



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 11.2.2003
COM(2003) 63 final

2003/0032 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information

(présentée par la Commission)

eEurope
2005

EXPOSÉ DES MOTIFS

1. HISTORIQUE

Aujourd'hui, plus de 90% des entreprises de l'Union européenne disposent d'une connexion internet et la majorité d'entre elles exploitent un site web. Un très grand nombre d'employés utilisent un téléphone mobile, un ordinateur portable ou un équipement similaire pour envoyer ou obtenir des informations à des fins professionnelles. Il peut d'agir de données ayant une valeur considérable, dans le cas par exemple de la description d'une opération commerciale ou d'informations ayant un contenu technique.

Au-delà des applications professionnelles, l'informatique et les réseaux sont désormais une composante essentielle de notre vie quotidienne. En 2002, environ 40% des foyers de l'UE disposaient de leur propre connexion internet et plus de 2/3 de la population utilisait un téléphone mobile. Les écoles et les universités possèdent aussi des connexions internet et l'utilisation de l'internet à des fins d'apprentissage et d'étude est désormais entrée dans les mœurs. Les administrations publiques s'emploient activement à passer au gouvernement électronique. Ce sont des systèmes informatiques et des réseaux de communications qui contrôlent des infrastructures telles que les systèmes d'approvisionnement en eau et en électricité ou les réseaux de transports publics. Depuis le 11 septembre 2001, ces aspects sont également devenus des enjeux de sécurité nationale.

Compte tenu de l'importance que revêtent les réseaux et les systèmes d'information, leur sécurité de fonctionnement est devenue une préoccupation essentielle. De même que les usagers considèrent désormais l'approvisionnement en électricité ou en eau comme une évidence, ils s'attendent aussi tout naturellement à entendre une tonalité quand ils décrochent un téléphone ou à ce qu'un ordinateur fonctionne correctement lorsqu'ils en ont besoin. Ils veulent pouvoir accéder aux informations stockées sans retards ou interruptions exagérés. Les défaillances de réseau et les pannes informatiques ne sont plus des problèmes spécifiques qui ne concernent que les informaticiens. Aujourd'hui, les dysfonctionnements des réseaux et des systèmes informatiques affectent tout le monde, qu'il s'agisse des citoyens, des entreprises ou administrations publiques.

La sécurité est donc devenue un aspect essentiel pour de nombreuses activités commerciales, et notamment pour celles qui se déroulent en ligne. Elle constitue donc désormais un secteur d'activité économique, dans lequel des entreprises spécialisées vendent des produits et des services, et elle fait aussi l'objet d'accords commerciaux. Ainsi, les consommateurs achètent des logiciels antivirus et installent des dispositifs coupe-feu sur leurs ordinateurs. Les entreprises investissent dans la sécurité, établissent des intranets protégés et chiffrent les courriers électroniques ou les communications sans fil. Pour la transmission de données sensibles, on a recours au chiffrement. Certains utilisateurs semblent bien conscients de la vulnérabilité des systèmes et des moyens d'y faire face tandis que d'autres sont moins bien informés ou moins préoccupés.

Actuellement, veiller à la sécurité des réseaux et de l'information consiste à assurer la disponibilité des services et des données, à éviter la perturbation et l'interception non autorisée des communications, à confirmer que les données qui ont été envoyées,

reçues ou stockées sont complètes et qu'elles n'ont pas été modifiées, à garantir la confidentialité des données et la protection des systèmes informatiques contre l'accès non autorisé, à protéger les systèmes contre les attaques par des logiciels malveillants et à garantir une authentification fiable, c'est-à-dire en confirmant l'identité supposée d'entités ou d'utilisateurs.

Les exigences de sécurité vont évoluer rapidement dans l'avenir car la mise en réseau et l'informatique continuent à se développer et les ordinateurs vont devenir omniprésents. Cela signifie que, grâce aux connexions à large bande, les utilisateurs pourront se connecter à l'internet n'importe quand, que les nouvelles applications sans fil leur permettront d'accéder à l'internet quel que soit l'endroit où ils se trouvent, et que les possibilités de connecter à l'internet tous les appareils imaginables, des imprimantes aux réfrigérateurs, vont continuer à se multiplier, ce qui enrichira encore la palette des utilisations de l'internet.

La gestion de la sécurité s'est révélée être une tâche complexe et difficile car l'utilisateur doit être assuré de la disponibilité, de l'authenticité, de l'intégrité et de la confidentialité des données et des services. En raison de la complexité de la technologie, les composantes et les acteurs qui doivent interagir sont nombreux, et le comportement humain est devenu un facteur crucial.

Il est probable qu'il ne sera jamais possible de parvenir à une sécurité totale, du moins pas à des coûts raisonnables. Dans ce domaine comme dans celui des autres technologies, et comme dans tous les aspects de notre existence, il y aura toujours des faiblesses, des attaques, des incidents et des défaillances qui provoqueront des dégâts et affaibliront la confiance dans les systèmes et les services. La société dans son ensemble, ainsi que les individus, doivent apprendre à gérer les risques inhérents aux réseaux et aux systèmes d'information.

2. POURQUOI FAUT-IL AGIR?

La sécurité est devenue une préoccupation politique majeure. En matière de sécurité, les gouvernements ont une responsabilité plus étendue à l'égard de la société. Ils intensifient donc leur action pour améliorer la sécurité sur leur territoire. Ils souhaitent promouvoir la sécurité, par exemple en soutenant la création d'équipes d'intervention en cas d'urgence informatique, les activités de recherche et l'organisation de campagnes de sensibilisation. Ils donnent également aux organes chargés de faire respecter la loi les moyens et la formation nécessaires pour lutter contre la criminalité informatique et la criminalité liée à l'internet.

Toutefois, l'état d'avancement des actions engagées varie selon les États membres et ces derniers ont adopté des orientations prioritaires différentes. En dehors de réseaux administratifs tels que TESTA, il n'existe pas de coopération transfrontière systématique entre États membres en matière de sécurité des réseaux et de l'information, bien que les questions de sécurité ne puissent pas être considérées comme un problème isolé ne concernant qu'un seul pays. Il n'existe pas de mécanisme qui garantisse des réactions efficaces en cas de menaces pour la sécurité. La mise en œuvre du cadre juridique est variable. La certification des produits se fait au niveau national alors que les normes essentielles sont développées par le secteur au niveau mondial et les exploitants et les fournisseurs sont confrontés à des attitudes

différentes de la part des gouvernements. Tous ces facteurs entraînent un manque d'interopérabilité qui nuit à une bonne utilisation des produits et services de sécurité.

Une intensification de la coordination entre les États membres serait bénéfique pour la Communauté européenne car elle permettrait de parvenir à un niveau de sécurité suffisamment élevé dans tous les États membres. Tel est l'objectif de la communication de la Commission sur la sécurité des réseaux et de l'information de juin 2001¹, qui proposait un certain nombre de mesures ayant trait notamment à des actions de sensibilisation, à l'amélioration des mécanismes d'échange d'information et au soutien à une normalisation et à une certification orientées vers les besoins du marché.

La communication proposait également la création d'un système européen d'alerte et d'information. La résolution du Conseil du 28 janvier 2002 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information a encore approfondi ce concept. Il est devenu manifeste que les dispositions institutionnelles actuelles ne permettraient pas d'aborder les problèmes de sécurité des réseaux et de l'information de manière appropriée au niveau européen.

Dans cette résolution, le Conseil se félicite que la Commission ait l'intention de faire des propositions en vue de la mise en place d'un groupe de travail sur la cybersécurité afin de tirer profit des efforts entrepris au niveau national pour améliorer la sécurité des réseaux et de l'information et la capacité des États membres à faire face, isolément et collectivement, à de graves problèmes de sécurité des réseaux et de l'information;

En réponse aux suggestions de la Commission, le Parlement européen a adopté un avis dans lequel il appelle avec force à la formulation d'une réponse européenne au problème grandissant que pose la sécurité.

En juin 2002, l'OCDE a adopté ses lignes directrices sur la sécurité des systèmes et des réseaux d'information: Vers une culture de la sécurité. Elles soulignent l'importance de l'application de certains principes communs de sécurité de l'information et viennent étayer les travaux qui se déroulent au niveau européen.

3. PROPOSITION VISANT A INSTITUER UNE AGENCE CHARGÉE DE LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION

3.1. Historique

Le Parlement européen, le Conseil et la Commission préconisent un renforcement de la coordination européenne dans le domaine de la sécurité de l'information. La création d'une entité dotée de la personnalité juridique constituerait le moyen le plus efficace de parvenir à cet objectif. La présente proposition de règlement propose donc d'instituer une agence de régulation européenne en conformité avec les dispositions de la Communication de la Commission « L'encadrement des Agences

¹ Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions - Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne COM(2001) 298 final.

Européennes de Régulation », COM(2002) 718 final,. Cette Agence s'appellera - Agence Européenne chargée de la Sécurité des Réseaux et de l'Information,-, ci-après dénommée «l'Agence».

Cependant, la législation spécifique relative aux communications électroniques, et plus particulièrement la directive-cadre sur les communications électroniques, attribue un rôle important aux organismes compétents nationaux. C'est pourquoi, l'Agence fournira son assistance non seulement à la Commission mais aussi aux autorités de réglementation nationales.

Cette proposition tient compte d'un certain nombre de craintes qui ont été exprimées durant les consultations avec les États membres organisées par la Commission. Les contributions reçues du secteur privé faisaient état de préoccupations analogues portant principalement sur la nécessité d'assurer que l'agence proposée présente des garanties en matière de flexibilité, de fiabilité, de compétence, d'efficacité et de cohérence. Les exigences qui ont été particulièrement mises en exergue sont les suivantes:

- a) Compte tenu de la vitesse à laquelle la situation évolue dans le domaine de la sécurité des réseaux et de l'information, les meilleures dispositions institutionnelles peuvent être appelées à être modifiées avec le temps. Il faudrait donc prévoir pour l'Agence une période de fonctionnement limitée au terme de laquelle un processus de révision serait entrepris,
- b) l'Agence doit inspirer confiance aux institutions et organes publics des États membres ainsi qu'au secteur privé,
- c) l'Agence doit constituer un centre d'expertise en rapprochant les intervenants compétents de tous les États membres.
- d) l'Agence doit être en mesure d'agir de manière efficace et rapide. Par conséquent, il faudra prévoir les ressources humaines et financières nécessaires pour permettre un fonctionnement harmonieux et flexible mais la taille de l'Agence devra cependant rester raisonnable, et
- e) la Commission doit pouvoir être capable de fournir des orientations à l'Agence pour ses travaux.

Ces exigences constituent les orientations sur lesquelles repose la proposition de règlement. Elles expliquent pourquoi les tâches de l'Agence sont clairement décrites et prévoient en même temps la flexibilité nécessaire. Elles exposent les motifs qui justifient une évaluation des travaux de l'Agence après les trois premières années. Enfin, elles précisent qu'une coopération étroite avec les institutions et organes des États membres ainsi qu'avec les institutions communautaires est capitale pour le bon fonctionnement de cette Agence.

L'Agence bénéficiera, dans ses travaux, de l'appui scientifique fourni par les activités de recherche menées par le Centre commun de recherche et par d'autres programmes de recherche de la Communauté.

3.2. Choix de la base juridique

La présente proposition aborde donc deux questions d'intérêt communautaire qui sont étroitement liées, à savoir le bon fonctionnement du marché intérieur et l'interopérabilité des réseaux électroniques transeuropéens. Premièrement, l'introduction au niveau des États membres et de la Communauté d'exigences techniquement complexes relatives à la sécurité des réseaux et de l'information pourrait entraver la mise en œuvre complète des principes du marché intérieur. Deuxièmement, le bon fonctionnement de ce marché dépend aussi de l'interopérabilité des fonctions de sécurité dans les réseaux et systèmes d'information.

Les chapitres suivants se rapportent aux chapitres 1 à 5 de la proposition.

3.3. Chapitre 1 - Objectifs et Tâches

3.3.1. Objectifs

Le principal objectif de l'Agence consiste à créer en Europe une conception commune des questions de sécurité de l'information, qui est nécessaire pour garantir la disponibilité et la sécurité des réseaux et systèmes d'information dans l'Union. Pour atteindre cet objectif, il faut adopter une définition de la sécurité des réseaux et de l'information qui soit suffisamment large pour couvrir toutes les activités susceptibles d'avoir des effets néfastes sur la sécurité des réseaux et systèmes d'information.

L'Agence sera capable de fournir une assistance pour l'application des mesures communautaires relatives à la sécurité des réseaux et de l'information. Cette assistance permettra d'assurer l'interopérabilité des fonctions de sécurité de l'information dans les réseaux et systèmes d'information, ce qui contribuera au fonctionnement du marché intérieur. Elle renforcera la capacité de la Communauté et des États membres en matière de réaction aux problèmes de sécurité des réseaux et de l'information. L'Agence aura un rôle crucial à jouer dans la sécurité des réseaux et systèmes d'information européens et dans le développement de la société de l'information en général.

3.3.2. Tâches

L'Agence aura une fonction consultative et une mission de coordination, dans le cadre desquelles elles recueillera et analysera des données sur la sécurité de l'information. Actuellement, des organismes tant publics que privés, poursuivant des objectifs différents, recueillent des données sur les incidents dans le domaine des technologies de l'information et d'autres renseignements pertinents pour la sécurité de l'information. Cependant, il n'existe pas, au niveau européen, d'organe central capable de mettre en œuvre une démarche d'ensemble pour la collecte et l'analyse des données et la formulation d'avis et de conseils en vue de soutenir l'activité politique de la Commission sur la sécurité des réseaux et de l'information. L'Agence fera office de centre d'expertise auprès duquel les États membres comme les institutions communautaires pourront demander conseil sur des questions techniques liées à la sécurité.

En outre, l'Agence contribuera à l'instauration d'une coopération de grande envergure entre les différents acteurs dans le domaine de la sécurité de l'information, en

apportant par exemple une assistance aux activités de suivi qui accompagnent les travaux sur la sécurité du commerce électronique. Cette coopération sera une condition préalable capitale pour la sécurité du fonctionnement des réseaux et des systèmes d'information en Europe. La participation et l'engagement de tous les intéressés est donc requise.

Cette Agence contribuera à l'instauration d'une approche coordonnée de la sécurité de l'information en fournissant une assistance aux États membres, par exemple en ce qui concerne la promotion de l'évaluation des risques et des actions de sensibilisation. Pour assurer l'interopérabilité des réseaux et systèmes d'information, l'Agence fournira également des avis et une assistance relatifs à des procédés et procédures harmonisés dans les États membres lors de l'application d'exigences techniques qui ont une incidence sur la sécurité. En effet, outre les exigences juridiques, les exigences techniques peuvent aussi, dans une large mesure, nuire à l'interopérabilité et entraver le bon fonctionnement du marché intérieur.

L'Agence apportera également son concours à l'inventaire des besoins pertinents en matière de normalisation, ainsi qu'à la promotion de normes de sécurité et des systèmes de certification et de leur utilisation la plus large possible par les États membres et par la Commission pour le soutien de l'application de la législation européenne.

Étant donné que les problèmes de sécurité des réseaux et de l'information ont une dimension mondiale, il est également nécessaire d'instituer une coopération internationale dans ce domaine. L'Agence fournira une assistance en ce qui concerne les contacts de la Communauté avec les parties concernées dans les pays tiers.

De nouveaux points faibles et de nouvelles menaces apparaissent constamment dans le secteur des réseaux et des systèmes d'information. Il faut que la Commission puisse assigner des tâches supplémentaires à cette Agence afin de rester en prise avec l'évolution actuelle de la technique et de la société, en conformité avec les dispositions du cadre opérationnel pour les Agences Européennes de Régulation.

3.4. Chapitre 2 - Organisation

3.4.1. Gestion

La structure organisationnelle devrait permettre aux diverses parties intéressées de participer aux travaux de l'Agence, et de garantir l'indépendance de cette dernière vis-à-vis des pressions extérieures ainsi que la transparence de son action et sa responsabilité devant les institutions démocratiques. Il est donc proposé de créer un conseil d'administration composé de membres nommés par le Conseil et par la Commission. Ainsi, les représentants de la Commission comprendront un membre de la Direction de la sécurité. Il est également proposé que le conseil d'administration comprenne des représentants des secteurs professionnels et des consommateurs proposés par la Commission et nommés par le Conseil. Les représentants des secteurs professionnels ne disposeront pas du droit de vote.

L'Agence sera dirigée par un directeur exécutif qui jouira d'un grand degré d'indépendance et de flexibilité et qui sera responsable de l'organisation du fonctionnement interne de l'Agence. Il sera également chargé de la préparation et de l'exécution du budget et du programme de travail de l'Agence, ainsi que de toutes les

questions de personnel. Pour conférer au directeur exécutif la légitimité nécessaire, il est préférable qu'il soit nommé par le conseil d'administration sur proposition de la Commission.

En tant qu'organe communautaire, l'Agence doit veiller à utiliser au mieux les compétences et les ressources existantes dans la réalisation de sa mission tout en respectant l'exigence générale d'indépendance. C'est pourquoi il est proposé que l'Agence comporte un conseil consultatif restreint composé d'experts chargés de faciliter la coopération et l'échange d'informations entre l'Agence et les institutions et organes compétents dans les différents États membres (par exemple un expert de la protection des données ou un représentant de la communauté de la recherche). Le conseil consultatif aura un rôle consultatif et sera également chargé, avec le directeur exécutif, de la préparation du programme de travail annuel de l'Agence.

3.5. Chapitre 3 - Fonctionnement

3.5.1. Programme de travail

L'Agence devra avoir la souplesse nécessaire pour adapter ses travaux à l'évolution rapide dans le domaine de la technologie et modifier l'orientation de ses activités. Par conséquent, le conseil d'administration adoptera chaque année, sur proposition du directeur exécutif, un programme de travail approuvé par la Commission. Les résultats des activités correspondant au programme de travail de l'année seront consignés dans le rapport général, qui sera établi par le directeur exécutif et adopté par le conseil d'administration.

3.5.2. Avis

Étant donné que l'Agence risque d'être surchargée de demandes d'avis et d'assistance, il conviendrait de prévoir des dispositions spécifiques relatives aux personnes habilitées à présenter des demandes et aux modalités de traitement de ces demandes.

3.5.3. Groupes de travail

Même si l'Agence sera dotée d'un personnel hautement qualifié, il est probable que des problèmes de nature plus technique risquent de se poser. Par conséquent, l'Agence aura la possibilité de créer des groupes de travail temporaires composés d'experts de différents domaines. Conformément à la politique suivie en matière de transparence, des représentants de la Commission seront habilités à assister aux réunions de ces groupes de travail.

3.5.4. Indépendance

Pour que les conseils et les avis formulés par l'Agence soient acceptés par les particuliers, par les administrations publiques et les entreprises, il convient d'établir un modèle d'indépendance. Par conséquent, les membres du conseil d'administration et du conseil consultatif, le directeur exécutif et les experts externes qui font partie des groupes de travail seront tenus de faire une déclaration concernant l'absence d'intérêt susceptible de remettre leur indépendance en question.

3.5.5. *Transparence et confidentialité*

L'Agence adoptera les règles qu'elle appliquera en ce qui concerne la transparence et l'accès aux documents conformément aux décisions du Parlement européen et du Conseil, dans le cadre de l'article 255 du traité CE et des dispositions relatives à la sécurité de la Commission².

Bien qu'il soit nécessaire, pour l'acceptation des travaux de l'Agence, de garantir un niveau élevé de transparence ainsi qu'un accès aisé aux documents qu'elle publie, elle recueillera aussi des informations qui devront être tenues confidentielles.

3.6. **Chapitre 4 - Dispositions financières**

Pour la période comprise entre 2004 et 2008, l'Agence doit être dotée d'un budget suffisant pour pouvoir engager son personnel selon les modalités décrites ci-dessus et pour lui fournir les équipements techniques appropriés afin qu'il soit en mesure d'effectuer les tâches qui lui sont confiées et de fonctionner de manière harmonieuse. Le budget est précisé dans la fiche financière législative.

Le budget de l'Agence sera financé par une contribution de la Communauté avec d'éventuelles contributions des pays tiers participant aux travaux de l'Agence. Le directeur exécutif sera chargé de l'établissement d'un projet d'état prévisionnel. Le conseil d'administration fournira un état prévisionnel des recettes et des dépenses à la Commission qui poursuit la procédure conformément aux règles usuelles en matière budgétaire.

Le directeur exécutif sera chargé de l'exécution du budget. Le Parlement européen, sur recommandation du Conseil, donne décharge au directeur exécutif de l'Agence sur l'exécution du budget. Le contrôle financier sera assuré par le contrôleur financier de la Commission. La Cour des comptes examinera les comptes et publiera un rapport annuel.

3.7. **Chapitre 5 - Dispositions générales**

3.7.1. *Personnalité juridique et privilèges*

L'Agence sera dotée de la personnalité juridique la plus large dans tous les États membres et jouira des mêmes privilèges et immunités que ceux accordés par le protocole sur les privilèges et immunités des Communautés européennes.

3.7.2. *Responsabilité*

Le régime de la responsabilité contractuelle et non contractuelle de l'Agence correspond au régime applicable à la Communauté en application de l'article 288 du traité.

² Décision du Conseil 2001/264/CE du 19 mars 2001 adoptant le règlement de sécurité du Conseil et décision de la Commission C(2001) 3831.

3.7.3. *Personnel*

Étant donné que l'Agence doit être un centre d'expertise, il est capital qu'elle dispose d'un effectif suffisant de personnes hautement qualifiées. Actuellement, les professionnels correspondant à ce profil sont rares et très recherchés en Europe. L'Agence recrutera dans le secteur public comme dans le secteur privé. Le statut des fonctionnaires des Communautés européennes et le régime applicable aux autres agents s'appliquent au personnel de l'Agence. Sans préjudice de la nécessité de disposer des services d'un personnel qualifié, stable et en nombre suffisant, ces agents seront recrutés sur la base de contrats temporaires d'une durée maximale de cinq ans.

3.7.4. *Protection des données à caractère personnel*

L'Agence sera aussi amenée, lors de l'exécution de ses tâches, à traiter des données à caractère personnel et elle se conformera à cet égard à la réglementation applicable aux institutions communautaires dans ce domaine.

3.7.5. *Participation des pays tiers*

L'Agence est ouverte à la participation des pays tiers qui ont conclu avec la Communauté européenne des accords en vertu desquels ils ont adopté et appliquent la législation communautaire dans le domaine couvert par le présent règlement.

3.8. Chapitre 6 - Dispositions finales

3.8.1. *Révision*

Étant donné que la sécurité des réseaux et de l'information est un domaine à forte intensité technologique, dans lequel la situation évolue par conséquent très vite, les meilleures dispositions institutionnelles peuvent être appelées à être modifiées avec le temps. Dans un délai de trois ans à compter de la date de démarrage fixée à l'article 26, ou plus tôt si le conseil d'administration le juge nécessaire, il conviendrait d'entreprendre un processus de révision pour démontrer le bien-fondé d'une poursuite des activités de l'Agence après cette période initiale de cinq ans et, si nécessaire, proposer d'apporter d'éventuelles modifications à ses responsabilités, objectifs et mandats futurs.

Cette révision examinera notamment dans quelle mesure l'absence de participation des organes chargés de faire respecter la loi a eu des conséquences négatives sur l'efficacité et l'utilité des activités de l'Agence. Si l'évaluation révèle l'existence de conséquences négatives, la Commission étudiera le bien-fondé d'une proposition visant à compléter le présent règlement.

3.8.2. *Siège*

Le siège de l'Agence devra satisfaire aux critères suivants:

- être facilement accessible en termes de communications, et notamment disposer d'installations de communication électroniques et, sur le plan des transports, de liaisons efficaces et rapides;

- permettre à l'Agence de travailler efficacement et en étroite collaboration avec les services des institutions qui sont chargés des questions de sécurité des réseaux et de l'information;
- être économiquement avantageux et permettre à l'Agence de commencer ses travaux immédiatement.
- fournir l'infrastructure nécessaire au personnel de l'Agence.

3.8.3. *Durée*

Il est proposé que l'Agence devienne opérationnelle au 1er janvier 2004 et qu'elle fonctionne pendant 5 ans. La poursuite des activités de l'Agence dépendra des résultats de l'évaluation réalisée par la Commission en collaboration avec le conseil consultatif.

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,
vu le traité instituant la Communauté européenne, et notamment ses articles 95 et 156,
vu la proposition de la Commission³,
vu l'avis du Comité économique et social européen⁴,
vu l'avis du Comité des régions⁵,
statuant conformément à la procédure visée à l'article 251 du traité⁶,
considérant ce qui suit:

- (1) Les réseaux de communication et les systèmes d'information sont devenus un facteur clé du développement de l'économie et de la société. L'informatique et les réseaux deviennent désormais tout aussi omniprésents que des services tels que l'approvisionnement en électricité ou en eau. Par conséquent, la sécurité des réseaux de communication et des systèmes d'information, et en particulier leur disponibilité, est devenu un sujet de préoccupation grandissant pour la société.
- (2) La sécurité des réseaux et de l'information consiste à assurer la disponibilité des services et des données, à éviter la perturbation et l'interception non autorisée des communications, à confirmer que les données qui ont été envoyées, reçues ou stockées sont complètes et qu'elles n'ont pas été modifiées, à garantir la confidentialité des données, à protéger les systèmes d'information contre l'accès non autorisé et contre les attaques par des logiciels malveillants et à garantir une authentification fiable.
- (3) La multiplication des violations de la sécurité des réseaux a déjà provoqué des dommages financiers considérables, elle a ébranlé la confiance des utilisateurs et a été préjudiciable au développement du commerce électronique. Les particuliers, les administrations publiques et les entreprises ont réagi en faisant appel à des mesures technologiques de sécurité et à des procédures de gestion de la sécurité. Les États membres ont adopté plusieurs mesures de soutien, telles que des campagnes

³ JO C [...] du [...], p. [...].

⁴ JO C [...] du [...], p. [...].

⁵ JO C [...] du [...], p. [...].

⁶ JO C [...] du [...], p. [...].

d'information et des projets de recherche, afin d'améliorer la sécurité des réseaux et de l'information dans la société.

- (4) Les réactions des États membres ont été disparates et pas suffisamment coordonnées pour qu'il soit possible d'apporter une réponse efficace aux problèmes de sécurité. En raison de la complexité technique des réseaux et des systèmes d'information, de la diversité des produits et des services qui sont interconnectés, et de la multitude d'acteurs privés et publics dont la responsabilité propre est engagée, aucune réaction cohérente en matière de sécurité n'a encore été élaborée au niveau européen. Le manque d'interopérabilité des produits et services de sécurité a notamment posé un problème particulier, ce qui compromet l'interopérabilité des réseaux concernés. C'est également en raison de ces caractéristiques que l'application effective des mesures communautaires a fait l'objet d'analyses techniques complexes et que sa compréhension s'est révélée difficile.
- (5) L'absence de réponse européenne commune aux problèmes de sécurité de l'information qui se posent dans l'application des mesures communautaires risque de porter préjudice au fonctionnement harmonieux du marché intérieur.
- (6) La directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre")⁷ fixe les tâches incombant aux autorités de régulation nationales, qui consistent notamment à encourager la mise en place et le développement de réseaux transeuropéens et l'interopérabilité des services paneuropéens, à coopérer entre elles ainsi qu'avec la Commission, de manière transparente, afin de veiller à l'élaboration de pratiques réglementaires cohérentes contribuant à assurer un niveau élevé de protection des données à caractère personnel et de la vie privée et à garantir l'intégrité et la sécurité des réseaux de communications publics.
- (7) La directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques⁸ autorise les États membres à assortir les autorisations générales de conditions ayant trait à la protection des réseaux publics contre l'accès non autorisé conformément à la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.
- (8) La directive 2002/22/CE du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques⁹ exige que les États membres prennent toutes les mesures nécessaires pour assurer l'intégrité et la disponibilité des réseaux téléphoniques publics et pour que les entreprises fournissant des services téléphoniques accessibles au public à des emplacements fixes prennent toutes les mesures appropriées pour garantir un accès ininterrompu aux services d'urgence.
- (9) La directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques¹⁰ que les fournisseurs de services de communications

⁷ JO L 108 du 24.4.2002, p.33.

⁸ JO L 108 du 24.4.2002, p.21.

⁹ JO L 108 du 24.4.2002, p.51.

¹⁰ JO L 201 du 31.7.2002, p.37.

électroniques accessibles au public prennent les mesures techniques et organisationnelles appropriées pour assurer la sécurité de leurs services et requiert également que la confidentialité des données liées aux communications et au trafic soit assurée. En application de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données¹¹, les États membres doivent veiller à ce que le responsable du traitement mette en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

- (10) La directive cadre et la directive 1999/93/CE du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques¹² contiennent des dispositions concernant des normes qui doivent être publiées au Journal officiel des Communautés européennes. Les États membres utilisent également des normes établies par des organismes internationaux ainsi que des standards élaborés par l'ensemble du secteur concerné. La Commission et les États membres doivent être en mesure d'évaluer quelles sont les normes qui satisfont aux exigences de la législation communautaire
- (11) Ces mesures relatives au marché intérieur nécessitent l'adoption de différentes modalités d'application techniques et opérationnelles par les États membres et la Commission. Il s'agit de tâches techniques complexes pour lesquelles il n'existe pas de solutions uniques et évidentes. Une application hétérogène de ces exigences peut déboucher sur des solutions qui non seulement ne seraient pas efficaces et créeraient des obstacles au marché intérieur mais compromettraient en outre l'interopérabilité des fonctions de la sécurité de l'information. Il est donc nécessaire de créer au niveau européen un centre d'expertise chargé de fournir des conseils, une assistance et des avis sur la mise en œuvre technique et organisationnelle de ces exigences, et sur lequel la Commission, les autorités de régulation nationales et les organes compétents des États membres peuvent compter. Les organes chargés de faire respecter la loi et les autorités judiciaires dans les États membres font partie des organes compétents dans le domaine de la sécurité des réseaux et de l'information.
- (12) L'établissement d'une agence européenne, l'Agence européenne chargée de la sécurité des réseaux et de l'information, ci-après dénommée «l'Agence», qui constituerait une référence et inspirerait confiance du fait de son indépendance, de la qualité des avis qu'elle formule et de l'information qu'elle diffuse, de la transparence de ses procédures et de ses modes de fonctionnement et de la diligence avec laquelle elle s'acquitte des tâches qui lui sont confiées répondrait à ces besoins. L'Agence devra exécuter ses tâches en totale coopération avec les États membres et être ouverte à tous contacts avec le secteur professionnel et les autres groupes intéressés.
- (13) Compte tenu de l'incidence de plus en plus marquée des incidents liés à la sécurité, au niveau communautaire comme au niveau mondial, il est impératif de pallier ces défaillances efficacement et sans retard. Actuellement, cependant, il n'existe pas en Europe d'organe habilité à recueillir systématiquement des données qui pourraient être utilisées pour l'analyse des violations de sécurité.

¹¹ JO L 281 du 23.11.1995, p.31.

¹² JO L 13 du 19.1.2000, p.12.

- (14) Pour faire en sorte d'instaurer la confiance dans les réseaux et systèmes d'information, il importe que les particuliers, les entreprises et les administrations publiques soient suffisamment informés et au fait de l'actualité dans le domaine de la sécurité. Les pouvoirs publics ont pris des mesures pour accroître la sensibilisation en organisant des actions d'information auprès du public. Toutefois, il faut encore développer ces mesures, notamment en ce qui concerne les nouveaux points faibles et les risques qu'ils comportent. Une intensification des échanges d'information entre les États membres facilitera la mise en place de ces actions de sensibilisation.
- (15) Malgré le besoin de processus fiables, il est souvent difficile d'évaluer dans quelle mesure les produits et les services sont dignes de confiance. Il existe des systèmes d'évaluation et de certification publics et privés. Cependant, ces processus d'évaluation et de certification ont tendance à être lourds, chers et lents. Tous les intervenants du secteur, y compris les pouvoirs publics, gagneraient à être mieux conseillés dans leurs efforts pour promouvoir des systèmes de certification efficaces. Par conséquent, un organe européen techniquement compétent pour fournir des conseils objectifs sur la qualité des différentes normes améliorerait les possibilités de promouvoir des normes de sécurité fiables en Europe, y compris, le cas échéant, en matière de technologies de renforcement du respect de la vie privée.
- (16) L'efficacité des politiques de sécurité repose sur des méthodes d'évaluation des risques bien développées, dans le secteur public comme dans le secteur privé. Les procédures et méthodes d'évaluation des risques sont utilisées à des niveaux différents et il n'existe pas de pratiques communes permettant de garantir leur application efficace. La promotion et le développement des meilleures pratiques d'évaluation des risques amélioreront l'interopérabilité et renforceront la sécurité des réseaux et systèmes d'information en Europe.
- (17) Le travail de l'Agence devrait prendre en compte les activités en cours de recherche, de développement et d'évaluation technologique, et plus particulièrement celles menées par le Centre Commun de Recherche et dans le cadre des autres initiatives communautaires de recherche.
- (18) Les questions de sécurité des réseaux et de l'information sont des problèmes de dimension mondiale qui ne sont limités ni aux États membres ni à la Communauté. En effet, un problème de sécurité peut provenir, à l'origine, d'un pays tiers. Les produits et les services sont souvent développés et évalués dans des pays tiers. Une fois entrés sur le territoire de la Communauté, les produits de sécurité peuvent circuler pratiquement sans restriction, et les services peuvent être offerts librement. Il faut renforcer la coopération au niveau mondial pour améliorer les normes de sécurité, améliorer l'information et mettre au point des mécanismes de réaction communs. Plusieurs partenaires internationaux de la Communauté ont commencé à mettre en place des organes de sécurité permettant d'améliorer les réactions et le développement des politiques. Il est devenu impératif, au niveau européen également, d'instaurer une coopération efficace avec ces pays et avec la communauté internationale.
- (19) Pour veiller à la bonne exécution des fonctions de l'Agence, les États membres et la Commission seront représentés par un conseil d'administration doté des pouvoirs nécessaires pour établir le budget, vérifier son exécution, adopter des règles financières appropriées, établir des procédures de travail transparentes pour la prise de décisions par l'Agence, adopter le programme de travail, examiner les demandes d'assistance technique émanant des États membres et nommer le directeur exécutif.

Compte tenu du caractère hautement technique et scientifique de la mission et des tâches qui incombent à l'Agence, il serait judicieux que le conseil d'administration soit composé de membres possédant un haut niveau d'expertise pour les questions qui relèvent des attributions de l'Agence, telles qu'elles ont été déterminées par le Conseil et la Commission.

- (20) Un conseil consultatif devra être créé pour conseiller le directeur exécutif sur les questions de coopération et pour faciliter un échange d'informations approprié entre les États membres et l'Agence. Dans le cadre de son rôle consultatif, le conseil consultatif sera également amené à préparer le projet de programme de travail annuel de l'Agence. Lors de la désignation des membres du conseil consultatif, il faudrait s'assurer qu'ils possèdent l'expertise relevante, en ce compris dans le domaine de la protection des données.
- (21) Pour le bon fonctionnement de l'Agence, il est impératif que son directeur exécutif soit désigné sur la base de son mérite et de ses capacités attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes dans le domaine de la sécurité des réseaux et de l'information, et qu'il s'acquitte de sa mission en toute indépendance et en faisant preuve de souplesse quand à l'organisation du fonctionnement interne de l'Agence. A cette fin, le directeur exécutif devra élaborer et arrêter toutes les mesures nécessaires pour veiller à la bonne exécution du programme de travail de l'Agence, préparer chaque année un projet de rapport général à soumettre au conseil d'administration, établir un état prévisionnel des recettes et des dépenses de l'Agence et exécuter le budget.
- (22) L'Agence devra appliquer la législation communautaire pertinente en ce qui concerne l'accès du public aux documents¹³ et la protection des individus en matière de traitement des données personnelles¹⁴.
- (23) Dans la mesure où l'Agence sera chargée du traitement de données relatives à des actes illégaux commis contre les systèmes d'information, à des procédures de traitement d'incidents et à des fonctions d'évaluation des risques, il faudra assurer une certaine coordination politique globale, au niveau national comme au niveau européen. Cette coordination devra s'inscrire dans le cadre du conseil consultatif visé à l'article 7 et elle devra se dérouler sans compromettre les exigences de confidentialité mentionnées à l'article 13.
- (24) Pour assurer la pleine autonomie et l'indépendance de l'Agence, il est jugé nécessaire de la doter d'un budget autonome dont l'essentiel des recettes proviendra d'une contribution de la Communauté. La procédure budgétaire communautaire reste applicable en ce qui concerne les subventions imputables sur le budget général des Communautés. En outre, le contrôle des comptes est effectué par la Cour des comptes.

¹³ Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, JO L 145 du 31.5. 2001, p.43.

¹⁴ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. JO L 8 du 12.1.2001, p.1.

- (25) L'Agence devrait donc être initialement créée pour une période limitée et son fonctionnement fera ensuite l'objet d'une évaluation visant à déterminer si cette période doit être prolongée.

ONT ARRÊTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE 1 OBJECTIFS ET TÂCHES

Article premier Objectifs

1. La présent règlement institue une Agence chargée de la sécurité des réseaux et de l'information, ci-après dénommée «l'Agence».
2. Cette Agence facilite l'application des mesures communautaires relatives à la sécurité des réseaux et de l'information et permet d'assurer l'interopérabilité des fonctions de sécurité dans les réseaux et systèmes d'information, ce qui contribuera au fonctionnement du marché intérieur. Elle renforce la capacité de la Communauté et des États membres en matière de réaction aux problèmes de sécurité des réseaux et de l'information.

Article 2 Tâches

Afin d'atteindre les objectifs fixés à l'article premier, les tâches que l'Agence doit accomplir sont les suivantes:

- (a) collecter et analyser des données, et notamment des données sur les risques actuels et émergents et, en particulier, sur ceux qui auraient une incidence sur la capacité de récupération des réseaux de communications d'importance critique et sur les informations accessibles et transmises par leur intermédiaire;
- (b) fournir à la Commission et à d'autres organes compétents une assistance ainsi que des avis entrant dans le cadre de ses objectifs;
- (c) renforcer la coopération entre les différents acteurs dans le domaine de la sécurité des réseaux et de l'information, notamment en créant un réseau d'organes nationaux et communautaires;
- (d) contribuer à la disponibilité rapide, pour tous les utilisateurs, d'informations objectives et complètes sur la sécurité des réseaux et de l'information, notamment par la promotion des échanges de meilleures pratiques sur les méthodes d'alerte des utilisateurs, en particulier en ce qui concerne les attaques informatiques, et par la recherche de synergies entre initiatives du secteur public et du secteur privé;
- (e) assister, lorsqu'elle y est invitée, la Commission et les autorités de régulation nationales dans l'analyse de la mise en œuvre des exigences de sécurité en matière de sécurité des réseaux et de l'information qui incombent aux

opérateurs et aux fournisseurs de service, en ce compris les exigences en matière de protection des données, en vertu de la législation communautaire;

- (f) contribuer à l'évaluation des normes en matière de sécurité des réseaux et de l'information;
- (g) promouvoir des activités d'évaluation des risques et encourager l'adoption de solutions interopérables de gestion des risques au sein des organisations;
- (h) contribuer à l'approche communautaire de la coopération avec les pays tiers, notamment en facilitant les contacts avec les instances internationales;
- (i) accomplir toute autre tâche entrant dans le cadre de ses objectifs qui pourrait lui être assignée par la Commission.

Article 3 *Définitions*

Au sens du présent règlement, on entend par:

- «*réseau*», les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;
- «*système d'information*», les ordinateurs et réseaux de communication électroniques, ainsi que les données électroniques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance;
- «*sécurité des réseaux et de l'information*», la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, aux événements accidentels ou aux actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles;
- «*disponibilité*», le fait que les données sont accessibles et les services opérationnels;
- «*authentification*», la confirmation de l'identité supposée d'entités ou d'utilisateurs;
- «*intégrité des données*», la confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées;
- «*confidentialité des données*», la protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées;
- «*risque*», une fonction de la probabilité d'une incidence d'une vulnérabilité du système sur la disponibilité, l'authentification, l'intégrité ou la confidentialité des données

traitées ou transmises et le degré de gravité de cette incidence, découlant d'une utilisation intentionnelle ou non de cette vulnérabilité;

- «évaluation du risque», un processus reposant sur une base scientifique et technologique et comprenant quatre étapes: l'identification des dangers, leur caractérisation, l'évaluation de l'exposition et la caractérisation des risques.
- «gestion du risque», le processus, distinct de l'évaluation des risques, consistant à mettre en balance les différentes politiques possibles, en consultation avec les parties intéressées, à prendre en compte l'évaluation des risques et d'autres facteurs légitimes, et, au besoin, à choisir les mesures de prévention et de contrôle appropriées.

CHAPITRE 2

ORGANISATION

Article 4 *Organes de l'Agence*

L'Agence se compose:

- (a) d'un conseil d'administration;
- (b) d'un directeur exécutif et de son personnel;
- (c) d'un conseil consultatif et
- (d) le cas échéant, de groupes de travail.

Article 5 *Conseil d'administration*

1. Le conseil d'administration est composé de six représentants nommés par le Conseil, de six représentants nommés par la Commission et de deux représentants des secteurs professionnels et d'un représentant des consommateurs sans voix délibérative proposés par la Commission et nommés par le Conseil.
2. Les représentants peuvent être remplacés par des suppléants qui sont nommés en même temps qu'eux. Leur mandat sera d'une durée de deux ans et demi et il pourra être prorogé une fois.
3. Le directeur exécutif participe aux réunions du conseil d'administration, sans voix délibérative, et veille à ce que le secrétariat en soit assuré.
4. Le conseil d'administration élit son président parmi ses membres, pour une période de deux ans et demi renouvelable.
5. Le conseil d'administration adopte son règlement intérieur approuvé au préalable par la Commission. Sauf disposition contraire, les délibérations du conseil d'administration sont acquises à la majorité des membres qui le composent.

6. Le conseil d'administration se réunit sur convocation du président ou à la demande d'au moins un tiers de ses membres.
7. Le conseil d'administration adopte le règlement intérieur de l'Agence sur la base d'une proposition de la Commission. Ledit règlement est rendu public.
8. Le conseil d'administration définit les orientations générales du fonctionnement de l'Agence et veille à ce que cette dernière exécute sa mission dans des conditions lui permettant de jouer un rôle de référence du fait de son indépendance, de la qualité des avis qu'elle rend et des informations qu'elle diffuse, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à s'acquitter des tâches qui lui sont confiées.
9. Avant le 31 janvier de chaque année, le conseil d'administration adopte, après approbation de la Commission, le programme de travail de l'Agence pour l'année en question. Le conseil d'administration veille à assurer la cohérence de ce programme de travail avec les priorités législatives et politiques de la Communauté en matière de sécurité des réseaux et de l'information.
10. Avant le 31 mars de chaque année, le conseil d'administration adopte le rapport général des activités de l'Agence pour l'année qui précède.
11. Les règles financières applicables à l'Agence sont adoptées par le conseil d'administration après consultation de la Commission. Elles ne s'écartent du règlement financier cadre adopté par la Commission en application de l'article 185 du règlement (CE, Euratom) n° 1605/2002¹⁵ (ci-après dénommé «le règlement financier général») que si les exigences spécifiques du fonctionnement de l'Agence le nécessitent et avec l'accord préalable de la Commission.

Article 6
Directeur exécutif

1. L'Agence est gérée par son directeur exécutif, qui est indépendant dans l'exercice de ses fonctions.
2. Le directeur exécutif est nommé par le conseil d'administration sur la base d'une liste de candidats proposée par la Commission à la suite d'une mise en concurrence ouverte, après parution au Journal officiel des Communautés européennes et dans d'autres publications d'un appel à manifestation d'intérêt. Avant d'être nommé, le candidat retenu par le conseil d'administration est invité sans délai à faire une déclaration devant le Parlement européen et à répondre aux questions posées par ses membres. Le conseil d'administration peut révoquer le directeur exécutif avec l'accord de la Commission.
3. Le mandat du directeur exécutif aura une durée de deux ans et demi et il pourra être prorogé une fois.
4. Le directeur exécutif est chargé

¹⁵ JO L 248 du 16.9.2002, p.1.

- (a) de l'administration courante de l'Agence;
 - (b) d'établir des propositions de programmes de travail pour l'Agence, en consultation avec le conseil consultatif;
 - (c) de la mise en œuvre des programmes de travail et des décisions adoptées par le conseil d'administration;
 - (d) de veiller à ce que l'Agence exerce sa mission selon des modalités permettant de répondre aux besoins de ceux qui font appel à ses services, notamment en termes d'adéquation des services rendus;
 - (e) de la préparation de l'état prévisionnel des recettes et des dépenses de l'Agence et de l'exécution de son budget;
 - (f) de toutes les questions de personnel;
 - (g) d'établir et de maintenir le contact avec le Parlement européen et d'assurer un dialogue régulier avec les commissions compétentes du Parlement.
5. Le directeur exécutif soumet chaque année, pour approbation, au conseil d'administration:
- (a) un projet de rapport général d'activités couvrant l'ensemble des tâches de l'Agence pour l'année écoulée;
 - (b) un projet de programme de travail.
6. Le directeur exécutif transmet, après son adoption par le conseil d'administration, le programme de travail au Parlement européen, au Conseil, à la Commission et aux États membres, et en assure la publication.
7. Le directeur exécutif transmet, après son adoption par le conseil d'administration, le rapport général de l'Agence au Parlement européen, au Conseil, à la Commission, à la Cour des comptes, au Comité économique et social et au Comité des régions et en assure la publication.

Article 7
Conseil consultatif

1. Le conseil consultatif est composé de neuf experts proposés par le conseil d'administration et désignés par le directeur exécutif. Les représentants peuvent être remplacés par des suppléants qui sont nommés en même temps qu'eux. Les représentants des services de la Commission peuvent être présents aux réunions et participer aux travaux du conseil consultatif.
2. Les membres du conseil consultatif ne peuvent pas être membres du conseil d'administration.
3. Le conseil consultatif est présidé par le directeur exécutif. Il se réunit régulièrement à l'invitation du président ou à la demande d'au moins un tiers de ses membres. Ses

modalités de fonctionnement sont précisées dans le règlement intérieur de l'Agence et sont rendues publiques.

4. Les avis du conseil consultatif peuvent faire l'objet d'un vote.
5. L'Agence apporte le soutien technique et logistique nécessaire au conseil consultatif et assure le secrétariat de ses réunions.
6. Le conseil consultatif:
 - (a) conseille le directeur exécutif dans l'exercice des responsabilités qui lui incombent en vertu du présent règlement, notamment en vue de l'élaboration d'une proposition relative au programme de travail de l'Agence.
 - (b) conseille le directeur exécutif en ce qui concerne l'instauration d'une coopération étroite entre l'Agence et les institutions et organes compétents dans les différents États membres et notamment en ce qui concerne la cohérence entre les travaux de l'Agence et les activités menées par les États membres.
7. Le directeur exécutif peut inviter des représentants du Parlement européen et d'autres instances compétentes à participer aux réunions du conseil consultatif.

CHAPITRE 3

FONCTIONNEMENT

Article 8

Programme de travail

Les activités de l'Agence consisteront à exécuter le programme de travail adopté conformément à l'article 5, paragraphe 9. Le programme de travail n'empêche pas l'Agence d'entreprendre des activités imprévues, dans le cadre de ses objectifs et des limites budgétaires fixées.

Article 9

Avis

1. Les demandes d'avis et d'assistance qui entrent dans le cadre des objectifs de l'Agence sont adressées au directeur exécutif et accompagnées d'informations générales expliquant la nature de la question devant être traitée. Le directeur exécutif transmet la demande à la Commission dans les dix jours ouvrables.
2. Les demandes visées au paragraphe 1 peuvent être introduites par:
 - (a) la Commission
 - (b) une autorité de régulation nationale au sens de l'article 2 de la directive-cadre ou un autre organe compétent d'un État membre reconnu à cette fin par le conseil d'administration.

3. Lorsque l'Agence a des difficultés à satisfaire une demande ou lorsqu'une demande n'est pas conforme aux dispositions du paragraphe 1, ou lorsque différentes demandes concernent le même sujet, le directeur exécutif consulte le conseil d'administration avant de prendre une décision. Si l'Agence refuse une demande, elle doit motiver son refus. Le directeur exécutif peut également demander l'avis du conseil consultatif sur la hiérarchisation des demandes d'avis.

Article 10
Groupes de travail

1. En tant que de besoin, et dans le cadre de ses objectifs, l'Agence peut créer des groupes de travail composés d'experts proposés par le conseil consultatif et désignés par le directeur exécutif, notamment en ce qui concerne des sujets scientifiques et techniques.
2. Des groupes de travail seront créés par le conseil consultatif, sur proposition du directeur exécutif, après consultation du conseil d'administration.
3. Les représentants des services de la Commission peuvent être présents aux réunions des groupes de travail.
4. Les modalités de nomination des experts et de fonctionnement du groupe de travail sont fixées dans le règlement intérieur de l'Agence.

Article 11
Indépendance

1. Les membres du conseil d'administration, le directeur exécutif et les membres du conseil consultatif s'engagent à agir au service de l'intérêt public et dans un esprit d'indépendance. A cette fin, ils font une déclaration d'engagement ainsi qu'une déclaration d'intérêt qui indique l'absence de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance. Ces déclarations sont faites par écrit.
2. Les experts externes participant aux groupes de travail déclarent, lors de chaque réunion, les intérêts qui pourraient être considérés comme préjudiciables à leur indépendance par rapport aux points à l'ordre du jour.

Article 12
Transparence

1. L'Agence fait en sorte que ses activités se déroulent dans la plus grande transparence et qu'elles soient conformes aux dispositions des articles 13 et 14.
2. L'Agence veille à ce que le public et toute partie intéressée reçoivent une information objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux, le cas échéant. Elle publie également les déclarations d'intérêt faites par les membres du conseil d'administration, le directeur exécutif et le conseil consultatif ainsi que les déclarations d'intérêt faites par les experts en relation avec les points de l'ordre du jour des groupes de travail.

3. Le conseil d'administration peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu'observateurs à certains travaux de l'Agence.
4. L'Agence fixe dans son règlement intérieur les modalités pratiques assurant l'application des règles de transparence visées aux paragraphes 1 et 2.

Article 13
Confidentialité

1. L'Agence ne divulgue pas à des tiers les informations qu'elle traite ou qu'elle reçoit et pour lesquelles un traitement confidentiel a été demandé et justifié, à l'exception des informations qui, conformément aux législations nationales, doivent être rendues publiques pour protéger la sécurité publique et permettre la prévention, la recherche, la détection et la poursuite d'infractions pénales.
2. Les membres du conseil d'administration et du conseil consultatif, le directeur exécutif ainsi que les experts externes participant à leurs groupes de travail, et les membres du personnel de l'Agence, même après la cessation de leurs fonctions, sont soumis à l'obligation de confidentialité visée à l'article 287 du traité CE.
3. L'Agence fixe dans son règlement intérieur les modalités pratiques assurant l'application des règles de confidentialité visées aux paragraphes 1 et 2.
4. Aux fins du premier paragraphe, « les tiers » ne comprendront pas la Commission.

Article 14
Accès aux documents

1. Le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission¹⁶ est applicable aux documents détenus par l'Agence.
2. Le Conseil d'administration adopte des dispositions pour la mise en œuvre du règlement (CE) n° 1049/2001 dans les six mois suivant le démarrage des activités de l'Agence.
3. Il peut être fait appel des décisions prises par l'Agence en application de l'article 8 du règlement (CE) n° 1049/2001, soit en présentant une plainte au médiateur, soit en formant un recours devant la Cour de justice des Communautés européennes, conformément aux articles 195 et 230 du traité CE, respectivement.

¹⁶ JO L 145 du 31.5.2001, p.43.

CHAPITRE 4

DISPOSITIONS FINANCIERES

Article 15 *Adoption du budget*

1. Les recettes de l'Agence se composent d'une contribution de la Communauté et de toute contribution octroyée par les pays tiers participant aux travaux de l'Agence conformément aux dispositions de l'article 22
2. Les dépenses de l'Agence comprennent la rémunération du personnel, l'assistance administrative et technique, les dépenses d'infrastructure et de fonctionnement, ainsi que les dépenses résultant de contrats passés avec des tiers.
3. Chaque année, avant le 1 mars au plus tard, le directeur exécutif établit une estimation des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant, et la transmet au conseil d'administration, accompagnée d'une liste de postes.
4. Les recettes et les dépenses doivent être équilibrées.
5. Le conseil d'administration établit, au plus tard le 31 mars de chaque année, sur la base d'un projet élaboré par le directeur exécutif, un état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant. Le conseil d'administration transmet cet état prévisionnel, comprenant le projet d'organigramme accompagné du programme de travail provisoire à la Commission ainsi qu'aux États avec lesquels la Communauté a conclu les accords visés à l'article 22.
6. Sur la base de cet état prévisionnel, la Commission inscrit les estimations correspondantes dans l'avant-projet de budget général des Communautés européennes, qu'elle soumet au Parlement européen et au Conseil (ci-après dénommés «l'autorité budgétaire» conformément à l'article 272 du traité.
7. L'autorité budgétaire détermine les crédits disponibles au titre de la subvention destinée à l'Agence.
8. L'autorité budgétaire arrête l'organigramme de l'Agence.
9. Après que le budget général des Communautés européennes a été arrêté par l'autorité budgétaire, le conseil d'administration adopte le budget final et le programme de travail de l'Agence en les adaptant au besoin à la contribution de la Communauté. Il les transmet sans tarder à la Commission et à l'autorité budgétaire.

Article 16 *Lutte contre la fraude*

1. Aux fins de lutte contre la fraude, la corruption et autres actes illégaux, les dispositions du règlement (CE) n° 1073/1999 du Parlement européen et du Conseil du

25 mai 1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF)¹⁷ s'appliquent sans restriction.

2. L'Agence adhère à l'accord interinstitutionnel du 25 mai 1999 relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF)¹⁸ et arrête immédiatement les dispositions appropriées, lesquelles s'appliquent à tous les agents de l'Agence.

Article 17
Exécution du budget

1. Le directeur exécutif exécute le budget de l'Agence.
2. L'auditeur interne de la Commission exerce à l'égard de l'Agence les mêmes compétences que celles qui lui sont attribuées à l'égard des services de la Commission.
3. Au plus tard le 31 mars suivant l'exercice clos, le comptable de l'Agence transmet les comptes provisoires au comptable de la Commission, accompagnés d'un rapport sur la gestion budgétaire et financière de l'exercice. Le comptable de la Commission procède à la consolidation des comptes provisoires des institutions et des organismes décentralisés au sens de l'article 128 du règlement financier général.
4. Au plus tard le 31 mars suivant l'exercice clos, le comptable de la Commission transmet les comptes provisoires de l'Agence à la Cour des comptes, ainsi qu'un rapport sur la gestion budgétaire et financière de l'exercice. Le rapport sur la gestion budgétaire et financière de l'exercice est également transmis au Parlement européen et au Conseil.
5. A réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'Agence, selon les dispositions de l'article 129 du règlement financier général, le directeur exécutif établit les comptes définitifs de l'Agence sous sa propre responsabilité et les transmet pour avis au conseil d'administration.
6. Le conseil d'administration émet un avis sur les comptes définitifs de l'Agence.
7. Le directeur exécutif transmet les comptes définitifs accompagnés de l'avis du conseil de direction au plus tard le 1 juillet suivant l'exercice clos, au Parlement européen, au Conseil, à la Commission et à la Cour des comptes.
8. Les comptes définitifs sont publiés.
9. Le Directeur exécutif adresse à la Cour des comptes une réponse aux observations de celle-ci le 30 septembre au plus tard. Il adresse cette réponse également au conseil d'administration.

¹⁷ JO L 136, 31.5.1999, p.1.

¹⁸ JO L 136, 31.5.1999, p.15.

10. Le Parlement européen, sur recommandation du Conseil qui statue à la majorité qualifiée, donne avant le 30 avril de l'année N+ 2 décharge au directeur exécutif sur l'exécution du budget de l'exercice N.

CHAPITRE 5

DISPOSITIONS GÉNÉRALES

Article 18

Personnalité juridique et privilèges

1. L'Agence est un organe de la Communauté. Elle a la personnalité juridique.
2. Dans chaque État membre, l'Agence jouit de la capacité juridique la plus étendue accordée aux personnes morales en droit national. Elle peut notamment acquérir et aliéner des biens immobiliers et mobiliers et ester en justice.
3. L'Agence est représentée par son directeur exécutif.
4. Le protocole sur les privilèges et immunités des Communautés européennes s'applique à l'Agence ainsi qu'à son personnel.

Article 19

Responsabilité

1. La responsabilité contractuelle de l'Agence est régie par la législation applicable au contrat en question. La Cour de justice des Communautés européennes est compétente pour se prononcer en vertu de toute clause compromissoire contenue dans un contrat conclu par l'Agence.
2. En cas de responsabilité non contractuelle, l'Agence, conformément aux principes généraux communs aux droits des États membres, répare tout dommage causé par ses services ou par ses agents dans l'exercice de leurs fonctions. La Cour de justice est compétente pour tout litige relatif à la réparation de tels dommages.
3. La responsabilité personnelle à l'égard de l'Agence de ses propres agents est régie par les dispositions pertinentes applicables au personnel de l'Agence.

Article 20

Personnel

1. Le personnel de l'Agence est soumis aux règles et réglementations applicables aux fonctionnaires et autres agents des Communautés européennes.
2. Sans préjudice de l'article 5, les compétences conférées à l'autorité investie du pouvoir de nomination par le statut ainsi qu'à l'autorité habilitée à conclure les contrats d'engagement par le régime applicable aux autres agents sont exercées par l'Agence en ce qui concerne son propre personnel.

Article 21
Protection des données à caractère personnel

Lorsque l'Agence traite des données relatives aux individus, elle est soumise aux dispositions du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données¹⁹.

Article 22
Participation des pays tiers

1. L'Agence est ouverte à la participation des pays qui ont conclu avec la Communauté européenne des accords en vertu desquels ils ont adopté et appliquent la législation communautaire dans le domaine couvert par le présent règlement.
2. Dans le cadre des dispositions pertinentes de ces accords, des arrangements sont élaborés qui spécifient notamment la nature, l'étendue et les modalités de la participation de ces pays aux travaux de l'Agence, y compris des dispositions relatives à la participation aux réseaux gérés par l'Agence, aux contributions financières et au personnel.

CHAPITRE 6
DISPOSITIONS FINALES

Article 23
Clause de révision

1. Dans un délai de trois ans à compter de la date fixée à l'article 26, ou plus tôt si le conseil d'administration le juge nécessaire, la Commission, en collaboration avec le conseil consultatif, procède à une évaluation sur la base d'un mandat délivré par le conseil d'administration. Cette évaluation vise à:
 - (a) évaluer les pratiques de travail et l'impact de l'Agence
 - (b) examiner sérieusement les objectifs et mécanismes établis;
 - (c) envisager, le cas échéant, les modifications appropriées, à la lumière de l'évolution de la situation institutionnelle et juridique dans l'Union européenne et compte dûment tenu de problèmes de sécurité de portée plus vaste, et notamment de questions de sécurité publique et de participation des organes chargés de faire respecter la loi.
2. Cette évaluation est rendue publique.

¹⁹ JO L 8 du 12.1.2001, p.1.

3. La Commission entreprend cette évaluation notamment dans le but de déterminer si la période pour laquelle l'Agence a été créée doit être prolongée au-delà de la date fixée à l'article 26.

Article 24
Contrôle administratif

Les activités de l'Agence sont soumises au contrôle du médiateur, conformément aux dispositions de l'article 195 du traité.

Article 25
Siège

Le siège de l'Agence sera fixé par les autorités compétentes, au plus tard six mois après l'adoption de ce règlement, sur proposition de la Commission.

Article 26
Durée

L'agence sera opérationnelle du 1^{er} janvier 2004 au 31 décembre 2008.

Article 27
Entrée en vigueur

Le présent règlement entre en vigueur le [...] suivant sa publication au *Journal officiel des Communautés européennes*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le [...]

Par le Parlement européen
Le président

Par le Conseil
Le Président

FICHE FINANCIÈRE LÉGISLATIVE

Domaine(s) politique(s): Société de l'information

Activité: Sécurité des réseaux et de l'information

DENOMINATION DE L'ACTION: PROPOSITION DE REGLEMENT DU PARLEMENT EUROPEEN ET DU CONSEIL INSTITUANT UNE AGENCE CHARGEE DE LA SECURITE DES RESEAUX ET DE L'INFORMATION

1. LIGNE(S) BUDGÉTAIRE(S) + INTITULÉ(S)

Une nouvelle ligne budgétaire sera proposée (la présente action fait partie de l'APS 2003)

2. DONNÉES CHIFFRÉES GLOBALES

2.1. Enveloppe totale de l'action (partie B): millions d'euros en CE

24,300 millions d'euros pour l'UE avec ses 15 États membres actuels (avec l'adhésion des 10 nouveaux pays, 9 millions d'euros supplémentaires seront nécessaires, ce qui portera le coût total de l'action à 33,3 millions d'euros).

L'action a été retenue par la Commission dans sa communication au Parlement européen et au Conseil du 27 février 2002 (SEC (2002)217/9)

2.2. Période d'application:

2004 - 2008

2.3. Estimation globale pluriannuelle des dépenses:

a) Échéancier crédits d'engagement/crédits de paiement (intervention financière)

Millions d'euros (*à la 3e décimale*)

	2004	2005	2006	2007	2008	Total
CE	2,500	5,000	5,600	5,600	5,600	24,300
CP	2,500	5,000	5,600	5,600	5,600	24,300

b) Assistance technique et administrative et dépenses d'appui

CE						
CP						

Sous-total a+b							
CE							
CP							

c) Incidence financière globale des ressources humaines et autres dépenses de fonctionnement

CE/CP							
-------	--	--	--	--	--	--	--

TOTAL a+b+c							
CE	2,500	5,000	5,600	5,600	5,600	24,300	
CP	2,500	5,000	5,600	5,600	5,600	24,300	

2.4. Compatibilité avec la programmation financière et les perspectives financières

Cette proposition nécessite une reprogrammation de la rubrique concernée des perspectives financières.

2.5. Incidence financière sur les recettes²⁰

Aucune implication financière (concerne des aspects techniques relatifs à la mise en œuvre d'une mesure).

3. CARACTÉRISTIQUES BUDGÉTAIRES

Nature de la dépense		Nouvel le	Participatio n AELE	Participation pays candidats	Rubrique PF
DNO	Diff/	OUI	OUI	NON	3

4. BASE JURIDIQUE

Articles 95 et 156 du traité.

5. DESCRIPTION ET JUSTIFICATION

5.1. Nécessité d'une intervention communautaire²¹

L'évaluation ex ante démontre que les différentes possibilités envisageables, telles que la création d'un réseau interne au sein de la Commission ou d'un réseau de correspondants dans les États membres ne satisfont pas aux critères qualitatifs

²⁰ Pour plus d'informations, voir l'évaluation ex ante séparée.

²¹ Pour plus d'informations, voir l'évaluation ex ante séparée.

objectifs (transparence, coût, efficacité et visibilité) et qu'elles ne créeraient pas non plus de valeur ajoutée comme une structure du type d'une agence de régulation.

La première possibilité n'est pas réalisable car la Commission ne dispose pas en interne des compétences nécessaires en matière de sécurité des réseaux et de l'information. La seconde, à savoir le réseau de correspondants nationaux, présente les inconvénients majeurs suivants:

- la Commission ne serait plus à même de superviser les travaux et un réseau exigerait davantage de ressources humaines et financières puisque les fonctions ne seraient pas centralisées mais multipliées par le nombre d'États membres.
- la sensibilisation à la dimension transnationale serait limitée, car on peut s'attendre que les autorités nationales se concentrent principalement sur les préoccupations qui leur sont propres.
- la visibilité des travaux serait limitée et il n'existerait pas de point de contact unique pour les discussions internationales, qui sont absolument nécessaires dans ce domaine.

Par conséquent, la présente proposition suit la structure esquissée dans la communication récemment adoptée par la Commission et intitulée «L'encadrement des agences européennes de régulation» (COM(2002)718 final du 11 décembre 2002). L'objectif principal consiste à axer les activités (comme cela ressort de la liste des tâches) sur des problèmes de régulation et, dans le même temps, à fournir aux États membres et à la Commission une assistance sur les questions à caractère hautement technique et technologique ayant trait à la sécurité des réseaux et de l'information.

La concentration des efforts sur une réponse coordonnée de la Communauté aux menaces croissantes qui pèsent sur la sécurité, ainsi que la mise en relief de cette réponse revêtent une importance particulière après les événements du 11 septembre qui ont fait de la sécurité des réseaux et de l'information une priorité politique.

5.1.1. Objectifs poursuivis

Compte tenu de l'importance que revêtent les réseaux et les systèmes d'information, leur sécurité de fonctionnement est devenue une préoccupation essentielle. Les systèmes d'informations sont essentiels pour l'ensemble de l'économie, non seulement pour la plupart des secteurs industriels, mais également pour le secteur public et la population. Les dysfonctionnements de ces systèmes affectent tout le monde, qu'il s'agisse des citoyens, des entreprises ou des administrations publiques.

La sécurité est donc devenue une préoccupation politique majeure. En matière de sécurité, les gouvernements ont une responsabilité plus étendue à l'égard de la société. Ils intensifient donc leur action pour améliorer la sécurité sur leur territoire. Toutefois, l'état d'avancement des actions engagées varie selon les États membres et ces derniers ont adopté des orientations prioritaires différentes. En matière de sécurité des réseaux et de l'information, il n'existe pas de coopération transfrontière systématique entre États membres, bien que les questions de sécurité ne puissent pas être considérées comme un problème isolé ne concernant qu'un seul pays. Il n'existe pas de mécanisme qui garantisse des réactions efficaces en cas de menaces pour la

sécurité. La mise en œuvre du cadre juridique est variable. On constate un manque d'interopérabilité qui empêche d'utiliser correctement les produits et services de sécurité.

Même si une harmonisation totale des différentes politiques serait inutile, l'Union tirerait avantage d'une coordination accrue entre les États membres et d'un niveau de sécurité suffisamment élevé dans tous les États membres. Une approche européenne coordonnée de la sécurité des réseaux et de l'information comporterait des avantages pour le marché intérieur, qui pourrait aussi bénéficier de l'ensemble du savoir-faire acquis par les États membres. En même temps, une telle approche serait favorable à l'innovation et permettrait aux entreprises européennes de mieux affronter la concurrence au niveau mondial.

L'Agence proposée aura pour tâche d'améliorer la sécurité des réseaux et de l'information en Europe, ainsi que la capacité des États membres de répondre, aussi bien individuellement que collectivement, aux grands problèmes de sécurité qui se posent pour les réseaux et l'information

5.1.2. Dispositions prises relevant de l'évaluation ex ante

La communication de la Commission intitulée "Sécurité des réseaux et de l'information: proposition pour une approche politique européenne" (COM (2001)298 final) proposerait un certain nombre de mesures pour renforcer la sécurité de l'information en Europe. La résolution du Conseil du 28 janvier 2002 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information a encore approfondi ce concept. Il est toutefois devenu manifeste que les dispositions institutionnelles actuelles ne permettent pas de traiter les problèmes de sécurité des réseaux et de l'information de manière appropriée au niveau européen.

C'est la raison pour laquelle les auteurs de la résolution souhaitent également que la Commission présente une proposition sur la création d'un «groupe de travail pour la cybersécurité» pour répondre aux problèmes que pose la sécurité des réseaux et de l'information. Ce groupe de travail pour la cybersécurité a maintenant pris la forme d'une agence de régulation à durée limitée.

Un certain nombre d'autres solutions que celle de l'Agence ont été envisagées, mais aucune ne s'est révélée appropriée pour les tâches prévues pour une entité de ce type. L'évaluation ex ante contient une analyse plus détaillée des considérations qui ont présidé à l'établissement d'une nouvelle agence.

5.2. Lignes d'action envisagées

5.2.1. Objectifs

Le principal objectif de l'Agence consiste à créer en Europe une conception commune des questions de sécurité de l'information, qui est nécessaire pour garantir la disponibilité et la sécurité des réseaux et systèmes d'information dans l'Union.

L'Agence doit être en mesure de:

- fournir une **assistance pour l'application des mesures communautaires** relatives à la sécurité des réseaux et de l'information.

- cette assistance permettra d'assurer l'**interopérabilité** des fonctions de sécurité de l'information dans les réseaux et systèmes d'information, ce qui contribuera au **fonctionnement du marché intérieur**.
- renforcer la capacité de la Communauté et des États membres en matière de **réaction aux problèmes de sécurité des réseaux et de l'information**.

L'Agence aura un rôle crucial à jouer dans la sécurité des réseaux et systèmes d'information européens et dans le développement de la société de l'information en général.

5.2.2. *Tâches*

L'Agence

- aura une fonction consultative et une mission de coordination, dans le cadre desquelles elles **recueillera et analysera des données sur la sécurité de l'information**. Actuellement, des organismes tant publics que privés, poursuivant des objectifs différents, recueillent des données sur les incidents dans le domaine des technologies de l'information et d'autres renseignements pertinents pour la sécurité de l'information. Cependant, il n'existe pas, au niveau européen, d'organe central capable de mettre en œuvre une démarche d'ensemble pour la collecte et l'analyse des données et la formulation d'avis et de conseils en vue de soutenir l'activité politique de la Commission sur la sécurité des réseaux et de l'information.
- **fera office de centre d'expertise** auprès duquel les États membres comme les institutions communautaires pourront demander des **avis et des conseils sur des questions techniques** liées à la sécurité.
- contribuera à **l'instauration d'une coopération de grande envergure entre les différents acteurs** dans le domaine de la sécurité de l'information, en apportant par exemple une assistance aux activités de suivi qui accompagnent les travaux sur la sécurité du commerce électronique. Cette coopération sera une condition préalable capitale pour la sécurité du fonctionnement des réseaux et des systèmes d'information en Europe. La participation et l'engagement de tous les intéressés est donc requise.
- contribuera à l'instauration d'une approche coordonnée de la sécurité de l'information en fournissant une **assistance aux États membres**, par exemple en ce qui concerne la **promotion de l'évaluation des risques** et des actions de sensibilisation.
- assurera **l'interopérabilité des réseaux et systèmes d'information** lorsque les États membres **appliquent** des exigences techniques qui ont une incidence sur la sécurité.
- inventoriera les besoins **pertinents en matière de normalisation**, évaluera les normes de sécurité et systèmes de certification existants et œuvrera pour que leur utilisation par les États membres soit la plus large possible pour le soutien de l'application de la législation européenne.

- favorisera, dans ce domaine, une **coopération internationale** qui devient de plus en plus nécessaire car les problèmes de sécurité des réseaux et de l'information ont une dimension mondiale.

5.3. Modalités de mise en œuvre

La proposition vise à la création, pour une période initiale de cinq ans, d'une agence de régulation qui serait une entité extérieure à la Commission, l'«Agence». L'Agence est dotée de la personnalité juridique.

L'Agence comprend un conseil d'administration, un directeur exécutif et un conseil consultatif. La responsabilité générale des travaux et des questions de gestion, ainsi que de la nomination du directeur exécutif, incombe au conseil d'administration.

Le conseil consultatif sera composé d'experts et aura des fonctions consultatives. Il assurera une coopération étroite avec les États membres et les organisations concernées dans les États membres.

6. INCIDENCE FINANCIÈRE

6.1. Incidence financière totale sur la partie B (pour toute la période de programmation)

Étant donné que la tâche principale de l'Agence est de jouer le rôle de centre d'expertise, les avis et les opinions devront être fournis, dans une large mesure, par son personnel lui-même. Cela signifie également que les coûts administratifs de l'Agence représenteront une proportion élevée de son budget global.

6.1.1. Intervention financière

Crédits d'engagement en millions d'euros (à la 3e décimale)

Ventilation	2004	2005	2006	2007	2008	Total
Contribution à l'Agence	2,500	5,000	5,600	5,600	5,600	24,300
TOTAL	2,500	5,000	5,600	5,600	5,600	24,300

6.1.2. Assistance technique et administrative (ATA), dépenses d'appui (DDA) et dépenses TI (crédits d'engagement)

	2004	2005	2006	2007	2008	Total
1) Assistance technique et administrative (ATA):						
a) Bureaux d'assistance technique (BAT)						
b) Autre assistance technique et administrative: - intra-muros: - extra-muros: <i>dont pour la construction et la maintenance de systèmes de gestion informatisés:</i>						
Sous-total 1						
2) Dépenses d'appui (DDA):						
a) Études						
b) Réunion d'experts						
c) Information et publications						
Sous-total 2						
TOTAL	0	0	0	0	0	0

6.2. Calcul des coûts par mesure envisagée en partie B (pour toute la période de programmation)

Le tableau ci-dessous présente la ventilation des coûts de l'Agence pendant la période de fonctionnement proposée. La méthode de calcul établit une distinction entre la situation actuelle, où l'UE compte 15 États membres et celle qu'elle connaîtra dans le courant de l'année 2004 qui verra l'adhésion de 10 nouveaux pays. Des précisions sur les chiffres sont données aux points (a) à (f).

	2004		2005		2006		2007		2008		Total	
	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10
Ressources humaines	1,080	0,540	3,132	0,972	3,348	1,404	3,348	1,404	3,348	1,404	14,256	5,184
	(10*108)	(5*108)	(29*108)	(9*108)	(31*108)	(13*108)	(31*108)	(13*108)	(31*108)	(13*108)		
Equipements												
Mobilier	0,100	0,050	0,025	0,020	0,025	0,020	0,025	0,020	0,025	0,020	0,200	0,080
TI	0,220	0,120	0,480	0,170	0,528	0,200	0,528	0,200	0,528	0,200	2,284	0,770
Site web	0,150	0,050	0,050	0,000	0,050	0,000	0,050	0,000	0,050	0,000	0,350	0,000
Fonctionnement												
Publications	0,035	0,010	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,235	0,200
Conférences	0,100	0,000	0,150	0,000	0,200	0,000	0,200	0,000	0,200	0,000	0,850	0,000
Missions	0,140	0,060	0,200	0,065	0,200	0,065	0,200	0,065	0,200	0,065	0,940	0,260
Réunions	0,090	0,040	0,165	0,060	0,165	0,060	0,165	0,060	0,165	0,060	0,750	0,240
Traductions	0,160	0,050	0,200	0,250	0,200	0,300	0,200	0,300	0,200	0,300	0,960	1,150
Études	0,420	0,080	0,550	0,220	0,825	0,300	0,825	0,300	0,825	0,300	3,445	1,120
Total	2,495	1,000	5,002	1,807	5,591	2,399	5,591	2,399	5,591	2,399	24,270	9,004
Montant arrondi	2,500	1,000	5,000	1,800	5,600	2,400	5,600	2,400	5,600	2,400	24,300	9,000
Total EUR 15 et EUR +10	3,500		6,800		8,000		8,000		8,000		33,300	

a) *Travaux préparatoires*

L'Agence sera opérationnelle en janvier 2004.

Même s'il n'est pas directement lié à ce poste budgétaire, un budget est prévu dans le cadre du programme Modinis dans le budget 2003²². L'une des principales actions prévues par ce programme est l'«amélioration de la sécurité des réseaux et de l'information» et la «préparation de l'établissement du groupe de travail sur la cybersécurité» mentionné dans la résolution du Conseil du 28 janvier 2002 et dans le plan d'action «Europe 2005, notamment par le financement d'enquêtes, d'études et d'ateliers sur des sujets tels que les mécanismes de sécurité et leur interopérabilité, la protection et la fiabilité des réseaux, la cryptographie avancée, la protection de la vie privée et la sécurité dans les communications sans fil.

b) *Ressources humaines (bâtiments et dépenses administratives y afférentes compris)*

L'Agence devra disposer d'un personnel hautement qualifié et spécialisé pour s'acquitter des tâches qui lui incomberont. Actuellement, les professionnels correspondant à ce profil sont rares et très recherchés en Europe. L'Agence recrutera dans le secteur public comme dans le secteur privé. Elle emploiera 31 personnes lorsqu'elle sera entièrement opérationnelle dans une Union comptant 15 États membres. Cinq de ces personnes seront chargées de la gestion et de l'administration générales de l'Agence et 26 seront recrutées pour effectuer les tâches mentionnées à l'article 2 du projet de règlement. Les effectifs prévus pour l'encadrement et l'assistance administrative sont basés sur l'expérience acquise dans les agences communautaires existantes.

Sur les 26 personnes qui seront chargées d'accomplir les tâches opérationnelles, une sera chargée du secrétariat, et les autres seront recrutées sur la base de leur expérience spécifique: 6 spécialistes de l'analyse de risques et de la gestion de risques, 6 spécialistes de la surveillance de réseaux, 3 spécialistes des composants techniques des réseaux et systèmes d'information, 2 spécialistes de l'information et de la communication, 4 spécialistes des incidents informatiques et de la gestion d'intervention et 4 spécialistes de la coordination des activités de sécurité informatique menées par les autorités des États membres. La composition de l'effectif est basée sur une analyse approfondie, après des débats avec les directions de la sécurité des autorités nationales et des organismes de sécurité similaires dans les secteurs privé et public, tels que des équipes d'intervention en cas d'incident lié à la sécurité informatique. Elle tient compte des prévisions de charge de travail et découle directement de la liste des tâches de l'Agence. L'effectif est réduit au strict minimum en raison des restrictions budgétaires.

Lorsque l'Agence sera entièrement opérationnelle, le coût total annuel du personnel pour 15 États membres s'élèvera à 3,348 millions d'euros sur la base d'un coût moyen de 108 000 euros par fonctionnaire et par an pour la Commission, bâtiments et dépenses administratives y afférentes compris.

²²

Un accord politique a été trouvé lors du Conseil Télécommunications du 5 décembre et l'adoption officielle aura lieu lors du Conseil Télécommunications de mars 2003.

Étant donné que les effectifs ne devraient pas être au complet dès le début, le tableau figurant au point 6.2 est basé sur une hypothèse de recrutement progressif selon laquelle les effectifs seraient d'abord de 10 personnes en 2004, puis de 29 personnes en 2005 pour atteindre enfin le chiffre total de 31 personnes en 2006.

Conformément à l'article 20 de la proposition, le personnel de l'Agence est soumis aux règles et réglementations applicables aux fonctionnaires et autres agents des Communautés européennes.

Domaine d'activité	TOTAL	Grade A	Grade B	Grade C
Administration générale <ul style="list-style-type: none"> • Directeur exécutif • Secteur financier • Secteur des TI • Secrétariat 	5	1 1 1	1	1
Experts de la sécurité des réseaux et de l'information: <ul style="list-style-type: none"> • Experts • Secrétariat 	26	25		1
TOTAL	31	28	1	2

c) *Frais d'équipement*

Mobilier: le coût d'acquisition du mobilier et des équipements de bureau sera de 0,1 million d'euros pour la première année et de 0,025 million d'euros les années suivantes. Les locaux et les dépenses administratives y afférentes sont couverts par les coûts de personnel.

TI: Compte tenu des tâches qui lui sont assignées, l'Agence est susceptible d'être la cible de tentatives de piratage informatique et d'autres attaques visant les systèmes d'information. Elle doit être suffisamment protégée contre ce type de menaces. Elle devra donc impérativement disposer d'équipements de technologie de l'information très perfectionnés et dotés de dispositifs de sécurité d'un niveau élevé. En raison de la nécessité de garantir une protection optimale, le coût total d'équipements de TI par fonctionnaire et par an devrait représenter, en moyenne, 15 500 à 18 000 euros. **Les coûts dans le domaine des TI seront de 0,22 million d'euros pour la première année, de 0,48 million d'euros pour la deuxième année et de 0,528 million d'euros par an pour les années suivantes.**

Maintenance du site web: L'une des principales tâches de l'Agence consistera à mettre des informations à la disposition du grand public comme des spécialistes. Cela se fera essentiellement par l'intermédiaire du web. Le coût minimal (pour la seule

couverture des besoins d'information fondamentaux) de ces actions est estimé à 0,15 million d'euros la première année et à 0,05 million d'euros en coûts annuels par la suite.

d) *Coûts de fonctionnement*

Publications: Le site web servira de plate-forme pour la plupart des publications, mais l'agence publiera néanmoins, dans une certaine mesure, des rapports officiels et de la documentation sur papier, notamment pour l'information des institutions communautaires pertinentes. Les coûts de ces publications devraient représenter 35 000 euros pour la première année et 50 000 euros les années suivantes.

Conférences: 0,1 million d'euros devrait être consacré à l'organisation de conférences la première année, 0,15 million la deuxième année et 0,2 million d'euros l'année suivante. Ces conférences viseront principalement à assurer la diffusion des résultats des travaux de l'Agence à un public plus large composé d'entités publiques et privées.

Missions: La mise en réseau étroite avec les États membres ainsi que, compte tenu de la dimension mondiale du problème de la sécurité des réseaux, avec les pays tiers constitue une composante essentielle de la stratégie de l'Agence. Le coût des missions nécessaires pour mener à bien cette tâche est estimé à 0,14 million d'euros pour la première année et à 0,2 million d'euros par an pour les années suivantes.

Réunions: Le projet de règlement prévoit la création d'un conseil d'administration, d'un conseil consultatif ainsi que la création de groupes de travail. C'est le règlement intérieur de l'Agence qui fixera les modalités de fonctionnement de ces organes (fréquence des réunions, etc). Toutefois, selon la pratique en usage, l'estimation des coûts se fonde sur 3 réunions annuelles du conseil d'administration et une réunion mensuelle du conseil consultatif.

Le nombre total de réunions du conseil d'administration et du conseil consultatif sera de 15 par an. Pour chaque réunion, le coût des salles de réunion et des traductions s'élève à 7000 euros et les frais de déplacement à 700 euros. Les coûts annuels s'élèveront donc à 115 000 euros.

Le groupes de travail seront certainement mis en place après un certain temps. Il y aura moins de réunion de groupes d'experts la première année.

Traduction: Afin de réduire les coûts et les délais de traduction, les documents de travail internes de l'Agence ainsi que les documents qu'elle fournit à la Commission seront disponibles dans une des langues de travail seulement. Cependant, il pourra être nécessaire de traduire des documents en provenance et à destination des États membres. Le coût de ces traductions devra être adapté sur la base de l'expérience acquise. Un montant de 0,16 million d'euros pour la première année et de 0,2 million d'euros pour les années suivantes sont prévus pour couvrir les coûts.

e) *Études et recherches*

Étant donné que la sécurité des réseaux et de l'information est un domaine extrêmement spécialisé et que le monde en réseaux est très changeant, des défis nouveaux et imprévisibles ne manqueront pas d'apparaître au niveau mondial. Comme l'Agence disposera d'effectifs limités, il faudra faire appel à des experts

extérieurs pour certaines tâches. On aura recours à ces experts extérieurs notamment pour réaliser des études visant à recueillir des données et des statistiques, pour connaître l'incidence de l'évolution technologique sur les aspects liés à la sécurité tels que l'évaluation des risques et les modèles de gestion des risques, pour l'intégration des résultats des activités de recherche dans les technologies futures et émergentes, ainsi que pour l'information sur les solutions en matière de sécurité des réseaux mises au point dans les pays tiers.

Sur la base des informations recueillies, l'Agence fournira notamment à la Commission et à d'autres organes compétents une assistance ainsi que des avis; elle proposera des solutions pour améliorer la coopération entre les différents protagonistes, contribuera à la disponibilité rapide d'informations objectives et complètes et contribuera à l'approche communautaire de la coopération avec les pays tiers.

Le coût total de ces études s'élèvera à 3,445 millions d'euros. Pendant les premières années, l'Agence pourrait ne pas être entièrement opérationnelle et on estime qu'un montant de 0,42 million d'euros pour 2004 et de 0,55 millions d'euros pour 2005 sera consacré à ces études, alors qu'il atteindra 0,825 million d'euros les années suivantes. Le coût moyen de ces études se situe entre 0,2 et 0,3 million d'euros.

f) *Calculs avec les 10 nouveaux pays*

Avec l'entrée de 10 nouveaux pays, les effectifs augmenteront en conséquence car de nouveaux besoins en matière de participation des États membres et d'expertise se feront jour. Cette augmentation sera réalisée progressivement, avec 5 personnes supplémentaires en 2004, 9 en 2005 et 13 entre 2006 et 2008. Sur ces 13 personnes, 10 représenteront les nouveaux pays alors que 3 rempliront des fonctions de secrétariat ou d'encadrement.

L'accroissement des effectifs entraînera aussi une augmentation des besoins de *mobilier et d'équipements de TI* pour le personnel. Par rapport à l'augmentation des effectifs, la hausse du coût des équipements sera linéaire, sauf pour la première année pendant laquelle les coûts seront plus élevés (voir les calculs ci-dessus).

L'arrivée des nouveaux pays ne devrait pas entraîner de coûts supplémentaires pour les conférences, mais les *publications* devront être élaborées pour un public plus large et seront dès lors plus onéreuses. Il faudra aussi organiser des *missions* dans les nouveaux pays de manière à les faire participer à des programmes de coopération et d'échange d'information, etc. Les participants aux *réunions* seront plus nombreux et il y aura également des besoins supplémentaires en matière de *traduction* avec les nouveaux pays. Les calculs de ces coûts ont été établis avec le même rapport que les calculs établis avec les 15 États membres.

La somme consacrée aux *études* devra également être augmentée avec les nouveaux pays car il est important d'avoir une description complète de la situation en matière de sécurité des réseaux d'information dans ces pays et de connaître les besoins spécifiques qui pourraient se faire jour du fait de leur adhésion à l'Union. En 2004, il sera trop tôt pour avoir plus qu'une étude de base, mais en 2005 il sera important d'avoir une image complète de la situation dans les nouveaux pays, et le coût des études sera donc relativement plus élevé pour cette année-là.

7. INCIDENCE SUR LES EFFECTIFS ET LES DÉPENSES ADMINISTRATIVES

Les besoins en ressources humaines et administratives seront couverts par les crédits alloués à la DG gestionnaire dans le cadre de la procédure d'allocation.

7.1. Incidence sur les ressources humaines

Types d'emplois		Effectifs à affecter à la gestion de l'action par utilisation des ressources existantes et/ou supplémentaires		Total	Description des tâches découlant de l'action
		Nombre d'emplois permanents	Nombre d'emplois temporaires		
Fonctionnaires ou agents temporaires	A	2		2	
	B			1	
	C	1			
Autres ressources humaines - Experts du secteur privé -END -Auxiliaires					
Total		3		3	

7.2. Incidence financière globale des ressources humaines

Type de ressources humaines	Montants en euros	Mode de calcul *
Fonctionnaires		
Agents temporaires	324.000	
Autres ressources humaines -Experts du secteur privé -END -Auxiliaires (indiquer la ligne budgétaire)		
Total	324.000	

Les montants correspondent aux dépenses totales de l'action pour 12 mois.

7.3. Autres dépenses de fonctionnement découlant de l'action

Ligne budgétaire (n° et intitulé)	Montants en euros	Mode de calcul
Enveloppe globale (Titre A7)		
A0701 - Missions	10.000	Environ 6 missions par an
A07030 - Réunions		
A07040 - Conférences		
A0705 - Études et consultations		
Autres dépenses (indiquer lesquelles)		
-Locaux		
-Dépenses de fonctionnement		
Systèmes d'information (A-5001/A-4300)		
Autres dépenses - partie A (indiquer lesquelles)		
Total	10.000	

Les montants correspondent aux dépenses totales de l'action pour 12 mois.

Préciser le type de comité ainsi que le groupe auquel il appartient.

I.	Total annuel (7.2 + 7.3)	334.000
II.	Durée de l'action	5 ans
III.	Coût total de l'action (I x II)	1.670.000 €

8. SUIVI ET ÉVALUATION

8.1. Système de suivi

Pour assurer une utilisation efficace des crédits communautaires, la Commission doit assurer que les activités prévues par le présent règlement ne sont engagées qu'après l'application des procédures d'appel d'offre publiques, et que les activités sont surveillées et évaluées correctement.

8.2. Modalités et périodicité de l'évaluation prévue

La Commission et le Conseil consultatif procéderont à un examen des pratiques de travail de l'Agence et des effets de l'action de l'Agence. Cet examen doit avoir lieu dans les trois ans suivant la date de démarrage, c'est-à-dire avant le 31 décembre 2007.

9. MESURES ANTIFRAUDE

Le contrôle du paiement de tout service ou étude nécessaire est effectué par les services de l'Agence avant le paiement, compte tenu de toute obligation contractuelle, des principes économiques et des bonnes pratiques financières ou de gestion. Des dispositions anti-fraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.