COMMISSION EUROPÉENNE

Bruxelles, le 30.9.2010
SEC(2010) 1127

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

Document accompagnant la

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

{COM(2010) 521final}
{SEC(2010) 1126}

RÉSUMÉ DE L'ANALYSE D'IMPACT

1. CHAMP D'APPLICATION ET CONTEXTE

1.1. Champ d'application

La présente analyse d'impact vise à déterminer comment une agence chargée de la sécurité des réseaux et de l'information (SRI) modernisée, qui est largement reconnue comme étant un instrument politique approprié et nécessaire pour relever les défis SRI, devrait être structurée au mieux pour aider les organismes des États membres et la Commission à atteindre les objectifs stratégiques en matière de SRI lorsque le mandat de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) expirera en mars 2012.

1.2. Contexte

Dans le monde d'aujourd'hui, les activités sociales et économiques sont largement conditionnées par le bon fonctionnement des technologies de l'information et des communications (TIC). Il est donc extrêmement important de veiller à ce que les systèmes TIC soient stables et à ce que les utilisateurs leur fassent confiance. La multiplication des menaces, attaques et maliciels visant ces systèmes pourrait compromettre le bon fonctionnement des réseaux et infrastructures d'information de base. Étant donné que ces systèmes et réseaux sont transnationaux, une réponse européenne au défi de la SRI s'impose.

Pour traiter ces questions, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été instituée en mars 2004[1], pour une durée 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*».

Depuis lors, les défis SRI n'ont cessé de changer en fonction des évolutions technologiques et commerciales. Aussi, bien avant l'expiration du règlement ENISA en mars 2009, la Commission a-t-elle engagé un processus pour déterminer avec les parties intéressées quelles propositions politiques contribueraient le mieux à la réalisation des objectifs SRI de l'UE à partir de 2009. Après une évaluation à mi-parcours[2] de l'ENISA et une consultation publique[3] en 2007, le Conseil et le Parlement européen ont adopté, le 24 septembre 2008, un règlement[4] prolongeant de trois ans, jusqu'au 13 mars 2012, le mandat de l'ENISA dans sa forme initiale. Dans les considérants de ce règlement, le Conseil et le Parlement européen préconisaient de

---

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.

2 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 du 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:FR:NOT

3 La consultation publique s'est déroulée du 13 juin au 7 septembre 2007.

4 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.

«***poursuivre les discussions concernant l'Agence [et] l'orientation générale que doivent suivre les efforts européens visant à accroître la sécurité des réseaux et de l'information***».

La Commission a contribué à la discussion en lançant, en novembre 2008, une autre consultation publique à l'échelle de l'UE sur les objectifs possibles d'une politique SRI renforcée et sur les moyens d'atteindre ces objectifs[5]. La Commission a également organisé, en décembre 2008, un atelier avec des experts en SRI des organismes compétents des États membres sur les instruments et mécanismes d'une politique SRI renforcée dans l'UE. De plus, en mars 2009, la Commission a adopté une communication relative à la protection des infrastructures d'information critiques[6] (PIIC) qui donne à l'ENISA un rôle clé consistant à aider l'UE à améliorer la sécurité, la résilience et la préparation. Cette approche a été approuvée par la conférence ministérielle sur la PIIC qui s'est tenue à Tallinn les 27 et 28 avril 2009 et dont l'une des conclusions était que «***les nouveaux défis auxquels nous serons confrontés durant de nombreuses années exigent que le mandat de l'Agence soit profondément repensé et reformulé 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 européennes, et de soutenir l'efficacité opérationnelle de l'Agence ainsi que son impact général. C'est de cette façon que l'ENISA pourra devenir un atout permanent pour chaque État membre et l'Union européenne dans son ensemble*».

Le 18 décembre 2009, le Conseil a adopté une résolution sur «*une approche concertée en matière de sécurité des réseaux et de l'information*»[7], qui soulignait notamment que «***l'ENISA, dans le cadre d'un mandat révisé, devrait servir de centre d'expertise de l'UE pour les questions de sécurité des réseaux et de l'information liées à l'UE***».

Dans la communication de la Commission *Europe 2020 Une stratégie pour une croissance intelligente, durable et inclusive*[8], l'une des initiatives phare visant à promouvoir Europe 2020 est la stratégie numérique pour l'Europe dans laquelle la SRI joue un rôle central. **L'objectif de cette initiative politique en faveur de la confiance et de la sécurité dans la stratégie numérique pour l'Europe est de permettre à l'UE, aux États membres et aux parties prenantes de développer leurs moyens et d'atteindre un degré élevé de préparation pour prévenir et détecter les problèmes SRI et mieux y répondre.** Cela contribuera à renforcer la confiance et la sécurité dans le marché unique numérique en Europe et à accroître la compétitivité des entreprises européennes.

2. DEFINITION DU PROBLEME

2.1. Quel est le problème?

Ont été recensés les facteurs de problème suivants qui exposent les parties prenantes à des menaces et incidents SRI. Tous démontrent qu'il est nécessaire de disposer, au niveau de l'UE, d'une structure fiable pour traiter le problème et s'adapter, dans toute l'Europe, à l'évolution constante de l'environnement technologique et commercial de la SRI.

---

5 Du 7 novembre 2008 au 9 janvier 2009, rapport disponible à l'adresse: http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm

6 Communication de la Commission au Parlement européen et au Conseil relative à la protection des infrastructures d'information critiques, COM(2009) 149 du 30.3.2009.

7 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).

8 COM(2010) 2020.

- **La diversité et le caractère fragmentaire des approches nationales.** Les problèmes de SRI ne se limitent pas aux frontières nationales et ne peuvent donc pas être réglés efficacement au seul niveau national. De plus, le problème est traité par les pouvoirs publics de façon très différente d'un État membre à l'autre. Les multiples exigences de sécurité en vigueur dans les différents États membres impliquent un coût pour les entreprises opérant à l'échelle de l'UE et entraînent un morcellement et un manque de compétitivité sur le marché intérieur européen.

- **Les moyens limités de l'Europe en matière d'alerte rapide et d'intervention.** Les systèmes nationaux actuels d'alerte rapide et de gestion des incidents diffèrent considérablement d'un État membre à l'autre et il n'existe aucun système à l'échelle de l'UE. Il y a un besoin d'instruments politiques, au niveau de l'Union, qui permettent de recenser les risques et les faiblesses en matière de SRI, d'instaurer des mécanismes d'intervention appropriés et de faire en sorte que ces mécanismes soient connus et appliqués par les parties prenantes.

- **Un manque de données fiables et une connaissance limitée des problèmes évolutifs.** Il y a très peu d'informations quantitatives disponibles et fiables sur l'impact ou sur la survenance des incidents SRI. Aussi est-il difficile, pour les décideurs, d'arrêter les mesures politiques adéquates et, pour les entreprises, de prendre des décisions concernant l'investissement dans la sécurité.

- **Le faible niveau de sensibilisation aux risques et défis SRI.** La responsabilité d'assurer la SRI incombe aux parties prenantes à titre individuel, mais cette responsabilité n'est pas toujours clairement définie ni communiquée. D'une part, les utilisateurs sous-estiment souvent les risques SRI et ignorent quelle est leur part de responsabilité dans la sécurisation de leurs systèmes TIC. D'autre part, les entreprises voient surtout, en général, les coûts induits par la SRI et non les économies qu'elle peut permettre de réaliser.

- **La dimension internationale des problèmes de sécurité des réseaux et de l'information.** Les menaces pour la SRI, et les incidents qu'elles peuvent provoquer, ont une dimension internationale par nature. Aussi les actions de l'UE risquent-elles d'être peu efficaces si les problèmes SRI ne sont pas convenablement traités au niveau international aussi. Nous devons élaborer une stratégie et définir un point de référence européens en matière de SRI pour assurer la position de l'UE sur la scène internationale.

- **Le besoin de modèles de coopération pour assurer une mise en œuvre appropriée des politiques.** La mise en œuvre appropriée des politiques SRI exige des modèles de collaboration au niveau de l'UE. Les parties prenantes ont besoin d'indications pour identifier les menaces SRI et élaborer de bonnes pratiques de mise en œuvre des politiques SRI existantes.

- **Le besoin de lutter plus efficacement contre la cybercriminalité.** Les efforts en matière de SRI ont principalement été déployés au titre de l'ancien premier pilier, c'est-à-dire des questions débattues entre les institutions. Toutefois, avec l'entrée en vigueur du traité de Lisbonne, il est nécessaire de prendre en considération, pour une agence SRI, un ensemble plus complet de tâches couvrant aussi des domaines relevant des deuxième et troisième piliers, c'est-à-dire des questions qui étaient auparavant tranchées par le seul Conseil.

2.2. Qui est le plus affecté par le problème?

Les incidents SRI pourraient avoir des conséquences très importantes pour diverses parties prenantes, parmi lesquelles les grandes et petites entreprises, les pouvoirs et administrations publics et les particuliers. En d'autres termes, toute le monde est concerné par la SRI et en est responsable.

Il y a peu ou pas d'informations quantitatives disponibles et objectives sur le nombre exact d'incidents SRI ou sur leurs impacts économiques respectifs. Une indication est fournie par l'étude de marché IDC EMEA[9] qui a révélé que 28 % des ménages de l'UE-27 ont connu des problèmes de pollupostage ou de virus au cours des 12 derniers mois. En moyenne, environ 7 % des utilisateurs en entreprise ont fait l'expérience d'un incident de sécurité l'année dernière.

3. JUSTIFICATION DE L'ACTION DE L'UE, VALEUR AJOUTEE ET SUBSIDIARITE

Du fait de l'interdépendance des réseaux et systèmes d'information, il est extrêmement difficile, voire impossible, pour les acteurs individuels d'évaluer correctement l'impact économique et sociétal global de leurs mesures de protection contre les incidents SRI. La diversité des politiques et pratiques nationales influe sur le marché intérieur en raison des effets négatifs induits par les incidents SRI (toute politique inappropriée dans un État membre a des conséquences sur les marchés des autres États membres) et des effets positifs induits par les bonnes pratiques SRI (toute bonne pratique dans un État membre améliore la SRI dans son ensemble et procure donc un bienfait social patent). Par conséquent, l'action politique de l'UE se justifie car elle procurerait une véritable valeur ajoutée au fonctionnement du marché intérieur. Cette valeur ajoutée a également été reconnue dans le règlement (CE) n° 460/2004 instituant l'ENISA, lequel prévoit que les compétences de l'Agence doivent contribuer au bon fonctionnement du marché intérieur.

En outre, l'action de l'UE en matière de politique SRI se justifie par le *principe de subsidiarité*. Comme indiqué dans la communication sur la PIIC, une stratégie européenne de stricte non-intervention de l'UE dans les politiques SRI nationales revient à demander à chaque État membre de ne surveiller que son pré carré en faisant fi de l'interdépendance des systèmes d'information. Une certaine coordination entre les États membres, pour faire en sorte de gérer correctement les conséquences transnationales des risques SRI, est donc conforme au principe de subsidiarité. En outre, l'action de l'UE accroîtrait l'efficacité des politiques nationales existantes.

Les Européens confient de plus en plus leurs données à des systèmes informatiques complexes (informatique en nuage par exemple). Une action politique SRI concertée peut donc avoir un fort impact positif sur la *protection* effective *des droits fondamentaux* et, en particulier, sur le droit à la *protection des données personnelles et de la vie privée*. C'est aussi pourquoi une nouvelle action politique de l'UE semble amplement justifiée.

---

[9] IDC EMEA, *The European Network and Information Security Market, Scenario, Trends and Challenges*, avril 2009, avec référence à l'enquête Eurobaromètre sur les communications électroniques, avril 2007.

4. OBJECTIFS STRATEGIQUES

La présente analyse d'impact consiste à déterminer dans quelle mesure une agence SRI modernisée, qui est largement reconnue comme étant la structure organisationnelle la plus appropriée, devrait être conçue au mieux pour contribuer, avec d'autres instruments de l'Union, à la réalisation des objectifs stratégiques.

L'objectif général est de permettre à l'UE, aux États membres et aux parties prenantes de développer leurs moyens et d'atteindre un degré élevé de préparation pour prévenir et détecter les problèmes SRI et mieux y répondre. Cela contribuera à renforcer la confiance et la sécurité dans le marché unique numérique en Europe et à accroître la compétitivité des entreprises européennes.

Cet objectif général se décompose en sept **objectifs spécifiques**:

(1) **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.

(2) **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.

(3) **Soutien à l'élaboration des politiques** – prêter assistance et donner des conseils à la Commission et aux États membres.

(4) **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 des PME, et développer une culture de la sensibilisation à la SRI.

(5) **Faire de l'Europe un acteur viable sur la scène internationale** – 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.

(6) **Mise en œuvre concertée** – faciliter la collaboration dans la mise en œuvre des politiques SRI.

(7) **Lutte contre la cybercriminalité** – trouver un moyen efficace d'intégrer les aspects SRI de la cybercriminalité par la coopération avec les autorités des (anciens) 2e et 3e piliers, par exemple Europol.

5. TYPES D'ORGANISATION POSSIBLES ET OPTIONS STRATEGIQUES

Pour mettre en œuvre les options stratégiques ci-dessus, sont examinés dans l'analyse d'impact (chapitre 4 et annexe 4) plusieurs types d'organisation possibles, parmi lesquels: (i) une agence, (ii) un partenariat public-privé plus ou moins officialisé, (iii) un réseau de contact informel, (iv) un réseau permanent d'organismes compétents, et (v) une intégration complète dans un service de la Commission.

Après comparaison de ces différents types d'organisation, l'agence semble la mieux adaptée comme instrument politique du fait des avantages qu'elle présente concernant: (1) la sécurité

juridique de la structure organisationnelle ainsi que relativement au contenu, (2) l'adéquation aux problèmes spécifiques d'un secteur aussi sensible que la SRI (organe regroupant des experts externes, coordination des relations avec les parties prenantes, participation/engagement des États membres) et (3) l'acceptation et la réputation de l'ENISA dans la communauté SRI.

Aussi les options stratégiques suivantes ont-elles été élaborées et évaluées en détail pour le type d'organisation en agence.

Option stratégique 1: aucune politique

L'option «Aucune politique» repose sur l'hypothèse que l'ENISA cesserait d'exister après mars 2012 et qu'aucune autre institution de l'UE ne reprendrait, en totalité ou en partie, les activités actuelles de l'ENISA.

Fermer l'ENISA signifierait que tous les investissements réalisés jusqu'à maintenant, par exemple pour mettre sur pied une organisation capable d'attirer un personnel hautement spécialisé, acquérir de l'expérience et créer des réseaux avec et entre les parties prenantes et les institutions internationales, seraient supprimés à un moment où l'Agence actuelle a atteint sa vitesse de croisière.

Le caractère complexe du problème SRI en Europe exige de disposer d'une agence modernisée et renforcée, non de fermer celle qui existe. Cela est confirmé par le rôle explicitement confié à l'ENISA, par exemple dans le cadre réglementaire révisé pour les communications électroniques[10], et par le soutien général, exprimé par les parties prenantes, en faveur d'un rôle plus important d'une agence européenne dans le domaine de la SRI.

Option stratégique 2: statu quo

L'option 2 correspond au scénario consistant à maintenir l'instrument politique existant, sous une forme inchangée et avec les mêmes ressources. Les parties prenantes s'accordent généralement à reconnaître que l'ENISA est devenue un point de référence crédible pour les questions de SRI et s'est imposée comme centre d'excellence dans son domaine.

Étant donné les restrictions de personnel et budgétaires actuelles, l'Agence ne pourra avoir d'impact que sur un nombre très limité de questions SRI. Toutefois, cela contraste avec les attentes globales des parties prenantes. Ne pas donner à l'Agence la possibilité d'évoluer encore et de répondre à ces attentes pourrait, à terme, entamer sa crédibilité.

Option stratégique 3: étendre les fonctions actuelles 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

Selon cette option, le rôle d'une agence SRI serait étendu et consisterait surtout à:

- mettre en place et maintenir en activité un réseau de liaison entre parties prenantes et un réseau de connaissances;
- 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

[10] Voir http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:FR:HTML

signature électronique, l'identification électronique et les normes d'acquisition en matière de SRI);

- soutenir la politique de l'UE en matière de PIIC et de résilience (exercices, EP3R[11], Système européen de partage d'information et d'alerte, etc.);
- établir un cadre de l'UE 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 et en rendre compte;
- 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 aux aspects SRI du maintien de l'ordre et de la coopération judiciaire.

L'Agence disposerait de toutes les ressources nécessaires pour exercer ses activités de façon pleinement satisfaisante, c'est-à-dire en produisant un impact réel. Avec davantage de ressources disponibles, l'ENISA pourrait assumer un rôle beaucoup plus proactif et prendre plus d'initiatives pour encourager la participation active des parties prenantes. En outre, cette nouvelle situation offrirait une plus grande souplesse pour réagir rapidement aux changements dans l'environnement SRI en constante évolution.

Option stratégique 4: ajouter des fonctions opérationnelles consistant à contrer les cyberattaques et à réagir aux incidents informatiques

En plus des activités exposées au titre de l'option 3, l'Agence aurait des fonctions opérationnelles comme assumer un rôle plus actif dans la PIIC de l'UE, par exemple en matière de prévention et d'intervention en cas d'incident, à savoir agir en tant qu'équipe d'intervention en cas d'urgence informatique (CERT) SRI de l'UE et coordonner les CERT nationales en tant que centre de crise SRI de l'UE, ainsi que des activités de gestion quotidienne et des services d'urgence.

Cette option impliquerait une augmentation significative du budget et des ressources humaines de l'Agence, ce qui pose des problèmes de capacité d'absorption et d'utilisation efficace du budget par rapport aux bénéfices escomptés.

Option stratégique 5: ajouter des fonctions opérationnelles consistant à prêter assistance aux autorités de police et judiciaires dans leur lutte contre la cybercriminalité

Cette option conférerait à l'Agence, en plus des activités énumérées au titre de l'option 4, des fonctions consistant à:

- fournir une assistance en matière de droit procédural (cf. convention sur la cybercriminalité): par exemple, collecte de données sur le trafic, interception de données sur le contenu, contrôle des flux en cas d'attaque par déni de service;
- être un centre d'expertise pour les enquêtes criminelles présentant des aspects SRI.

Comme l'option 4, celle-ci impliquerait une augmentation significative des ressources de l'Agence et poserait des problèmes de capacité d'absorption et d'utilisation efficace du budget.

[11] Partenariat public-privé européen pour la résilience, voir COM(2009) 149.

6. COMPARAISON DES OPTIONS STRATEGIQUES ET ANALYSE DES IMPACTS

L'analyse des possibles impacts économiques, sociaux et environnementaux révèle que l'***option 1*** produirait des effets négatifs à tous égards et que la situation empirerait.

L'***option 2*** s'avère imparfaite car l'Agence ne disposerait pas des ressources nécessaires pour relever convenablement les défis dans un paysage SRI en constante évolution, ce qui pourrait nuire à sa réputation et, à terme, entamer sa crédibilité.

Au titre de l'***option 3***, une agence SRI modernisée contribuerait à:

rapprocher les approches nationales (facteur de problème 1), développer l'élaboration de politiques et la prise de décisions basées sur des données, des connaissances et des informations (facteur de problème 3), sensibiliser davantage aux risques et défis SRI (facteur de problème 4) et y faire face en:

- permettant à chaque État membre de recueillir plus efficacement des informations pertinentes sur les risques, menaces et faiblesses;
- mettant à disposition davantage d'informations sur les défis et risques SRI actuels et futurs;
- permettant aux États membres d'adopter une politique SRI de plus haute qualité;

développer les moyens de l'Europe en matière d'alerte rapide et d'intervention (facteur de problème 2) en:

- aidant la Commission et les États membres à instaurer des exercices paneuropéens et réalisant ainsi des économies d'échelle en ce qui concerne la réaction aux incidents au niveau de l'UE;
- facilitant le fonctionnement de l'EP3R, ce qui pourrait, à terme, entraîner le déblocage d'un volume plus important d'investissements du fait de l'existence d'objectifs stratégiques communs et de normes de sécurité et de résilience à l'échelle de l'UE;

promouvoir une approche globale commune de la SRI (facteur de problème 5) en:

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

lutter plus efficacement contre la cybercriminalité (facteur de problème 7) en:

- participant à des tâches non opérationnelles liées aux aspects SRI du maintien de l'ordre et de la coopération judiciaire, comme l'échange bidirectionnel d'informations et la formation (en coopération avec le Collège européen de police – CEPOL).

L'***option 4*** produirait, en plus des impacts escomptés de l'option 3, un impact plus marqué au niveau opérationnel. En agissant en tant que CERT SRI de l'UE et en coordonnant les CERT nationales, l'Agence permettrait de réaliser de plus grandes économies d'échelle en ce qui

concerne la réaction aux incidents au niveau de l'UE, et de limiter les risques opérationnels pour les entreprises du fait du niveau plus élevé de sécurité et de résilience par exemple.

L'***option 5***, par l'ajout de fonctions opérationnelles consistant à prêter assistance aux autorités de police et judiciaires, permettrait de lutter contre la cybercriminalité avec une plus grande efficacité que les options 3 et 4.

Les options 4 et 5 auraient certes de plus grands impacts positifs que l'option 3, mais elles seraient toutes deux politiquement sensibles pour les États membres relativement à leurs responsabilités en matière de PIIC (c'est-à-dire que plusieurs États membres ne seraient pas favorables à des fonctions opérationnelles centralisées). De plus, étendre le mandat de l'Agence, comme envisagé au titre des options 4 et 5, risque de la mettre dans une situation ambiguë. En outre, ajouter ces nouvelles fonctions opérationnelles complètement différentes au mandat de l'Agence pourrait s'avérer très problématique à court terme et il y aurait un risque important que l'Agence ne soit pas en mesure d'exécuter correctement ce type de tâche dans des délais raisonnables. Enfin, et surtout, le coût de la mise en œuvre des options 4 et 5 est prohibitif car le budget nécessaire équivaudrait à quatre à cinq fois le budget actuel de l'ENISA.

Si l'on compare les impacts des cinq options stratégiques pour une d'organisation du type «agence SRI modernisée», les options 1 et 2 doivent être écartées car aucune ne permettrait de traiter correctement le problème complexe de la SRI au niveau de l'UE. Les options 3, 4 et 5, en revanche, permettaient à l'UE d'appréhender de façon appropriée les futures options stratégiques en matière de SRI. Les options 4 et 5 semblent, pour l'instant, trop ambitieuses tant à cause du caractère politiquement sensible pour la majorité des États membres que des incidences budgétaires. Par conséquent, ***l'option 3 semble être la meilleure solution pour régler les sept problèmes SRI recensés aussi efficacement que possible***.

7. SUIVI ET EVALUATION: COMMENT FAUT-IL APPRECIER LES COUTS ET AVANTAGES REELS ET L'OBTENTION DES EFFETS ESCOMPTES?

Au titre de cette initiative politique, seraient prévues des évaluations périodiques que la Commission transmettrait au Parlement européen et au Conseil et qui seraient rendues publiques. Ces évaluations tiendraient compte des avis de toutes les parties intéressées, sur la base d'un cahier des charges convenu par le conseil d'administration de l'Agence, et consisteraient à évaluer la capacité de l'Agence à atteindre ses objectifs, à déterminer si une agence constitue toujours un instrument efficace et si des changements doivent être apportés au mandat de l'Agence ou à d'autres aspects du règlement qui l'institue. Après évaluation, le conseil d'administration de l'Agence formulerait des recommandations à l'adresse de la Commission concernant toute modification souhaitable du règlement. Le conseil d'administration et le directeur exécutif de l'Agence devraient prendre les résultats des évaluations en considération dans la planification pluriannuelle de l'Agence.

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