Informations de base

2012/2096(INI) INI - Procédure d'initiative	Procédure terminée
Cybersécurité et défense **Subject** 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 6.10.02 Politique de sécurité et de défense commune (PSDC); UEO, OTAN	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
AFET Affaires étrangères	KELAM Tunne (PPE)	06/03/2012
	Rapporteur(e) fictif/fictive YÁÑEZ-BARNUEVO GARCÍA Luis (S&D) NICOLAI Norica (ALDE) TARAND Indrek (Verts/ALE) VAN ORDEN Geoffrey (ECR) LÖSING Sabine (GUE/NGL) TERHO Sampo (EFD)	

Commission européenne

DG de la Commission	Commissaire
Réseaux de communication, contenu et technologies	KROES Neelie

Evénements clés

Date	Evénement	Référence	Résumé
24/05/2012	Annonce en plénière de la saisine de la commission		
10/10/2012	Vote en commission		
17/10/2012	Dépôt du rapport de la commission	A7-0335/2012	Résumé
21/11/2012	Débat en plénière		
22/11/2012	Décision du Parlement	T7-0457/2012	Résumé

22/11/2012	Résultat du vote au parlement		
22/11/2012	Fin de la procédure au Parlement		

Informations techniques	
Référence de la procédure	2012/2096(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d'initiative
Base juridique	Règlement du Parlement EP 55
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	AFET/7/09320

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE489.358	22/06/2012	
Amendements déposés en commission		PE494.798	11/09/2012	
Rapport déposé de la commission, lecture unique		A7-0335/2012	17/10/2012	Résumé
Texte adopté du Parlement, lecture unique		T7-0457/2012	22/11/2012	Résumé

Commission Européenne

Type de document	Référence	Date	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2013)110	02/04/2013	

Cybersécurité et défense

2012/2096(INI) - 17/10/2012 - Rapport déposé de la commission, lecture unique

La commission des affaires étrangères a adopté un rapport d'initiative de Tunne KELAM (PPE, EE) sur la sécurité et la défense du cyberespace. Les principales recommandations contenues dans le rapport sont les suivantes :

Actions et coordination au sein de l'Union européenne : face aux menaces et aux attaques informatiques contre les organes gouvernementaux, administratifs, militaires et internationaux qui sont de plus en plus fréquentes à la fois au niveau mondial et de l'Union, le rapport souligne la nécessité de définir une approche globale et coordonnée de ces défis au niveau de l'Union avec le développement d'une **stratégie européenne globale en matière de cybersécurité** qui devrait :

- établir une **définition commune** des notions de cybersécurité et de cyberdéfense, ainsi que de ce qui constitue une attaque informatique touchant à la défense,
- définir une **vision opérationnelle commune** et
- prendre en compte la **valeur ajoutée** des agences et des organes existants, de même que les **bonnes pratiques** des États membres qui disposent déjà de stratégies nationales en matière de cybersécurité.

Le rapport demande à la Commission et à la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité de tenir compte de la possibilité d'une attaque informatique grave à l'encontre d'un État membre dans leur future proposition sur les modalités de mise en œuvre de la clause de solidarité (article 222 du traité FUE).

La Commission et le Conseil sont invités à reconnaître les **libertés numériques** en tant que droits fondamentaux et conditions indispensables à l'exercice de droits de l'homme universels et à élaborer, avec les États membres, un **livre blanc** sur la défense du cyberespace.

Au niveau de l'Union européenne, les députés soulignent la nécessité d'une **coopération et d'une coordination horizontales** dans le domaine de la cybersécurité entre les institutions et les agences de l'Union et au sein de chacune d'entre elles.

Les institutions de l'UE sont invitées à : i) élaborer pour leurs propres systèmes, dans les plus brefs délais, des stratégies de cybersécurité et des plans d'urgence; ii) inclure la question de la gestion des crises informatiques dans leurs plans d'évaluation des risques et de gestion des crises.

Le rapport souligne également l'importance :

- d'un développement efficient de **l'équipe d'intervention** en cas d'urgence informatique de l'Union (EU-CERT) et des équipes nationales de même nature, ainsi que de l'élaboration de plans d'urgence en cas de nécessité d'agir;
- de créer dès que possible, au niveau européen, **le réseau d'alerte** concernant les infrastructures critiques;
- des **exercices paneuropéens** dans la préparation aux incidents de grande envergure affectant la sécurité des réseaux ;
- de la définition d'un **ensemble unique de normes** relatives à l'évaluation de la menace.

Le rapport demande aux États membres d'établir une **coopération étroite avec l'Agence européenne de défense (AED)** dans la perspective du développement de leurs capacités nationales de défense du cyberespace. Il encourage l'AED à renforcer sa coopération avec l'OTAN, avec des centres d'excellence nationaux et internationaux, avec le Centre européen de lutte contre la cybercriminalité, rattaché à Europol, contribuant à une plus grande rapidité de réaction en cas d'attaques informatiques.

Les États membres sont pour leur part invités à :

- parachever sans délai leurs **stratégies nationales** respectives en matière de sécurité et de défense du cyberespace et à garantir un environnement réglementaire et législatif solide, des procédures complètes de gestion des risques ainsi que des mesures et des mécanismes de préparation adéquats;
- créer des **unités** consacrées à la sécurité et à la défense du cyberespace dans le cadre de leurs structures militaires, en vue de coopérer avec des organes similaires dans d'autres États membres de l'Union;
- introduire des **pôles juridictionnels spécialisés** à l'échelle régionale destinés à mieux réprimer les atteintes aux systèmes d'information;
- développer leurs **plans de réaction d'urgence** et à inclure la gestion des crises informatiques dans leurs plans d'évaluation des risques et de gestion des crises;
- faire de la **recherche et du développement** un des piliers de la sécurité et de la défense du cyberespace, et à encourager la formation d'ingénieurs spécialisés dans la protection des systèmes informatiques.

La Commission et les États membres sont invités à **présenter des programmes** visant à promouvoir une utilisation globalement sûre de l'internet, ainsi qu'à sensibiliser les particuliers et les entreprises à cette question. Les députés suggèrent à la Commission de lancer, à cet égard, une **initiative publique paneuropéenne à vocation pédagogique** et invitent les États membres à inclure l'éducation à la sécurité informatique dans les programmes scolaires, ce dès le plus jeune âge.

Enfin, le rapport :

- souligne le rôle crucial d'une **coopération** dans le domaine de la cybersécurité **entre les autorités publiques et le secteur privé**, tant au niveau européen qu'au niveau national, dans l'objectif d'instaurer un climat de confiance mutuelle ;
- appelle à une **intensification de la coopération** et des échanges d'informations sur la manière d'aborder la problématique de la cybersécurité **avec les pays tiers**;
- demande à tous les organismes compétents de l'Union qui s'occupent de la question de la sécurité et de la défense du cyberespace d'exploiter les activités complémentaires existantes en matière de développement des capacités de défense pour renforcer leur **coopération sur le plan pratique avec l'OTAN** en vue d'échanger des expériences;
- insiste sur la nécessité, aussi bien pour **les États-Unis** que pour l'Union européenne, de renforcer leur coopération mutuelle dans la lutte contre les cyberattaques et la cybercriminalité, étant donné qu'il d'une priorité des relations transatlantiques établie lors du sommet UE - États-Unis de Lisbonne en 2010.

Cybersécurité et défense

2012/2096(INI) - 22/11/2012 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 454 voix pour, 39 contre et 96 abstentions, une résolution sur la sécurité et la défense du cyberespace.

Les députés rappellent que les menaces informatiques constituent un risque majeur pour la sécurité, la stabilité et la compétitivité des États nations et du secteur privé, et qu'elles ne doivent pas être considérées comme une problématique de demain. Il existe dans l'Union et ses États membres de nombreux obstacles de nature politique, juridique et organisationnelle à l'élaboration d'une approche complète et unifiée de la défense du cyberespace et de la cybersécurité. En juin 2012, seuls dix États membres de l'Union avaient officiellement adopté une stratégie nationale en matière de cybersécurité.

Sur la base de ce constat, le Parlement formule les recommandations suivantes :

Actions et coordination au sein de l'Union européenne : face aux menaces et aux attaques informatiques contre les organes gouvernementaux, administratifs, militaires et internationaux qui sont de plus en plus fréquentes à la fois au niveau mondial et de l'Union, les députés soulignent la nécessité de définir une approche globale et coordonnée de ces défis au niveau de l'Union avec le développement d'une **stratégie européenne globale en matière de cybersécurité** qui devrait :

- établir une **définition commune** des notions de cybersécurité et de cyberdéfense, ainsi que de ce qui constitue une attaque informatique touchant à la défense,
- définir une **vision opérationnelle commune** et
- prendre en compte la **valeur ajoutée** des agences et des organes existants, de même que les **bonnes pratiques** des États membres qui disposent déjà de stratégies nationales en matière de cybersécurité.

Le Parlement demande à la Commission et à la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité de tenir compte de la possibilité d'une attaque informatique grave à l'encontre d'un État membre dans leur future proposition sur les modalités de mise en œuvre de la clause de solidarité (article 222 du traité FUE).

La Commission et le Conseil sont invités à reconnaître les **libertés numériques** en tant que droits fondamentaux et conditions indispensables à l'exercice de droits de l'homme universels et à élaborer, avec les États membres, un **livre blanc** sur la défense du cyberespace.

Au niveau de l'Union européenne, les députés soulignent la nécessité d'une **coopération et d'une coordination horizontales** dans le domaine de la cybersécurité entre les institutions et les agences de l'Union et au sein de chacune d'entre elles.

Les institutions de l'UE sont invitées à : i) élaborer pour leurs propres systèmes, dans les plus brefs délais, des stratégies de cybersécurité et des plans d'urgence; ii) inclure la question de la gestion des crises informatiques dans leurs plans d'évaluation des risques et de gestion des crises.

La résolution souligne également l'importance :

- d'un développement efficient de **l'équipe d'intervention** en cas d'urgence informatique de l'Union (EU-CERT) et des équipes nationales de même nature, ainsi que de l'élaboration de plans d'urgence en cas de nécessité d'agir;
- de créer dès que possible, au niveau européen, **le réseau d'alerte** concernant les infrastructures critiques;
- des **exercices paneuropéens** dans la préparation aux incidents de grande envergure affectant la sécurité des réseaux ;
- de la définition d'un **ensemble unique de normes** relatives à l'évaluation de la menace.

Le Parlement demande aux États membres d'établir une **coopération étroite avec l'Agence européenne de défense (AED)** dans la perspective du développement de leurs capacités nationales de défense du cyberespace. Il encourage l'AED à renforcer sa coopération avec l'OTAN, avec des centres d'excellence nationaux et internationaux, avec le Centre européen de lutte contre la cybercriminalité, rattaché à Europol, contribuant à une plus grande rapidité de réaction en cas d'attaques informatiques.

Les États membres sont pour leur part invités à :

- parachever sans délai leurs **stratégies nationales** respectives en matière de sécurité et de défense du cyberespace et à garantir un environnement réglementaire et législatif solide, des procédures complètes de gestion des risques ainsi que des mesures et des mécanismes de préparation adéquats;
- créer des **unités** consacrées à la sécurité et à la défense du cyberespace dans le cadre de leurs structures militaires, en vue de coopérer avec des organes similaires dans d'autres États membres de l'Union;
- introduire des **pôles juridictionnels spécialisés** à l'échelle régionale destinés à mieux réprimer les atteintes aux systèmes d'information;
- développer leurs **plans de réaction d'urgence** et à inclure la gestion des crises informatiques dans leurs plans d'évaluation des risques et de gestion des crises;
- faire de la **recherche et du développement** un des piliers de la sécurité et de la défense du cyberespace, et à encourager la formation d'ingénieurs spécialisés dans la protection des systèmes informatiques.

La Commission et les États membres sont invités à **présenter des programmes** visant à promouvoir une utilisation globalement sûre de l'internet, ainsi qu'à sensibiliser les particuliers et les entreprises à cette question. Les députés suggèrent à la Commission de lancer, à cet égard, une **initiative publique paneuropéenne à vocation pédagogique** et invitent les États membres à inclure l'éducation à la sécurité informatique dans les programmes scolaires, ce dès le plus jeune âge.

Enfin, le Parlement :

- souligne le rôle crucial d'une **coopération** dans le domaine de la cybersécurité **entre les autorités publiques et le secteur privé**, tant au niveau européen qu'au niveau national, dans l'objectif d'instaurer un climat de confiance mutuelle ;
- appelle à une **intensification de la coopération** et des échanges d'informations sur la manière d'aborder la problématique de la cybersécurité **avec les pays tiers**;
- demande à tous les organismes compétents de l'Union qui s'occupent de la question de la sécurité et de la défense du cyberespace d'exploiter les activités complémentaires existantes en matière de développement des capacités de défense pour renforcer leur **coopération sur le plan pratique avec l'OTAN** en vue d'échanger des expériences;
- insiste sur la nécessité, aussi bien pour **les États-Unis** que pour l'Union européenne, de renforcer leur coopération mutuelle dans la lutte contre les cyberattaques et la cybercriminalité, étant donné qu'il d'une priorité des relations transatlantiques établie lors du sommet UE - États-Unis de Lisbonne en 2010.