

Résolution sur la stratégie de cybersécurité de l'Union européenne: un cyberspace 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.