COMMISSION EUROPÉENNE

Bruxelles, le 30.9.2010
COM(2010) 521 final

2010/0275 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

1.1. Contexte politique

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été instituée en mars 2004 par le règlement (CE) n° 460/2004[1], pour une durée initiale de cinq ans, avec pour objectif principal d'«*assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de [l'Union], […] en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur*». Le règlement (CE) n° 1007/2008[2] a prolongé le mandat de l'ENISA jusqu'en mars 2012.

La prolongation du mandat de l'ENISA en 2008 a aussi fourni l'occasion d'entamer un débat concernant l'orientation générale que doivent suivre les efforts européens en faveur de la sécurité des réseaux et de l'information (SRI), débat auquel la Commission a contribué en lançant une consultation publique sur les objectifs possibles d'une politique SRI renforcée au niveau de l'Union. Cette consultation publique s'est déroulée de novembre 2008 à janvier 2009 et a permis de recueillir près de 600 contributions[3].

Le 30 mars 2009, la Commission a adopté une communication relative à la protection des infrastructures d'information critiques[4] (PIIC) visant à protéger l'Europe des cyberattaques et des perturbations en améliorant la préparation, la sécurité et la résilience, qui comportait un plan d'action invitant l'ENISA à jouer un rôle, principalement de soutien aux États membres. Le plan d'action a été largement approuvé lors des discussions de la conférence ministérielle sur la PIIC qui s'est tenue à Tallinn, en Estonie, les 27 et 28 avril 2009[5]. Dans ses conclusions, la conférence de la présidence de l'Union européenne souligne combien il est important de «*mettre à profit le soutien opérationnel*» de l'ENISA; elle affirme que l'ENISA «*constitue un instrument précieux permettant d'appuyer les efforts de coopération menés à travers l'UE en la matière*» et souligne la nécessité de repenser et de reformuler le mandat de l'Agence «*afin de mieux mettre l'accent sur les priorités et les besoins de l'UE, de pouvoir y répondre de manière plus souple, de développer des savoirs et des compétences, et de soutenir l'efficacité opérationnelle de l'Agence ainsi que son impact général*» de sorte que l'Agence devienne «*un atout permanent pour chaque État membre et l'Union européenne dans son ensemble*».

---

1 Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

2 Règlement (CE) n° 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 293 du 31.10.2008, p. 1).

3 Le rapport de synthèse contenant les résultats de la consultation publique «Vers une politique renforcée de la sécurité des réseaux et de l'information en Europe» est joint en annexe 11 à l'analyse d'impact qui accompagne la présente proposition.

4 COM(2009) 149 du 30.3.2009.

5 Document de réflexion: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Conclusions de la présidence:
http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

Après discussion au Conseil Télécommunications du 11 juin 2009, à l'occasion duquel les États membres ont approuvé la prolongation du mandat de l'ENISA et l'accroissement de ses ressources eu égard à l'importance de la SRI et aux problèmes en constante évolution qui se posent dans ce domaine, il a été mis un terme au débat sous la présidence suédoise de l'Union. La résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de SRI[6] reconnaît le rôle et le potentiel de l'ENISA ainsi que la nécessité de «*continuer à développer cette agence pour en faire un organisme efficace*». Elle souligne aussi la nécessité de moderniser et de renforcer l'Agence pour que celle-ci aide la Commission et les États membres à combler le fossé entre technologie et politiques, servant ainsi de centre d'expertise de l'Union pour les questions de SRI.

1.2. Contexte général

L'ensemble de l'économie et de la société européenne repose désormais sur les technologies de l'information et des communications (TIC). Les TIC peuvent faire l'objet de menaces que les frontières nationales n'arrêtent plus et qui ont pris de nouvelles formes du fait de l'évolution des technologies et du marché. Étant donné que les TIC ont une dimension planétaire et qu'elles sont interconnectées avec d'autres infrastructures, dont elles sont interdépendantes, il est impossible de garantir leur sécurité et leur résilience en adoptant des approches strictement nationales et non coordonnées. En même temps, les problèmes liés à la SRI évoluent rapidement. Aussi les réseaux et systèmes informatiques doivent-ils être protégés efficacement contre toutes sortes de perturbations et de pannes, y compris contre les attaques délibérées.

Les politiques concernant la SRI ont une fonction essentielle dans la stratégie numérique pour l'Europe[7], initiative phare au titre de la stratégie Europe 2020, visant à exploiter et développer le potentiel des TIC et à le transformer en croissance durable et en innovation. Encourager l'adoption des TIC et susciter la confiance dans la société de l'information sont des priorités absolues de la stratégie numérique pour l'Europe.

À l'origine, l'ENISA a été créée pour assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union. Compte tenu de l'expérience acquise ainsi que des défis et menaces actuels, la nécessité s'est imposée de moderniser le mandat de l'Agence pour qu'il réponde mieux aux besoins de l'Union européenne justifiés par:

- la diversité des approches nationales pour relever les nouveaux défis;
- l'absence de modèle de coopération dans la mise en œuvre des politiques SRI;
- le niveau de préparation insuffisant également dû aux moyens limités de l'Europe en matière d'alerte rapide et d'intervention;
- le manque de données européennes fiables et la connaissance limitée des problèmes évolutifs;
- le faible niveau de sensibilisation aux risques et défis SRI;

---

6 Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (JO C 321, du 29.12.2009, p. 1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:FR:PDF

7 COM(2010) 245 du 19.5.2010.

- la difficulté d'intégrer des aspects SRI dans les politiques pour lutter plus efficacement contre la cybercriminalité.

1.3. Objectifs stratégiques

L'objectif général du règlement proposé est de permettre à l'Union, aux États membres et aux parties prenantes de se doter de moyens importants et d'atteindre un degré élevé de préparation pour prévenir et détecter les problèmes SRI et mieux y répondre. Cela contribuera à créer un climat de confiance, qui est à la base du développement de la société de l'information, à accroître la compétitivité des entreprises européennes et à faire en sorte que le marché intérieur fonctionne efficacement.

1.4. Dispositions en vigueur dans le domaine de la proposition

La présente proposition complète les initiatives politiques, réglementaires et non réglementaires, en matière de sécurité des réseaux et de l'information qui ont été prises au niveau de l'Union pour renforcer la sécurité et la résilience des TIC:

- Le plan d'action lancé par la communication PIIC prévoyait la création de deux entités:

  (1) Un Forum européen des États membres destiné à promouvoir l'échange d'informations et de bonnes pratiques afin de fixer des priorités et des objectifs stratégiques communs en matière de sécurité et de résilience des infrastructures TIC, en tirant directement parti des travaux effectués et du soutien apporté par l'Agence.

  (2) Un Partenariat public-privé européen pour la résilience (EP3R) constituant le cadre européen souple de gestion de la résilience des infrastructures TIC et consistant à encourager la coopération entre le secteur public et le secteur privé sur des objectifs, exigences de base, bonnes pratiques et mesures en matière de sécurité et de résilience.

- Le programme de Stockholm, adopté par le Conseil européen le 11 décembre 2009, vise à promouvoir des politiques garantissant la sécurité des réseaux et permettant de réagir plus rapidement en cas de cyberattaque dans l'Union.

- Ces initiatives contribuent à donner forme à la stratégie numérique pour l'Europe. Pour le volet de la stratégie destiné à susciter la confiance et à accroître la sécurité dans la société de l'information, les politiques concernant la SRI ont une fonction essentielle. Elles complètent aussi les mesures de soutien et la politique de la Commission sur la protection de la vie privée (notamment «dès la conception») et des données personnelles (réexamen du cadre), le réseau CPC, la gestion des identités et le programme pour un internet plus sûr.

1.5. Évolutions de la politique SRI actuelle en rapport avec la proposition

Plusieurs des évolutions en cours en matière de politique SRI, notamment celles annoncées dans le cadre de la stratégie numérique pour l'Europe, impliquent le soutien et l'expertise de l'ENISA. Il s'agit notamment de:

- Renforcer la coopération politique SRI en développant les activités au sein du **Forum européen des États membres**, ce qui, avec le soutien direct de l'ENISA, permettra:

– de définir les moyens d'établir un réseau européen efficace par la coopération transnationale entre équipes d'intervention en cas d'urgence informatique (CERT) nationales/gouvernementales;

– de fixer des objectifs et priorités à long terme pour des exercices paneuropéens à grande échelle concernant des incidents SRI;

– de recourir à des exigences minimales dans les marchés publics pour renforcer la sécurité et la résilience des systèmes et réseaux publics;

– de définir des mesures incitatives, de nature économique et réglementaire, en faveur de la sécurité et de la résilience;

– d'évaluer la situation de la SRI en Europe.

- Renforcer la coopération et la collaboration entre le secteur public et le secteur privé en soutenant le **Partenariat public-privé européen pour la résilience (EP3R)**. L'ENISA joue un rôle croissant dans la facilitation des réunions et activités de l'EP3R. Les prochaines activités de l'EP3R impliqueront de:

  – discuter des mesures et instruments innovants permettant d'accroître la sécurité et la résilience, tels que:

  (1) exigences de base en matière de sécurité et de résilience, en particulier dans les marchés publics de produits ou services TIC, afin d'uniformiser les règles du jeu tout en garantissant un niveau adéquat de préparation et de prévention;

  (2) questions relatives à la responsabilité des opérateurs économiques, par exemple lorsqu'ils instaurent des exigences de sécurité minimales;

  (3) mesures incitatives, de nature économique, en faveur de l'élaboration et de l'adoption de méthodes de gestion des risques, de processus et de produits en matière de sécurité;

  (4) systèmes d'évaluation et de gestion des risques afin d'apprécier et de maîtriser les incidents majeurs selon une base de référence commune;

  (5) coopération entre le secteur privé et le secteur public en cas d'incident de grande ampleur;

  (6) organisation d'un **sommet économique** sur les facteurs économiques favorables et défavorables à la sécurité et la résilience.

- Mettre en pratique les exigences de sécurité du paquet réglementaire sur les communications électroniques, domaine dans lequel l'expertise et l'assistance de l'ENISA sont nécessaires pour:

  – aider les États membres et la Commission, compte tenu de l'avis du secteur privé le cas échéant, à établir un cadre de règles et de procédures pour appliquer les dispositions relatives à la notification des atteintes à la sécurité (figurant à l'article 13 *bis* de la directive-cadre révisée);

– instituer un forum annuel des organismes nationaux compétents en matière de SRI, autorités réglementaires nationales et parties prenantes du secteur privé pour discuter des enseignements tirés et échanger de bonnes pratiques sur l'application des mesures réglementaires dans ce domaine.

- Faciliter les **exercices de préparation à la cybersécurité à l'échelle de l'UE** avec le soutien de la Commission et la contribution de l'ENISA en vue d'étendre ces exercices, à un stade ultérieur, au niveau international.

- **Créer une CERT (équipe d'intervention en cas d'urgence informatique) pour les institutions de l'UE**. L'action clé 6 de la stratégie numérique pour l'Europe consiste, pour la Commission, à présenter des «*mesures ayant pour but une politique renforcée et de haut niveau en matière de sécurité des réseaux et de l'information, y compris […] des mesures permettant de réagir plus rapidement en cas d'attaque informatique, notamment une CERT pour les institutions de l'UE*»[8]. Cela impliquera que la Commission et les autres institutions de l'Union procèdent à une analyse et mettent en place une équipe d'intervention en cas d'urgence informatique à laquelle l'ENISA pourra apporter soutien et expertise techniques.

- Mobiliser les États membres et les aider à compléter les **CERT nationales/gouvernementales** et, si nécessaire, à en créer **afin d'établir un réseau performant de CERT couvrant toute l'Europe**. Cette activité contribuera aussi au développement d'un système européen de partage d'information et d'alerte (SEPIA) pour les particuliers et les PME qui doit être mis en place à l'aide de ressources et de moyens nationaux d'ici à la fin de 2012.

- **Sensibiliser** aux défis SRI, ce qui impliquera:

  – que la Commission collabore avec l'ENISA afin de fournir des indications pour promouvoir des normes SRI, de bonnes pratiques et une culture de gestion des risques. La première série d'indications sera établie;

  – que l'ENISA organise, en coopération avec les États membres, le **«mois européen de la sécurité des réseaux et de l'information pour tous»** comportant des concours nationaux/européens de cybersécurité.

1.6. Cohérence avec les autres politiques et les objectifs de l'Union

La proposition est compatible avec les politiques existantes et les objectifs de l'Union européenne et parfaitement conforme à l'objectif de contribuer au bon fonctionnement du marché intérieur en améliorant la préparation et la réactivité aux défis en matière de sécurité des réseaux et de l'information.

---

[8] La résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information prévoyait aussi que: «*Le Conseil […] est conscient […] qu'il est important d'étudier les effets, les risques et les perspectives stratégiques de la création d'équipes d'intervention en cas d'urgence informatique pour les institutions de l'UE et de réfléchir au futur rôle éventuel de l'ENISA dans ce domaine*».

2. RÉSULTATS DES CONSULTATIONS ET DE L'ANALYSE D'IMPACT

2.1. Consultation des parties intéressées

La présente initiative politique est le résultat d'un large débat qui a été mené selon une approche intégratrice et dans le respect des principes de participation, d'ouverture, de responsabilité, d'efficacité et de cohérence. Dans le cadre de ce processus général, ont eu lieu une évaluation de l'Agence en 2006-2007 suivie par des recommandations du conseil d'administration de l'ENISA, deux consultations publiques (en 2007 et en 2008-2009) et plusieurs ateliers sur des questions relatives à la SRI.

La première consultation publique a été lancée parallèlement à la communication de la Commission sur l'évaluation à mi-parcours de l'ENISA. Elle était axée sur l'avenir de l'Agence, s'est déroulée du 13 juin au 7 septembre 2007 et a permis de recueillir un total de 44 contributions en ligne et deux autres par écrit. Les réponses ont été fournies par diverses parties prenantes et intéressées parmi lesquelles des ministères nationaux, des organismes réglementaires, des associations professionnelles et de consommateurs, des établissements universitaires, des entreprises et des particuliers.

Ces réponses ont mis en évidence un certain nombre de questions intéressantes concernant l'évolution du scénario de menace; la nécessité de clarifier et d'assouplir le règlement pour permettre à l'ENISA de relever les défis; l'importance d'une interaction effective avec les parties prenantes; et la possibilité d'un accroissement de ses ressources.

La seconde consultation publique, qui s'est déroulée du 7 novembre 2008 au 9 janvier 2009, visait à définir les objectifs prioritaires d'une politique SRI renforcée au niveau européen et les moyens d'atteindre ces objectifs. Près de 600 contributions ont été fournies par des autorités nationales, des établissements universitaires et de recherche, des associations professionnelles, des entreprises privées et d'autres parties prenantes, comme des organismes de protection des données et de conseil, et des particuliers.

Une grande majorité des répondants[9] a approuvé la prolongation du mandat de l'Agence et préconisé d'accroître son rôle dans la coordination des activités SRI au niveau européen ainsi que ses ressources. Parmi les grandes priorités figuraient la nécessité d'une approche plus coordonnée des menaces informatiques à travers l'Europe, la coopération transnationale pour faire face aux cyberattaques de grande ampleur, la création d'un climat de confiance et l'amélioration de l'échange d'informations entre parties prenantes.

Une analyse d'impact de la proposition a été réalisée, qui a commencé en septembre 2009, sur la base d'une étude préparatoire réalisée par un sous-traitant. Y ont participé un large éventail de parties prenantes et d'experts. Parmi les participants figuraient des organismes nationaux chargés de la SRI, des autorités réglementaires nationales, des opérateurs de télécommunications et fournisseurs de services internet ainsi que leurs associations professionnelles, des associations de consommateurs, des fabricants de TIC, des CERT, des universitaires et des utilisateurs en entreprise. Un groupe de pilotage interservices, composé des directions générales concernées de la Commission, a été créé pour faciliter la réalisation de l'analyse d'impact.

---

[9] Voir l'annexe XI de l'analyse d'impact.

2.2. Analyse d'impact

Il a été établi que conserver une agence était une solution adaptée pour atteindre les objectifs stratégiques de l'Union[10]. Après examen préalable, ont été retenues cinq options stratégiques soumises à une analyse plus poussée:

- Option 1 – Aucune politique;
- Option 2 – Statu quo, c'est-à-dire conserver un mandat analogue et le même niveau de ressources;
- Option 3 – Étoffer les tâches de l'ENISA en impliquant les autorités chargées du respect de la loi et de la vie privée en tant que parties prenantes de plein droit;
- Option 4 – Ajouter aux tâches de l'Agence la lutte contre les cyberattaques et la réaction aux incidents informatiques;
- Option 5 – Ajouter aux tâches de l'Agence l'assistance aux autorités de police et judiciaires dans leur lutte contre la cybercriminalité.

Après une analyse comparative des coûts et bénéfices, l'option 3 a été retenue comme la plus rentable et un moyen efficace d'atteindre les objectifs stratégiques.

L'option 3 prévoit un rôle accru de l'ENISA qui consistera plus précisément à:

- mettre en place et maintenir en activité un réseau de liaison entre parties prenantes et un réseau de connaissances pour faire en sorte que l'ENISA ait une vision exhaustive du paysage SRI européen;
- servir de centre de soutien SRI pour l'élaboration des politiques et leur mise en œuvre (notamment en ce qui concerne la vie privée et les communications électroniques, la signature électronique, l'identification électronique et les normes d'acquisition en matière de SRI);
- soutenir la politique de l'Union en matière de PIIC et de résilience (exercices, EP3R, SEPIA, etc.);
- établir un cadre de l'Union pour la collecte des données SRI et élaborer des méthodes et des pratiques pour leur enregistrement légal et leur partage;
- étudier l'économie de la SRI;
- favoriser la coopération avec les pays tiers et les organisations internationales pour promouvoir une approche globale commune de la SRI et encourager des initiatives internationales de haut niveau en Europe;
- exécuter des tâches non opérationnelles liées à des aspects SRI de la lutte contre la cybercriminalité et de la coopération judiciaire.

[10] Voir l'annexe IV de l'analyse d'impact.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

3.1. Résumé des mesures proposées

Le règlement proposé vise à renforcer et moderniser l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et à définir un nouveau mandat pour une durée de cinq ans.

La proposition comporte certains changements importants par rapport au règlement initial:

(1) **Plus grande souplesse, adaptabilité et capacité de ciblage**. Les tâches sont actualisées et reformulées dans leurs grandes lignes de façon à étendre le champ des activités de l'Agence; elles sont assez précises pour décrire les moyens par lesquels les objectifs doivent être atteints. Cela permet de mieux cadrer la mission de l'Agence, accroît la capacité de celle-ci à atteindre ses objectifs et renforce ses tâches de soutien à la mise en œuvre de la politique de l'Union.

(2) **Meilleur alignement de l'Agence sur le processus politique et réglementaire de l'Union**. Les institutions et organismes européens peuvent s'adresser à l'Agence pour obtenir une assistance et des conseils. Cela est conforme à l'évolution politique et réglementaire: dans ses résolutions, le Conseil a commencé à s'adresser directement à l'Agence et, dans le cadre réglementaire sur les communications électroniques, le Parlement européen et le Conseil ont confié à l'Agence des tâches relatives à la sécurité des réseaux et de l'information.

(3) **Interface avec la lutte contre la cybercriminalité**. Dans la réalisation de ses objectifs, l'Agence prend en compte la lutte contre la cybercriminalité. Les autorités chargées du respect de la loi et de la vie privée deviennent des parties prenantes de plein droit de l'Agence, notamment au sein du groupe permanent des parties prenantes.

(4) **Renforcement de la structure de gestion**. La proposition accroît le rôle de surveillance du conseil d'administration de l'Agence au sein duquel les États membres et la Commission sont représentés. Par exemple, le conseil d'administration peut fixer des orientations générales concernant le personnel, ce qui relevait de la seule responsabilité du directeur exécutif auparavant. Il peut aussi créer des organes de travail pour l'assister dans l'exécution de ses tâches, y compris dans le suivi de la mise en œuvre de ses décisions.

(5) **Rationalisation des procédures**. Les procédures qui se sont révélées inutilement lourdes sont simplifiées. Exemples: (a) la procédure concernant les règles internes du conseil d'administration est simplifiée, (b) l'avis sur le programme de travail de l'ENISA est rendu par les services de la Commission plutôt que par une décision de la Commission. De plus, les ressources nécessaires sont mises à la disposition du conseil d'administration au cas où celui-ci aurait besoin de prendre des décisions exécutoires et de les faire appliquer (par exemple, si un membre du personnel dépose une plainte contre le directeur exécutif ou le conseil lui-même).

(6) **Accroissement progressif des ressources**. Pour faire face au resserrement des priorités européennes et à l'ampleur croissante des défis, et sans préjudice de la proposition de Commission concernant le prochain cadre financier pluriannuel, il est prévu d'accroître progressivement les ressources financières et humaines de l'Agence

entre 2012 et 2016. Sur la base de la proposition de la Commission concernant le règlement fixant le cadre financier pluriannuel au-delà de 2013 et compte tenu des conclusions de l'analyse d'impact, la Commission présentera une fiche financière législative modifiée.

(7) **Possibilité de prolonger le mandat du directeur exécutif**. Le conseil d'administration peut prolonger de trois ans le mandat du directeur exécutif.

3.2. Base juridique

La présente proposition se fonde sur l'article 114 du traité sur le fonctionnement de l'Union européenne[11] (TFUE).

Conformément à l'arrêt de la Cour de justice de l'Union européenne[12], avant l'entrée en vigueur du traité de Lisbonne, l'**article 95 du traité CE** était considéré comme la base juridique appropriée à la création d'un organisme destiné à assurer un niveau élevé et efficace de SRI dans l'Union. Par l'expression «*mesures relatives au rapprochement*» figurant à l'article 95, les auteurs du traité ont voulu conférer au législateur de l'Union une marge d'appréciation quant au choix des mesures appropriées afin d'aboutir au résultat souhaité. Améliorer la sécurité et la résilience des infrastructures TIC est donc un facteur déterminant du bon fonctionnement du marché intérieur.

En vertu du traité de Lisbonne, l'**article 114 du TFUE**[13] décrit – presque dans les mêmes termes – la responsabilité en matière de marché intérieur. Pour les motifs exposés plus haut, il continuera à être la base juridique applicable pour l'adoption de mesures d'amélioration de la SRI. La responsabilité en matière de marché intérieur est désormais une compétence partagée entre l'Union et les États membres (article 4, paragraphe 2, point a), du TFUE). Cela signifie que l'Union et les États membres peuvent adopter des mesures (contraignantes) et que les États membres exercent leur compétence si l'Union n'a pas exercé ou a décidé de cesser d'exercer la sienne (article 2, paragraphe 2, du TFUE).

Les mesures relevant de la responsabilité en matière de marché intérieur exigeront une procédure législative ordinaire (articles 289 et 294 du TFUE), laquelle est similaire[14] à l'ancienne procédure de codécision (article 251 du traité CE).

Dans le traité de Lisbonne, l'ancienne distinction entre les piliers a disparu. La prévention et la lutte contre la criminalité font désormais partie des compétences partagées de l'Union. Cela a fourni à l'ENISA la possibilité de jouer un rôle de plateforme concernant les aspects SRI de la lutte contre la cybercriminalité et d'échanger des vues et de bonnes pratiques avec les autorités chargées de la cyberdéfense, du respect de la loi et de la vie privée.

---

11 JO C 115 du 9.5.2008, p. 94.

12 Arrêt de la Cour du 2.5.2006 dans l'affaire C-217/04, *Royaume-Uni de Grande-Bretagne et d'Irlande du Nord contre Parlement européen et Conseil de l'Union européenne*.

13 Cf. supra.

14 La procédure législative ordinaire diffère notamment en ce qui concerne les conditions de majorité au Conseil et au Parlement européen.

3.3. Principe de subsidiarité

La proposition est conforme au principe de subsidiarité. La politique SRI exige une approche concertée et les objectifs de la proposition ne peuvent être atteints par les États membres individuellement.

Une stratégie de stricte non-intervention de l'Union dans les politiques SRI nationales laisserait aux États membres l'intégralité de la tâche, en dépit de l'interdépendance évidente des systèmes informatiques existants. Une mesure garantissant un degré adéquat de coordination entre les États membres pour faire en sorte que les risques SRI soient bien gérés dans le contexte transnational dans lequel ils se présentent, respecte donc bel et bien le principe de subsidiarité. En outre, une action au niveau européen accroîtrait l'efficacité des politiques nationales existantes et procurerait une valeur ajoutée.

De plus, mettre en place une politique SRI concertée aura un impact positif sur la protection des droits fondamentaux et, en particulier, sur le droit à la protection des données personnelles et de la vie privée. Il est aujourd'hui essentiel de protéger les données car les Européens confient de plus en plus de données personnelles à des systèmes informatiques complexes, par choix ou nécessité, sans être forcément en mesure d'évaluer correctement les risques qui en découlent. Ils ne seront donc peut-être pas capables de prendre les mesures qui s'imposent si un incident se produit, de même qu'il n'est pas certain que, sans coordination SRI européenne, les États membres puissent réagir efficacement à tout incident international.

3.4. Principe de proportionnalité

La présente proposition est conforme au principe de proportionnalité car elle n'excède pas ce qui est nécessaire pour atteindre son objectif.

3.5. Choix des instruments

Instrument proposé: un règlement, qui est directement applicable dans tous les États membres.

4. INCIDENCE BUDGÉTAIRE

La proposition aura une incidence sur le budget de l'Union.

Étant donné que les tâches devant figurer dans le nouveau mandat de l'ENISA sont définies, il est prévu de mettre les ressources nécessaires à la disposition de l'Agence pour qu'elle exerce ses activités de façon satisfaisante. Il se dégage de l'évaluation de l'Agence, du processus de consultation approfondie des parties prenantes à tous les niveaux et de l'analyse d'impact un consensus général concernant la taille de l'Agence, jugée inférieure à la masse critique, et la nécessité d'accroître ses ressources. Les conséquences et les effets d'une augmentation des effectifs de l'Agence sont étudiés dans l'analyse d'impact accompagnant la proposition.

Le financement de l'UE au-delà de 2013 sera examiné dans le contexte d'un débat au sein de la Commission sur toutes les propositions pour la période après 2013.

5. REMARQUES COMPLÉMENTAIRES

5.1. Durée

Le règlement couvrira une période de cinq ans.

5.2. Clause de révision

Le règlement prévoit une évaluation de l'Agence couvrant la période écoulée depuis la précédente évaluation en 2007. Il s'agira d'évaluer la capacité de l'Agence à atteindre ses objectifs, tels qu'ils sont définis dans le règlement, de déterminer si elle constitue toujours un instrument efficace et si son mandat doit être prolongé. En fonction des conclusions de cette évaluation, le conseil d'administration formulera des recommandations, à l'intention de la Commission, concernant l'éventuelle modification du règlement, l'Agence et ses méthodes de travail. Pour permettre à la Commission de préparer à temps une éventuelle proposition de prolongation de mandat, l'évaluation devra avoir été effectuée avant la fin de la deuxième année du mandat prévu par le règlement.

5.3. Mesures provisoires

La Commission est consciente du fait que la procédure législative au Parlement européen et au Conseil peut demander un certain temps pour que la proposition soit débattue et il y a donc un risque de vide juridique au cas où le nouveau mandat de l'Agence ne serait pas adopté en temps voulu avant expiration du mandat actuel. Aussi la Commission soumet-elle, en même temps que la présente proposition, une proposition de règlement prolongeant de 18 mois le mandat actuel de l'Agence pour qu'un délai suffisant permette le déroulement des débats et des procédures.

2010/0275 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

vu l'avis du Comité économique et social européen[15],

vu l'avis du Comité des régions[16],

après transmission de la proposition aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Les communications, infrastructures et services électroniques sont un facteur déterminant du développement économique et de la société. Ils remplissent une fonction essentielle pour la société et sont devenus des services aussi indispensables que l'approvisionnement en électricité ou en eau. Toute perturbation de ces services peut causer des dommages économiques considérables, d'où l'importance de mesures de protection et de résilience accrues visant à assurer la continuité des services vitaux. La sécurité des communications, infrastructures et services électroniques, en particulier leur intégrité et leur disponibilité, constituent des défis toujours plus nombreux. C'est un sujet de préoccupation croissante pour la société, notamment parce que pourraient se poser des problèmes, en raison de la complexité des systèmes, d'un accident, d'une erreur ou d'une attaque, susceptibles d'avoir des répercussions sur l'infrastructure physique qui fournit des services essentiels au bien-être des Européens.

(2) La nature de la menace évolue constamment et les incidents relatifs à la sécurité peuvent ébranler la confiance des utilisateurs. De graves perturbations des communications, infrastructures et services électroniques peuvent avoir un impact économique et social important, mais les atteintes à la sécurité, les problèmes et les nuisances subis quotidiennement risquent aussi d'entamer la confiance du public dans les technologies, les réseaux et les services.

---

15 JO C […] du […], p. […].
16 JO C […] du […], p. […].

(3) Il est donc important pour les décideurs, les entreprises et les utilisateurs que la situation en matière de sécurité des réseaux et de l'information en Europe soit régulièrement évaluée à partir de données européennes fiables.

(4) Les représentants des États membres, réunis au Conseil européen le 13 décembre 2003, ont décidé que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui devait être instituée sur la base de la proposition soumise par la Commission, aurait son siège dans une ville de Grèce qui sera déterminée par le gouvernement grec.

(5) En 2004, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 460/2004[17] instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information afin de contribuer à la réalisation de l'objectif d'assurer un niveau élevé de sécurité des réseaux et de l'information au sein de l'Union et de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. En 2008, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 1007/2008[18] prolongeant le mandat de l'Agence jusqu'en mars 2012.

(6) Depuis que l'Agence a été instituée, les défis en matière de sécurité des réseaux et de l'information ont changé en fonction des évolutions technologiques, commerciales et socioéconomiques, et ont fait l'objet de réflexions et de débats approfondis. Face aux défis toujours nouveaux, l'Union a revu les priorités de sa politique en matière de sécurité des réseaux et de l'information dans plusieurs documents dont la communication de la Commission de 2006 *Une stratégie pour une société de l'information sûre – Dialogue, partenariat et responsabilisation*[19], la résolution du Conseil de 2007 relative à une stratégie pour une société de l'information sûre en Europe[20], la communication de 2009 relative à la protection des infrastructures d'information critiques *Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience*[21], les conclusions de la présidence de la conférence ministérielle sur la protection des infrastructures d'information critiques (PIIC) et la résolution du Conseil sur une approche européenne concertée en matière de sécurité des réseaux et de l'information[22]. La nécessité a été admise de moderniser et de renforcer l'Agence pour contribuer avec succès aux efforts des institutions européennes et des États membres pour mettre en place, en Europe, des moyens permettant de relever les défis de la sécurité des réseaux et de l'information. Plus récemment, la Commission a adopté la stratégie numérique pour l'Europe[23], initiative phare au titre de la stratégie Europe 2020. Cette stratégie globale vise à exploiter et développer le potentiel des TIC et à le transformer en croissance durable et en innovation. Susciter la confiance dans la société de l'information est l'un des principaux objectifs de la stratégie, au titre de

---

17 JO L 77 du 13.3.2004, p. 1.
18 JO L 293 du 31.10.2008, p. 1.
19 COM(2006) 251 du 31.5.2006.
20 Résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe (JO C 68 du 24.3.2007, p. 1).
21 COM(2009) 149 du 30.3.2009.
22 Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (JO C 321 du 29.12.2009, p. 1).
23 COM(2010) 245 du 19.5.2010.

laquelle ont été annoncées plusieurs actions que la Commission doit engager dans ce domaine, y compris la présente proposition.

(7) Dans le domaine de la sécurité des communications électroniques et, plus généralement, de la sécurité des réseaux et de l'information, les mesures relatives au marché intérieur nécessitent l'adoption de différentes modalités d'application techniques et organisationnelles par les États membres et la Commission. L'application hétérogène de ces exigences peut nuire à l'efficacité et créer des obstacles au marché intérieur. Il est donc nécessaire de créer, au niveau européen, un centre d'expertise chargé de fournir des indications, des conseils et, lorsqu'il y est invité, une assistance concernant les questions relatives à la sécurité des réseaux et de l'information, sur lequel les États membres et les institutions européennes peuvent compter. L'Agence peut répondre à ces besoins en acquérant et en conservant un niveau élevé d'expertise et en assistant les États membres, la Commission et, par conséquent, le secteur des entreprises en vue de les aider à satisfaire aux exigences juridiques et réglementaires en matière de sécurité des réseaux et de l'information, contribuant ainsi au bon fonctionnement du marché intérieur.

(8) L'Agence devrait exécuter les tâches qui lui sont confiées en vertu de la législation actuelle de l'Union dans le domaine des communications électroniques et, en général, contribuer à rehausser le niveau de sécurité des communications électroniques, notamment en fournissant une expertise et des conseils et en promouvant l'échange de bonnes pratiques.

(9) La directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre»)[24] exige aussi que les fournisseurs de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public prennent les mesures appropriées pour assurer leur intégrité et sécurité et instaurent des dispositions concernant la notification de toute atteinte à la sécurité ou perte d'intégrité. Le cas échéant, l'Agence doit aussi être informée par les autorités réglementaires nationales qui doivent soumettre à la Commission et à l'Agence un rapport annuel succinct sur les notifications reçues et l'action engagée. La directive 2002/21/CE invite également l'Agence à contribuer à l'harmonisation des mesures techniques et organisationnelles appropriées en matière de sécurité en formulant des avis.

(10) La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)[25] exige que les fournisseurs de services de communications électroniques accessibles au public prennent les mesures techniques et organisationnelles appropriées pour assurer la sécurité de leurs services et requiert également la confidentialité des communications et des données relatives au trafic y afférentes. La directive 2002/58/CE impose aux fournisseurs de services de communications électroniques des exigences en matière d'information et de notification des violations des données à caractère personnel. Elle exige aussi de la

[24] JO L 108 du 24.4.2002, p. 33.
[25] JO L 201 du 31.7.2002, p. 37.

Commission de consulter l'Agence sur toute mesure technique d'application à adopter concernant les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification. En application de la directive 95/46/CE du Parlement européen et du Conseil 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 données[26], les États membres doivent veiller à ce que le responsable du traitement mette en œuvre les mesures techniques et organisationnelles 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.

(11) L'Agence devrait contribuer à un niveau élevé de sécurité des réseaux et de l'information dans l'Union et à l'émergence d'une culture de la sécurité des réseaux et de l'information, dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, prenant part ainsi au bon fonctionnement du marché intérieur.

(12) Un ensemble de tâches assignées à l'Agence permettrait d'indiquer comment elle doit atteindre ses objectifs tout en lui laissant une certaine souplesse de fonctionnement. Au nombre des tâches exécutées par l'Agence devrait figurer la collecte des informations et données nécessaires à l'analyse des risques pour la sécurité et la résilience des communications, infrastructures et services électroniques et à l'évaluation, en coopération avec les États membres, de la situation en matière de sécurité des réseaux et de l'information en Europe. L'Agence devrait assurer la coordination avec les États membres et renforcer la coopération entre les parties prenantes en Europe, notamment en faisant participer à ses activités les organismes nationaux compétents et les experts du secteur privé dans le domaine de la sécurité des réseaux et de l'information. L'Agence devrait prêter assistance à la Commission et aux États membres dans leur dialogue avec les entreprises pour traiter les problèmes liés à la sécurité que posent les produits matériels et logiciels, contribuant ainsi à une approche concertée de la sécurité des réseaux et de l'information.

(13) L'Agence servirait de point de référence et instaurerait la confiance du fait de son indépendance, de la qualité des conseils fournis et des informations diffusées, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à exécuter les tâches qui lui seraient assignées. L'Agence devrait s'appuyer sur les efforts déployés aux niveaux national et de l'Union et par conséquent exécuter ses tâches en totale coopération avec les États membres et être ouverte à tout contact avec les entreprises et les autres parties intéressées. De plus, l'Agence devrait s'appuyer sur les informations fournies par le secteur privé et travailler en coopération avec celui-ci, lequel joue un rôle important dans la sécurisation des communications, infrastructures et services électroniques.

(14) La Commission a lancé un Partenariat public-privé européen pour la résilience, constituant un cadre européen souple de gestion de la résilience des infrastructures TIC, dans lequel l'Agence devrait jouer un rôle de facilitateur consistant à réunir les parties prenantes des secteurs public et privé pour qu'elles discutent des priorités de

[26] JO L 281 du 23.11.1995, p. 31.

politique générale, des aspects économiques et commerciaux des problèmes et des mesures en faveur de la résilience des infrastructures TIC et pour qu'elles définissent leurs responsabilités.

(15) L'Agence devrait, de sa propre initiative ou à la demande de la Commission, fournir à celle-ci des conseils, sous la forme d'avis et d'analyses techniques et socioéconomiques, pour l'assister dans l'élaboration de sa politique en matière de sécurité des réseaux et de l'information. L'Agence devrait aussi assister les États membres et les institutions et organismes européens, à leur demande, dans leurs efforts pour mettre en place une politique et des moyens en matière de sécurité des réseaux et de l'information.

(16) L'Agence devrait assister les États membres et les institutions européennes dans leurs efforts pour mettre en place et développer des moyens transnationaux de préparation afin de prévenir les problèmes et incidents de sécurité des réseaux et de l'information, de les détecter, de les atténuer et d'y faire face. À cet égard, l'Agence devrait faciliter la coopération entre les États membres et entre les États membres et la Commission. À cette fin, l'Agence devrait jouer un rôle actif de soutien des États membres dans leurs efforts continus pour développer leurs moyens d'intervention et pour organiser et réaliser des exercices nationaux et européens concernant des incidents de sécurité.

(17) La directive 95/46/CE régit le traitement des données à caractère personnel effectué en vertu du présent règlement.

(18) Pour mieux comprendre les défis dans le domaine de la sécurité des réseaux et de l'information, l'Agence doit analyser les risques actuels et émergents. À cet effet, l'Agence devrait, en coopération avec les États membres et, le cas échéant, les instituts de statistiques, recueillir les informations appropriées. En outre, l'Agence devrait assister les États membres et les institutions et organismes européens dans leurs efforts pour recueillir, analyser et diffuser des données sur la sécurité des réseaux et de l'information.

(19) Dans l'exercice d'activités de suivi dans l'Union, l'Agence devrait faciliter la coopération entre l'Union et les États membres en vue d'évaluer la situation en matière de sécurité des réseaux et de l'information en Europe et contribuer aux activités d'évaluation en coopération avec les États membres.

(20) L'Agence devrait faciliter la coopération entre les organismes publics compétents des États membres, notamment en favorisant la mise au point et l'échange de bonnes pratiques et de normes pour des programmes éducatifs et de sensibilisation. Une intensification des échanges d'informations entre les États membres facilitera cette action. L'Agence devrait aussi favoriser la coopération entre les parties prenantes publiques et privées au niveau de l'Union, en particulier par la promotion du partage d'informations, des campagnes de sensibilisation et des programmes éducatifs et de formation.

(21) Des politiques de sécurité efficaces devraient reposer sur des méthodes d'évaluation des risques bien élaborées, dans le secteur public comme dans le secteur privé. Les méthodes et procédures d'évaluation des risques sont utilisées à différents niveaux et il n'existe pas de pratiques communes en ce qui concerne leur application efficace. La promotion et le développement des meilleures pratiques en matière d'évaluation des

risques et de solutions interopérables de gestion des risques dans les organisations des secteurs public et privé rehausseront le niveau de sécurité des réseaux et systèmes d'information en Europe. À cette fin, l'Agence devrait favoriser la coopération entre parties prenantes publiques et privées au niveau de l'Union, accompagner leurs efforts concernant la mise au point et l'adoption de normes en matière de gestion des risques et de sécurité mesurable des produits, systèmes, réseaux et services électroniques.

(22) Les travaux de l'Agence devraient prendre en compte les activités en cours en matière de recherche, de développement et d'évaluation technologique, et plus particulièrement celles menées dans le cadre des différentes initiatives de recherche de l'Union européenne.

(23) Le cas échéant, pour autant que cela soit utile à la réalisation de son champ d'application, de ses objectifs et de ses tâches, l'Agence devrait partager expérience et informations générales avec les organismes et agences créés en vertu de la législation de l'Union européenne et traitant de la sécurité des réseaux et de l'information.

(24) Dans ses relations avec les organismes chargés du maintien de l'ordre concernant les aspects «sécurité» de la cybercriminalité, l'Agence utilise les moyens d'information existants et les réseaux établis comme les points de contact mentionnés dans la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI, ou l'équipe d'Europol composée des chefs d'unités chargées de la criminalité utilisant les technologies avancées.

(25) Pour pouvoir atteindre pleinement ses objectifs, l'Agence devrait établir des relations avec les autorités chargées du respect de la loi et de la vie privée pour dégager et analyser correctement les aspects «sécurité des réseaux et de l'information» de la lutte contre la cybercriminalité. Les représentants de ces autorités devraient devenir des parties prenantes de plein droit de l'Agence et être représentées au sein de son groupe permanent des parties prenantes.

(26) Les questions de sécurité des réseaux et de l'information sont des problèmes de dimension mondiale. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de sécurité ainsi que l'échange d'informations et pour promouvoir une approche globale commune des problèmes de sécurité des réseaux et de l'information. À cette fin, l'Agence devrait favoriser la coopération avec les pays tiers et les organisations internationales de concert, le cas échéant, avec le SEAE.

(27) Dans l'exécution de ses tâches, l'Agence ne devrait pas porter atteinte aux compétences et ne devrait pas empiéter sur les pouvoirs et les tâches, ni les entraver ou les recouper, qui sont attribués: aux autorités réglementaires nationales définies dans les directives relatives aux réseaux et services de communications électroniques ainsi qu'à l'Organe des régulateurs européens des communications électroniques (ORECE) institué par le règlement (CE) n° 1211/2009 du Parlement européen et du Conseil[27] et au comité des communications visé dans la directive 2002/21/CE, aux organismes européens de normalisation, aux organismes nationaux de normalisation et au comité permanent prévu dans la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998

[27] JO L 337 du 18.12.2009, p. 1.

prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information[28], et aux autorités de contrôle des États membres pour ce qui est de la protection des personnes physiques à l'égard du traitement des données à caractère personnel et de la libre circulation de ces données.

(28) Afin d'assurer l'efficacité de l'Agence, les États membres et la Commission devraient être représentés au sein d'un conseil d'administration chargé de fixer l'orientation générale du fonctionnement de l'Agence et de veiller à ce qu'elle exécute ses tâches conformément au présent règlement. Le conseil d'administration devrait être doté des pouvoirs nécessaires pour établir le budget, vérifier son exécution, adopter les règles financières appropriées, instaurer des procédures de travail transparentes pour la prise de décisions par l'Agence, adopter le programme de travail de l'Agence, son propre règlement intérieur et les règles internes de fonctionnement de l'Agence, nommer le directeur exécutif et décider de la prolongation ou de l'expiration du mandat de ce dernier. Le conseil d'administration devrait être en mesure de créer des organes de travail pour l'assister dans ses tâches, organes qui pourraient par exemple élaborer ses décisions ou suivre leur mise en œuvre.

(29) Pour le bon fonctionnement de l'Agence, il est impératif que son directeur exécutif soit nommé 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 en matière de sécurité des réseaux et de l'information, et qu'il s'acquitte de sa mission en toute indépendance quant à l'organisation du fonctionnement interne de l'Agence. À cette fin, le directeur exécutif devrait élaborer une proposition de programme de travail pour l'Agence, après consultation préalable des services de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne exécution de ce programme de travail. Il devrait préparer chaque année un projet de rapport général à soumettre au conseil d'administration, établir un projet d'état prévisionnel des recettes et des dépenses de l'Agence et exécuter le budget.

(30) Le directeur exécutif devrait avoir la possibilité de créer des groupes de travail *ad hoc* pour traiter des questions spécifiques, en particulier de nature scientifique, technique, juridique ou socioéconomique. Lors de la création de ces groupes, le directeur exécutif devrait recueillir et prendre en compte les avis des experts externes concernés pour permettre à l'Agence d'avoir accès aux informations disponibles les plus récentes concernant les défis que pose, en matière de sécurité, l'évolution de la société de l'information. L'Agence devrait veiller à ce que les membres des groupes de travail *ad hoc* soient sélectionnés selon les critères de compétence les plus stricts, compte dûment tenu de la nécessité d'assurer une représentation équilibrée, en fonction des questions spécifiques le cas échéant, des administrations publiques des États membres, du secteur privé et des entreprises, des utilisateurs et des experts universitaires en matière de sécurité des réseaux et de l'information. Si nécessaire, l'Agence peut inviter à titre individuel des experts dont les compétences dans le domaine concerné sont reconnues à participer aux activités des groupes de travail au cas par cas. Leurs dépenses devraient être couvertes par l'Agence conformément à ses règles internes de fonctionnement et aux règlements financiers en vigueur.

---

[28] JO L 204 du 21.7.1998, p. 37.

(31) L'Agence devrait comprendre, comme organe consultatif, un groupe permanent des parties prenantes pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties intéressées. Le groupe permanent des parties prenantes, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions d'importance pour toutes les parties prenantes et à les porter à l'attention de l'Agence. Le directeur exécutif peut, le cas échéant et en fonction de l'ordre du jour des réunions, inviter des représentants du Parlement européen et d'autres organismes intéressés à participer aux réunions du groupe.

(32) L'Agence doit fonctionner dans le respect, respectivement, (i) du principe de subsidiarité, en garantissant un degré adéquat de coordination entre les États membres sur les questions de sécurité des réseaux et de l'information, en accroissant l'efficacité des politiques nationales et en leur procurant donc une valeur ajoutée, et (ii) du principe de proportionnalité, en n'excédant pas ce qui est nécessaire pour atteindre les objectifs fixés dans le présent règlement.

(33) L'Agence devrait appliquer la législation pertinente de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil[29] et la protection des individus en matière de traitement des données à caractère personnel comme prévu par le 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[30].

(34) Dans le cadre de son champ d'application et de ses objectifs ainsi que dans l'accomplissement de ses tâches, l'Agence devrait respecter en particulier les dispositions applicables aux institutions européennes et la législation nationale en matière de traitement des documents sensibles. Le conseil d'administration devrait avoir le pouvoir de prendre une décision autorisant l'Agence à traiter des informations classifiées.

(35) Pour garantir l'autonomie et l'indépendance complètes de l'Agence, il est jugé nécessaire de la doter d'un budget autonome dont l'essentiel des recettes provient d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'Agence. L'État membre d'accueil, ou tout autre État membre, devrait être autorisé à apporter des contributions volontaires aux recettes de l'Agence. La procédure budgétaire de l'Union reste applicable en ce qui concerne les subventions imputables sur le budget général de l'Union européenne. En outre, la Cour des comptes devrait procéder au contrôle des comptes.

---

29 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).

30 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).

(36) L'Agence devrait succéder à l'ENISA qui a été instituée par le règlement (CE) n° 460/2004. Dans le cadre de la décision des représentants des États membres réunis au Conseil européen du 13 décembre 2003, l'État membre d'accueil devrait maintenir et développer les modalités pratiques actuelles afin d'assurer le bon fonctionnement de l'Agence, compte tenu notamment des missions de coopération et d'assistance de l'Agence vis-à-vis de la Commission, des États membres et de leurs organismes compétents, des autres institutions et organes de l'Union et des parties prenantes publiques et privées en Europe.

(37) L'Agence devrait être créée pour une période limitée. Son fonctionnement devrait être évalué en fonction de l'efficacité de réalisation des objectifs et de ses méthodes de travail afin de déterminer si les objectifs de l'Agence sont toujours valables ou pas et, de ce fait, si sa durée de fonctionnement doit être prolongée,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE 1 CHAMP D'APPLICATION, OBJECTIFS ET TÂCHES

Article premier
Objet et champ d'application

1. Le présent règlement institue une Agence européenne chargée de la sécurité des réseaux et de l'information (ci-après dénommée «l'Agence») afin de contribuer à un niveau élevé de sécurité des réseaux et de l'information au sein de l'Union et en vue d'y sensibiliser la société et de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information, dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur.

2. Les objectifs et les tâches de l'Agence ne portent pas atteinte aux compétences des États membres en matière de sécurité des réseaux et de l'information ni, en tout état de cause, aux activités liées à la sécurité publique, à la défense, à la sûreté de l'État (y compris à la prospérité économique de l'État lorsqu'il s'agit de questions touchant à la sûreté de l'État) ou aux activités de l'État dans les domaines du droit pénal.

3. Aux fins du présent règlement, on entend par «*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, à des événements accidentels ou à des 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.

Article 2
Objectifs

1. L'Agence assiste la Commission et les États membres en vue de les aider à satisfaire aux exigences juridiques et réglementaires de la législation actuelle et future de l'Union en matière de sécurité des réseaux et de l'information, contribuant ainsi au bon fonctionnement du marché intérieur.

2. L'Agence renforce les moyens et améliore la préparation de l'Union et des États membres pour prévenir les problèmes et incidents de sécurité des réseaux et de l'information, les détecter et y faire face.

3. L'Agence acquiert et conserve un niveau élevé d'expertise qu'elle met à profit pour favoriser une large coopération entre les acteurs des secteurs public et privé.

Article 3
Tâches

1. Aux fins exposées à l'article 1er, l'Agence accomplit les tâches suivantes:

(a) assister la Commission, à la demande de celle-ci ou de sa propre initiative, dans l'élaboration de la politique en matière de sécurité des réseaux et de l'information en lui fournissant des conseils et des avis, des analyses techniques et socioéconomiques, et des travaux préparatoires à l'élaboration et à l'actualisation de la législation de l'Union dans le domaine de la sécurité des réseaux et de l'information;

(b) faciliter la coopération au sein des États membres, et entre les États membres et la Commission, dans leurs efforts pour atteindre une dimension transnationale afin de prévenir les problèmes et incidents de sécurité des réseaux et de l'information, de les détecter et d'y faire face;

(c) assister les États membres et les institutions et organismes européens dans leurs efforts pour recueillir, analyser et diffuser des données sur la sécurité des réseaux et de l'information;

(d) évaluer régulièrement, en coopération avec les États membres et les institutions européennes, la situation en matière de sécurité des réseaux et de l'information en Europe;

(e) favoriser la coopération entre les organismes publics compétents en Europe et, en particulier, accompagner leurs efforts pour mettre au point et échanger de bonnes pratiques et des normes;

(f) assister l'Union et les États membres dans la promotion du recours à de bonnes pratiques et à des normes de gestion des risques et de sécurité pour les produits, systèmes et services électroniques;

(g) favoriser la coopération entre parties prenantes publiques et privées au niveau de l'Union, notamment en promouvant le partage d'informations et la sensibilisation et en accompagnant leurs efforts pour mettre au point et adopter des normes en matière de gestion des risques et de sécurité des produits, réseaux et services électroniques;

(h) faciliter le dialogue et l'échange de bonnes pratiques, entre parties prenantes publiques et privées, concernant la sécurité des réseaux et de l'information, y compris les aspects de la lutte contre la cybercriminalité; assister la Commission dans la fixation d'orientations politiques qui tiennent compte des aspects «sécurité des réseaux et de l'information» de la lutte contre la cybercriminalité;

(i) assister les États membres et les institutions et organismes européens, à leur demande, dans leurs efforts pour mettre en place des moyens de détection, d'analyse et d'intervention en matière de sécurité des réseaux et de l'information;

(j) favoriser le dialogue et la coopération avec les pays tiers et les organisations internationales de concert, le cas échéant, avec le SEAE, pour promouvoir une coopération internationale et une approche globale commune des problèmes de sécurité des réseaux et de l'information;

(k) exécuter les tâches confiées à l'Agence par les actes législatifs de l'Union.

CHAPITRE 2 ORGANISATION

Article 4
Organes de l'Agence

L'Agence comprend:

(a) un conseil d'administration;

(b) un directeur exécutif et du personnel; et

(c) un groupe permanent des parties prenantes.

Article 5
Conseil d'administration

1. Le conseil d'administration fixe l'orientation générale du fonctionnement de l'Agence et veille à ce qu'elle travaille conformément aux règles et principes énoncés dans le présent règlement. Il assure aussi la cohérence des travaux de l'Agence avec les activités menées par les États membres ainsi qu'au niveau de l'Union.

2. Le conseil d'administration adopte son règlement intérieur en accord avec les services concernés de la Commission.

3. Le conseil d'administration adopte les règles internes de fonctionnement de l'Agence en accord avec les services concernés de la Commission. Ces règles sont rendues publiques.

4. Le conseil d'administration nomme le directeur exécutif conformément à l'article 10, paragraphe 2, et peut le révoquer. Le conseil d'administration exerce l'autorité disciplinaire sur le directeur exécutif.

5. Le conseil d'administration adopte le programme de travail de l'Agence conformément à l'article 13, paragraphe 3, et le rapport général sur les activités de l'Agence au cours de l'année précédente conformément à l'article 14, paragraphe 2.

6. Le conseil d'administration adopte les règles financières applicables à l'Agence. Elles ne peuvent s'écarter du règlement (CE, Euratom) n° 2343/2002 de la Commission du 19 novembre 2002 portant règlement financier-cadre des organismes visés à l'article 185 du règlement (CE, Euratom) n° 1605/2002 du Conseil portant règlement financier applicable au budget général des Communautés européennes[31] que si les exigences spécifiques du

[31] JO L 357 du 31.12.2002, p. 72.

fonctionnement de l'Agence le nécessitent et si la Commission a préalablement donné son accord.

7. Le conseil d'administration, en accord avec la Commission, arrête les modalités d'application nécessaires, conformément à l'article 110 du statut.

8. Le conseil d'administration peut créer des organes de travail, composés de ses membres, pour l'assister dans l'exécution de ses tâches, y compris dans l'élaboration de ses décisions et le suivi de leur mise en œuvre.

9. Le conseil d'administration peut adopter le plan pluriannuel en matière de politique du personnel après avoir consulté les services de la Commission et dûment informé l'autorité budgétaire.

Article 6
Composition du conseil d'administration

1. Le conseil d'administration est composé d'un représentant de chaque État membre, de trois représentants nommés par la Commission ainsi que de trois représentants sans droit de vote, nommés par la Commission, représentant chacun l'un des groupes suivants:

(a) les entreprises du secteur des technologies de l'information et des communications;

(b) les consommateurs;

(c) les experts universitaires en sécurité des réseaux et de l'information.

2. Les membres du conseil d'administration et leurs suppléants sont nommés sur la base de leur expérience et de leurs compétences dans le domaine de la sécurité des réseaux et de l'information.

3. Le mandat des représentants des groupes visés au paragraphe 1, points a), b) et c), a une durée de quatre ans. Il peut être prolongé une fois. Si un représentant cesse d'appartenir à son groupe d'intérêt respectif, la Commission nomme un remplaçant.

Article 7
Présidence du conseil d'administration

Le conseil d'administration élit son président et un vice-président parmi ses membres, pour une durée de trois ans renouvelable. Le vice-président remplace d'office le président lorsque celui-ci n'est pas en mesure d'assumer ses fonctions.

Article 8
Réunions

1. Les réunions du conseil d'administration sont convoquées par son président.

2. Le conseil d'administration tient une réunion ordinaire deux fois par an. Il tient aussi des réunions extraordinaires à l'initiative du président ou à la demande d'au moins un tiers de ses membres disposant du droit de vote.

3. Le directeur exécutif participe aux réunions du conseil d'administration sans voix délibérative.

Article 9
Vote

1. Les décisions du conseil d'administration sont prises à la majorité de ses membres disposant du droit de vote.

2. Une majorité des deux tiers des membres du conseil d'administration disposant du droit de vote est nécessaire pour adopter le règlement intérieur, les règles internes de fonctionnement de l'Agence, le budget et le programme de travail annuel ainsi que pour nommer le directeur exécutif, prolonger son mandat ou le révoquer.

Article 10
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 et révoqué par le conseil d'administration. La nomination résulte d'une sélection dans une liste de candidats proposés par la Commission pour une période de cinq ans, sur la base du mérite et des capacités attestées dans le domaine de l'administration et de la gestion, ainsi que des compétences et de l'expérience spécifiques. Avant d'être nommé, le candidat retenu par le conseil d'administration peut être invité à faire une déclaration devant la commission compétente du Parlement européen et à répondre aux questions posées par les membres de cette dernière.

3. Dans les neuf mois précédant le terme de ce mandat, la Commission procède à une évaluation. Ce faisant, la Commission évalue en particulier:

– les résultats obtenus par le directeur exécutif;

– les fonctions et les exigences de l'Agence dans les années à venir.

4. Le conseil d'administration, statuant sur proposition de la Commission, compte tenu du rapport d'évaluation et dans les seuls cas où les fonctions et exigences de l'Agence peuvent le justifier, peut prolonger le mandat du directeur exécutif d'une durée maximale de trois ans.

5. Le conseil d'administration informe le Parlement européen de son intention de prolonger le mandat du directeur exécutif. Dans le mois précédant la prolongation de son mandat, le directeur exécutif peut être invité à faire une déclaration devant la commission compétente du Parlement et à répondre aux questions posées par les membres de cette dernière.

6. Si le mandat n'est pas prolongé, le directeur exécutif reste en fonction jusqu'à la nomination de son successeur.

7. Le directeur exécutif est chargé:

(a) d'assurer l'administration courante de l'Agence;

(b) de mettre en œuvre le programme de travail et les décisions adoptées par le conseil d'administration;

(c) de veiller à ce que l'Agence exerce ses activités conformément aux exigences de ceux qui font appel à ses services, notamment en termes d'adéquation des services rendus;

(d) de toutes les questions de personnel, conformément aux orientations générales du conseil d'administration et à ses décisions d'ordre général;

(e) d'établir et de maintenir le contact avec les institutions et organismes européens;

(f) d'établir et de maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d'assurer un dialogue régulier avec les parties intéressées;

(g) de toutes les autres tâches qui lui sont confiées en vertu du présent règlement.

8. En tant que de besoin et dans le cadre des objectifs et des tâches de l'Agence, le directeur exécutif peut créer des groupes de travail *ad hoc* composés d'experts. Le conseil d'administration en est préalablement informé. Les modalités concernant en particulier la composition des groupes de travail *ad hoc*, la nomination des experts par le directeur exécutif et le fonctionnement de ces groupes sont précisés dans les règles internes de fonctionnement de l'Agence.

9. Le directeur exécutif met du personnel administratif d'appui et d'autres ressources à la disposition du conseil d'administration chaque fois que c'est nécessaire.

Article 11
Groupe permanent des parties prenantes

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts représentant les parties intéressées, comme les entreprises du secteur des technologies de l'information et des communications, les organisations de consommateurs, les experts universitaires en matière de sécurité des réseaux et de l'information et les autorités chargées du respect de la loi et de la vie privée.

2. Les modalités relatives notamment au nombre de membres, à la composition du groupe, à la nomination des membres par le conseil d'administration sur proposition du directeur exécutif et au fonctionnement du groupe sont précisées dans les règles internes de fonctionnement de l'Agence et sont rendues publiques.

3. Le groupe est présidé par le directeur exécutif.

4. La durée du mandat des membres du groupe est de deux ans et demi. Les membres du conseil d'administration ne peuvent pas être membres du groupe. Des membres du personnel de la Commission peuvent être présents aux réunions et participer aux travaux du groupe.

5. Le groupe conseille l'Agence dans l'exercice de ses activités. Le groupe conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour ce qui est de communiquer avec les parties intéressées sur toutes les questions liées au programme de travail.

CHAPITRE 3 FONCTIONNEMENT

Article 12
Programme de travail

1. L'Agence exécute ses tâches conformément au programme de travail qui contient l'ensemble de ses activités planifiées. Le programme de travail n'empêche pas l'Agence d'entreprendre des activités imprévues qui relèvent de ses objectifs et de ses tâches et s'inscrivent dans les limites de son budget. Le directeur exécutif informe le conseil d'administration des activités de l'Agence qui ne sont pas prévues dans le programme de travail.

2. Le directeur exécutif est chargé d'établir le projet de programme de travail de l'Agence après consultation des services de la Commission. Avant le 15 mars de chaque année, le directeur exécutif soumet au conseil d'administration le projet de programme de travail pour l'année suivante.

3. Avant le 30 novembre de chaque année, le conseil d'administration adopte le programme de travail de l'Agence pour l'année suivante en concertation avec les services de la Commission. Le programme de travail comprend un aperçu pluriannuel. Le conseil d'administration veille à assurer la cohérence de ce programme de travail avec les objectifs de l'Agence ainsi qu'avec les priorités législatives et politiques de l'Union en matière de sécurité des réseaux et de l'information.

4. Le programme de travail est structuré selon le principe de la gestion par activités (GPA). Il est conforme à l'état prévisionnel des recettes et des dépenses de l'Agence et au budget de l'Agence pour l'exercice correspondant.

5. Le directeur exécutif transmet le programme de travail, après adoption par le conseil d'administration, au Parlement européen, au Conseil, à la Commission et aux États membres et en assure la publication.

Article 13
Rapport général

1. Chaque année, le directeur exécutif soumet au conseil d'administration un projet de rapport général couvrant toutes les activités de l'Agence au cours de l'année précédente.

2. Avant le 31 mars de chaque année, le conseil d'administration adopte le rapport général sur les activités de l'Agence au cours de l'année précédente.

3. Le directeur exécutif transmet le rapport général de l'Agence, après adoption par le conseil d'administration, au Parlement européen, au Conseil, à la Commission, à la Cour des comptes, au Comité économique et social européen ainsi qu'au Comité des régions et en assure la publication.

Article 14
Demandes adressées à l'Agence

1. Les demandes de conseils et d'assistance qui relèvent des objectifs et des tâches de l'Agence sont adressées au directeur exécutif et accompagnées d'informations générales expliquant la question devant être traitée. Le directeur exécutif informe le conseil d'administration des demandes reçues et, le moment venu, de la suite qui leur a été donnée. Si l'Agence rejette une demande, elle doit motiver son refus.

2. Les demandes visées au paragraphe 1 peuvent être introduites par:

(a) le Parlement européen;

(b) le Conseil;

(c) la Commission;

(d) tout organisme compétent désigné par un État membre, tel qu'une autorité réglementaire nationale au sens de l'article 2 de la directive 2002/21/CE.

3. Les modalités pratiques d'application des paragraphes 1 et 2 en ce qui concerne notamment la présentation, la hiérarchisation et le suivi des demandes adressées à l'Agence ainsi que l'information du conseil d'administration au sujet de ces demandes sont prévues par le conseil d'administration dans les règles internes de fonctionnement de l'Agence.

Article 15
Déclaration d'intérêt

1. Le directeur exécutif et les fonctionnaires détachés par les États membres à titre temporaire font par écrit une déclaration d'engagements et une déclaration indiquant l'absence de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance.

2. Les experts externes participant aux groupes de travail *ad hoc* déclarent, lors de chaque réunion, les intérêts qui pourraient être considérés comme préjudiciables à leur indépendance eu égard aux points inscrits à l'ordre du jour, et s'abstiennent de prendre part aux discussions sur ces points.

Article 16
Transparence

1. L'Agence veille à exercer ses activités avec un niveau élevé de transparence et conformément 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 le directeur exécutif et les fonctionnaires détachés par les États membres à titre temporaire ainsi que les déclarations d'intérêt faites par les experts en relation avec les points inscrits à l'ordre du jour des réunions des groupes de travail *ad hoc*.

3. Le conseil d'administration peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités de l'Agence.

4. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de transparence visées aux paragraphes 1 et 2.

Article 17
Confidentialité

1. Sans préjudice de l'article 14, 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.

2. Les membres du conseil d'administration, le directeur exécutif, les membres du groupe permanent des parties prenantes, les experts externes participant aux groupes de travail *ad hoc* et les membres du personnel de l'Agence, y compris les fonctionnaires détachés par les États membres à titre temporaire, sont soumis à l'obligation de confidentialité visée à l'article 339 du traité, même après la cessation de leurs fonctions.

3. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de confidentialité visées aux paragraphes 1 et 2.

4. Le conseil d'administration peut décider d'autoriser l'Agence à traiter des informations classifiées. Dans ce cas, le conseil d'administration, en accord avec les services de la Commission concernés, adopte des règles internes de fonctionnement respectant les principes de sécurité énoncés dans la décision 2001/844/CE, CECA, Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur[32]. Cela couvre, entre autres, les dispositions relatives à l'échange, au traitement et à l'archivage des informations classifiées.

Article 18
Accès aux documents

1. Le règlement (CE) n° 1049/2001 s'applique 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 la création de l'Agence.

3. Les décisions prises par l'Agence en application de l'article 8 du règlement (CE) n° 1049/2001 peuvent faire l'objet d'une plainte auprès du médiateur ou d'un recours devant la Cour de justice de l'Union européenne, conformément aux articles 228 et 263 du traité respectivement.

[32] JO L 317 du 3.12.2001, p. 1.

CHAPITRE 4 DISPOSITIONS FINANCIÈRES

Article 19
Adoption du budget

1. Les recettes de l'Agence se composent d'une contribution provenant du budget de l'Union européenne, de contributions apportées par les pays tiers participant aux travaux de l'Agence conformément aux dispositions de l'article 29, et de contributions des États membres.

2. Les dépenses de l'Agence comprennent la rémunération du personnel, l'assistance administrative et technique, les dépenses d'infrastructure et de fonctionnement et les dépenses résultant de contrats passés avec des tiers.

3. Au plus tard le 1er mars de chaque année, le directeur exécutif établit un projet d'état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant et le transmet au conseil d'administration avec un projet de tableau des effectifs.

4. Les recettes et les dépenses doivent être équilibrées.

5. Le conseil d'administration établit chaque année, sur la base du projet d'état prévisionnel des recettes et des dépenses élaboré par le directeur exécutif, un état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant.

6. Le conseil d'administration transmet, au plus tard le 31 mars, cet état prévisionnel comprenant le projet de tableau des effectifs ainsi que le projet de programme de travail, à la Commission et aux États avec lesquels l'Union européenne a conclu les accords visés à l'article 24.

7. L'état prévisionnel est transmis par la Commission au Parlement européen et au Conseil (ci-après dénommés l'«autorité budgétaire»), avec le projet de budget général de l'Union européenne.

8. Sur la base de cet état prévisionnel, la Commission inscrit dans le projet de budget général de l'Union européenne les prévisions qu'elle estime nécessaires en ce qui concerne le tableau des effectifs et le montant de la subvention à la charge du budget général et les soumet à l'autorité budgétaire conformément à l'article 314 du traité.

9. L'autorité budgétaire autorise les crédits au titre de la subvention destinée à l'Agence.

10. L'autorité budgétaire adopte le tableau des effectifs de l'Agence.

11. Le conseil d'administration adopte le budget de l'Agence en même temps que le programme de travail. Ce budget devient définitif après l'adoption définitive du budget général de l'Union européenne. Le cas échéant, le conseil d'administration ajuste le budget de l'Agence et le programme de travail conformément au budget général de l'Union européenne. Le conseil d'administration le transmet sans délai à la Commission et à l'autorité budgétaire.

Article 20
Lutte contre la fraude

1. Afin de lutter contre la fraude, la corruption et les autres actes illégaux, le 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)[33] s'applique sans restriction.

2. L'Agence adhère à l'accord interinstitutionnel du 25 mai 1999 entre le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF)[34] et arrête sans délai les dispositions applicables à tout le personnel de l'Agence.

Article 21
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 1er mars suivant l'achèvement de l'exercice, le comptable de l'Agence transmet les comptes provisoires, accompagnés d'un rapport sur la gestion budgétaire et financière durant l'exercice, au comptable de la Commission. Le comptable de la Commission procède à la consolidation des comptes provisoires des institutions et des organismes décentralisés conformément à l'article 128 du règlement (CE, Euratom) n° 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes[35] (ci-après dénommé le «règlement financier général»).

4. Au plus tard le 31 mars suivant l'achèvement de l'exercice, le comptable de la Commission transmet les comptes provisoires de l'Agence, accompagnés d'un rapport sur la gestion budgétaire et financière durant l'exercice, à la Cour des comptes. Le rapport sur la gestion budgétaire et financière durant l'exercice est également transmis à l'autorité budgétaire.

5. À la 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. Au plus tard le 1er juillet suivant l'achèvement de l'exercice, le directeur exécutif transmet les comptes définitifs, accompagnés de l'avis du conseil d'administration, au Parlement européen, au Conseil, à la Commission et à la Cour des comptes.

8. Le directeur exécutif publie les comptes définitifs.

---

33 JO L 136 du 31.5.1999, p. 1.
34 JO L 136 du 31.5.1999, p. 15.
35 JO L 248 du 16.9.2002, p. 1.

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 également cette réponse au conseil d'administration.

10. Le directeur exécutif soumet au Parlement européen, à la demande de celui-ci, comme prévu à l'article 146, paragraphe 3, du règlement financier général, toute information nécessaire au bon déroulement de la procédure de décharge pour l'exercice budgétaire en question.

11. Le Parlement européen, statuant sur recommandation du Conseil, 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 22
Statut juridique

1. L'Agence est un organisme de l'Union. 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.

Article 23
Personnel

1. Les règles et réglementations applicables aux fonctionnaires et autres agents de l'Union européenne s'appliquent au personnel de l'Agence, y compris à son directeur exécutif.

2. Le conseil d'administration exerce à l'égard du directeur exécutif les pouvoirs qui sont conférés à l'autorité investie du pouvoir de nomination par le statut et à l'autorité habilitée à conclure les contrats d'engagement par le régime.

3. Le directeur exécutif exerce à l'égard du personnel de l'Agence les pouvoirs qui sont conférés à l'autorité investie du pouvoir de nomination par le statut et à l'autorité habilitée à conclure les contrats d'engagement par le régime.

4. L'Agence peut employer des experts nationaux détachés par les États membres. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application de cette disposition.

Article 24
Privilèges et immunités

Le protocole sur les privilèges et immunités des Communautés européennes s'applique à l'Agence ainsi qu'à son personnel.

Article 25
Responsabilité

1. La responsabilité contractuelle de l'Agence est régie par la législation applicable au contrat en question.

La Cour de justice de l'Union européenne est compétente pour statuer 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 26
Langues

1. Les dispositions du règlement n° 1 du 15 avril 1958 portant fixation du régime linguistique de la Communauté économique européenne[36] s'appliquent à l'Agence. Les États membres et les autres organismes désignés par ceux-ci peuvent s'adresser à l'Agence et en recevoir une réponse dans la langue de l'Union européenne de leur choix.

2. Les travaux de traduction nécessaires au fonctionnement de l'Agence sont effectués par le Centre de traduction des organes de l'Union européenne.

Article 27
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.

Article 28
Participation de pays tiers

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

2. Conformément aux dispositions pertinentes de ces accords, sont élaborés des arrangements précisant en particulier la nature, l'étendue et les modalités de la participation de ces pays aux travaux de l'Agence. Ces arrangements comprennent notamment des dispositions relatives à la participation aux initiatives prises par l'Agence, aux contributions financières et au personnel.

---

[36] JO 17 du 6.10.1958, p. 385/58. Règlement modifié en dernier lieu par l'acte d'adhésion de 1994.

CHAPITRE 6 DISPOSITIONS FINALES

Article 29
Clause de révision

1. Dans les trois ans suivant la date d'institution visée à l'article 34, la Commission, en tenant compte de la position de toutes les parties intéressées, procède à une évaluation sur la base d'un mandat convenu avec le conseil d'administration. Cette évaluation vise à apprécier l'impact et l'efficacité de l'Agence dans la réalisation des objectifs visés à l'article 2, ainsi que l'efficacité des méthodes de travail de l'Agence. La Commission entreprend cette évaluation notamment afin de déterminer si une agence constitue toujours un instrument efficace et si le mandat de l'Agence doit être prolongé au-delà de la période visée à l'article 34.

2. Les conclusions de l'évaluation sont transmises par la Commission au Parlement européen et au Conseil et sont rendues publiques.

3. Le conseil d'administration reçoit cette évaluation et formule des recommandations, qu'il communique à la Commission, concernant la modification du présent règlement, l'Agence et ses méthodes de travail. Le conseil d'administration et le directeur exécutif prennent les résultats de l'évaluation en considération dans la planification pluriannuelle.

Article 30
Coopération de l'État membre d'accueil

L'État membre d'accueil offre les meilleures conditions possibles aux fins du bon fonctionnement de l'Agence.

Article 31
Contrôle administratif

Les activités de l'Agence sont soumises au contrôle du médiateur, conformément à l'article 228 du traité.

Article 32
Abrogation et succession

1. Le règlement (CE) n° 460/2004 est abrogé.

Les références au règlement (CE) n° 460/2004 et à l'ENISA s'entendent comme faites au présent règlement et à l'Agence.

2. L'Agence succède à l'Agence qui a été instituée par le règlement (CE) n° 460/2004 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités.

Article 33
Durée

L'Agence est instituée à partir du […] pour une période de cinq ans.

Article 34
Entrée en vigueur

Le présent règlement entre en vigueur le jour suivant celui de sa publication au Journal officiel de l'Union européenne et il est applicable à partir du 14 mars 2012 ou, en cas de publication postérieure à cette date, à partir du jour suivant la publication.

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

Fait à

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE DES PROPOSITIONS

1. CADRE DE LA PROPOSITION / DE L'INITIATIVE

1.1. Dénomination de la proposition / de l'initiative

Proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

1.2. Domaine(s) politique(s) concerné(s) dans la structure GPA/EBA[37]

Société de l'information et médias.

Cadre réglementaire de la stratégie numérique.

1.3. Nature de la proposition / de l'initiative

☐ La proposition / l'initiative porte sur **une action nouvelle**.

☐ La proposition / l'initiative porte sur **une action nouvelle suite à un projet pilote / une action préparatoire**[38].

☑ La proposition / l'initiative porte sur **la prolongation d'une action existante**.

☐ La proposition / l'initiative porte sur **une action réorientée vers une nouvelle action**.

1.4. Objectifs

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition l'/initiative

Cohérence des approches réglementaires – fournir des indications et des conseils à la Commission et aux États membres pour qu'ils actualisent et élaborent un cadre normatif global dans le domaine de la SRI.

Prévention, détection et intervention – améliorer la préparation en contribuant au développement de moyens en matière d'alerte rapide et d'intervention en cas d'incident, de plans d'urgence et d'exercices paneuropéens.

Développement des connaissances des décideurs – prêter assistance et donner des conseils à la Commission et aux États membres pour qu'ils atteignent un niveau élevé de connaissances, dans l'Union, sur les questions relatives à la SRI et à son application aux entreprises concernées. Cela consiste aussi à produire, analyser et mettre à disposition: données concernant l'économie de la SRI et l'impact des atteintes à la SRI, facteurs incitant les parties

[37] GPA: gestion par activités – EBA: établissement du budget par activités.

[38] Tels que visés à l'article 49, paragraphe 6, point a) ou b), du règlement financier.

prenantes à investir dans des mesures de SRI, identification des risques, indicateurs de la situation de la SRI dans l'Union, etc.

Responsabilisation des parties prenantes – favoriser l'émergence d'une culture de la sécurité et de la gestion des risques en encourageant le partage d'informations et une large coopération entre les acteurs du secteur public et du secteur privé, ainsi que dans l'intérêt direct des citoyens, et développer une culture de la sensibilisation à la SRI.

Protection de l'Europe contre les menaces internationales – atteindre un niveau élevé de coopération avec les pays tiers et les organisations internationales pour promouvoir une approche globale commune de la SRI et encourager des initiatives internationales de haut niveau en Europe.

Vers une mise en œuvre concertée – faciliter la collaboration dans la mise en œuvre des politiques SRI.

Lutte contre la cybercriminalité – intégrer les aspects SRI de la lutte contre la cybercriminalité dans le dialogue et l'échange de bonnes pratiques entre parties prenantes publiques et privées, en particulier par la coopération avec les autorités des (anciens) 2e et 3e piliers, par exemple Europol.

1.4.2. Objectif(s) spécifique(s) et activité(s) GPA/EBA concernée(s)

Objectif spécifique

Accroître la sécurité des réseaux et de l'information (SRI), favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public, et recenser les défis politiques que représentent les réseaux et l'internet futurs.

Activité(s) GPA/EBA concernée(s)

Politique des communications électroniques et sécurité des réseaux.

1.4.3. Résultat(s) et impact(s) attendu(s)

L'initiative est censée produire les effets économiques suivants:

- plus grande disponibilité des informations sur les défis actuels et futurs et sur les risques pour la sécurité et la résilience;

- non-duplication des efforts de chaque État membre pour recueillir des informations pertinentes sur les risques, menaces et faiblesses;

- niveau plus élevé d'information des décideurs lors de la prise de décision;

- meilleure qualité des politiques SRI dans les États membres du fait de la diffusion des meilleures pratiques;

- économies d'échelle en ce qui concerne la réaction aux incidents au niveau de l'UE;

- davantage d'investissements débloqués du fait de l'existence d'objectifs stratégiques communs et de normes de sécurité et de résilience au niveau de l'UE;

- moins de risques de fonctionnement pour les entreprises du fait du niveau plus élevé de sécurité et de résilience;

- plus grande cohérence des mesures de lutte contre la cybercriminalité.

L'initiative est censée produire les effets sociaux suivants:

- plus grande confiance des utilisateurs dans les services et systèmes de la société de l'information;

- plus grande confiance dans le fonctionnement du marché intérieur de l'UE du fait du niveau plus élevé de protection des consommateurs;

- intensification des échanges d'informations et de connaissances avec les pays hors UE;

- meilleure protection des droits fondamentaux dans l'UE du fait de la garantie d'un même niveau de protection des données personnelles et de la vie privée pour tous les Européens.

Les incidences escomptées sur l'environnement sont marginales:

- limitation de l'impact des émissions de CO_2 du fait, par exemple, de la réduction des déplacements résultant de l'utilisation accrue des systèmes et services informatiques, et de la réduction de la consommation d'énergie résultant des économies d'échelle dans la mise en œuvre des obligations de sécurité.

1.4.4. Indicateurs de résultats et d'impacts

Les indicateurs de suivi par objectif sont les suivants:

Cohérence des approches réglementaires:

- Nombre d'États membres ayant appliqué les recommandations de l'Agence dans leur processus d'élaboration de politique.

- Nombre d'études visant à recenser les lacunes et les incohérences dans le paysage normatif en rapport avec la SRI.

- Rapprochement des approches de la SRI des États membres.

Prévention, détection et intervention:

- Nombre de formations organisées sur la sécurité des réseaux.

- Existence d'un système opérationnel d'alerte rapide en cas de risques émergents et d'attaques.

- Nombre d'exercices SRI coordonnés par l'Agence au niveau de l'UE.

Développement des connaissances des décideurs:

- Nombre d'études visant à recueillir des informations sur les risques SRI actuels et prévisibles et sur les technologies de prévention des risques.

- Nombre de consultations des organismes publics chargés de la SRI.

- Existence d'un cadre européen pour l'organisation de la collecte de données sur la SRI.

Responsabilisation des parties prenantes:

- Nombre de bonnes pratiques établies pour les entreprises.

- Importance de l'investissement des parties prenantes privées dans des mesures de sécurité.

Protection de l'Europe contre les menaces internationales:

- Nombre de conférences/réunions entre les États membres de l'UE pour convenir en commun d'objectifs SRI.

- Nombre de réunions entre experts de la SRI européens et internationaux.

Vers une mise en œuvre concertée:

- Nombre d'évaluations de la conformité à la réglementation.

- Nombre de pratiques SRI à l'échelle de l'UE.

Lutte contre la cybercriminalité:

- Régularité des interactions avec les agences des anciens 2e et 3e piliers.

- Nombre d'affaires dans lesquelles une expertise a été fournie en matière d'enquête criminelle.

1.5. Justification(s) de la proposition / de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

L'ENISA a été créée à l'origine en 2004 afin de faire face aux menaces pour la SRI et aux atteintes à la SRI pouvant en découler. Depuis lors, les défis concernant la sécurité des réseaux et de l'information ont changé en fonction des évolutions technologiques et commerciales et ont fait l'objet de réflexions et de débats approfondis, ce qui implique aujourd'hui d'actualiser et de décrire plus en détail les problèmes précis qui se posent et la façon dont ils sont impactés par les changements dans le paysage SRI.

1.5.2. Valeur ajoutée de l'intervention de l'UE

Les problèmes de SRI ne s'arrêtent pas aux frontières nationales et ne peuvent donc pas être réglés efficacement au seul niveau national. En même temps, les façons dont le problème est traité par les pouvoirs publics des différents États membres sont très diverses. Ces différences constituent un obstacle de taille à l'instauration de mécanismes appropriés, à l'échelle de l'Union, pour une SRI accrue en Europe. Comme les infrastructures TIC sont par nature interconnectées, l'efficacité des mesures prises au niveau national dans un État membre est

toujours fortement affectée par l'ampleur plus limitée des mesures dans les autres États membres et par le manque de coopération transnationale systématique. Si l'insuffisance des mesures de SRI provoque un incident dans un État membre, elle peut aussi entraîner des perturbations dans d'autres États membres.

De plus, la multiplication des exigences de sécurité implique un coût pour les entreprises opérant au niveau de l'Union européenne et entraîne un morcellement et un manque de compétitivité sur le marché intérieur européen.

Compte tenu de la dépendance croissante vis-à-vis des réseaux et systèmes informatiques, la préparation pour faire face aux incidents s'avère insuffisante.

Les systèmes nationaux actuels d'alerte rapide et d'intervention en cas d'incident ont des défauts importants. Les processus et les pratiques en matière de surveillance et de notification des incidents dans le domaine de la sécurité des réseaux varient considérablement selon les États membres. Dans certains pays, les processus ne sont pas formalisés tandis que, dans d'autres, il n'y a pas d'autorité compétente pour recevoir et traiter les rapports d'incident. En fait, il n'existe pas de systèmes européens. Par conséquent, un incident SRI pourrait perturber complètement les systèmes permettant de répondre aux besoins de base et il convient d'anticiper les réactions appropriées. Dans sa communication sur la PIIC, la Commission a également souligné la nécessité de moyens européens en matière d'alerte rapide et d'intervention en cas d'incident, éventuellement étayés par des exercices à l'échelle européenne.

Le besoin se fait nettement sentir de disposer d'instruments politiques destinés à recenser, de façon proactive, les risques et faiblesses SRI, d'instaurer les mécanismes d'intervention appropriés (par exemple, en recensant et en diffusant de bonnes pratiques), et de faire en sorte que ces mécanismes soient connus et appliqués par les parties prenantes.

1.5.3. Principales leçons tirées d'expériences similaires

Voir les points 1.5.1 et 1.5.2.

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments financiers

Cette initiative est en totale conformité avec le débat général sur la SRI et d'autres initiatives politiques axées sur l'avenir de la SRI. C'est l'un des principaux éléments de la stratégie numérique pour l'Europe, laquelle constitue une initiative phare de la stratégie Europe 2020.

1.6. Durée de l'action et de son impact financier

☑ Proposition/initiative à **durée limitée**

– ☑ Le point de départ de la prolongation de 5 ans sera le 14.3.2012 ou le jour où le nouveau règlement entrera en vigueur si cela tombe plus tard.

– ☑ Impact financier de 2012 à 2017.

☐ Proposition/initiative à **durée illimitée**

– Mise en œuvre avec une période de démarrage de AAAA à AAAA,

– suivie d'un fonctionnement à plein rendement.

1.7. Mode(s) de gestion prévu(s)[39]

☐ **Gestion centralisée directe** par la Commission.

☑ **Gestion centralisée indirecte** par délégation de tâches d'exécution à:

– ☐ des agences exécutives

– ☑ des organismes créés par les Communautés[40]

– ☐ des organismes publics nationaux/organismes avec mission de service public

– ☐ des personnes chargées de l'exécution d'actions spécifiques en vertu du titre V du traité sur l'Union Européenne, identifiées dans l'acte de base concerné au sens de l'article 49 du Règlement financier.

☐ **Gestion partagée** avec des États membres.

☐ **Gestion décentralisée** avec des pays tiers.

☐ **Gestion conjointe** avec des organisations internationales ***(à préciser)***.

---

[39] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

[40] Tels que visés à l'article 185 du règlement financier.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Le directeur exécutif est responsable du contrôle effectif et de l'évaluation des performances de l'Agence par rapport à ses objectifs, et rend compte de son activité chaque année au conseil d'administration.

Le directeur exécutif rédige un rapport général couvrant toutes les activités de l'Agence au cours de l'année précédente, qui compare notamment les résultats obtenus avec les objectifs du programme de travail annuel. Une fois adopté par le conseil d'administration, ce rapport est transmis au Parlement européen, au Conseil, à la Commission, à la Cour des comptes, au Comité économique et social européen ainsi qu'au Comité des régions, et est publié.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Depuis la création de l'ENISA en 2004, celle-ci a fait l'objet d'évaluations externes et internes.

Conformément à l'article 25 du règlement instituant l'ENISA, la première étape de ce processus a été une évaluation indépendante de l'ENISA réalisée par un groupe d'experts externes en 2006/2007. Le rapport[41] qu'il a établi a confirmé la validité du raisonnement politique à la base de la création de l'ENISA et des objectifs initiaux, et a largement contribué à soulever certaines des questions qui doivent être traitées.

En mars 2007, la Commission a présenté son rapport sur l'évaluation au conseil d'administration qui a ensuite formulé ses propres recommandations sur l'avenir de l'Agence et sur les modifications à apporter au règlement ENISA[42].

En juin 2007, la Commission a soumis sa propre appréciation des résultats de l'évaluation externe et des recommandations du conseil d'administration dans le cadre d'une communication au Parlement européen et au Conseil[43]. La Commission y expose le choix à faire entre la prolongation du mandat de l'Agence et le remplacement de celle-ci par un autre mécanisme tel qu'une assemblée permanente des parties prenantes ou un réseau d'organisations travaillant dans le domaine de la sécurité des réseaux. La Commission a aussi lancé une consultation publique sur ce sujet, en sollicitant les suggestions et réactions des parties prenantes européennes par une liste de questions visant à orienter les débats ultérieurs[44].

---

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm

42 Conformément à l'article 25 du règlement ENISA. L'intégralité du document adopté par le conseil d'administration de l'ENISA, qui contient aussi les réflexions du conseil, est disponible sur le site web suivant: http://enisa.europa.eu/pages/03_02.htm

43 Communication de la Commission au Parlement européen et au Conseil sur l'évaluation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), COM(2007) 285 final du 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:FR:NOT

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en

2.2.2. Moyen(s) de contrôle prévu(s)

Voir le point 2.1 et le point 2.2.1 ci-dessus.

2.3. Mesures de prévention des fraudes et irrégularités

Le contrôle du paiement de tout service ou étude nécessaire est effectué par le personnel 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 antifraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION / DE L'INITIATIVE*

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses impactées

- Lignes budgétaires existantes

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro / Description	CD/CND[45]	de pays AELE[46]	de pays candidats[47]	de pays tiers	au sens de l'article 18, paragraphe 1, point a) *bis*, du règlement financier
1.a Compétitivité pour la croissance et l'emploi	09 02 03 01 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention aux titres 1 et 2	CD	OUI	NON	NON	NON
	09 02 03 02 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention au titre 3	CD	OUI	NON	NON	NON
5 Dépenses administratives	09 01 01 Dépenses liées au personnel en activité du domaine politique «Société de l'information et médias»	CND	NON	NON	NON	NON
	09 01 02 11 Autres dépenses de gestion	CND	NON	NON	NON	NON

* L'incidence financière estimée de la proposition pour la période au-delà de la période de programmation financière actuelle (2007-2013) n'est pas couverte par la présente fiche financière législative. Sur la base de la proposition de la Commission concernant le règlement fixant le cadre financier pluriannuel au-delà de 2013 et compte tenu des conclusions de l'analyse d'impact, la Commission présentera une fiche financière législative modifiée.

45 CD = crédits dissociés / CND = crédits non dissociés.

46 AELE: Association européenne de libre-échange.

47 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Impact estimé sur les dépenses

3.2.1. Synthèse de l'impact estimé sur les dépenses

Millions d'euros (à la 3e décimale)

Rubrique du cadre financier pluriannuel:	1.a	Compétitivité pour la croissance et l'emploi

ENISA			1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	**TOTAL 14 mars 2012 – 13 mars 2017**
Crédits d'exploitation										
09 02 03 02 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention au titre 3	Engagements	(1)	0,454	1,976	2,470	--	--	--	--	--
	Paiements	(2)	0,454	1,976	2,470	--	--	--	--	--
Crédits administratifs										
09 02 03 01 Agence européenne chargée de la sécurité des réseaux et de l'information – Subvention aux titres 1 et 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTAL des crédits sous la RUBRIQUE 1.a	Engagements	=1+3	1,747	6,673	8,590	--	--	--	--	--
	Paiements	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTAL des crédits	Engagements	(4)	0,454	1,976	2,470	--	--	--	--	--

d'exploitation	Paiements	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTAL des crédits de nature administrative financés par l'enveloppe des programmes spécifiques		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTAL des crédits sous la RUBRIQUE 1.a du programme-cadre pluriannuel	Engagements	=4+ 6	1,747	6,673	8,590	--	--	--	--	--
	Paiements	=5+ 6	1,747	6,673	8,590	--	--	--	--	--

Millions d'euros (à la 3e décimale)

Rubrique du cadre financier pluriannuel:	5	Dépenses administratives

		1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	Total
Ressources humaines		0,085	0,342	0,427	--	--	--	--	--
Autres dépenses administratives		0,002	0,013	0,015	--	--	--	--	--
TOTAL DG INFSO	Crédits	0,087	0,355	0,442	--	--	--	--	--

TOTAL des crédits sous la RUBRIQUE 5 du cadre financier pluriannuel	(Total des engagements = total des paiements)	0,087	0,355	0,442	--	--	--	--	--

		1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	Total
TOTAL des crédits sous les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements	1,834	7,028	9,032	--	--	--	--	--
	Paiement	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Impact estimé sur les crédits opérationnels

– ☐ La proposition / l'initiative n'implique pas l'utilisation de crédits opérationnels.

– ☑ La proposition / l'initiative implique l'utilisation de crédits opérationnels, comme expliqué ci-après:

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

Indiquer les objectifs et résultats ⇩	1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	**TOTAL 14 mars 2012 – 13 mars 2017**
Cohérence des approches réglementaires	0,114	0,494	0,620	--	--	--	--	--
Prévention, détection et intervention	0,114	0,494	0,620	--	--	--	--	--
Développement des connaissances des décideurs	0,068	0,297	0,370	--	--	--	--	--
Responsabilisation des parties prenantes	0,050	0,218	0,270	--	--	--	--	--
Protection de l'Europe contre les menaces internationales	0,023	0,099	0,120	--	--	--	--	--
Vers une mise en œuvre concertée	0,064	0,276	0,340	--	--	--	--	--
Lutte contre la cybercriminalité	0,023	0,098	0,120	--	--	--	--	--
COÛT TOTAL	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Impact estimé sur les crédits de nature administrative[48]

3.2.3.1. Résumé

– ☐ La proposition / l'initiative n'implique pas l'utilisation de crédits de nature administrative.

– ☑ La proposition / l'initiative implique l'utilisation de crédits de nature administrative, comme expliqué ci-après:

a) Dépenses administratives sous la rubrique 5 du cadre financier pluriannuel

Millions d'euros (à la 3e décimale)

RUBRIQUE 5 du cadre financier pluriannuel	1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	**TOTAL 14 mars 2012 – 13 mars 2017**
Ressources humaines	0,085	0,342	0,427	--	--	--	--	--
Autres dépenses administratives	0,002	0,013	0,015	--	--	--	--	--
TOTAL	0,087	0,355	0,442	--	--	--	--	--

b) Dépenses administratives relatives à l'ENISA – couvertes par la ligne budgétaire «09.020301 Agence européenne chargée de la sécurité des réseaux et de l'information: Titre 1 – Personnel et Titre 2 – Fonctionnement de l'Agence».

Millions d'euros (à la 3e décimale)

	1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	**TOTAL 14 mars 2012 – 13 mars 2017**
Ressources humaines – Titre 1 – Personnel	1,153	4,329	5,607	--	--	--	--	--
Autres dépenses de nature administrative – Titre 2 – Fonctionnement de l'Agence	0,140	0,368	0,513	--	--	--	--	--

[48] L'annexe de la fiche financière législative n'est pas remplie car elle ne s'applique pas à la présente proposition.

TOTAL	**1,293**	**4,697**	**6,120**	--	--	--	--	--

3.2.3.2. Besoins estimés en ressources humaines

Chaque année, le tableau des effectifs de l'Agence est expliqué et justifié dans un document appelé «plan en matière de politique du personnel» qui est soumis à l'autorité budgétaire.

– ☐ La proposition / l'initiative n'implique pas l'utilisation de ressources humaines.

– ☑ La proposition / l'initiative implique l'utilisation de ressources humaines, comme expliqué ci-après:

a) Ressources humaines au sein de la Commission

	1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017
Emplois du tableau des effectifs (postes de fonctionnaires et d'agents temporaires)							
XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission)	3,5	3,5	3,5	--	--	--	--
TOTAL	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Ressources humaines de l'ENISA

		1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017
Tableau des effectifs de l'ENISA (en équivalent temps plein - ETP)								
Fonctionnaires ou agents temporaires	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTAL des fonctionnaires ou agents temporaires		44	47	47	--	--	--	--
Autre personnel (en ETP)								
Agents contractuels		13	14	14	--	--	--	--
Experts nationaux détachés (END)		5	5	5	--	--	--	--
Total des autres personnels		18	19	19	--	--	--	--
TOTAL		**62**	**66**	**66**	--	--	--	--

Description des tâches devant être exécutées par le personnel de l'Agence:

Fonctionnaires et agents temporaires	L'Agence continuera à: – avoir une fonction consultative et de coordination, dans le cadre de laquelle elle **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 l'Union sur la sécurité des réseaux et de l'information; – **faire office** de **centre d'expertise** auprès duquel les États membres comme les institutions européennes pourront demander **des avis et des conseils sur des questions techniques** liées à la sécurité; – contribuer 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; – contribuer 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; – assurer l'**interopérabilité des réseaux et systèmes d'information** lorsque les États membres **appliquent** des exigences techniques qui ont une incidence sur la sécurité; – recenser les besoins **pertinents en matière de normalisation**, évaluer les normes de sécurité et systèmes de certification existants et œuvrer pour que leur utilisation par les États membres soit la plus large possible afin de soutenir l'application de la législation européenne; – favoriser, 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.
Personnel externe	Voir ci-dessus.

3.2.4. Compatibilité avec la programmation financière existante

– ☑ La proposition / l'initiative est compatible avec la programmation financière existante.

– ☐ La proposition / l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

– ☐ La proposition / l'initiative nécessite le recours à l'instrument de flexibilité ou à la révision du cadre financier pluriannuel[49].

Le financement de l'UE au-delà de 2013 sera examiné dans le contexte d'un débat au sein de la Commission sur toutes les propositions pour la période après 2013. Cela signifie que, une fois que la Commission aura fait sa proposition concernant le prochain cadre financier pluriannuel, la Commission présentera une fiche financière législative modifiée tenant compte des conclusions de l'analyse d'impact.

3.2.5. Participation de tiers au financement

– ☐ La proposition / l'initiative ne prévoit pas de cofinancement par des tiers.

– ☑ La proposition prévoit un cofinancement par des tiers estimé ci-après:

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

	1er janv.-13 mars 2012	14 mars-31 déc. 2012	2013	2014	2015	2016	1er janv.-13 mars 2017	**TOTAL 14 mars 2012 – 13 mars 2017**
AELE	0,042	0,160	0,206	--	--	--	--	--

3.3. Incidence estimée sur les recettes

– ☑ La proposition / l'initiative n'a pas d'incidence financière sur les recettes.

– ☐ La proposition / l'initiative a l'incidence financière suivante:

  – ☐ sur ses ressource propres

  – ☐ sur les recettes diverses.

[49] Voir les points 19 et 24 de l'accord interinstitutionnel.