Cyberdéfense

2018/2004(INI) - 13/06/2018 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 476 voix pour, 151 contre et 36 abstentions, une résolution sur la cyberdéfense.

L'Union et les États membres sont confrontés à une menace sans précédent prenant la forme de cyberattaques politiques d'État ainsi que de cybercriminalité et de terrorisme. Compte tenu de sa **vulnérabilité actuelle**, due principalement à la fragmentation des stratégies européennes de défense, il est urgent de **renforcer les capacités de l'UE** dans le domaine de la cyberdéfense.

Développement des capacités de cyberdéfense: le Parlement a souligné qu'une politique commune de cyberdéfense devrait constituer un **élément central** du développement de l'Union européenne de défense (UED). Il a appelé à un développement cohérent des capacités de cyberdéfense dans toutes les institutions et organes de l'UE, ainsi que dans les États membres.

Les députés ont exhorté les États membres à **coopérer étroitement au développement de leur cyberdéfense respective**, en utilisant une feuille de route claire en vue de mieux rationaliser les structures de cyberdéfense dans les États membres. Un **réseau européen sécurisé** pour les informations et les infrastructures critiques devrait être développé.

Les États membres ont été invités à utiliser au mieux le cadre fourni par la **Coopération structurée permanente (CSP)** et le **Fonds européen de défense (FED)** pour proposer des projets de coopération. Les députés se sont félicités du lancement de deux cyberprojets dans le cadre de la CSP, à savoir une plateforme d'échange d'informations sur les cyberincidents et la mise en place d'une assistance mutuelle en matière de cybersécurité. Ils espèrent que cela conduira à la création d'une **équipe européenne d' intervention rapide**, qui coordonnerait, détecterait et contrerait les cyber-menaces collectives.

Instruction et formation: le Parlement a invité l'Union et les États membres à renforcer leur coopération en matière d'éducation, de formation et d'exercices. Il a appuyé l'initiative de **l'Erasmus militaire** et d'autres initiatives communes de formation et d'échange entre jeunes militaires. Il a souligné la nécessité de **renforcer la sensibilisation et l'expertise** dans le domaine de la cybersécurité. Tous les États membres devraient informer, sensibiliser et conseiller les entreprises, les écoles et les citoyens au sujet de la cybersécurité et des principales menaces numériques.

Coopération UE-OTAN en matière de cyberdéfense: le Conseil a été invité à examiner les moyens d'apporter un soutien au niveau de l'Union pour **intégrer le cyberespace dans les doctrines militaires des États membres**, d'une manière harmonisée et en étroite coopération avec l'OTAN. Les députés sont convaincus de l'importance d'une coopération accrue entre l'UE et l'OTAN en tant que moyen de prévenir, détecter et dissuader les cyberattaques.

Normes internationales: les députés ont appelé à intégrer les capacités de cyberdéfense dans la PESC et l'action extérieure de l'UE et de ses États membres et ont plaidé pour une **coordination plus étroite** en matière de cyberdéfense entre les États membres, les institutions de l'UE, l'OTAN, les Nations unies, les États-Unis et d'autres partenaires stratégiques, en particulier en ce qui concerne les règles, les normes et les mesures d'application dans le cyberespace.

Les États membres devraient poursuivre la mise en œuvre de l'approche commune et globale de l'UE en matière de cyberdiplomatie et de cyber-normes existantes, et élaborer, avec l'OTAN, **des critères et des définitions** de ce qui constitue une cyberattaque au niveau de l'UE, afin d'améliorer la capacité de l'UE à

parvenir rapidement à une position commune à la suite d'un acte internationalement illicite sous la forme d'une cyberattaque.

Coopération civilo-militaire: le Parlement a invité toutes les parties prenantes à consolider les partenariats de transfert de connaissances et à mettre en œuvre des modèles économiques adaptés afin de créer des synergies entre les marchés civil et militaire, c'est-à-dire **un marché unique européen pour la cybersécurité et les produits de cybersécurité,** dans l'optique de préserver et de renforcer l'autonomie stratégique de l'Union.

Les États membres devraient soutenir davantage l'industrie européenne de la cybersécurité et réduire les charges administratives, en particulier pour les PME innovantes, et promouvoir une coopération plus étroite avec les organismes de recherche universitaires afin de réduire les dépendances vis-à-vis des produits de cybersécurité provenant de sources externes et de créer une chaîne d'approvisionnement stratégique au sein de l'Union.

La résolution a demandé:

- une feuille de route pour une approche coordonnée de la cyberdéfense européenne;
- la mise en place d'une coopération internationale et d'initiatives multilatérales pour établir des cadres de cyberdéfense et de cybersécurité rigoureux en vue de lutter contre la captation de l'État par la corruption, la fraude financière, le blanchiment d'argent, le financement du terrorisme;
- de s'attaquer aux défis posés par le cyberterrorisme et par les cryptomonnaies et autres méthodes de paiement alternatives.

Sur le plan institutionnel, le Parlement a suggéré que les États membres lancent un **nouveau** programme de cybercoopération dans le cadre de la CSP afin de soutenir une planification, un commandement et un contrôle rapides et efficaces des opérations et des missions actuelles et futures de l'Union. Ce nouveau programme devrait permettre une meilleure coordination des capacités opérationnelles dans le cyberespace et pourrait aboutir à la création d'un **commandement commun de la cyberdéfense** lorsque le Conseil européen en décidera ainsi.