COMMISSION
EUROPÉENNE

Bruxelles, le 12.9.2018
SWD(2018) 404 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document:

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Résumé de l'analyse d'impact

Analyse d'impact relative à la proposition de création du Réseau de centres de compétences et du Centre européen de recherche et de compétences en matière de cybersécurité

A. Nécessité d'une action

Pourquoi? Quel est le problème abordé?

L'Union européenne (UE) ne dispose toujours pas, à l'heure actuelle, des capacités technologiques et industrielles suffisantes pour sécuriser de manière autonome son économie et ses infrastructures critiques et pour se hisser au rang de chef de file mondial dans le domaine de la cybersécurité. La présente initiative a pour objectif de contribuer à remédier aux problèmes suivants et aux facteurs responsables de cette situation, à savoir:

Problème n° 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 ne permet pas de protéger l'économie, la société et la démocratie avec des solutions européennes de pointe en matière de cybersécurité.

Problème n° 2: les investissements sont réalisés à trop petite échelle et l'accès aux infrastructures, aux compétences et au savoir-faire en matière de cybersécurité à travers l'Europe est limité.

Problème n° 3: 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.

Les sources sous-jacentes de ces problèmes sont multiples: manque de confiance entre les différents acteurs du marché de la cybersécurité, limitations inhérentes aux mécanismes de coopération et de regroupement des fonds existants, absence de cadre pour la passation conjointe de marchés pour des infrastructures et produits/solutions de cybersécurité coûteux, ou encore inexploitation du potentiel des mécanismes de pression et d'attraction du marché.

Quels objectifs cette initiative devrait-elle atteindre?

L'initiative a pour objectif de veiller, d'une part, 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. L'initiative vise également à renforcer la compétitivité au niveau mondial des entreprises de l'UE spécialisées dans la cybersécurité et à 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. Ces objectifs devraient être atteints en développant des mécanismes efficaces de coopération stratégique à long terme entre tous les acteurs concernés (autorités publiques, industries, communauté de la recherche des sphères civile et militaire), en mettant en commun les connaissances et les ressources pour fournir des capacités et infrastructures de pointe, en encourageant le déploiement à grande échelle de produits et solutions européens de cybersécurité dans toute l'économie et le secteur public, en soutenant les start-ups et les PME spécialisées dans le domaine de la cybersécurité et en comblant le déficit de compétences en cybersécurité.

Quelle est la valeur ajoutée d'une action à l'échelle 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. Elle devrait encourager 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. Elle devrait aussi aider l'UE et les États membres à adopter une approche à plus long terme, proactive et stratégique afin de mener une politique industrielle en matière de cybersécurité qui aille au-delà des seuls domaines de la recherche et du développement. Cette approche devrait contribuer non seulement à faire surgir des solutions innovantes aux défis auxquels sont confrontés les secteurs privé et public en matière de cybersécurité, mais aussi à soutenir le déploiement efficace de ces solutions. Elle permettra aussi aux communautés concernées dans les sphères de l'industrie et de la recherche, ainsi qu'aux pouvoirs publics, d'accéder aux capacités essentielles telles que les infrastructures d'essais et d'expérimentation, qui ne sont pas à

la portée d'un État membre seul, faute de ressources financières et humaines suffisantes. Elle contribuera aussi à combler le déficit de compétences et à éviter la fuite des cerveaux en assurant aux meilleurs talents un accès à des projets européens de grande envergure et en leur offrant ainsi des défis professionnels intéressants. Tous ces éléments sont également considérés comme nécessaires pour permettre à l'Europe d'être mondialement reconnue en tant que chef de file de la cybersécurité.

B. Solutions

Quelles sont les options législatives et non législatives envisagées? Y a-t-il une option privilégiée? Pourquoi?

Plusieurs options envisageables, législatives ou non, ont été prises en considération. Les options suivantes ont été retenues en vue d'une évaluation approfondie:

1. **Scénario de référence**: option collaborative qui prévoit de poursuivre l'approche actuelle en ce qui concerne le renforcement des capacités industrielles et technologiques en matière de cybersécurité dans l'UE en soutenant la recherche et l'innovation et les mécanismes de collaboration connexes dans le cadre du programme «Horizon Europe».
2. **Option 1:** 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.
3. **Option 2:** création d'un Réseau de centres de compétences en cybersécurité avec un Centre européen de recherche et de compétences en matière de cybersécurité dont les activités seraient limitées à la recherche et à l'innovation.

Les options écartées à un stade précoce incluaient 1) l'absence d'action; 2) la création d'un réseau regroupant uniquement des centres de compétences existants et 3) le recours à une agence existante (ENISA, REA ou INEA).

Compte tenu de la volonté générale déjà exprimée par la Commission de mettre en œuvre la présente initiative, ainsi que du rôle important que les États membres devront jouer à cet égard, la principale différence entre les deux options ayant fait l'objet d'une analyse plus approfondie réside dans leur champ d'application, ainsi qu'il ressort de leur base juridique: une entité fondée uniquement sur la base de l'article 187 du TFUE (option 2) limiterait le champ d'application de l'initiative à la sphère de la recherche et de l'innovation, et supposerait une contribution financière du secteur privé. En revanche, une entité fondée sur une double base juridique, à savoir l'article 187 et l'article 173 du TFUE (option 1), disposerait d'un mandat plus large qui permettrait de couvrir également, notamment, le déploiement et le soutien à l'industrie et de créer des synergies plus fortes avec le secteur de la cyberdéfense. Elle permettrait par ailleurs d'accorder un rôle plus important aux États membres — tant en termes de gouvernance que d'achats potentiels de technologies de cybersécurité.

L'analyse a montré que l'option 1 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. Les principaux arguments en faveur de cette option sont sa flexibilité permettant à la communauté et au Réseau de centres de compétences de coopérer selon différents modèles afin d'optimiser l'utilisation des ressources et des connaissances existantes; sa capacité à structurer la coopération des parties prenantes publiques et privées provenant de tous les secteurs concernés, y compris la défense; et sa capacité à élaborer une véritable politique industrielle dans le domaine de la cybersécurité en soutenant des activités liées non seulement à la recherche et au développement mais aussi au déploiement sur le marché. Dernier point, mais non des moindres, l'option 1 permet aussi d'accroître la cohérence en agissant en tant que mécanisme de mise en œuvre pour le financement de la cybersécurité au titre du programme pour une Europe numérique et du programme «Horizon Europe», et de renforcer les synergies entre les dimensions civile et militaire de la cybersécurité en rapport avec le Fonds européen de la défense.

Qui soutient quelle option?

Il ressort de la consultation et du processus de collecte de données qu'il existe une demande manifeste pour que les milieux de l'industrie et de la recherche disposent d'un mécanisme permettant à l'UE de mener une politique industrielle cohérente en matière de cybersécurité qui aille au-delà des activités de R&D et, partant, de devenir un

chef de file mondial dans le domaine de la cybersécurité. Dans le même temps, les parties prenantes ont souligné que, pour y parvenir, il faudra, d'une part, définir précisément le rôle du Centre en termes de soutien et de facilitation des efforts déployés par le Réseau et les communautés concernées et, d'autre part, adopter une approche inclusive et collaborative à l'égard du Réseau afin d'éviter l'apparition de tout nouveau cloisonnement. Il faudrait également veiller à la souplesse de la structure, afin de pouvoir l'adapter facilement à l'évolution rapide de la cybersécurité. Tout au long du processus, les États membres ont insisté sur la nécessité d'être inclusif à l'égard de tous les États membres et de leurs centres d'excellence et de compétences existants et d'accorder une attention particulière à la complémentarité des actions. En ce qui concerne plus spécifiquement le Centre, les États membres ont souligné l'importance de son rôle de coordination du Réseau et de soutien à celui-ci. Par conséquent, toute initiative de la Commission devra trouver le juste équilibre entre les structures de gouvernance et de mise en œuvre et refléter cet équilibre dans lesdites structures pour garantir une coordination efficace au niveau européen tout en tenant compte des évolutions au niveau national.

C. Incidences de l'option privilégiée

Quels sont les avantages de l'option privilégiée (ou, à défaut, des options principales)?

L'option privilégiée permettra aux autorités publiques et aux industries des États membres de lutter plus efficacement contre les cybermenaces et de mieux y réagir en proposant et en se dotant de produits et solutions plus sûrs. Cela vaut tout particulièrement pour la protection de l'accès aux services essentiels (par exemple, les transports, la santé, les services bancaires et financiers). Elle aurait également une incidence positive sur la compétitivité de l'UE et ses PME, étant donné qu'elle prévoit la 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. Cette option permet la 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. Cela est susceptible de permettre aux PME, aux industries et aux chercheurs de disposer d'un accès accru aux infrastructures, ce qui stimulera l'innovation et raccourcira les processus de développement. Cela permettra également de réduire les coûts pour certaines entreprises du côté de la demande et de les aider à faire de la cybersécurité un avantage concurrentiel. L'option privilégiée permet de tirer parti des débouchés commerciaux à double usage en offrant à la communauté de la défense et à la sphère civile les moyens de travailler ensemble sur des défis communs. Elle est également susceptible d'apporter une valeur ajoutée aux efforts nationaux déployés pour remédier au déficit de compétences en cybersécurité. Au niveau de l'UE, cette option permet aussi de renforcer la cohérence et les synergies entre les différents mécanismes de financement.

Enfin, elle pourrait avoir une 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) en les aidant à éviter les conséquences potentiellement dévastatrices des cyberattaques contre ce type d'infrastructure.

Quels sont les coûts de l'option privilégiée (ou, à défaut, des options principales)?

Les coûts de l'option privilégiée sont essentiellement liés au fonctionnement du Centre et des centres nationaux de coordination. Les coûts liés à la mise en œuvre des différents programmes de financement (programme pour une Europe numérique et programme «Horizon Europe») font l'objet d'analyses d'impact distinctes.

Quelle sera l'incidence sur les entreprises, les PME et les microentreprises?

Les entreprises européennes, tant du côté de l'offre que du côté de la demande, y compris les PME et les microentreprises actives dans le domaine de la cybersécurité, feront partie des groupes de parties prenantes les plus impactés. La structure du Centre de compétences et du Réseau n'aura pas pour effet de leur imposer des obligations réglementaires, mais elle ouvrira des perspectives en termes de réduction des coûts liés à la conception de nouveaux produits et elle leur permettra d'accéder plus facilement à la communauté des investisseurs et d'attirer les financements nécessaires pour déployer des solutions commercialisables. Dans le cas des PME et des microentreprises, l'accès aux infrastructures d'essais et d'expérimentation financées par des fonds publics est encore plus important puisqu'elles manquent de ressources pour acheter ou pénétrer sur d'autres marchés (souvent en dehors de l'UE) afin de trouver les infrastructures nécessaires. Il est également à espérer que la présente initiative ouvrira de nouveaux marchés pour les PME et les microentreprises européennes actives dans le domaine de la cybersécurité. Par ailleurs, le mécanisme retenu garantira la coordination entre les

communautés de la recherche et de l'industrie et permettra donc d'orienter les efforts de recherche vers des besoins industriels concrets. La fourniture d'une expertise et d'outils de pointe en matière de cybersécurité aidera indirectement les opérateurs économiques à se conformer à la directive SRI.

Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?

L'initiative permettra aux États membres de coordonner les investissements dans les infrastructures de cybersécurité nécessaires aux niveaux national et européen. Le mécanisme permettra de regrouper les ressources pour les outils et les infrastructures qui seraient sinon plus coûteux ou hors de prix pour les différents États membres. Une telle approche permettrait de diminuer les coûts par un effet d'échelle et de rationalisation. La contribution financière des États membres au Centre de compétences et aux actions à mener devraient être proportionnelles à la contribution de l'Union.

Y aura-t-il d'autres incidences notables?

Oui, 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; les États membres seront à même de sécuriser suffisamment leurs actifs existants et de concevoir des produits innovants et sûrs tout en réduisant les coûts de R&D dans le domaine de la sécurité. 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.

D. Suivi

Quand la législation sera-t-elle réexaminée?

Une clause explicite relative au suivi des indicateurs de performance clés (IPC) ainsi qu'une clause d'évaluation et de révision, qui prévoit que la Commission européenne procédera à une évaluation intermédiaire afin d'évaluer l'incidence de l'instrument et sa valeur ajoutée, seront intégrées dans l'instrument juridique. La Commission européenne transmettra ensuite au Parlement européen et au Conseil un rapport sur son évaluation. À la suite de cette évaluation, la Commission pourra proposer une révision et une prorogation du mandat du Centre de compétences et du Réseau.