COMMISSION
EUROPÉENNE

Bruxelles, le 7.2.2013
SWD(2013) 31 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document:

Proposition de directive du Parlement européen et du Conseil

concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union

{COM(2013) 48 final}
{SWD(2013) 32 final}

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document:

Proposition de directive du Parlement européen et du Conseil

concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union

1. CHAMP D'APPLICATION

La présente analyse d'impact porte sur des options stratégiques en vue d'accroître la sécurité d'Internet et des autres réseaux et systèmes informatiques sur lesquels reposent les services dont dépend le fonctionnement de notre société (p. ex. administrations publiques, finance et banque, énergie, transports, santé et certains services Internet nécessaires à des activités économiques et sociétales clés, comme les plateformes de commerce électronique et les réseaux sociaux). C'est ce que l'on appelle la sécurité des réseaux et de l'information (SRI).

2. CONTEXTE POLITIQUE

C'est en 2001 que la Commission a reconnu pour la première fois l'importance croissante de la SRI pour nos économies et nos sociétés et, en 2004, la Communauté européenne a décidé d'instituer l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) afin d'assurer un niveau élevé et efficace de SRI dans l'UE. L'approche adoptée jusqu'à maintenant par l'Union européenne dans le domaine de la SRI a surtout consisté à arrêter une série de plans d'action et de stratégies enjoignant aux États membres de se doter de moyens accrus et de coopérer pour faire face aux problèmes transnationaux de SRI.

Les parties prenantes ont été consultées sur les différents aspects de l'initiative (définition du problème et possibilités de remédier aux inconvénients existants) par:

- une **consultation publique en ligne** sur le thème «Accroître la SRI dans l'UE» qui s'est déroulée du 23 juillet au 15 octobre 2012. La Commission a reçu 169 réponses par l'intermédiaire de l'outil en ligne et 10 réponses par écrit;
- des discussions avec les **États membres** dans le cadre du Forum européen des États membres (EFMS), dans des réunions bilatérales et à la conférence de l'UE sur la cybersécurité organisée le 6 juillet 2012 par la Commission et le Service européen pour l'action extérieure;
- des discussions avec des entreprises et associations du **secteur privé** dans le cadre du Partenariat public-privé européen pour la résilience (EP3R) et dans des réunions bilatérales;
- des discussions avec l'**ENISA** et l'équipe d'intervention en cas d'urgence informatique de l'UE (**CERT-UE**);
- des discussions dans le cadre de l'**Assemblée de la stratégie numérique de 2012**.

3. EXPOSE DU PROBLEME

3.1. Définition du problème

Le problème peut être décrit globalement comme un ***niveau insuffisant de protection contre les incidents, risques et menaces pour la sécurité des réseaux et de l'information dans l'UE et préjudiciable au bon fonctionnement du marché intérieur***.

Étant donné que les réseaux et systèmes informatiques sont interconnectés et qu'Internet a une dimension mondiale, nombre d'incidents de SRI dépassent les frontières nationales et nuisent au fonctionnement du marché intérieur.

Les atteintes à la sécurité peuvent entraîner l'indisponibilité, la suspension ou l'interruption de services transnationaux comme lors des attaques contre *eBay* et *PayPal*, et la nécessité d'agir rapidement pour remédier aux problèmes et de partager les informations sur tout incident significatif a été mise en lumière par l'exemple des attaques contre *Diginotar*, société néerlandaise de certification Internet. Compte tenu des incidents passés, les États membres commencent à instaurer leur propre réglementation. Or, la multiplication d'actions réglementaires non coordonnées risque d'entraîner un morcellement et de créer des entraves au marché intérieur, générant ainsi des coûts de mise en conformité pour les entreprises ayant une activité dans plus d'un État membre.

Ce problème concerne tous les secteurs de la société et de l'économie (pouvoirs publics, entreprises et particuliers). Plusieurs secteurs jouent toutefois un rôle majeur dans la fourniture de services de support essentiels à notre économie et à notre société et la sécurité de leurs systèmes revêt une importance particulière pour le fonctionnement du marché intérieur. Il s'agit notamment des secteurs de la banque, des bourses de valeurs, de la production, du transport et de la distribution d'énergie, des transports (aérien, ferroviaire, maritime), de la santé, des facilitateurs de services Internet clés et des administrations publiques. La consultation publique a révélé que les parties prenantes soutiennent résolument le projet de s'attaquer au problème de la SRI dans ces secteurs et de prendre les mesures qui s'imposent au niveau de l'UE.

Si aucune mesure n'est adoptée pour enrayer l'augmentation du nombre d'incidents, la confiance des consommateurs dans les services en ligne risque d'en pâtir, ce qui peut compromettre la réalisation des objectifs de la stratégie numérique.

3.2. Sources du problème

Le problème défini découle d'une série de facteurs.

Premièrement, **tous les membres de l'UE ne disposent pas des mêmes moyens au niveau national**, ce qui nuit à la création d'un climat de confiance entre pairs, lequel est une condition préalable à la coopération et au partage d'informations.

Deuxièmement, **le partage des informations sur les incidents, risques et menaces est insuffisant**. La plupart des incidents de SRI ne sont pas signalés et passent inaperçus, principalement parce que les entreprises hésitent à communiquer une telle information de crainte des conséquences en termes d'image ou de responsabilité. Par ailleurs, l'échange d'informations dans le cadre des actuels partenariats public-privé/plateformes, comme l'EFMS et l'EP3R, se limite aux meilleures pratiques.

4. EFFICACITE DES MESURES ACTUELLES

4.1. Lacunes du cadre réglementaire existant

Les règles actuelles n'exigent que des seules entreprises de télécommunications qu'elles adoptent des mesures de gestion des risques et signalent les incidents de SRI alors que tous les acteurs s'appuyant sur des réseaux et systèmes informatiques courent des risques en matière de sécurité. Cela aboutit à une inégalité de traitement dès lors que le même incident touchant, par exemple, un opérateur de télécommunications et une société fournissant des services téléphoniques sur IP devrait être notifié à l'autorité nationale compétente dans le premier cas, mais pas dans le second.

Tous les acteurs qui sont responsables du traitement des données (p. ex. une banque ou un hôpital) sont obligés par le cadre réglementaire en matière de protection des données d'instaurer des mesures de sécurité qui soient proportionnées aux risques encourus, mais lesdits responsables sont tenus de notifier seulement les atteintes à la sécurité qui compromettent des données à caractère personnel.

La directive 2008/114/CE du Conseil concernant le recensement et la désignation des infrastructures critiques européennes couvre uniquement les secteurs de l'énergie et des transports et, jusqu'à maintenant, seules quelques-unes de ces infrastructures ont été recensées comme telles par les États membres. La directive n'impose pas aux opérateurs d'obligation de signaler les atteintes significatives à la sécurité et n'instaure pas non plus de mécanisme de coopération et d'intervention des États membres en cas d'incident.

Les colégislateurs discutent actuellement de la proposition de directive, soumise par la Commission, sur les attaques contre les systèmes informatiques[1], laquelle ne couvre que la pénalisation d'actes précis mais n'aborde pas la prévention des risques et incidents SRI, l'intervention en cas d'incidents de SRI ni l'atténuation de leurs conséquences.

4.2. Limites de l'approche volontaire

L'approche volontaire suivie jusqu'à maintenant a eu pour résultat un niveau inégal de préparation et une coopération limitée.

L'EFMS a un mandat limité car les États membres ne partagent pas d'informations sur les incidents, risques et menaces, pas plus qu'ils ne coopèrent pour faire face aux menaces transnationales, et il n'a donc pas le pouvoir d'exiger de ses membres qu'ils mettent en place un minimum de moyens.

L'ENISA n'a pas de compétences opérationnelles et, par exemple, ne peut intervenir pour remédier à des problèmes de SRI.

L'EP3R n'a pas de statut officiel et ne peut exiger des entreprises du secteur privé qu'elles signalent des incidents aux autorités nationales. Il n'y a en son sein aucun cadre relatif au partage d'informations de confiance ou à la communication d'informations sur les menaces, risques et incidents SRI.

5. NECESSITE DE L'INTERVENTION DE L'UE, SUBSIDIARITE ET PROPORTIONNALITE

Assurer la SRI est essentiel au bon fonctionnement du marché intérieur et au bien-être de notre société. L'article 114 du TFUE constitue une base juridique appropriée pour harmoniser les exigences de SRI et instaurer un niveau minimum de sécurité commun à toute l'UE.

[1] COM(2010) 517 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:FR:PDF).

L'intervention de l'Union dans le domaine de la SRI se justifie en termes de **subsidiarité** par la dimension transnationale du problème et par l'efficacité (et donc la valeur ajoutée) accrue qui en résulterait pour les politiques nationales actuelles.

Afin de garantir que la coopération englobe l'intégralité des États membres, il faut s'assurer qu'ils disposent tous du niveau minimum de moyens requis. De plus, il est clair que des mesures politiques SRI concertées peuvent avoir un impact très 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.

Les mesures au titre de l'option privilégiée se justifient en termes de **proportionnalité** parce que les exigences imposées aux États membres correspondent à ce qui est strictement nécessaire pour atteindre le niveau approprié de préparation et permettre la coopération sur la base de la confiance, et que les exigences imposées aux entreprises et aux pouvoirs publics en matière de gestion des risques et de signalement des incidents visent uniquement les entités critiques et impliquent des mesures qui sont proportionnées aux risques et concernent les incidents ayant un impact significatif. En outre, les mesures au titre de l'option privilégiée n'impliqueraient pas de coûts disproportionnés.

6. OBJECTIFS

L'objectif général est de relever le niveau de protection contre les incidents, risques et menaces pour la sécurité des réseaux et de l'information dans l'UE. Les objectifs spécifiques sont les suivants:

- **Objectif 1** – Instaurer un niveau minimum commun de SRI dans les États membres et donc relever le niveau global de préparation et d'intervention.
- **Objectif 2** – Améliorer la coopération en matière de SRI au niveau de l'UE en vue de faire face efficacement aux menaces et incidents transnationaux.
- **Objectif 3** – Créer une culture de gestion des risques et améliorer le partage d'informations entre le secteur privé et le secteur public.

7. OPTIONS STRATEGIQUES

Les options stratégiques qui ont été envisagées dans le cadre de la présente analyse d'impact sont: *statu quo*, approche réglementaire et approche mixte. L'option consistant à interrompre toutes les activités de l'UE en matière de SRI a été écartée.

7.1. Option 1 – *Statu quo* (scénario de référence)

La Commission, avec l'aide de l'ENISA, continuerait à suivre l'actuelle approche volontaire consistant à inviter les États membres à mettre en place des moyens SRI au niveau national (p. ex. équipes CERT, plans nationaux d'urgence en cas d'incident informatique, stratégies nationales de cybersécurité) et à coopérer au niveau de l'UE (p. ex. par un réseau de CERT en Europe et un plan européen d'urgence/de coopération en cas d'incident informatique).

7.2. Option 2 – Approche réglementaire

La Commission exigerait de tous les États membres qu'ils mettent en place un minimum de moyens au niveau national (équipes CERT, autorités compétentes, plans nationaux d'urgence en cas d'incident informatique, stratégies nationales de cybersécurité).

En vertu de cette option réglementaire, les autorités nationales compétentes et les CERT devraient faire partie d'un **réseau** de coopération au niveau de l'UE. Au sein du réseau, les autorités et les CERT échangeraient des informations et coopéreraient pour faire face aux

menaces et incidents SRI conformément au **plan européen d'urgence/de coopération en cas d'incident informatique** dont les États membres devraient convenir.

Les entreprises (autres que les micro-entreprises) de secteurs critiques précis, c.-à-d. la banque, l'énergie (électricité et gaz naturel), les transports, la santé, les facilitateurs de services Internet clés et les administrations publiques, seraient tenues d'évaluer les risques qu'elles courent et d'adopter des mesures appropriées et proportionnées pour dimensionner les risques réels. En outre, ces entités seraient tenues de signaler aux autorités compétentes les incidents qui compromettent sérieusement le fonctionnement de leurs réseaux et systèmes informatiques et ont donc un impact significatif sur la continuité des services et la fourniture des biens qui dépendent de ces réseaux et systèmes. Ce schéma s'inspire des articles 13 *bis* et 13 *ter* de la directive «cadre» sur les communications électroniques.

7.3. Option 3 – Approche mixte

La Commission combinerait des initiatives basées sur la bonne volonté des États membres, destinées à mettre en place ou renforcer leurs moyens SRI et à instaurer des mécanismes de coopération au niveau de l'UE, avec des exigences réglementaires concernant les principaux acteurs privés et les administrations publiques.

Les initiatives volontaires seraient, en substance, similaires à celles prises en vertu de l'option 1, tandis que les exigences réglementaires seraient identiques à celles imposées en vertu de l'option 2 en ce qui concerne tant les entités visées que la teneur des obligations.

L'ENISA apporterait soutien et expertise technique à la Commission, aux États membres et au secteur privé, par exemple en publiant des orientations et recommandations techniques.

8. ANALYSE DES INCIDENCES

L'analyse couvre, outre le niveau de sécurité, les incidences économiques et sociales des trois options ainsi que les coûts qui seraient encourus en vertu des options 2 et 3.

Aucune des options recensées n'aura d'incidence sur l'environnement qui soit prévisible avec précision.

8.1. Option 1 – *Statu quo* (scénario de référence)

Niveau de sécurité: il est peu probable que tous les États membres atteignent, sur le plan national, des niveaux comparables concernant les moyens et la préparation nécessaires pour accroître la sécurité et permettre la coopération et le partage d'informations de confiance au niveau de l'UE. S'agissant de la gestion des risques et d'une transparence accrue en matière d'incidents, les règles ne seraient pas les mêmes partout et les lacunes réglementaires resteraient à combler.

Incidences économiques: elles dépendraient de la mesure dans laquelle les États membres suivraient les recommandations de la Commission. Le niveau insuffisant de sécurité dans les États membres les moins développés nuirait à leur compétitivité et à leur croissance et les exposerait à des risques et des incidents. Eu égard aux tendances actuelles, les incidents de SRI deviendraient de plus en plus visibles pour les entreprises et les particuliers et retarderaient l'achèvement du marché intérieur.

Incidences sociales: la poursuite et l'aggravation prévisible des incidents, risques et menaces entameraient la confiance du public dans le monde en ligne.

8.2. Option 2 – Approche réglementaire

Niveau de sécurité: les obligations imposées aux États membres garantiraient qu'ils sont tous correctement équipés et contribueraient à créer un climat de confiance mutuelle, lequel est une condition préalable à une coopération efficace au niveau de l'UE.

Les exigences imposées aux administrations publiques et principaux acteurs privés en matière de gestion des risques SRI constitueraient une forte incitation à gérer et dimensionner efficacement les risques pour la sécurité. Le total des coûts supplémentaires qui devraient être supportés dans l'UE, tous secteurs confondus, pour satisfaire à ces exigences se situerait entre **1 et 2 milliards d'EUR**. Le coût de mise en conformité **par petite et moyenne entreprise** se situerait dans une fourchette de **2 500 à 5 000 EUR**.

Incidences économiques: le relèvement du niveau de sécurité permettrait de limiter les pertes financières imputables aux risques et incidents SRI. La confiance des entreprises et des particuliers dans le monde numérique serait plus grande et plus propice au marché intérieur. La promotion d'une culture de meilleure gestion des risques stimulerait également la demande en faveur de produits et solutions TIC sécurisés.

Incidences sociales: un niveau plus élevé de sécurité accroîtrait la confiance du public dans le monde en ligne et permettrait de tirer pleinement parti de l'environnement numérique (p. ex. médias sociaux, apprentissage en ligne, santé en ligne).

8.3. Option 3 – Approche mixte

Niveau de sécurité: comme avec l'option 1, rien ne garantit que les initiatives volontaires permettraient de relever le niveau de sécurité en termes de moyens SRI mis en place au niveau national et de coopération au niveau de l'UE. Par ailleurs, les exigences de sécurité imposées aux administrations publiques et principaux acteurs privés constitueraient une forte incitation à gérer et dimensionner efficacement les risques pour la sécurité. Ces mécanismes resteraient toutefois sans effet dans les États membres qui ne suivraient pas les recommandations de la Commission concernant la mise en place de moyens SRI.

Incidences économiques: le rythme de développement varierait considérablement d'un État membre à l'autre. Le niveau insuffisant de sécurité dans les États membres les moins développés nuirait à leur compétitivité et à leur croissance et les exposerait aux conséquences néfastes des risques et incidents.

Incidences sociales: la poursuite et l'aggravation prévisible des incidents, risques et menaces entameraient la confiance du public à l'égard du monde en ligne, surtout dans les États membres où la SRI n'est pas considérée comme une priorité.

9. COMPARAISON DES OPTIONS

Les options 1 et 3 ne sont pas considérées comme valables pour atteindre les objectifs politiques car leur efficacité dépendrait de ce que donnerait effectivement l'approche volontaire en termes de niveau minimum de SRI et, concernant l'option 3, de la bonne volonté des États membres pour mettre en place des moyens et coopérer. Elles ne sont donc pas recommandées.

L'option 2 est l'option privilégiée car elle permettrait d'améliorer considérablement la protection des particuliers, entreprises et pouvoirs publics de l'UE contre les incidents, menaces et risques SRI. En outre, en mettant de l'ordre chez elle, l'UE pourrait davantage s'imposer sur la scène internationale et apparaître comme un partenaire encore plus crédible en matière de coopération au niveau bilatéral et multilatéral. Elle serait donc aussi mieux

placée pour promouvoir à l'étranger les droits fondamentaux et les valeurs essentielles de l'UE.

10. SUIVI ET EVALUATION

Au chapitre 10 du rapport d'analyse d'impact figurent plusieurs indicateurs principaux permettant d'évaluer les progrès accomplis dans la réalisation des objectifs. Il s'agit par exemple des indicateurs suivants:

- Pour l'objectif 1, le nombre d'États membres ayant désigné une autorité compétente en matière de SRI et une CERT ou ayant adopté une stratégie nationale de cybersécurité et un plan national d'urgence/de coopération en cas d'incident informatique.
- Pour l'objectif 2, le nombre d'autorités compétentes et de CERT nationales participant au réseau et le volume d'informations échangées au sein du réseau sur les risques et incidents SRI.
- Pour l'objectif 3, le niveau des investissements en matière de SRI des principaux acteurs privés et des administrations publiques et le nombre de notifications d'incidents SRI ayant un impact significatif.