Cyberdéfense

2018/2004(INI) - 25/05/2018 - Rapport déposé de la commission, lecture unique

La commission des affaires étrangères a adopté un rapport d'initiative d'Urmas PAET (ALDE, EE) 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 rapport souligne 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, et à fournir les solutions politiques et pratiques nécessaires pour surmonter les derniers obstacles politiques, législatifs et organisationnels à la coopération en matière de cyberdéfense.

Les députés ont exhorté les États membres à **coopérer étroitement au développement de leur cyberdéfense respective**, en utilisant une feuille de route claire, alimentant ainsi un processus coordonné par la Commission, le Service européen pour l'action extérieure (SEAE) et l'Agence européenne de défense (AED) 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.

La Coopération structurée permanente (CSP) et le Fonds européen de défense (FED): ces deux nouvelles initiatives sont dotées de la portée nécessaire pour favoriser un écosystème pouvant offrir des opportunités aux PME et aux jeunes entreprises, et pour faciliter les projets de coopération dans le domaine de la cyberdéfense, et elles devraient contribuer à façonner le cadre réglementaire et institutionnel.

Les États membres sont invités à **utiliser au mieux le cadre fourni par la CSP et le FED** pour proposer des projets de coopération. Les députés se sont félicités du lancement de deux cyberprojets, à savoir une plateforme d'échange d'informations sur les cyberincidents et la création d'une équipe d'intervention rapide en cas de cyberincidents. Ils espèrent que cela conduira à la création d'une équipe européenne d' intervention rapide, qui coordonnerait, détecterait et contrerait les cyber-menaces collectives.

Éducation et formation: les députés estiment que la rationalisation du paysage européen de l'éducation et de la formation en matière de cyberdéfense atténuerait sensiblement les menaces. Ils appuient l'initiative de **l'Erasmus militaire** et d'autres initiatives communes de formation et d'échange visant à renforcer l'interopérabilité des forces armées des États membres et le développement d'une culture stratégique commune grâce à un échange accru de jeunes militaires. Ils soulignent la nécessité de renforcer la sensibilisation et l'expertise dans le domaine de la cybersécurité.

Coopération UE-OTAN en matière de cyberdéfense: le Conseil est invité à examiner les moyens d'apporter, dès que possible, 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 qu'une coopération accrue entre l'UE et l'OTAN est importante et utile dans le domaine de la cyberdéfense 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: notant le rôle central que les **entreprises privées** de cybersécurité jouent dans l'alerte précoce et l'attribution des cyber-attaques, les députés ont appelé toutes les parties prenantes à renforcer les partenariats de transfert de connaissances, à mettre en œuvre des modèles commerciaux appropriés et à développer la confiance entre les entreprises et les utilisateurs finaux civils et de la défense.

Un soutien plus concret devrait être apporté à **l'industrie européenne de la cybersécurité** et aux autres acteurs économiques concernés, afin de réduire les charges bureaucratiques, en particulier pour les PME, et de promouvoir une coopération plus étroite avec les organismes de recherche universitaires en vue de réduire la dépendance vis-à-vis des produits de cybersécurité provenant de sources extérieures et de créer une chaîne d'approvisionnement stratégique à l'intérieur de l'UE pour renforcer son autonomie stratégique.

À cet égard, les députés ont encouragé la Commission à intégrer des éléments de cyberdéfense dans un réseau de centres européens de compétence et de recherche en matière de cybersécurité, en vue de fournir des ressources suffisantes pour permettre le double usage des capacités et des cybertechnologies dans le cadre du prochain CFP.

Le rapport a également 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.

Renforcement institutionnel: les députés ont demandé :

- aux États membres de s'engager dans une coopération plus ambitieuse dans le domaine du cyberespace au sein de la CSP;
- aux États membres et à la Haute représentante de présenter un livre blanc de l'UE sur la sécurité et la défense;
- la création d'un Conseil de l'UE sur la défense;
- le maintien voire le renforcement du Fonds européen de défense dans le prochain CFP, avec un budget suffisant pour la cyberdéfense;
- des ressources accrues pour moderniser et rationaliser la cybersécurité et la diffusion du renseignement entre le SEAE/Centre de renseignement et de situation de l'Union européenne (INTCEN), le Conseil et la Commission.