PUBLIC

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 22 mai 2014
(OR. en)

10097/14

LIMITE

Dossier interinstitutionnel: 2013/0027 (COD)

TELECOM 118
DATAPROTECT 77
CYBER 31
MI 446
CSC 111
CODEC 1338

NOTE

de la:	présidence
aux:	délégations
n° prop. Cion.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD 1 + ADD 2
n° doc. préc.:	9757/14 TELECOM 111 DATAPROTECT 69 CYBER 27 MI 419 CSC 103 CODEC 1264
Objet:	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 - Rapport sur l'état d'avancement des travaux

Le présent rapport a été élaboré sous la responsabilité de la présidence grecque. Il expose les travaux menés à ce jour par les instances préparatoires du Conseil, rend compte de l'état d'avancement de l'examen de la proposition visée en objet et définit des orientations et des approches en vue de l'élaboration d'une version modifiée de la proposition et de la préparation des négociations à tenir avec le PE, le moment venu.

ASPECTS LIÉS À LA PROCÉDURE

1. Le 12 février 2013, la Commission a présenté sa 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* (ci-après dénommée "la directive sur la SRI"), qui a pour base juridique l'article 114 du TFUE[1]. Cette proposition s'inscrit dans la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé[2], à propos de laquelle le Conseil a adopté des conclusions le 25 juin 2013[3]. Lors de ses sessions du 6 juin[4] et du 5 décembre[5] 2013, le Conseil TTE a pris acte des progrès accomplis dans l'examen de la proposition de directive sur la SRI.

2. Le Comité économique et social européen[6] et le Comité des régions[7] ont adopté des avis sur la proposition respectivement le 22 mai et les 3 et 4 juillet 2013. Le 13 mars 2014, le Parlement européen a adopté en première lecture une résolution législative et 138 amendements rédigés par la commission du marché intérieur (IMCO) agissant en tant que chef de file, en association avec les commissions de l'industrie (ITRE) et des libertés civiles (LIBE)[8].

---

1 Doc. 6342/13.
2 Doc. 6225/13.
3 Doc. 11357/13.
4 Doc. 10076/13 et 10457/13.
5 Doc. 16630/13 et 17341/13.
6 Doc. TEN/513.
7 Doc. 2013/C 280/05.
8 Doc. 7451/14.

3. Sous la présidence grecque, le groupe "Télécommunications et société de l'information" a poursuivi les travaux par un examen article par article de la proposition, au cours de six réunions[9]. Sur la base des discussions au sein du groupe, pour lesquelles elle avait établi des documents de réflexion[10], et des observations écrites transmises par la plupart des États membres, la présidence grecque a élaboré le présent rapport sur l'état d'avancement des travaux, qui présente les principales questions qui se posent au sujet de la proposition et, dans la mesure du possible, indique les points à propos desquels les États membres s'accordent en principe sur la ligne à adopter. Parallèlement au présent rapport et à des fins d'illustration, la présidence a établi une première version modifiée du texte de la proposition[11], qu'elle a présentée au groupe le 26 mai et sur la base de laquelle les travaux pourraient se poursuivre sous la présidence italienne en vue d'entamer le dialogue avec le PE au moment opportun.

4. Des inquiétudes ont été exprimées quant à la question de savoir si la base juridique proposée (article 114 du TFUE) est suffisante pour couvrir l'ensemble de la proposition, étant donné l'objectif, le champ d'application et le contenu de celle-ci. Il convient de poursuivre la réflexion et les discussions à ce sujet. Le Service juridique du Conseil rendra un avis écrit.

FOND

Chapitre I: dispositions générales (articles 1er à 3)

5. Les délégations sont dans l'ensemble d'accord avec l'objet et le champ d'application proposés à l'article 1er ("objet") et sont aussi d'avis que la directive proposée serait une composante essentielle de la stratégie globale de l'UE en matière de cybersécurité. La présidence est convaincue qu'une majorité d'États membres pourrait être favorable à ce que le texte de l'article 1er soit affiné de la manière suivante:

   - A*u paragraphe 1, le terme "assurer" devrait être remplacé par "atteindre" ou "faciliter", pour tenir compte du fait que les États membres ne peuvent, ni individuellement, ni collectivement, "assurer" pleinement un niveau de sécurité à toute épreuve des réseaux et de l'information.*

---

9 Les 27 février, 13 et 28 mars, 10 et 28 avril et 21 mai 2014.
10 Doc. 7404/14.
11 Doc. 10061/14.

- *Plutôt que d'évoquer la création d'un nouveau "mécanisme de coopération" entre les États membres, le paragraphe 2, point b), devrait s'appuyer sur les mécanismes existants qui permettent de "regrouper" les États membres afin de mettre en œuvre la directive à un niveau stratégique de politique générale. Une coopération opérationnelle plus concrète pourrait être étudiée, éventuellement sur une base volontaire, par exemple dans le cadre des CERT[12] et/ou des autorités compétentes.*
- *L'État membre victime d'un incident et/ou sa CERT devraient décider si, et le cas échéant dans quelle mesure, il convient d'échanger des informations pertinentes (et éventuellement des données à caractère personnel), tout en prenant en considération les intérêts nationaux en matière de sécurité et les dispositions législatives pertinentes, notamment en ce qui concerne la protection des données à caractère personnel ou les attaques contre des systèmes d'information.*
- *Dans le cadre de la nécessaire clarification juridique, évoquée au point 4 ci-dessus, une autre question qui se pose est celle de savoir si et dans quelle mesure il y a lieu d'inclure ou d'exclure les "administrations publiques" du champ d'application de la proposition (article 14 en particulier).*

6. Les délégations souscrivent dans l'ensemble à l'article 2 ("harmonisation minimale").

7. En ce qui concerne les définitions figurant à l'article 3, tout en observant qu'elles devront être revues au fur et à mesure de l'avancement des travaux, la présidence estime que les délégations soutiennent d'une manière générale la ligne suivante:

- *Il y a lieu d'ajouter, à la liste de définitions, celle des termes "services essentiels", car cela permettrait de mieux cerner les acteurs qui fournissent ces services "essentiels" et d'évaluer les risques ou "les menaces" pesant sur la sécurité et la continuité de ces derniers.*
- *La directive devrait mentionner une liste des secteurs d'infrastructures critiques communs et définir des critères afin de déterminer quels opérateurs en font partie. Les États membres doivent encore préciser leurs positions en ce qui concerne le niveau de détail qui doit figurer dans la directive (et notamment à l'ANNEXE II) en décidant, par exemple, si et dans quelle mesure les "services de la société de l'information" et les "facilitateurs de services internet" devraient également être inclus dans le champ d'application de la directive.*
- *Il y a lieu d'examiner plus avant la nécessité d'ajouter des définitions portant par exemple sur les services informatiques critiques, un plan national de gestion des risques ou une stratégie et un plan de coopération en matière de SRI.*

---

[12] CERT: équipe d'intervention en cas d'urgence informatique. Il a été fait remarquer que, CERT étant une marque déposée de l'UE, il pourrait être nécessaire d'employer une terminologie différente dans la directive, par exemple: "équipe d'intervention en cas d'incident de sécurité informatique (CSIRT)".

Chapitre II: cadres nationaux de sécurité des réseaux de l'information (articles 4 à 7)

8. Les délégations sont dans l'ensemble favorables à la suppression de l'article 4 ("principe").

9. En ce qui concerne l'article 5 ("stratégies nationales en matière de SRI"), la présidence a pris note d'un large soutien en faveur de l'orientation suivante:

   - *Bien que l'idée d'élaborer des stratégies, assorties de plans de coopération, en matière de SRI, ne soit pas remise en cause, cet article devrait surtout s'attacher à énoncer des principes généraux, valables dans la durée, plutôt que d'énumérer les exigences matérielles auxquelles ces stratégies et plans de coopération devraient satisfaire; cela serait un excellent moyen d'établir la confiance.*

10. Au sujet de l'article 6 ("autorités compétentes") et gardant à l'esprit le principe de subsidiarité, les délégations semblent favorables à une approche qui tiendrait dûment compte des pratiques en cours dans les États membres:

   - *La directive devrait laisser suffisamment de latitude aux États membres en ce qui concerne la désignation ou le maintien d'une ou de plusieurs autorités compétentes pour les différents secteurs et pour les politiques à mener.*
   - *Les États membres seraient toutefois tenus de désigner un "point de contact unique", dont les missions devront être définies plus précisément.*

11. En ce qui concerne l'article 7 ("CERT"), les États membres sont, d'une manière générale, favorables à l'obligation prévue par la directive de mettre en place et de maintenir une ou plusieurs CERT, la CERT pouvant être la même entité que l'"autorité compétente" ou le "point de contact unique" et ils approuvent les orientations proposées dans le doc. 7404/14 en ce qui concerne les CERT, en particulier l'orientation suivante:

   - *Les États membres devraient disposer d'une latitude suffisante pour définir la structure technique et les ressources financières et humaines des CERT et cela devrait apparaître dans le libellé de cet article et de l'ANNEXE I, la directive ne devant toutefois pas transiger sur le niveau d'ambition à atteindre et les exigences à imposer aux CERT et à la coopération entre elles.*

Chapitre III: coopération (articles 8 à 13)

12. Le chapitre III de la proposition porte sur l'architecture de la coopération en matière de SRI. De l'avis de la présidence, tous les États membres admettent qu'une certaine forme de coopération permettrait d'atteindre, dans toute l'UE, des niveaux plus élevés et comparables de préparation en matière de SRI, ce qui pourrait éventuellement contribuer à faciliter également, en cas de besoin, la mise en place d'une intervention commune et coordonnée face à un problème de SRI. Les positions doivent toutefois encore se préciser quant à l'aspect que devrait revêtir ce réseau de coopération stratégique et la capacité qu'il aurait, le cas échéant, d'apporter des réponses opérationnelles coordonnées à des incidents informatiques nationaux et, éventuellement, transnationaux.

13. Pour ce qui est de l'article 8 ("réseau de coopération"), la présidence estime que les délégations soutiennent, d'une manière générale, l'approche suivante:

- *Au sujet du réseau de coopération (ou "groupe"), la directive devrait définir une approche stratégique qui, d'une part, s'appuie sur les capacités qui devraient être développées en application du chapitre II ci-dessus et qui, d'autre part, donne, le cas échéant, des orientations relatives à l'élaboration des modalités de la coopération opérationnelle au sein des instances compétentes.*
- *En cas d'urgence, l'intervention relève de la responsabilité des organismes nationaux, tels les CERT et/ou les autorités compétentes, et, si nécessaire dans des cas (transnationaux) devant encore être précisés, une coopération supplémentaire facultative pourrait être mise en place au sein d'une communauté de coopération opérationnelle composée de l'ensemble des 28 CERT nationales, ce qui est de nature à faciliter une intervention coordonnée de l'UE.*
- *Le réseau de coopération devrait organiser, sur la base du volontariat, des exercices d'évaluation par les pairs portant sur les capacités et l'état de préparation.*

14. Concernant l'article 9 ("système sécurisé d'échange d'informations"), la présidence a relevé que les États membres ne sont pas très favorables à l'établissement, dans la directive, d'exigences impératives en matière d'échange d'informations (sensibles sur le plan commercial ou confidentielles) au sein du réseau de coopération, ni à la création ou l'exploitation d'une infrastructure sécurisée spécifique, ni au rôle qu'il est proposé de confier à la Commission à cet égard. Compte tenu de ces réticences, la présidence juge que cet article devrait être remanié selon les modalités suivantes:

- *La directive ne devrait prévoir aucune exigence impérative en ce qui concerne l'échange d'informations et l'article 9 devrait l'indiquer dans son libellé ou, à défaut, il pourrait être supprimé, sachant que les informations non sensibles et non classifiées pourraient être échangées au sein du réseau de coopération ou que les informations pertinentes pourraient l'être entre les CERT et/ou les autorités compétentes.*

15. En ce qui concerne l'article 10 ("alerte rapide"), les délégations semblent globalement être en mesure de soutenir les orientations générales exposées dans le document 7404/14, et notamment les suivantes:

- *La diffusion d'alertes rapides devrait rester facultative et l'échange d'informations pertinentes dans le cadre du réseau de coopération devrait avant tout contribuer à favoriser l'instauration d'un climat de confiance entre le secteur privé et les autorités nationales compétentes, ainsi qu'entre ces dernières.*
- *L'échange d'informations relatives à des infractions pénales concernant des attaques contre les systèmes d'information étant couvert par la directive 2013/40/UE, il n'est pas nécessaire que la directive examinée traite de cet aspect (suppression du paragraphe 4).*
- *Les États membres devraient décider si des informations sont communiquées au réseau de coopération et, dans l'affirmative, lesquelles (suppression du paragraphe 5).*
- *Le mécanisme d'alerte rapide ne devrait pas entraver ou ralentir les mesures nationales visant à gérer les menaces et les incidents.*

16. Pour ce qui est de l'article 11 ("intervention coordonnée"), la présidence a également noté un large soutien en faveur des orientations exposées dans le document 7404/14, et notamment les suivantes:

- *Plutôt que de créer une compétence européenne de fait pour coordonner une intervention de l'UE en cas d'incidents (nationaux), il faudrait poursuivre le débat afin de préciser si, quand et dans quels cas une "intervention coordonnée de l'UE" serait requise: en cas de crise informatique transnationale majeure ou également dans le cas d'incidents quotidiens plus limités?*
- *Compte tenu de la compétence nationale en matière de sécurité, la directive devrait s'appuyer sur les dispositifs existants pour parvenir à une coordination politique au niveau de l'UE en cas de crises informatiques de grande envergure plutôt que de mettre en place des mécanismes nouveaux et potentiellement lents.*
- *Outre une coordination politique au niveau de l'UE, la directive devrait faciliter une coopération technique/concrète (par exemple entre les CERT), dans le cadre de laquelle d'autres exigences relatives à une intervention opérationnelle en cas de crises informatiques pourraient être mises au point.*

17. La présidence note que, même si la position finale des États membres sur l'article 12 ("plan de coopération de l'Union en matière de SRI") dépendra du résultat des discussions sur les articles 8 à 11, la plupart des délégations pourraient accepter qu'il soit tenu compte de l'approche ci-après dans le texte de la proposition:

- *La directive pourrait établir, plutôt qu'un "plan", un "cadre" de coopération de l'Union en matière de SRI, axé sur la coordination et l'élaboration des politiques, qui tire pleinement parti des compétences de l'ENISA en la matière et qui serait régulièrement réexaminé par le réseau de coopération mis en place en vertu de l'article 8.*

- *Ce "cadre" de coopération devrait porter sur des questions telles que les modalités de communication entre CERT, les échanges de bonnes pratiques, les mesures de sensibilisation et les exercices et les formations, et tirer avantage des compétences de l'ENISA à cet égard.*

18. En ce qui concerne l'article 13 ("coopération internationale"), la présidence a noté que les États membres souhaitaient qu'il ressorte du texte que tous les membres participant au cadre de coopération devraient approuver la participation de pays tiers ou d'organisations internationales audit cadre.

Chapitre IV: sécurité des réseaux (articles 14 à 16), chapitre V: dispositions finales (articles 17 à 23) et annexes I et II: CERT et acteurs du marché

19. En ce qui concerne l'article 14 ("exigences de sécurité et notification d'incidents"), la présidence a noté que les États membres dans lesquels une pratique nationale de notification volontaire a permis d'instaurer une coopération satisfaisante entre les parties prenantes concernées et les autorités publiques préféreraient que la directive s'appuie sur leur expérience. D'autres États membres se posent la question de savoir s'il conviendrait d'introduire en outre des exigences relatives à un signalement obligatoire. Tous les États membres conviennent qu'il est nécessaire d'apporter des précisions supplémentaires quant aux différentes exigences en matière de notification prévues par différents actes législatifs de l'UE. Compte tenu de ce qui précède, la présidence recommande que l'approche suivante soit examinée de manière plus approfondie:

- *La directive pourrait prévoir des exigences relatives à un signalement obligatoire dans le cas d'incidents ayant des répercussions transnationales notables touchant plusieurs États membres.*
- *Dans le cas d'incidents internes ayant des répercussions limitées, les États membres devraient avoir la possibilité de choisir, conformément à l'article 2, s'ils les signalent au niveau national et de quelle manière.*
- *La directive devrait fixer les critères permettant de déterminer les répercussions des incidents (par secteur), mais il reviendrait aux États membres de décider, sur la base de ces critères, s'il convient de signaler un incident donné.*
- *Les États membres devraient avoir le choix des modalités du signalement aux autorités sectorielles compétentes et/ou au "point de contact unique" national.*

20. Pour ce qui est de l'article 15 ("mise en œuvre et exécution"), compte tenu des avis exprimés par les délégations, la présidence propose ce qui suit:

- *La directive devrait laisser une marge de manœuvre suffisante au niveau national afin que le secteur privé joue un rôle plus important que ne le prévoit la proposition actuelle, par exemple en ce qui concerne les audits de sécurité, le renforcement des capacités techniques, les formations, etc.*
- *La directive devrait par ailleurs permettre de disposer, le cas échéant, de plusieurs autorités sectorielles compétentes, également dotées de compétences en matière de mise en œuvre et d'exécution.*

21. En ce qui concerne la question de la "normalisation", visée à l'article 16, la présidence conclut qu'il convient de poursuivre la réflexion sur une reformulation de cet article.

22. Il faut poursuivre l'examen de l'article 17 ("sanctions"), et notamment son paragraphe 2, afin de préciser davantage le lien entre la directive sur la SRI et le règlement sur la protection des données, qui est attendu.

23. Enfin, la présidence a noté que les délégations souhaitaient revenir ultérieurement sur les questions de la "période de transposition" et de l'"entrée en vigueur" (articles 21 et 22), et qu'il faudra réexaminer plus tard la mise au point de l'ANNEXE I concernant la portée des obligations et tâches des CERT et de l'ANNEXE II concernant les secteurs et les entités à inclure dans une liste "exhaustive" ou "indicative", sous réserve des négociations sur le fond des articles de la proposition.

CONCLUSION

24. La présidence grecque note que tous les États membres, sans exception, ont parfaitement conscience de l'urgence qu'il y a à améliorer la sécurité des réseaux et de l'information et à prendre des mesures à cet effet au niveau de l'UE. Dans ce contexte, les États membres ont examiné avec le plus grand soin la proposition de la Commission et des progrès considérables ont été accomplis au cours des derniers mois pour définir le sens dans lequel la proposition devrait évoluer, comme expliqué plus haut.

25. En ce qui concerne les dispositions des chapitres I, II et IV, compte tenu des discussions menées au sein des instances préparatoires du Conseil, la présidence est d'avis que les orientations et approches proposées dans le présent rapport sur l'état d'avancement des travaux devraient suffire pour poursuivre l'élaboration de la proposition sous la future présidence italienne. Ces orientations et approches ont été élaborées en tenant compte de la nécessité de trouver un juste équilibre entre les aspects suivants: améliorer la cybersécurité, instaurer la confiance nécessaire et, par souci d'efficacité, tirer pleinement parti de l'expérience acquise et éviter le chevauchement des compétences des organismes et mécanismes existants.

26. Pour ce qui est du chapitre III, comme indiqué ci-dessus (point 12), les États membres conviennent qu'il est nécessaire de renforcer la coopération stratégique en matière de SRI au niveau de l'UE. Un certain nombre d'États membres estiment que la directive devrait prévoir des critères et des exigences plus précis en ce qui concerne la coopération opérationnelle en cas d'incidents en matière de SRI. Néanmoins, pour la plupart des États membres, la priorité doit d'abord être donnée à la coopération stratégique afin d'instaurer la confiance nécessaire, mais, dans le même temps, les modalités d'une coopération opérationnelle pourraient continuer à être mises au point dans le cadre des mécanismes et organismes existants. Ainsi qu'il a été indiqué plus haut (points 12 à 18), la présidence ne considère pas la coopération stratégique et la coopération opérationnelle comme des options qui s'excluent mutuellement, mais elle estime que la directive devrait accorder la priorité à la coopération stratégique, tout en donnant des orientations, en matière de coopération opérationnelle, aux organismes et mécanismes existants.

*

* *

Une fois que le présent rapport sur l'état d'avancement des travaux aura été examiné par le Coreper le 28 mai, la présidence le soumettra au Conseil et invitera ce dernier à en prendre note.