemple de rédiger le projet de mandat et de structure organisationnelle de l'EC3, ainsi que d'élaborer des indicateurs permettant d'évaluer ses performances. Le rôle et le fonctionnement du comité de direction seront plus précisément définis et convenus par les parties prenantes concernées.

En vue de l'établissement d'une fonction de fusion complète des informations, l'équipe devrait se mettre en relation avec l'équipe de pré-configuration CERT-EU et, le cas échéant, avec l'ENISA (en tenant compte de leurs contraintes en termes de ressources). Pour améliorer le compte rendu des actes de cybercriminalité, elle dressera un inventaire des systèmes en ligne existant en la matière dans les États membres.

Un service «cybercriminalité» devrait être mis sur pied. Ce service pourrait s'appuyer sur une plate-forme communautaire sécurisée en ligne qui lui serait dédiée. Les activités de formation actuelles d'Europol, du CEPOL et du réseau ECTEG (*European Cybercrime Training and Education Group* – groupe européen de formation et d'enseignement sur la cybercriminalité) pourraient être évaluées et réorganisées sous la conduite de l'EC3 et de son comité de direction. Une analyse des besoins de formation, qui tienne également compte des impératifs des juges et des procureurs, devrait être menée. Cette analyse pourrait déboucher sur l'organisation d'un stage de formation qui porte sur les bases de la cybercriminalité; il serait ouvert aux membres du système pénal.

En outre, une évaluation plus précise de ressources humaines et financières nécessaires devra être menée et prévue par les décisions prises au titre du prochain cadre financier pluriannuel. Cette évaluation influera sur le développement futur de l'EC3.

4. CONCLUSION

Alors que le monde du crime organisé étend ses activités au cyberespace, les autorités répressives ne doivent pas se laisser distancer. L'UE est en mesure de fournir aux États membres et à l'industrie les outils nécessaires pour lutter contre la cybercriminalité, menace moderne et de nature changeante qui, par définition, ne connaît pas de frontières. À condition que les ressources humaines et financières nécessaires puissent être obtenues, un Centre européen de lutte contre la cybercriminalité jouera le rôle de point focal dans la lutte de l'Europe contre la cybercriminalité par une mise en commun du savoir-faire, l'apport d'un soutien aux enquêtes pénales et la promotion de solutions à l'échelle de l'UE, tout en sensibilisant le public au problème de la cybercriminalité. Ce faisant, l'EC3 contribuerait à sauvegarder la liberté de l'internet et de l'économie numérique légitime et à protéger les activités en ligne des citoyens et des entreprises d'Europe.

Le Conseil est invité à approuver la présente proposition, et le Parlement européen, ainsi que les autres parties concernées, sont encouragés à contribuer au développement du Centre.