Informations de base

2020/2256(INI) INI - Procédure d'initiative	Procédure terminée
État des capacités de cyberdéfense de l'Union **Subject** 3.30.07 Cybersécurité, politique cyberespace 6.10.02 Politique de sécurité et de défense commune (PSDC); UEO, OTAN	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
AFET Affaires étrangères	PAET Urmas (Renew)	03/11/2020
	Rapporteur(e) fictif/fictive JUKNEVIČIENĖ Rasa (EPP) OLEKAS Juozas (S&D) GREGOROVÁ Markéta (Greens/EFA) KANKO Assita (ECR) BONFRISCO Anna (ID) WALLACE Mick (The Left)	

Commission européenne

DG de la Commission	Commissaire
Service européen pour l'action extérieure	BORRELL FONTELLES Josep

Evénements clés

Date	Evénement	Référence	Résumé
17/12/2020	Annonce en plénière de la saisine de la commission		
01/07/2021	Vote en commission		
16/07/2021	Dépôt du rapport de la commission	A9-0234/2021	Résumé
05/10/2021	Débat en plénière		
07/10/2021	Décision du Parlement	T9-0412/2021	Résumé

Informations techniques	
Référence de la procédure	2020/2256(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d'initiative
Base juridique	Règlement du Parlement EP 55
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	AFET/9/04848

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE689.479	22/03/2021	
Amendements déposés en commission		PE691.415	28/04/2021	
Rapport déposé de la commission, lecture unique		A9-0234/2021	16/07/2021	Résumé
Texte adopté du Parlement, lecture unique		T9-0412/2021	07/10/2021	Résumé

État des capacités de cyberdéfense de l'Union

2020/2256(INI) - 16/07/2021 - Rapport déposé de la commission, lecture unique

La commission des affaires étrangères a adopté un rapport d'initiative d'Urmas PAET (Renew, EE) sur l'état des capacités de cyberdéfense de l'Union.

Le rapport souligne 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.

Selon les députés, 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», ainsi que **l'intensification de la coopération UE-OTAN** sur la base du partage d'informations entre les équipes chargées de la gestion des crises cyber, le partage des bonnes pratiques et le renforcement de la formation, de la recherche et des exercices dans ce domaine.

Le rapport invite le 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 invite les États membres à accroître sensiblement les capacités de partage d'informations classifiées afin de faciliter le partage d'informations là où il est utile et nécessaire, et à mettre en place un **réseau européen** rapide et sécurisé de détection, d'évaluation et de lutte contre les cyberattaques.

Vision stratégique - Parvenir à la résilience en matière de cyberdéfense

Le rapport souligne qu'il est 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. Les députés recommandent, entre autres:

- **d'accroître les ressources financières et humaines** consacrées à la cyberdéfense, en particulier le nombre d'analystes en cyberrenseignement et d' experts en investigation numérique, ainsi que d'améliorer leur formation dans les domaines de la réaction aux incidents informatiques et des enquêtes à leur sujet, y compris leurs compétences en matière de cybersécurité;

- **d'augmenter le financement de la CERT-UE** *(Computer Emergency Response Team*) et du Centre de situation et du renseignement de l'UE (INTCEN) et d'apporter un soutien plus appuyé aux États membres pour la création et le renforcement des centres d'opérations de sécurité (COS) afin de former un réseau de COS couvrant toute l'Union;

- **d'encourager la conclusion de partenariats avec le monde universitaire** visant à promouvoir des programmes de recherche et développement en matière de cybersécurité afin de développer de nouveaux outils communs ainsi que des compétences communes applicables à la fois au secteur civil et au secteur militaire;

- **de sensibiliser le public et d'améliorer les compétences des citoyens** afin qu'ils puissent se défendre contre les cyberattaques.

Le rapport préconise 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. Il appelle de ses vœux **un programme de «souveraineté numérique européenne»** afin de renforcer les capacités actuelles en matière d'outils cyber et de chiffrement, sur la base des droits fondamentaux européens, avec pour objectif d'améliorer la compétitivité de l'Europe sur le marché de la cybersécurité et de stimuler la demande intérieure.

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.

Selon le rapport, la coopération entre l'Union et l'OTAN devrait se concentrer sur les problèmes concernant les domaines du cyber, des menaces hybrides, des technologies émergentes et disruptives, de l'espace, du contrôle des armements et de la non-prolifération. Les députés appellent à une coopération entre l'Union et l'OTAN garantissant des réseaux à haut débit résilients, abordables et sécurisés conformes aux normes de sécurité européennes et nationales et permettant de sécuriser des réseaux d'information nationaux et internationaux capables de chiffrer les données et les communications sensibles.

Les députés recommandent notamment:

- **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.

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.