PARLEMENT EUROPÉEN 2009 - 2014

Commission de l'industrie, de la recherche et de l'énergie

2010/0273(COD)

11.11.2011

AVIS

de la commission de l'industrie, de la recherche et de l'énergie

à l'intention de la commission des libertés civiles, de la justice et des affaires intérieures

sur la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Rapporteur pour avis: Christian Ehler

PA_Legam

AMENDEMENTS

La commission de l'industrie, de la recherche et de l'énergie invite la commission des libertés civiles, de la justice et des affaires intérieures, compétente au fond, à incorporer dans son rapport les amendements suivants:

Amendement 1

Proposition de directive
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) ***La*** présente directive a pour objet de rapprocher les règles pénales appliquées par les États membres pour réprimer les attaques contre les systèmes d'information et de renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres.	(1) ***S'inscrivant dans le cadre de la stratégie générale de l'Union destinée à lutter contre la criminalité organisée, à augmenter la résilience des réseaux informatiques, à protéger les infrastructures d'information critiques et à garantir la protection des données, la*** présente directive a pour objet de rapprocher les règles pénales appliquées par les États membres pour réprimer les attaques contre les systèmes d'information et de renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres***, la Commission, Eurojust, Europol, les organismes appelés aux niveaux national et européen à intervenir en cas d'urgence informatique (les CERT – Computer Emergency Response Team) ainsi que l'Agence européenne chargée de la sécurité des réseaux et de l'information, ce dans le but de favoriser une approche européenne commune et exhaustive***.

Amendement 2

Proposition de directive
Considérant 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(1 bis) Les systèmes d'information représentent un élément essentiel de l'interaction politique, sociale et économique en Europe. La société est très dépendante de ce type de systèmes et ce phénomène va croissant. Le bon fonctionnement et la sécurité de ces systèmes en Europe sont fondamentaux pour le développement du marché intérieur et d'une économie compétitive et innovante. Cependant, tout en offrant de grands avantages, les systèmes d'information comportent un certain nombre de risques pour notre sécurité en raison de leur complexité et de leur vulnérabilité face aux différents types de cybercriminalité. Par conséquent, la sécurité des systèmes d'information est une préoccupation constante et appelle des réponses efficaces de la part des États membres et de l'Union.

Amendement 3

Proposition de directive
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) Les attaques contre les systèmes d'information***, en particulier celles qui pourraient émaner du milieu de la criminalité organisée,*** constituent une menace croissance, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information des infrastructures critiques des États membres et de l'Union suscite de plus en plus l'inquiétude. Cette situation risque de compromettre la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union	(2) Les attaques contre les systèmes d'information ***sont susceptibles d'être perpétrées par différents acteurs, qui peuvent être des terroristes, des organisations criminelles, des pays, ou encore des individus isolés. Elles*** constituent une menace croissante ***pour le bon fonctionnement des systèmes d'information dans l'Union et dans le monde***, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information des infrastructures critiques des États membres et de l'Union suscite de plus en plus l'inquiétude. ***La nature transfrontière de certaines infractions***

européenne.	***ainsi que les risques et les coûts relativement faibles encourus par leurs auteurs, au regard des avantages immenses qu'ils peuvent en retirer et des dommages qu'ils peuvent causer avec ces attaques, augmentent considérablement le degré de la menace.*** Cette situation risque de compromettre la réalisation d'une société de l'information plus sûre et d'un espace de liberté, ***de démocratie,*** de sécurité et de justice, ***hypothèque la création d'un marché intérieur européen du numérique*** et appelle donc une réaction ***tant*** au niveau de l'Union européenne ***qu'à l'échelle internationale, s'appuyant notamment sur la convention du Conseil de l'Europe sur la cybercriminalité de 2001***.

Amendement 4

Proposition de directive
Considérant 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 bis) De récentes cyberattaques, perpétrées contre les réseaux ou systèmes d'information européens, ont porté gravement préjudice à l'économie et à la sécurité de l'Union.

Justification

Il est ici fait référence aux cyberattaques dont ont été victimes en mars 2011 les institutions européennes, ainsi qu'aux nombreuses atteintes au système européen d'échange des droits d'émission, qui ont entraîné le vol de millions d'euros en émissions.

Amendement 5

Proposition de directive
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) On constate une tendance à la	(3) On constate une tendance à la

perpétration d'attaques à grande échelle de plus en plus dangereuses et régulières contre des systèmes d'information critiques pour les *États* ou certaines fonctions du secteur public ou privé. Parallèlement, ***des outils*** de plus en plus sophistiqués ***sont mis au point***, lesquels peuvent être utilisés par des criminels pour lancer des cyberattaques de divers types.

perpétration d'attaques à grande échelle de plus en plus dangereuses et régulières***, notamment des attaques distribuées par déni de service,*** contre des systèmes d'information critiques pour ***les organisations internationales,*** les *pays****, l'Union*** ou certaines fonctions du secteur public ou privé. ***De telles attaques sont susceptibles de provoquer des dommages économiques notables, tant du fait de l'interruption des systèmes d'information ou des communications elles-mêmes qu'en raison de la perte ou la modification d'informations confidentielles importantes d'un point de vue commercial ou d'autres données. Les PME innovantes, qui dépendent du bon fonctionnement et de la disponibilité des systèmes d'information mais sont susceptibles d'avoir moins de ressources à consacrer à la sécurité de l'information, sont particulièrement vulnérables.*** Parallèlement, ***le développement rapide de la technologie informatique permet la mise au point d'outils*** de plus en plus sophistiqués, lesquels peuvent être utilisés par des criminels pour lancer des cyberattaques de divers types***, dont certaines sont tout à fait susceptibles d'entraîner des dommages économiques et sociaux***.

Amendement 6

Proposition de directive
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) Il ***importe*** d'arrêter des définitions communes dans ce domaine, notamment pour les systèmes d'information ***et*** les données informatiques, de manière à garantir l'application cohérente de la présente directive dans tous les États membres.	(4) Il ***est fondamental*** d'arrêter des définitions communes dans ce domaine, notamment pour les systèmes d'information***,*** les données informatiques ***et les infractions commises à leur encontre***, de manière à garantir l'application cohérente ***et uniforme*** de la présente

directive dans tous les États membres.

Amendement 7

Proposition de directive
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) ***Il*** conviendrait que les États membres prévoient des sanctions pour réprimer ***les attaques contre les systèmes d'information***. Les sanctions ainsi fixées devraient être effectives, proportionnées et dissuasives.	(6) ***Outre les mesures mises en place par les États membres, l'Union et le secteur privé pour accroître la sécurité et l'intégrité des systèmes d'information, prévenir les attaques et limiter leurs répercussions, il*** conviendrait que les États membres prévoient ***tant des mesures efficaces pour empêcher les attaques contre les systèmes d'information que*** des sanctions ***harmonisées*** pour ***les*** réprimer, ***s'inscrivant dans le cadre de stratégies nationales plus générales de dissuasion et de lutte contre de telles attaques***. Les sanctions ainsi fixées devraient être effectives, proportionnées et dissuasives. ***La convergence des sanctions et des peines appliquées par les États membres est nécessaire étant donné la nature souvent transfrontière des menaces et vise à réduire les disparités entre les États membres dans le traitement des infractions commises dans l'Union.***

Amendement 8

Proposition de directive
Considérant 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(6 bis) Les États membres, l'Union et le secteur privé doivent, en collaboration avec l'Agence européenne chargée de la sécurité des réseaux et de l'information, adopter des mesures visant à accroître la sécurité et l'intégrité des systèmes d'information, à prévenir les attaques et à

limiter leurs répercussions.

Amendement 9

Proposition de directive
Considérant 8

Texte proposé par la Commission	*Amendement*
(8) Dans ses conclusions des 27 et 28 novembre 2008, le Conseil a invité les États membres et la Commission à définir une nouvelle stratégie, en prenant en considération le contenu de la convention du Conseil de l'Europe sur la cybercriminalité de 2001. Cette convention est le cadre juridique de référence de la lutte contre la cybercriminalité, y compris les attaques contre les systèmes d'information, et la présente directive ***s'en inspire***.	(8) Dans ses conclusions des 27 et 28 novembre 2008, le Conseil a invité les États membres et la Commission à définir une nouvelle stratégie, en prenant en considération le contenu de la convention du Conseil de l'Europe sur la cybercriminalité de 2001. ***Le Conseil et la Commission doivent encourager les États membres qui ne l'ont pas encore fait à ratifier la convention dès que possible.*** Cette convention est le cadre juridique de référence de la lutte contre la cybercriminalité, y compris les attaques contre les systèmes d'information, et la présente directive ***tient compte des dispositions pertinentes y figurant***.

Amendement 10

Proposition de directive
Considérant 10

Texte proposé par la Commission	*Amendement*
(10) La présente directive n'a pas pour objet d'engager la responsabilité pénale ***en l'absence*** d'intention délictueuse, notamment dans le cas d'interventions visant à tester ou à protéger un système d'information après en avoir obtenu l'autorisation.	(10) La présente directive ***ne s'étend pas aux mesures prises pour assurer la sécurité des systèmes d'information, comme la capacité d'un système d'information de résister à des actes criminels tels que définis dans la présente directive, ou la possibilité de se défaire d'outils qui sont utilisés ou susceptibles d'être utilisés pour de telles actions***. ***Elle*** n'a pas ***non plus*** pour objet d'engager la responsabilité pénale ***lorsque les critères objectifs des infractions énumérées dans la présente directive sont remplis mais que***

l'acte est dépourvu d'intention délictueuse, notamment dans le cas d'interventions visant à tester ou à protéger un système d'information après en avoir obtenu l'autorisation.

Justification

Étant donné que la frontière est parfois floue entre un accès malveillant et un accès sans intention de nuire (mises à jour automatiques, etc.), il s'agit ici de préciser que des opérations telles que le fonctionnement d'un logiciel anti-virus ou d'outils de suppression de virus, ou encore la mise en quarantaine de dispositifs infectés, sont totalement exclues du champ d'application de la directive.

Amendement 11

Proposition de directive
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) La présente directive renforce l'importance des réseaux, tels que le réseau de points de contact du G8 ou celui du Conseil de l'Europe dont les points de contact sont disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept pour échanger des informations afin de garantir une assistance immédiate aux enquêtes ou procédures portant sur des infractions pénales liées à des données et des systèmes d'information, ou pour recueillir des preuves ***électroniques*** d'une infraction pénale. Compte tenu de la rapidité avec laquelle des attaques à grande échelle peuvent être menées, il conviendrait que tous les États membres soient en mesure de répondre promptement aux demandes urgentes émanant de ce réseau de points de contact. L'assistance demandée devrait notamment consister à faciliter ou à exécuter directement des mesures telles que la fourniture ***de conseils techniques***, la conservation des données, la collecte de preuves, la communication d'informations juridiques ***et*** la localisation de suspects.	(11) La présente directive renforce l'importance des réseaux, tels que le réseau de points de contact du G8 ou celui du Conseil de l'Europe dont les points de contact sont disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept pour échanger des informations afin de garantir une assistance immédiate aux enquêtes ou procédures portant sur des infractions pénales liées à des données et des systèmes d'information, ou pour recueillir des preuves d'une infraction pénale ***ou d'une tentative d'infraction***. Compte tenu de la rapidité avec laquelle des attaques à grande échelle peuvent être menées, il conviendrait que tous les États membres***, l'Union et l'Agence européenne chargée de la sécurité des réseaux et de l'information*** soient en mesure de répondre promptement ***et efficacement*** aux demandes urgentes émanant de ce réseau de points de contact. L'assistance demandée devrait notamment consister à faciliter ou à exécuter directement des mesures telles que la fourniture ***d'une assistance technique, notamment en ce***

qui concerne la restauration des fonctionnalités des systèmes d'information, la conservation des données ***conformément aux principes de protection des données à caractère personnel***, la collecte de preuves, la communication d'informations juridiques***, l'identification des informations compromises et/ou extorquées, ainsi que*** la localisation ***et l'identification*** de suspects.

Amendement 12

Proposition de directive
Considérant 11 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(11 bis) La coopération des autorités publiques avec le secteur privé et la société civile est essentielle dans la prévention et la lutte contre les attaques visant les systèmes d'information. Il convient d'établir un dialogue permanent avec ceux-ci, étant donné le large usage qu'ils font des systèmes d'information et les responsabilités partagées, qui exigent la stabilité et le bon fonctionnement des systèmes. Il est important d'améliorer la prise de conscience de tous les acteurs intervenant dans l'utilisation des systèmes d'information pour créer une culture de sécurité informatique.

Amendement 13

Proposition de directive
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) Il est nécessaire de recueillir des données sur les infractions relevant de la présente directive pour avoir une vision plus complète du problème au niveau de l'Union et permettre ainsi de formuler des	(12) Il est nécessaire de recueillir des données sur les infractions relevant de la présente directive pour avoir une vision plus complète du problème au niveau de l'Union et permettre ainsi de formuler des

réponses plus efficaces. Grâce aux données recueillies, des agences ***spécialisées*** comme Europol et l'Agence européenne chargée de la sécurité des réseaux et de l'information pourront mieux évaluer l'ampleur de la cybercriminalité et le niveau de sécurité des réseaux et de l'information ***en Europe***.	réponses plus efficaces. ***Les États membres doivent améliorer l'échange d'informations relatives aux attaques contre les systèmes d'information, avec le soutien de la Commission et de l'Agence européenne chargée de la sécurité des réseaux et de l'information.*** Grâce aux données recueillies, des agences ***et des organes spécialisés*** comme ***les CERT des États membres, ainsi que des agences telles*** Europol et l'Agence européenne chargée de la sécurité des réseaux et de l'information pourront mieux évaluer l'ampleur de la cybercriminalité et le niveau de sécurité des réseaux et de l'information ***dans l'Union et aider les États membres à apporter des réponses aux incidents en matière de sécurité de l'information***. ***Une meilleure connaissance des risques présents et futurs permettra de prendre des décisions plus appropriées pour prévenir ou contrer les attaques contre les systèmes d'information, ou pour en atténuer les dommages.***

Amendement 14

Proposition de directive
Considérant 12 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 bis) Si la présente directive est tenue de respecter des règles strictes de sécurité juridique et de prévisibilité du droit pénal, il n'en convient pas moins de prévoir un mécanisme flexible permettant de s'adapter aux évolutions futures, ce qui conduira peut-être à élargir le champ d'application de la présente directive. Cet objectif est d'ailleurs servi par les dispositions de la présente directive concernant la collecte de données, l'échange d'informations et l'obligation pour la Commission de faire régulièrement rapport sur son application

et d'avancer toute proposition nécessaire. Les évolutions futures évoquées comprennent les développements technologiques permettant, par exemple, une répression plus efficace dans le domaine des attaques contre les systèmes d'information ou facilitant la prévention de telles attaques ou la limitation de leur impact.

Justification

S'il est entendu que l'instauration de sanctions est souhaitable, une approche exhaustive de l'Union pour lutter contre la cybercriminalité ne saurait se concentrer uniquement sur une répression efficace. Il convient d'élaborer également des stratégies et de mettre en place des instruments de prévention de ces activités criminelles.

Amendement 15

Proposition de directive
Considérant 12 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 ter) L'Agence européenne chargée de la sécurité des réseaux et de l'information devrait jouer un rôle stratégique dans la coordination des actions entre les États membres et les institutions de l'Union. L'Agence pourrait, par exemple, être chargée de superviser l'échange d'informations entre ces derniers, en tenant ainsi lieu de point de contact unique et de registre européen des incidents en matière de cybersécurité. Elle peut également être chargée de centraliser les statistiques sur les infractions visées par la présente directive au niveau européen et de les utiliser pour préparer des rapports concernant les conditions de sécurité des systèmes d'information et des données informatiques dans l'ensemble de l'Union.

Amendement 16

Proposition de directive
Considérant 13

Texte proposé par la Commission	*Amendement*
(13) L'existence de lacunes et de différences importantes dans les législations nationales en matière d'attaques contre des systèmes d'information risque d'entraver la lutte contre la criminalité organisée et le terrorisme, et de compliquer la coopération policière et judiciaire dans ce domaine. Les systèmes d'information modernes ayant un caractère transnational sans frontières, les attaques lancées contre eux ont une dimension transfrontière qui met en lumière la nécessité de prendre d'urgence des mesures complémentaires pour harmoniser ***le droit pénal*** dans ce domaine. Par ailleurs, il convient de faciliter la coordination des poursuites judiciaires en cas d'attaque contre des systèmes d'information par l'adoption de la décision-cadre 2009/948/JAI du Conseil relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales.	(13) L'existence de lacunes et de différences importantes dans les législations nationales en matière d'attaques contre des systèmes d'information risque d'entraver la lutte contre la criminalité organisée et le terrorisme, et de compliquer la coopération policière et judiciaire dans ce domaine. Les systèmes d'information modernes ayant un caractère transnational sans frontières, les attaques lancées contre eux ont une dimension transfrontière qui met en lumière la nécessité de prendre d'urgence des mesures complémentaires ***au niveau européen*** pour harmoniser ***les législations pénales nationales*** dans ce domaine. ***De même, l'Union doit viser à améliorer la coopération internationale en matière de sécurité des réseaux et des systèmes d'information, avec la participation de tous les acteurs internationaux concernés.*** Par ailleurs, il convient de faciliter la coordination des poursuites judiciaires en cas d'attaque contre des systèmes d'information par l'adoption de la décision-cadre 2009/948/JAI du Conseil relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales.

Amendement 17

Proposition de directive
Article 1 – alinéa 1

Texte proposé par la Commission	*Amendement*
La présente directive définit des infractions pénales en matière d'attaques contre les systèmes d'information et instaure des règles minimales pour l'établissement des peines sanctionnant ces infractions. Elle	La présente directive définit des infractions pénales en matière d'attaques contre les systèmes d'information et instaure des règles minimales ***harmonisées*** pour l'établissement des peines sanctionnant ces

vise également à mettre en place des dispositifs communs pour prévenir ces attaques ***et*** améliorer la coopération ***judiciaire*** européenne dans ce domaine.	infractions. Elle vise également à mettre en place des dispositifs communs ***tant*** pour prévenir ***et combattre*** ces attaques ***que pour*** améliorer la coopération européenne dans ce domaine***, notamment en matière de justice pénale***.

Amendement 18

Proposition de directive
Article 2 – point d

Texte proposé par la Commission	*Amendement*
d) "sans en avoir le droit": un accès ou une atteinte à l'intégrité non autorisé(e) par le propriétaire ou autre détenteur de droits au système ou à une partie du système, ou non prévu(e) par la législation nationale.	d) "sans en avoir le droit": un accès ou une atteinte à l'intégrité non autorisé(e) par le propriétaire ou autre détenteur de droits au système ou à une partie du système, ou non prévu(e) par la législation nationale ***ou le droit de l'Union***.

Amendement 19

Proposition de directive
Article 7 – point b

Texte proposé par la Commission	*Amendement*
b) le mot de passe d'un ordinateur, un code d'accès ou des données de même nature grâce auxquelles il est possible d'accéder à tout ou partie d'un système d'information.	b) le mot de passe d'un ordinateur, un code d'accès***, un jeton d'authentification numérique ou matériel*** ou des données de même nature grâce auxquelles il est possible d'accéder à tout ou partie d'un système d'information.

Amendement 20

Proposition de directive
Article 8 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Les États membres font en sorte que la transmission à une autre personne, sans autorisation, de toute donnée

	d'identification aux fins des opérations visées aux articles 3 à 7 constitue une infraction pénale.

Amendement 21

Proposition de directive
Article 8 – paragraphe 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter. Les États membres font en sorte qu'une infraction au sens des articles 3 à 7 commise par une personne qui, dans l'exercice de ses fonctions, a accès aux mécanismes de sécurité protégeant les systèmes d'information, soit considérée comme une circonstance aggravante et constitue une infraction pénale.

Amendement 22

Proposition de directive
Article 10 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 6 soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles sont commises au moyen d'un outil conçu pour lancer des attaques contre un nombre important de systèmes d'information ou des attaques causant un préjudice considérable, tel que la perturbation de services de réseau, des coûts financiers ou la perte de données à caractère personnel.	2. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 6 soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles sont commises au moyen d'un outil conçu pour lancer des attaques contre un nombre important de systèmes d'information ou des attaques causant un préjudice considérable, tel que la perturbation de services de réseau, des coûts financiers ou la perte de données à caractère personnel ***ou d'informations confidentielles***.

Amendement 23

Proposition de directive
Article 13 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) au profit d'une personne morale ***dont le siège est situé*** sur le territoire de l'État membre concerné.	c) au profit d'une personne morale ***constituée*** sur le territoire de l'État membre concerné.

Amendement 24

Proposition de directive
Article 14 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 8, et conformément aux règles régissant la protection des données, les États membres recourent au réseau ***existant*** de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept. Les États membres veillent également à mettre en place des procédures pour pouvoir répondre à des demandes *urgences* dans un délai maximal de huit heures. La réponse doit ***au moins*** préciser ***si la demande d'aide sera satisfaite,*** sous quelle forme et dans quel délai.	1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 8, et conformément aux règles régissant la protection des données, les États membres ***veillent à disposer d'un point de contact national fonctionnel,*** recourent au réseau de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept***, et transmettent en outre ces informations à la Commission ainsi qu'à l'Agence européenne chargée de la sécurité des réseaux et de l'information.*** Les États membres veillent également à mettre en place des procédures pour pouvoir répondre à des demandes *urgentes* dans un délai maximal de huit heures. La réponse doit ***être efficace et consister, le cas échéant, à faciliter ou à exécuter directement des mesures telles que la fourniture de conseils techniques, notamment en ce qui concerne la restauration des fonctionnalités des systèmes d'information, la conservation des données conformément aux principes de protection des données à caractère personnel, la collecte de preuves, la communication d'informations juridiques ainsi que la localisation et l'identification***

	de suspects. Le point de contact doit préciser sous quelle forme et dans quel délai ***la demande d'assistance sera satisfaite***.

Amendement 25

Proposition de directive
Article 14 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres communiquent à la Commission le point de contact qu'ils ont désigné aux fins de l'échange d'informations sur les infractions visées aux articles 3 à 8. La Commission transmet ces informations aux autres États membres.	2. Les États membres communiquent à la Commission***, à Eurojust et à l'Agence européenne chargée de la sécurité des réseaux et de l'information*** le point de contact qu'ils ont désigné aux fins de l'échange d'informations sur les infractions visées aux articles 3 à 8. La Commission transmet ces informations aux autres États membres.

Amendement 26

Proposition de directive
Article 15 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres transmettent à la Commission les données recueillies conformément au présent article***. Ils*** veillent ***aussi*** à ce qu'un état consolidé de ces rapports statistiques soit publié.	3. Les États membres transmettent à la Commission***, à Europol et à l'Agence européenne chargée de la sécurité des réseaux et de l'information*** les données recueillies conformément au présent article ***et*** ils veillent à ce qu'un état consolidé de ces rapports statistiques soit ***régulièrement*** publié.

Amendement 27

Proposition de directive
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Au plus tard le [QUATRE ANS À COMPTER DE L'ADOPTION] et ensuite tous les trois ans, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente directive dans les États membres, qui comprend toute proposition nécessaire.	1. Au plus tard le [QUATRE ANS À COMPTER DE L'ADOPTION] et ensuite tous les trois ans, la Commission présente au Parlement européen et au Conseil***, après avoir consulté toutes les parties prenantes concernées,*** un rapport sur l'application de la présente directive dans les États membres, qui comprend toute proposition nécessaire. ***Chaque rapport détermine les solutions techniques permettant une répression plus efficace, dans l'Union, des attaques contre les systèmes d'information, notamment des outils susceptibles de déjouer de telles attaques ou d'en limiter l'impact, et en tient compte dans toute proposition nécessaire.***

Amendement 28

Proposition de directive
Article 18 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres transmettent à la Commission toutes les informations nécessaires à l'élaboration du rapport visé au paragraphe 1. Ces informations contiennent une description détaillée des mesures législatives et non législatives adoptées pour transposer la présente directive.	2. Les États membres ***et l'Agence européenne chargée de la sécurité des réseaux et de l'information*** transmettent à la Commission toutes les informations nécessaires à l'élaboration du rapport visé au paragraphe 1. Ces informations contiennent une description détaillée des mesures législatives et non législatives adoptées pour transposer la présente directive.

PROCÉDURE

Titre	Attaques visant les systèmes d'information et abrogation la décision-cadre 2005/222/JAI du Conseil
Références	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Commission compétente au fond Date de l'annonce en séance	LIBE 7.10.2010
Commission(s) saisie(s) pour avis Date de l'annonce en séance	ITRE 7.10.2010
Rapporteur(s) Date de la nomination	Christian Ehler 24.11.2010
Examen en commission	13.4.2011 6.10.2011
Date de l'adoption	10.11.2011
Résultat du vote final	+: 49 –: 0 0: 1
Membres présents au moment du vote final	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean
Suppléant(s) présent(s) au moment du vote final	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Ţicău
Suppléant(s) (art. 187, par. 2) présent(s) au moment du vote final	Eider Gardiazábal Rubial