Avis du Comité économique et social européen sur la «Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union»

COM(2013) 48 final – 2013/0027 (COD)

(2013/C 271/25)

Rapporteur: **M. McDONOGH**

Le 21 février 2013 et le 15 avril 2013 respectivement, le Conseil et le Parlement européen ont décidé, conformément à l'article 114 du traité sur le fonctionnement de l'Union européenne, de consulter le Comité économique et social européen sur la

«Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union»

COM(2013) 48 final – 2013/0027 (COD)

La section spécialisée «Transports, énergie, infrastructures, société de l'information», chargée de préparer les travaux du Comité en la matière, a adopté son avis le 30 avril 2013.

Lors de sa 490e session plénière des 22 et 23 mai 2013 (séance du 22 mai 2013), le Comité économique et social européen a adopté le présent avis par 163 voix pour, 1 voix contre et 5 abstentions.

1. **Conclusions et recommandations**

1.1 Le Comité prend acte de la directive proposée, qui doit être envisagée dans le contexte plus large de la stratégie de cybersécurité ([1]) publiée récemment, qui définit une vision d'ensemble en matière de sécurité des réseaux et de l'information (SRI), visant à garantir un développement sûr de l'économie numérique tout en continuant à promouvoir les valeurs européennes de liberté et de démocratie.

1.2 Le CESE accueille favorablement cette proposition de directive dont le but est d'atteindre un niveau commun élevé de SRI dans toute l'UE. L'harmonisation et la gestion de la SRI au niveau européen sont essentielles à l'achèvement du marché unique du numérique et au bon fonctionnement du marché intérieur dans son ensemble. Le Comité partage la préoccupation de la Commission quant aux énormes dégâts que pourrait entraîner une défaillance de la SRI pour l'économie et le bien-être des citoyens. Toutefois, la directive proposée ne répond pas aux attentes du Comité, qui aurait souhaité des mesures législatives énergiques dans ce domaine crucial.

1.3 Le Comité est très déçu du manque de progrès de nombreux États membres dans la mise en œuvre d'une SRI effective au niveau national. Le CESE déplore les risques accrus que cet échec fait peser sur les citoyens ainsi que son incidence négative sur l'achèvement du marché unique numérique. Tous les États membres devraient veiller à s'acquitter sans délai de leurs obligations.

1.4 Cette absence de progrès crée un nouveau fossé numérique entre l'élite disposant d'une SRI hautement développée et les États membres les moins avancés. Ce fossé a une incidence néfaste sur la confiance et la collaboration en matière de SRI au niveau de l'UE et en l'absence d'une solution rapide, il est susceptible de provoquer des défaillances du marché intérieur liées aux différences de capacités entre les États membres.

1.5 Comme il l'avait déjà indiqué dans de précédents avis ([2]), le CESE estime que les mesures vagues et volontaires ne fonctionnent pas, et que des obligations réglementaires absolues doivent être imposées aux États membres pour garantir l'harmonisation, la gouvernance et l'application d'une SRI européenne. Malheureusement, le CESE ne pense pas que cette proposition de directive fournisse la législation claire et décisive nécessaire. Afin de garantir le niveau commun élevé de SRI requis, la Comité est d'avis qu'un règlement assorti d'obligations contraignantes bien définies pour les États membres serait plus efficace qu'une directive.

1.6 Malgré l'intention de la Commission européenne d'adopter des actes d'exécution pour garantir une certaine uniformité des conditions de mise en œuvre des éléments de la directive, le Comité constate un manque de normes, de définitions claires et d'obligations catégoriques dans l'acte proposé, ce qui laisse aux États membres une trop grande flexibilité au niveau de l'interprétation et de la transposition d'éléments critiques. Le Comité aimerait voir dans l'acte des définitions beaucoup plus explicites des normes, exigences et procédures à respecter par les États membres, les pouvoirs publics, les opérateurs du marché et les principaux facilitateurs de services internet.

([1]) «Un cyberespace ouvert, sûr et sécurisé», JOIN(2013) 1.

([2]) Avis du CESE sur «Protection des structures d'information critiques», JO C 255 du 22.9.2010, p. 98 et «Directive relative aux attaques visant les systèmes d'information», JO C 218 du 23.7.2011, p. 130.

1.7 Afin de garantir une politique de SRI efficace et sa mise en œuvre effective dans l'UE, le Comité souhaiterait que soit créée une autorité européenne en la matière, analogue à l'autorité centrale de l'industrie de l'aviation (EASA) ([3]). Cet organe fixerait les normes et assurerait le suivi de la mise en œuvre de tous les éléments de la SRI dans l'Union, depuis la certification d'équipements terminaux sûrs et leur utilisation à la sécurité des réseaux et des données.

1.8 Le CESE a pleinement conscience des risques accrus qu'entraîne, en matière de cybersécurité et de protection des données, l'adoption en Europe de l'informatique en nuage ([4]). Le Comité souhaiterait que l'acte proposé prévoie explicitement des exigences et obligations de sécurité spécifiques supplémentaires concernant la fourniture et l'utilisation de services en nuage.

1.9 Afin de garantir une responsabilisation appropriée en matière de SRI, l'acte devrait préciser que les entités ayant des obligations en vertu de la directive proposée ont le droit de tenir les fournisseurs de logiciels et de matériel responsables de tout défaut dans leurs produits ou services en rapport direct avec des incidents liés à la SRI.

1.10 Le CESE invite les États membres à veiller tout particulièrement à accroître les connaissances des petites et moyennes entreprises (PME) en matière de SRI ainsi que leurs compétences dans le domaine de la cybersécurité. Le Comité attire également l'attention de la Commission sur l'importance des «concours de hackers» aux États-Unis ([5]) et dans certains États membres ([6]) pour la sensibilisation à la cybersécurité et la constitution d'une pépinière de futurs professionnels de la SRI.

1.11 Compte tenu de l'importance du fait que tous les États membres doivent se conformer aux règles de SRI applicables dans toute l'UE, le CESE demande à la Commission d'examiner dans quelle mesure le cadre financier pluriannuel (CFP) pourrait contribuer au financement ciblé de cette mise en conformité afin de soutenir les pays ayant besoin d'une aide financière.

1.12 Le programme-cadre de l'UE pour la recherche et l'innovation, Horizon 2020, devrait accorder la priorité au financement de la recherche, du développement et de l'innovation dans le domaine des technologies de SRI afin que l'Europe puisse suivre l'évolution rapide des changements sur le front des cybermenaces.

1.13 Afin de préciser quelles sont les entités ayant des responsabilités légales en vertu de l'acte proposé, le CESE souhaiterait que chaque État membre soit tenu de publier un répertoire en ligne de l'ensemble des entités concernées par les exigences prévues par la directive en matière de gestion des risques et de notification d'incidents. Cette transparence et l'obligation de rendre compte créeraient un climat de confiance et favoriseraient le respect des prescriptions.

1.14 Le Comité attire l'attention de la Commission sur ses nombreux avis précédents traitant de la sécurité des réseaux et de l'information dans lesquels il soulignait la nécessité d'une société de l'information sûre et de la protection des infrastructures critiques ([7]).

2. **Contenu essentiel de la proposition de la Commission**

2.1 La proposition de directive sur la SRI a été publiée parallèlement à la stratégie européenne de cybersécurité, qui vise à renforcer la résilience des systèmes d'information, à réduire la cybercriminalité, à améliorer la politique de cybersécurité et de cyberdéfense internationale, et à développer les ressources industrielles et technologiques nécessaires à la sécurité du cyberespace, tout en promouvant les droits fondamentaux et autres valeurs essentielles de l'UE.

2.2 La RSI est liée à la protection d'internet et d'autres réseaux, des systèmes d'information et de ceux qui les sous-tendent, qui soutiennent le fonctionnement de notre société. La RSI est indispensable au bon fonctionnement du marché intérieur.

2.3 L'approche strictement volontaire en matière de SRI que l'UE a suivie jusqu'à présent ne fournit pas de protection suffisante contre les risques en matière de SRI. Les moyens de SRI existants ne sont pas suffisants pour suivre l'évolution rapide des changements sur le front des menaces et pour garantir un niveau commun élevé de protection dans tous les États membres.

([3]) Agence européenne de la sécurité aérienne: http://easa.europa.eu/

([4]) Avis du CESE sur «L'informatique en nuage en Europe», JO C 24 du 28.1.2012, p. 40 et «Exploiter le potentiel de l'informatique en nuage en Europe», JO C 76 du 14.3.2013, p. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) Avis du CESE sur «Une stratégie pour une société de l'information sûre», JO C 97 du 28.4.2007, p. 21.
Avis du CESE sur «Protection des structures d'information critiques», JO C 255 du 22.9.2010, p. 98.
Avis du CESE sur «Règlement ENISA», JO C 107 du 6.4.2011, p. 58.
Avis du CESE sur «Règlement général sur la protection des données», JO C 229 du 31.7.2012, p. 90.
Avis du CESE sur «Attaques visant les systèmes d'information», JO C 218 du 23.7.2011, p. 130.
Avis du CESE sur «Transactions électroniques au sein du marché intérieur», JO C 351 du 15.11.2012, p. 73.
Avis du CESE sur «Exploiter le potentiel de l'informatique en nuage en Europe», JO C 76 du 14.3.2013, p. 59.

2.4 Actuellement, les moyens disponibles et les niveaux de préparation sont très différents selon les États membres, ce qui se traduit par une fragmentation des approches dans l'UE. Étant donné que les réseaux et systèmes informatiques sont interconnectés, les États membres dont le niveau de protection est insuffisant affaiblissent l'ensemble de la SRI de l'UE. Cette situation nuit à la création d'un climat de confiance entre pairs, lequel est une condition préalable à la coopération et au partage d'informations. De ce fait, seule une minorité d'États membres disposant de moyens significatifs a établi une coopération.

2.5 La directive, proposée conformément à l'article 114 du TFUE, a pour objectif de faciliter l'achèvement et le bon fonctionnement du marché unique numérique:

— en instaurant un niveau commun minimum de SRI dans les États membres et en relevant ainsi le niveau global de préparation et d'intervention en cas d'incident;

— en améliorant la coopération en matière de SRI au niveau de l'UE en vue de faire face aux menaces et incidents transfrontaliers;

— en créant une culture de gestion des risques et en améliorant le partage d'informations entre le secteur privé et le secteur public.

2.6 La proposition de directive définit des exigences juridiques, notamment:

(a) L'obligation pour chaque État membre d'adopter une stratégie de SRI et de désigner une autorité nationale compétente dans ce domaine disposant de ressources financières et humaines adaptées pour prévenir, faire face et répondre aux risques et aux incidents.

(b) La création d'un mécanisme de coopération entre les États membres et la Commission afin de mettre en commun le système d'alerte rapide sur les incidents et les risques dans le cadre d'une infrastructure sécurisée; l'obligation de coopérer et d'organiser régulièrement des évaluations par les pairs.

(c) L'obligation, pour certaines entités spécifiques dans toute l'UE, d'adopter des pratiques de gestion des risques et de notifier à l'autorité nationale compétente tout incident majeur de sécurité affectant leurs services essentiels. Il s'agit notamment des opérateurs des infrastructures d'information critiques dans certains secteurs (services financiers, transport, énergie, santé), des facilitateurs de services de la société de l'information (entre autres les services informatiques en nuage, les plateformes de commerce électronique et de paiement par internet, les moteurs de recherche, les magasins d'applications en ligne et les réseaux sociaux) ainsi que les administrations publiques.

2.7 Les États membres devront mettre en œuvre la directive dans un délai de 18 mois à partir de son adoption par le Conseil et le Parlement européen (prévue en 2014).

3. **Observations générales**

3.1 Le développement d'internet et de la société numérique influence profondément notre vie quotidienne. Cependant, plus nous dépendrons d'internet, plus notre liberté, notre prospérité et notre qualité de vie dépendront d'une sécurité solide des réseaux et de l'information (SRI): si internet est en panne et que les dossiers médicaux sont inaccessibles en cas d'urgence, des personnes mourront. Pourtant, la sécurité de l'infrastructure informatique européenne critique est de plus en plus menacée et notre niveau de SRI n'est pas suffisant.

3.2 L'année dernière, le directeur d'Europol s'est déclaré très préoccupé par cette énorme confiance mal placée dans l'infaillibilité d'internet ([8]). Il n'est pas rare que nous apprenions que des infrastructures essentielles ont été la cible de cyberattaques de criminels, de terroristes ou de gouvernements étrangers. En général, les cibles de ces attaques n'en parlent pas car elles craignent pour leur réputation; toutefois, ces dernières semaines, nous avons été témoins d'attaques d'infrastructures internet ([9]) et de systèmes bancaires ([10]) européens qui ont entraîné trop de perturbations pour pouvoir être dissimulées. Un rapport ([11]) a estimé que les Pays-Bas ont subi 92 millions de cyberattaques en 2011 et l'Allemagne 82 millions. Le gouvernement britannique estime que le Royaume-Uni a subi 44 millions de cyberattaques en 2001, qui ont coûté près de 30 milliards d'euros à l'économie ([12]).

3.3 En 2007, le Conseil de l'UE s'est penché sur le problème de la SRI en Europe ([13]). Cependant, l'approche politique suivie depuis lors ([14]) a principalement reposé sur des mesures volontaires des États membres et seule une minorité d'entre eux en a effectivement pris. Le Comité constate que plusieurs États membres n'ont ni publié de stratégie nationale de cybersécurité ni développé de plan national d'urgence à appliquer en cas d'incident informatique, et que certains n'ont pas créé d'équipe d'intervention en cas d'urgence informatique (*Computer Emergency Response Team* - CERT). En outre, certains États membres n'ont pas encore ratifié la convention du Conseil de l'Europe sur la cybercriminalité ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UK Cyber Security Strategy – Landscape Review: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Résolution du Conseil 2007/C 68/01.
([14]) COM(2006) 251 et COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE

3.4 Dix États membres très avancés en matière de SRI ont constitué le groupe des CERT gouvernementaux européens (EGC) en vue de collaborer étroitement dans le domaine de la SRI et de l'intervention en cas d'incident. Il n'est désormais plus possible de rejoindre l'EGC: les 17 autres États membres et le CERT-UE ([16]) créé récemment sont actuellement exclus de ce groupe d'élite. Un nouveau fossé numérique se creuse entre les États membres très avancés en matière de SRI et les autres. À moins que ce fossé ne soit comblé, la fracture numérique s'attaquera au cœur du marché unique numérique, et limitera le développement de la confiance, de l'harmonisation et de l'interopérabilité. En outre, en l'absence de mesures énergiques, le fossé entre les pays très avancés et les autres est susceptible de s'élargir, tout comme les failles du marché intérieur associées aux différences de moyens entre les États membres.

3.5 La réussite de la stratégie de cybersécurité et l'efficacité de la directive proposée en matière de SRI dépendront de la puissance de l'industrie de la SRI en Europe et de la disponibilité d'une main-d'œuvre suffisante possédant des compétences spécialisées en la matière. Le CESE est heureux de constater que la directive proposée tient compte de la nécessité pour les États membres d'investir dans l'éducation, la sensibilisation et la formation à la SRI. Le Comité souhaiterait également que chaque État membre fournisse des efforts particuliers pour informer, éduquer et soutenir le secteur des PME en matière de cybersécurité. Les grandes entreprises peuvent facilement obtenir l'expertise dont elles ont besoin, alors que les PME ont besoin d'être aidées.

3.6 Le CESE tient beaucoup à coopérer avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) afin de promouvoir la SRI au cours du «mois de la cybersécurité» dans le courant de cette année. La stratégie de cybersécurité et la directive sur la SRI ont notamment pour objectif de développer une conscience de la sécurité dans toute l'Union et d'améliorer le niveau de compétences en matière de SRI; à cet égard, le Comité attire l'attention de la Commission sur les «concours de hackers» pour adolescents, qui ont permis de mieux sensibiliser le public dans certains États membres et aux États-Unis.

3.7 Le Comité se réjouit également de constater l'engagement de la stratégie de cybersécurité en faveur du financement de la recherche, du développement et de l'innovation dans le domaine de la SRI.

3.8 Le développement de l'informatique en nuage s'accompagne de plusieurs nouveaux risques pour la cybersécurité, auxquels il convient de s'attaquer. Ainsi, les cybercriminels disposent aujourd'hui d'une énorme puissance informatique à faible coût, et les données de milliers de sociétés sont désormais centralisées sur des serveurs vulnérables aux attaques ciblées. Le CESE a déjà réclamé une plus grande cyber-résilience pour l'informatique en nuage ([17]).

([16]) Le CERT-UE est une équipe permanente d'intervention en cas d'urgence informatique pour les institutions, agences et organes de l'UE.

([17]) Avis du CESE sur «L'informatique en nuage en Europe», JO C 24 du 28.1.2012 p. 40 et sur «Exploiter le potentiel de l'informatique en nuage en Europe», JO C 76 du 14.3.2013, p. 59.

3.9 Le Comité a demandé précédemment l'introduction d'un système européen volontaire d'identification électronique pour les transactions en ligne, qui complèterait les systèmes nationaux existants. Un tel système renforcerait la protection contre la fraude et le climat de confiance entre les opérateurs économiques, réduirait les coûts de fourniture des services et améliorerait la qualité des services et de la protection pour les citoyens.

4. **Observations particulières**

4.1 Il est regrettable que la proposition de directive sur la SRI présentée par la Commission soit si vague, manque de clarté et dépende trop largement de l'autoréglementation par les États membres. Le manque de normes, de définitions claires et d'obligations catégoriques, en particulier au chapitre IV de la directive, laisse aux États membres une trop grande flexibilité au niveau de l'interprétation et de la transposition d'éléments critiques de l'acte. Un règlement assorti d'obligations légales contraignantes et bien définies pour les États membres serait plus efficace qu'une directive.

4.2 Le Comité observe que l'article 6 de la directive exige que chaque État membre désigne une «autorité compétente» en vue de contrôler et de garantir l'application cohérente de la directive dans l'ensemble de l'Union. Le Comité observe d'autre part que l'article 8 prévoit la création d'un «réseau de coopération» qui, par les pouvoirs octroyés à ce dernier et à la Commission, assurera une fonction de direction, de gestion et, le cas échéant, d'exécution dans toute l'Europe jusqu'au niveau des États membres. Le CESE estime que sur la base de cadre de gouvernance, l'UE devrait envisager la création d'une autorité au niveau européen pour la SRI, similaire à l'Agence européenne de la sécurité aérienne (EASA), qui fixe des normes et gère l'application et le respect des mesures de sécurité pour les avions, les aéroports et les activités des compagnies aériennes.

4.3 L'autorité européenne de SRI proposée au paragraphe 4.2 ci-dessus pourrait être créée sur la base des travaux en matière de cybersécurité déjà réalisés, entre autres, par l'ENISA, le Comité européen de normalisation (CEN), les CERT et le groupe des CERT gouvernementaux européens (EGC). Une telle autorité fixerait les normes et assurerait le suivi de la mise en œuvre de tous les éléments de la SRI, de la certification d'équipements terminaux sûrs et de leur utilisation à la sécurité des réseaux et des données.

4.4 Étant donné le niveau élevé d'interdépendance entre les États membres pour garantir la SRI dans toute l'Union et le coût d'une défaillance de la SRI potentiellement très élevé pour toutes les parties, le CESE souhaiterait que la législation prévoie des sanctions explicites et proportionnées en cas de défaut de conformité; celles-ci devraient être harmonisées de manière à refléter la dimension paneuropéenne de la responsabilité et l'ampleur des dégâts éventuels, non seulement sur le marché national, mais aussi dans le reste de l'Union. L'article 17 de l'acte, qui traite des sanctions, est général, laisse trop de latitude aux États membres et ne donne pas suffisamment de lignes directrices pour pouvoir prendre en compte les effets transfrontaliers et paneuropéens.

4.5 Actuellement, les gouvernements et les fournisseurs de services vitaux ne divulguent pas les défaillances de sécurité et de résilience dont ils sont victimes, à moins que les événements ne les y contraignent. Cette absence d'information nuit à la capacité de l'Europe de réagir rapidement et efficacement aux menaces informatiques, et d'améliorer la sécurité générale des réseaux et de l'information par un apprentissage commun. Le Comité salue la décision de la Commission d'établir la notification obligatoire, au titre de la directive, de tous les incidents majeurs en matière de SRI. Le CESE ne croit pas que la notification volontaire de ces incidents pourrait fonctionner car les opérateurs pourraient être incités à passer sous silence des incidents en raison de craintes liées à leur bonne réputation et à une prise de responsabilités.

4.6 Cependant, l'article 14 de la directive, qui traite de la notification, ne définit pas ce qu'est un incident ayant un «impact significatif» sur la sécurité et laisse trop de latitude aux entités concernées et aux États membres en ce qui concerne la notification d'un incident. Pour être efficace, une législation doit poser des exigences claires. La directive proposée étant trop vague dans la définition d'exigences essentielles, il n'est pas possible de tenir les parties pour responsables des défauts de conformité faisant l'objet de l'article 17 de la directive.

4.7 Puisque les fournisseurs en matière de SRI sont issus dans une large mesure du secteur privé, il est essentiel d'encourager un haut degré de confiance et de coopération avec et entre les entreprises responsables de ces infrastructures et services d'information essentiels. Il convient de féliciter la Commission de l'initiative intitulée «Partenariat public-privé européen pour la résilience» (EP3R) qu'elle a lancée en 2009 et d'encourager cette dernière. Cependant, le Comité estime qu'il convient de renforcer et de soutenir cette initiative par une obligation réglementaire, dans l'acte relatif à la SRI, en vertu de laquelle les parties prenantes qui ne remplissent pas correctement leurs obligations seraient tenues de coopérer.

4.8 Chaque État membre devrait publier un répertoire en ligne de l'ensemble des entités concernées, dans sa juridiction, par les exigences prévues par l'article 14 de la directive proposée en matière de gestion des risques et de notification d'incidents. Cette transparence, ainsi que la clarification de la manière dont chaque État membre décide d'appliquer les définitions de l'article 3, contribueraient à instaurer la confiance et à encourager une culture de la gestion des risques parmi les citoyens.

4.9 Le CESE relève que les développeurs de logiciels et les fabricants de matériel sont explicitement exclus des exigences de la directive car ils ne sont pas fournisseurs de services de la société de l'information. Toutefois, le Comité estime que l'acte proposé devrait préciser que les entités ayant des obligations en vertu de la directive peuvent se retourner contre les fournisseurs de logiciels et de matériel pour tout défaut de leurs produits ou services en rapport direct avec des incidents liés à la SRI.

4.10 Bien que la Commission estime que le coût de la mise en œuvre de la directive proposée s'élèvera à environ 2 milliards d'euros par an, à répartir entre les secteurs public et privé en Europe, le Comité fait observer que certains États membres connaissant des difficultés financières devront se battre pour trouver les investissements requis pour assurer la conformité. Il convient d'examiner dans quelle mesure le CFP pourrait être utilisé pour financer la conformité en matière de SRI, grâce à divers instruments, y compris le Fonds européen de développement régional (FEDER) et éventuellement le Fonds pour la sécurité intérieure.

Bruxelles, le 22 mai 2013.

Le président
du Comité économique et social européen
Henri MALOSSE