État des capacités de cyberdéfense de l’Union

2020/2256(INI) - 07/10/2021 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 591 voix, 65 contre et 26 abstentions, une résolution sur l’état des capacités de cyberdéfense de l’Union.

État des capacités de cyberdéfense de l’Union

Les députés ont affirmé qu’une **politique de cyberdéfense commune** et une coopération accrue au niveau de l’Union visant à mettre en place des capacités communes et améliorées de cyberdéfense sont des éléments essentiels pour bâtir une Union européenne de la défense plus solide. La nature transfrontière du cyberespace, ainsi que le nombre important de cyberattaques et leur complexité croissante, nécessitent une **réaction coordonnée au niveau de l’Union**, y compris par la mobilisation des capacités de soutien communes des États membres et l’appui des États membres aux mesures prévues dans la «boîte à outils cyberdiplomatique de l’Union».

Le Parlement a invité le Service européen pour l’action extérieure (SEAE) et la Commission à poursuivre, en coopération avec les États membres, l’élaboration d’un **ensemble complet de mesures** et d’une politique cohérente en matière de sécurité informatique afin de renforcer la résilience, mais aussi la coordination en matière de cyberdéfense. Il a demandé le renforcement de la coopération avec l’équipe civile d’intervention en cas d’urgence informatique pour les institutions, organes et organismes de l’Union (CERT-UE) afin de protéger les réseaux utilisés par l’ensemble des institutions, des organes et des agences de l’Union.

Prenant acte de l’objectif du cadre stratégique de cyberdéfense de 2018 consistant à mettre en place un réseau CERT militaire de l’Union, les députés ont invité les États membres à **accroître les capacités de partage d’informations classifiées** et à mettre en place un réseau européen rapide et sécurisé de détection, d’évaluation et de lutte contre les cyberattaques. Ils ont souligné la nécessité **d’investir dans la cyberdéfense** en vue de renforcer la résilience et les capacités stratégiques de l’Union et de ses États membres.

Vision stratégique - Parvenir à la résilience en matière de cyberdéfense

Le Parlement a souligné qu’il était essentiel de **surmonter la fragmentation** et la complexité actuelles de l’architecture cyber globale au sein de l’Union et de définir une vision commune pour déterminer comment garantir la sécurité et la stabilité dans le cyberespace. Il a préconisé la création d’une **unité conjointe de cybersécurité** en vue de renforcer la coopération et de remédier à l’insuffisance du partage d’informations entre les institutions, les organes et les agences de l’Union.

Étant donné que les capacités de cyberdéfense comportent souvent une dimension duelle (civile et militaire), les députés ont rappelé que l’innovation technologique était principalement portée par des entreprises privées et que, par conséquent, la **coopération avec le secteur privé** et les parties prenantes civiles devrait être renforcée.

Le Parlement a également relevé que, contrairement à d’autres domaines militaires, l’infrastructure utilisée pour «créer» le cyberespace est principalement aux mains d’entités commerciales établies pour la plupart en dehors de l’Union, ce qui entraîne une dépendance industrielle et technologique vis-à-vis de tiers. L’Union devrait donc **renforcer sa souveraineté technologique** et stimuler l’innovation en investissant dans l’utilisation éthique de nouvelles technologies de sécurité et de défense, telles que l’ intelligence artificielle et l’informatique quantique.

En vue de surmonter la paralysie face aux menaces hybrides, les députés estiment que l'Union devrait s' efforcer de trouver une solution juridique qui prévoirait un **droit à une défense collective** et qui permettrait l'adoption par les États membres, sur la base du volontariat, de contre-mesures collectives.

Renforcer les partenariats et le rôle de l'Union dans le contexte international

Face à l'attitude systématiquement agressive dont font preuve notamment la Chine, la Russie et la Corée du Nord dans le cyberespace et aux nombreuses cyberattaques contre des institutions publiques et des entreprises privées, les députés estiment que l'Union et l'OTAN devraient se coordonner dans les domaines où des acteurs hostiles menacent les intérêts euro-atlantiques en matière de sécurité.

Les députés ont notamment recommandé :

- une **coopération plus étroite entre l'Union et l'OTAN**, notamment en ce qui concerne les exigences d' interopérabilité en matière de cyberdéfense;

- une meilleure coordination en matière de cyberdéfense entre les États membres, les institutions de l' Union, les alliés de l'OTAN, les Nations unies et l'Organisation pour la sécurité et la coopération en Europe (OSCE). Ils encouragent, à cet égard, la poursuite de la promotion des mesures de confiance de l' OSCE concernant le cyberespace;

- la mise en place d'un partenariat solide dans le domaine informatique avec le Royaume-Uni, qui est à la pointe en matière d'arsenal de cyberdéfense. La Commission est invitée à étudier la possibilité de relancer un processus visant à établir à l'avenir un cadre formel et structuré de coopération dans ce domaine.

Tous les États membres ainsi que l'Union sont invités à jouer un **rôle moteur** lors des discussions et initiatives menées sous les auspices des Nations unies, notamment en proposant un plan d'action, ainsi qu' à promouvoir un comportement responsable des États dans le cyberespace.