Centre européen de compétences en matière de cybersécurité

2018/0328(COD) - 12/09/2018 - Document annexé à la procédure

Le document de travail des services de la Commission résume l**'analyse d'impact** accompagnant la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

Nécessité d'une action : l'initiative proposée a pour objectif :

- de veiller à ce que l'UE conserve et développe les capacités essentielles (technologiques et industrielles) pour **sécuriser de manière autonome son économie numérique**, la société et la démocratie et, d'autre part, à ce que les États membres bénéficient des solutions de cybersécurité et des capacités de cyberdéfense les plus avancées;
- de **renforcer la compétitivité au niveau mondial des entreprises de l'UE** spécialisées dans la cybersécurité et de veiller à ce que les industries européennes dans différents secteurs aient accès aux capacités et aux ressources dont elles ont besoin pour faire de la cybersécurité un avantage concurrentiel.

Pour ce faire, elle vise à remédier aux problèmes suivants :

1) le **niveau insuffisant de coordination et de coopération stratégiques** et durables entre les industries, les communautés de la recherche dans le domaine de la cybersécurité et les gouvernements, qui ne permet pas de développer des solutions européennes de pointe en matière de cybersécurité;

2) des **investissements réalisés à trop petite échelle** et un accès limité aux infrastructures, aux compétences et au savoir-faire en matière de cybersécurité à travers l'Europe;

3) le fait que les **résultats européens de la recherche** et de l'innovation dans le domaine de la cybersécurité ne sont que rarement convertis en solutions commercialisables ou déployés dans l' ensemble de l'économie.

Solutions: plusieurs options envisageables, législatives ou non, ont été prises en considération.

L'option retenue est la création d'un **Réseau de centres de compétences en cybersécurité avec un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité** habilité à prendre des mesures en faveur des technologies industrielles ainsi que dans le domaine de la recherche et de l'innovation.

La création du Centre de compétences serait fondée sur une double base juridique en raison de sa nature et de ses objectifs spécifiques, à savoir **l'article 187 et l'article 173 du TFUE**.

L'analyse a montré que cette option est la plus appropriée pour atteindre les objectifs de l'initiative, tout en assurant les meilleures retombées économiques, sociétales et environnementales et en préservant au mieux les intérêts de l'Union. L'initiative apporterait une **valeur ajoutée** aux efforts actuels déployés au niveau national :

- en contribuant à créer un **écosystème** industriel et de recherche en matière de cybersécurité à l' échelle européenne;
- en encourageant une **meilleure coopération** entre les parties prenantes (notamment entre les secteurs civil et militaire de la cybersécurité) afin d'utiliser au mieux les ressources et l'expertise existantes réparties dans toute l'Europe.

Incidences de l'option privilégiée: les avantages escomptés seraient les suivants :

- possibilité pour les autorités publiques et aux industries des États membres de **lutter plus efficacement contre les cybermenaces** et de mieux y réagir en se dotant de produits et solutions plus sûrs, notamment en ce qui concerne l'accès aux services essentiels (par exemple, les transports, la santé, les services bancaires et financiers);
- création d'un **mécanisme capable de renforcer les capacités industrielles** des États membres et de l'Union en matière de cybersécurité et de convertir efficacement l'excellence scientifique européenne en solutions commercialisables pouvant être déployées dans l'ensemble de l'économie;
- mise en commun des ressources pour investir dans les capacités nécessaires au niveau des États membres et développer des actifs européens communs tout en réalisant des économies d'échelle;
- possibilité pour les **PME**, les industries et les chercheurs de disposer d'un accès accru aux infrastructures;
- **réduction des coûts** liés à la conception de nouveaux produits pour les PME et possibilité d' accéder plus facilement à la communauté des investisseurs et d'attirer les financements nécessaires pour déployer des solutions commercialisables;
- davantage de moyens pour permettre à la **communauté de la défense** et à la sphère civile de travailler ensemble sur des défis communs;
- renforcement de la cohérence et des **synergies** entre les différents mécanismes de financement;
- **incidence positive indirecte sur l'environnement** en permettant de mettre au point des solutions de cybersécurité spécifiques pour les secteurs ayant potentiellement un impact environnemental énorme (par exemple, les centrales nucléaires).

Selon la Commission, la présente initiative a une incidence clairement positive puisqu'elle est susceptible d'augmenter considérablement les capacités des États membres à sécuriser de manière autonome leurs économies, y compris à protéger les secteurs critiques et à renforcer la compétitivité des entreprises et industries européennes spécialisées dans la cybersécurité dans différents secteurs.

À terme, cela devrait permettre à l'UE de **se hisser au rang de chef de file** dans le domaine des technologies numériques et de cybersécurité de prochaine génération.