Informations de base

2013/2606(RSP) RSP - Résolutions d'actualité	Procédure terminée
Résolution sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé **Subject** 3.30.07 Cybersécurité, politique cyberespace	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
IMCO Marché intérieur et protection des consommateurs	SCHWAB Andreas (PPE) HARBOUR Malcolm (ECR)	20/03/2013 20/03/2013
	Rapporteur(e) fictif/fictive GARCÉS RAMÓN Vicente Miguel (S&D) MANDERS Antonius (ALDE) ENGSTRÖM Christian (Verts/ALE) SALVINI Matteo (EFD)	

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Affaires générales	3251	2013-06-25

Commission européenne

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

Evénements clés

Date	Evénement	Référence	Résumé
25/06/2013	Adoption de résolution/conclusions par le Conseil		Résumé
09/07/2013	Vote en commission		
10/09/2013	Débat en plénière		
12/09/2013	Décision du Parlement	T7-0376/2013	Résumé

12/09/2013	Résultat du vote au parlement		
12/09/2013	Fin de la procédure au Parlement		

Informations techniques	
Référence de la procédure	2013/2606(RSP)
Type de procédure	RSP - Résolutions d'actualité
Sous-type de procédure	Résolution sur déclaration
Base juridique	Règlement du Parlement EP 136-p2
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	IMCO/7/12435

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Proposition de résolution		B7-0386/2013	06/09/2013	
Texte adopté du Parlement, lecture unique		T7-0376/2013	12/09/2013	Résumé

Commission Européenne

Type de document	Référence	Date	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2013)816	19/12/2013	

Résolution sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

2013/2606(RSP) - 25/06/2013

Le 7 février 2013, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont adressé une communication conjointe au Parlement européen et au Conseil, intitulée "Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé".

Sur cette base, le Conseil a adopté une série de conclusions qui peuvent se résumer comme suit :

Caractère indispensable d'une approche globale : le Conseil estime qu'il est indispensable et urgent de poursuivre l'élaboration d'une approche globale en matière de cybersécurité et de la mettre en œuvre aux fins d'une politique de l'UE sur le cyberespace qui:

- protège et favorise l'exercice des droits de l'homme et repose sur les valeurs fondamentales de l'UE ;
- fasse progresser la prospérité en Europe et renforce les avantages économiques et sociaux du cyberespace, notamment l'Internet ;
- favorise une cybersécurité effective et renforcée dans l'ensemble de l'UE et au-delà,
- encourage les efforts visant à réduire la fracture numérique mondiale et soutient la coopération internationale dans le domaine de la cybersécurité,
- reflète le rôle et les droits des particuliers, du secteur privé et de la société civile à l'égard des questions inhérentes au cyberespace.

Dans ce contexte, le Conseil invite les États membres, la Commission et la haute représentante à coopérer, dans le respect des domaines de compétences de chacun et du principe de subsidiarité, en vue de la mise en œuvre des objectifs suivants :

1) **Valeurs** : d'une manière générale, le Conseil invite les États membres à prendre toutes les mesures raisonnables pour que **tous les citoyens de l'UE soient en mesure d'accéder à l'Internet et d'en tirer parti**.

2) **Prospérité** : le Conseil estime qu'il est indispensable que les technologies de l'information et de la communication (TIC) ainsi que la sécurité des TIC se développent pour favoriser l'innovation et la croissance. Il faut toutefois œuvrer à la protection des infrastructures et des fonctions clés que les États membres jugent indispensables, notamment en protégeant les infrastructures d'informations dites critiques (PIIC) au niveau national.

3) **Cyber-résilience** : les États membres sont appelés à prendre des mesures pour veiller à atteindre dans leur pays **un bon niveau en matière de cybersécurité**, en élaborant et en mettant en œuvre des politiques adéquates ainsi que des capacités organisationnelles et opérationnelles adaptées. Dans ce contexte, le Conseil appelle à une série de mesures dont : i) des actions de sensibilisation sur la nature des menaces et les bonnes pratiques en matière numérique ; ii) le renforcement des systèmes informatiques ; iii) le renforcement de la coopération paneuropéenne en matière de cybersécurité, iv) le renforcement de la coopération entre les États membres au niveau de l'UE, en vue de parvenir à une évaluation commune des menaces, v) la prise en compte des questions de cybersécurité à la lumière des travaux en cours sur **la clause de solidarité**.

4) **Lutte contre cybercriminalité** : le Conseil estime par ailleurs que des mesures d'envergure doivent être prises en matière de cybercriminalité pour au moins recenser les insuffisances des États membres et les moyens de renforcer leurs moyens d'enquête. Il suggère également l' utilisation du futur Fonds pour la sécurité intérieure, dans les limites de son budget, pour aider les autorités compétentes à lutter contre la cybercriminalité, ainsi que le recours à l'instrument de stabilité pour développer la lutte contre la cybercriminalité et lutter contre les organisations cybercriminelles. Il suggère en outre le renforcement de la coopération intercommunautaire, notamment en soutenant Europol.

D'autres propositions sont faites en vue de lutter contre la cybercriminalité via **la coopération avec les pays tiers** et **la politique de sécurité et de défense commune**.

Dans la foulée, le Conseil appelle la Commission et à la haute représentante à rédiger un rapport d'activité sur la stratégie de cybersécurité qui sera présenté lors de la conférence de haut niveau qui se tiendra en février 2014. Il propose également que se tiennent régulièrement des réunions des instances préparatoires compétentes du Conseil pour contribuer à définir les priorités et les objectifs stratégiques de l'UE concernant le cyberespace **au sein d'un cadre d'action global**.

Enfin, le Conseil appelle la Commission à présenter **les modalités de financement de la stratégie ainsi proposée, en tenant compte des futures négociations avec le Parlement européen**.

Résolution sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

2013/2606(RSP) - 12/09/2013 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté 585 voix pour, 45 voix contre et 8 abstentions, une résolution préparée par sa commission du marché intérieur et de la protection des consommateurs ainsi que celle des affaires étrangères sur la stratégie de cybersécurité de l'Union européenne, en réponse à la une communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, portant sur le même thème.

Les députés constatent les défis croissants qui se posent en matière de cybersécurité en raison des menaces et des attaques toujours plus sophistiquées qui mettent gravement en péril la sécurité, la stabilité et la prospérité économique des États membres de même que le commerce électronique tout en reconnaissant que les services en ligne constituent une force vitale pour atteindre la prospérité et garantir la liberté d'expression.

Dans ce contexte, le Parlement souligne qu'il est essentiel d'élaborer une politique de communication stratégique sur la cybersécurité de l'Union, les situations de cyber-crise, les repositionnements stratégiques, la collaboration entre le secteur public et le secteur privé et les alertes, ainsi que des recommandations à l'intention du public.

Il appelle de nouveau les États membres à adopter, dans les meilleurs délais, **des stratégies nationales de cybersécurité** qui : i) couvrent les aspects techniques, de coordination, de ressources humaines et d'allocations financières, ii) comprennent des règles spécifiques sur les avantages et les responsabilités du secteur privé, dans le but d'assurer la participation de ce dernier, et iii) prévoient des procédures complètes de gestion des risques et préservent le cadre réglementaire. Dans le même temps, **les États membres devraient s'efforcer de ne jamais compromettre les droits et les libertés de leurs citoyens** lorsqu'ils élaborent des réponses aux menaces et aux attaques informatiques.

La résolution évoque également la nécessité d'élaborer des programmes de formation visant à promouvoir et à améliorer la sensibilisation, les compétences et la formation des citoyens européens, notamment en ce qui concerne leur sécurité personnelle, dans le cadre d'un programme d'études dans le domaine des compétences numériques applicable dès le plus jeune âge.

Cyber-résilience : le Parlement insiste sur le développement de la cyber-résilience pour les infrastructures critiques et rappelle que les futures modalités de mise en œuvre de la clause de solidarité (article 222 du traité FUE) devraient tenir compte des risques d'attaques informatiques contre les États membres. Il invite la Commission et la haute représentante à prendre ces risques en considération dans leurs rapports conjoints d'évaluation intégrée des menaces et des risques, attendus pour 2015.

Il se félicite de l'idée émise par la Commission d'adopter une culture de gestion des risques en matière de cybersécurité et **prie les États membres et les institutions de l'Union d'inclure sans délai la gestion des crises informatiques dans leurs stratégies de gestion des risques et leurs analyses de**

risques. Il invite en outre les gouvernements des États membres et la Commission à encourager les acteurs du secteur privé à inclure la gestion des crises informatiques dans leurs stratégies de gestion de risques, et à former leur personnel à la cybersécurité.

Par ailleurs, le Parlement prie tous les États membres et les institutions de l'Union de mettre en place un réseau d'équipes d'intervention en cas d'urgence informatique (**CERT**) qui soient efficaces et opérationnelles 24 heures sur 24, sept jours sur sept. Il soutient également l'ENISA dans l'exercice de ses fonctions en ce qui concerne la sécurité des réseaux et de l'information, notamment en fournissant des indications et des conseils aux États membres.

Ressources industrielles et technologiques : le Parlement invite les institutions de l'Union et les États membres à prendre les mesures qui s'imposent pour instaurer un "marché unique de la cybersécurité" au sein duquel les utilisateurs et les fournisseurs pourraient tirer le meilleur parti des innovations, des synergies et des expertises combinées, et auquel les PME auraient accès. Il invite les États membres à envisager **des investissements conjoints dans la filière européenne de la cybersécurité**, à l'image de ce qui a été fait dans d'autres secteurs, comme celui de l'aviation.

Cybercriminalité : rappelant le fait que la cybercriminalité était un fléau international dont le coût était en constante augmentation, celui-ci s'élevant actuellement, selon les estimations à un montant annuel de 295 milliards EUR, le Parlement indique qu'il est essentiel d'accomplir des efforts conjoints et de procéder à des échanges d'expertise à l'échelle de l'Union, au-delà du niveau national, en associant Eurojust, Europol et les CERT. Il convient également que les universités et les centres de recherche disposent **des ressources et des capacités adéquates** pour remplir correctement leur rôle de pôles d'expertise, de coopération et de partage d'informations. En même temps, les citoyens devraient pouvoir accéder facilement aux informations sur les menaces informatiques et sur les moyens d'y faire face.

Les États membres qui ne l'ont pas encore fait devraient également ratifier la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest) le plus rapidement possible.

Cyberdéfense : le Parlement invite les États membres à **coopérer davantage avec l'Agence européenne de défense** (AED) afin d'élaborer des propositions et des initiatives en matière de capacités de cyberdéfense fondées sur des initiatives et des projets récents. Il demande également la vice-présidente de la Commission/haute représentante de l'Union d'**inclure la gestion des crises informatiques dans la planification de la gestion des crises** et appelle les États membres à élaborer des plans en coopération avec l'AED afin de protéger les missions et les opérations de la politique de sécurité et de défense commune (PSDC) contre les cyber-attaques.

Politique internationale : sachant que la coopération et le dialogue à l'échelle internationale jouent un rôle primordial dans l'instauration d'un climat de confiance et de transparence et dans la promotion d'un niveau élevé de coopération en réseau et d'échange d'informations au niveau mondial, le Parlement invite la Commission et le Service européen pour l'action extérieure (SEAE) à mettre sur pied une équipe de **cyber-diplomatie** chargée de favoriser le dialogue avec les pays et les organisations partageant les mêmes convictions. La vice-présidente de la Commission/haute représentante de l'Union est également appelée à **intégrer la dimension de la cybersécurité dans la politique extérieure de l'Union**. Dans ce contexte, le Parlement estime que **le groupe de travail UE–États-Unis sur la cybersécurité et la cybercriminalité** devrait permettre à l'Union et aux États-Unis d'échanger, dans la mesure du possible, les bonnes pratiques en matière de cybersécurité.

Mise en œuvre : enfin, le Parlement invite **la Commission à élaborer une feuille de route claire présentant le calendrier des objectifs à accomplir au niveau de l'Union** au titre de la stratégie de cybersécurité et demande aux États membres de convenir d'un calendrier similaire pour les actions entreprises au niveau national au titre de cette stratégie.