COM(2018) 630 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION EXTRAORDINAIRE DE 2017-2018

Reçu à la Présidence de l'Assemblée nationale
le 20 septembre 2018

Enregistré à la Présidence du Sénat
le 20 septembre 2018

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

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

E 13440

Conseil de
l'Union européenne

Bruxelles, le 14 septembre 2018
(OR. en)

12104/18

Dossier interinstitutionnel:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

NOTE DE TRANSMISSION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	12 septembre 2018
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2018) 630 final
Objet:	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

Les délégations trouveront ci-joint le document COM(2018) 630 final.

p.j.: COM(2018) 630 final

COMMISSION
EUROPÉENNE

Bruxelles, le 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

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

Contribution de la Commission européenne à la réunion des dirigeants des 19 et 20 septembre 2018 à Salzbourg

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

À mesure que la vie quotidienne et les économies deviennent de plus en plus tributaires des technologies numériques, les citoyens sont de plus en plus exposés à des cyberincidents graves. La sécurité future dépend du renforcement de la capacité à protéger l'Union contre les cybermenaces, car tant les infrastructures civiles que les capacités militaires reposent sur des systèmes numériques sûrs.

Afin de relever les défis de plus en plus nombreux, l'Union n'a cessé de renforcer ses activités dans ce domaine, en s'appuyant sur la stratégie de cybersécurité de 2013[1] et ses objectifs et principes pour favoriser un cyberécosystème fiable, sûr et ouvert. En 2016, l'Union a adopté une première série de mesures dans le domaine de la cybersécurité par l'intermédiaire de la directive (UE) 2016/1148 du Parlement européen et du Conseil[2] relative à la sécurité des réseaux et des systèmes d'information.

Compte tenu de l'évolution rapide de la cybersécurité, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont présenté, en septembre 2017, une communication conjointe[3] intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» afin de renforcer encore la résilience, la dissuasion et la capacité de réaction de l'Union face aux cyberattaques. La communication conjointe, qui s'appuie également sur des initiatives antérieures, a défini un ensemble d'actions proposées, notamment le renforcement de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), la création d'un cadre de certification volontaire à l'échelle de l'Union en matière de cybersécurité afin d'accroître la cybersécurité des produits et services dans le monde numérique, ainsi qu'un projet de réponse rapide et coordonnée aux incidents et crises de cybersécurité majeurs.

Dans cette communication conjointe, la Commission a reconnu qu'il était également dans l'intérêt stratégique de l'Union de veiller à maintenir et à développer des capacités technologiques essentielles en matière de cybersécurité pour consolider son marché unique numérique, et notamment pour protéger les réseaux et les systèmes d'information critiques et pour fournir des services clés en matière de cybersécurité. L'Union doit être en mesure d'assurer de façon autonome la sécurité de ses actifs numériques et d'être compétitive sur le marché mondial de la cybersécurité.

À l'heure actuelle, l'Union est un importateur net de produits et de solutions de cybersécurité et dépend dans une large mesure de fournisseurs non européens[4]. Sur le plan mondial, le marché de la cybersécurité, qui pèse 600 milliards d'EUR, devrait croître d'environ 17 % en moyenne au cours des cinq prochaines années en matière de ventes, de nombre d'entreprises

---

1 COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL: Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, JOIN(2013) 1 final.

2 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

3 COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL: «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide», JOIN(2017) 450 final.

4 Projet de rapport final sur l'étude du marché de la cybersécurité, 2018.

et d'emplois. Cependant, parmi les 20 pays à la pointe en matière de cybersécurité du point de vue du marché, on ne recense que six États membres[5].

Dans le même temps, l'Union dispose d'une expertise et d'une expérience considérables en matière de cybersécurité: plus de 660 organisations de toute l'UE ont participé à la récente enquête de la Commission répertoriant les centres d'expertise en cybersécurité[6]. Cette expertise, si elle est transformée en produits et solutions commercialisables, pourrait permettre à l'Union de couvrir l'ensemble de la chaîne de valeur de la cybersécurité. Cependant, les efforts de la communauté scientifique et des milieux industriels sont fragmentés, non harmonisés et caractérisés par l'absence d'une mission commune, ce qui entrave la compétitivité de l'UE dans ce domaine ainsi que sa capacité à sécuriser ses actifs numériques. Les secteurs de la cybersécurité (par exemple, l'énergie, l'espace, la défense, les transports) et les sous-domaines concernés ne bénéficient pas, à l'heure actuelle, d'un soutien suffisant[7]. Les synergies entre les secteurs civil et militaire de la cybersécurité ne sont pas non plus pleinement exploitées en Europe.

La création, en 2016, du partenariat public-privé sur la cybersécurité (PPPc) dans l'Union a constitué une première étape solide rassemblant les communautés de la recherche, de l'industrie et du secteur public afin de faciliter la recherche et l'innovation dans le domaine de la cybersécurité et, dans les limites du cadre financier 2014-2020, les résultats obtenus dans le domaine de la recherche et de l'innovation devraient être plus ciblés. Le PPPc a permis aux partenaires industriels de prendre des engagements à l'égard de leurs dépenses individuelles dans les domaines définis dans le programme stratégique de recherche et d'innovation du partenariat.

Toutefois, l'Union peut réaliser des investissements à plus grande échelle et doit disposer d'un mécanisme plus efficace qui permettrait de renforcer durablement les capacités, de mettre en commun les efforts et les compétences et de stimuler le développement de solutions innovantes pour relever les défis industriels en matière de cybersécurité dans le domaine des nouvelles technologies à usages multiples (par exemple, l'intelligence artificielle, l'informatique quantique, les chaînes de blocs et les identités numériques sûres) ainsi que dans des secteurs essentiels (par exemple, les transports, l'énergie, la santé, les services financiers, l'administration, les télécommunications, l'industrie manufacturière, la défense, l'espace).

La communication conjointe a examiné la possibilité de renforcer les capacités de l'Union en matière de cybersécurité au moyen d'un Réseau de centres de compétences en cybersécurité ayant comme pierre angulaire un Centre de compétences européen en matière de cybersécurité. Il s'agirait de compléter les efforts actuels de renforcement des capacités dans ce domaine au niveau de l'Union et au niveau national. Dans la communication conjointe, la Commission a exprimé son intention de lancer une analyse d'impact en 2018 afin d'examiner les options disponibles en vue de la mise en place de la structure. Dans un premier temps, et pour alimenter la réflexion, la Commission a lancé une phase pilote dans le cadre d'Horizon 2020 afin de contribuer à la mise en réseau des centres nationaux pour insuffler un nouvel élan en ce qui concerne le développement des compétences et des technologies en matière de cybersécurité.

---

5 Projet de rapport final sur l'étude du marché de la cybersécurité, 2018.

6 Rapports techniques du JRC: Centres européens d'expertise en matière de cybersécurité, 2018.

7 Rapports techniques du JRC: Résultats de l'exercice de cartographie (voir annexes 4 et 5 pour plus de précisions).

Lors du sommet numérique de Tallinn, en septembre 2017, les chefs d'État et de gouvernement ont enjoint l'Union de devenir «un acteur mondial de premier plan dans le domaine de la cybersécurité d'ici à 2025, afin de s'assurer de la confiance de nos citoyens, consommateurs et entreprises, d'assurer leur protection en ligne et de permettre un internet libre et réglementé».

Dans ses conclusions[8] adoptées en novembre 2017, le Conseil a invité la Commission à fournir rapidement une analyse d'impact sur les options envisageables et à proposer, d'ici la mi-2018, l'instrument juridique pertinent pour la mise en œuvre de l'initiative.

Le *programme pour une Europe numérique*[9] proposé par la Commission en juin 2018 vise à étendre et à maximiser les avantages de la transformation numérique pour les citoyens et les entreprises européens dans tous les domaines d'action pertinents de l'Union, en renforçant les politiques et en soutenant les ambitions du marché unique numérique. Le programme propose une approche cohérente et globale visant à assurer une utilisation optimale des technologies de pointe et la bonne combinaison de capacités techniques et de compétences humaines pour la transformation numérique (non seulement dans le domaine de la cybersécurité, mais aussi en ce qui concerne les infrastructures de données intelligentes, l'intelligence artificielle, les compétences et applications de pointe dans l'industrie et dans des domaines d'intérêt public). Ces éléments sont interdépendants, se renforcent mutuellement et, lorsqu'ils sont encouragés simultanément, peuvent atteindre le niveau nécessaire pour permettre à une économie fondée sur les données de prospérer[10]. La cybersécurité figure également parmi les priorités du *programme Horizon Europe*[11], le prochain programme-cadre de l'Union européenne en matière de recherche et d'innovation.

Dans ce contexte, le présent règlement propose la création d'un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, associé à un Réseau des centres nationaux de coordination. Pour stimuler l'écosystème industriel et technologique de la cybersécurité en Europe, le fonctionnement de ce modèle de coopération ad hoc devrait être le suivant: le Centre de compétence facilitera et aidera à coordonner les travaux du Réseau et à dynamiser la communauté des compétences en matière de cybersécurité, en faisant progresser l'agenda technologique et en facilitant l'accès à l'expertise ainsi acquise. À cet effet, le Centre de compétence mettra notamment en œuvre des parties pertinentes des programmes Europe numérique et Horizon Europe, à travers l'attribution de subventions et la passation de marchés. Compte tenu des investissements considérables consacrés à la cybersécurité dans d'autres parties du monde, et de la nécessité de coordonner et de mettre en commun les ressources pertinentes en Europe, il est proposé de mettre sur pied le Centre de compétences sous la forme d'un partenariat européen[12], ce qui

---

8 Conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide», adoptées par le Conseil «Affaires générales» le 20 novembre 2017.

9 COM(2018) 434, Proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027.

10 Voir le document SWD(2018) 305.

11 COM(2018) 435, Proposition de règlement du Parlement européen et du Conseil portant établissement du programme-cadre pour la recherche et l'innovation «Horizon Europe» et définissant ses règles de participation et de diffusion.

12 Tel que défini dans la proposition de règlement du Parlement européen et du Conseil portant établissement du programme-cadre pour la recherche et l'innovation «Horizon Europe» et définissant ses règles de participation et de diffusion, COM(2018) 435; et tel que mentionné dans la proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027, COM(2018) 434.

facilitera des investissements conjoints de la part de l'Union, des États membres et/ou de l'industrie. Par conséquent, la proposition prévoit que les États membres contribuent de manière proportionnée aux actions du Centre de compétences et du Réseau. L'organe décisionnel principal est le conseil de direction, où tous les États membres sont représentés. Cependant, seuls les États membres qui participent financièrement disposent du droit de vote. Le mécanisme de vote au sein du conseil de direction suit le principe d'une double majorité, exigeant 75 % des contributions financières et 75 % des voix. En raison de sa responsabilité à l'égard du budget de l'Union, la Commission détient 50 % des voix. Pour les besoins de ses tâches au conseil de direction, la Commission fera appel, s'il y a lieu, à l'expertise du Service européen pour l'action extérieure. Le conseil de direction est assisté d'un comité consultatif industriel et scientifique, afin d'assurer un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties prenantes concernées.

En étroite collaboration avec le Réseau des centres nationaux de coordination et la communauté des compétences en cybersécurité (faisant intervenir un groupe important et varié d'acteurs associés au développement des technologies de cybersécurité, tels que les entités de recherche, les secteurs de l'offre, les secteurs de la demande et le secteur public) établis par le présent règlement, le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité serait le principal organe de mise en œuvre des ressources financières de l'UE consacrées à la cybersécurité dans le cadre du programme pour une Europe numérique et du programme «Horizon Europe».

Une telle approche globale permettrait de soutenir la cybersécurité tout au long de la chaîne de valeur, de la recherche à l'appui du déploiement et de l'adoption des technologies clés. La participation financière des États membres devrait être proportionnelle à la contribution financière de l'Union à la présente initiative et constitue un élément indispensable à sa réussite.

Compte tenu de ses compétences particulières et de sa représentation large et pertinente des parties prenantes, l'Organisation européenne pour la cybersécurité, qui est l'homologue de la Commission dans le cadre du partenariat public-privé contractuel en matière de cybersécurité au titre d'Horizon 2020, devrait être invitée à contribuer aux travaux du Centre et du Réseau.

En outre, le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité devrait également s'efforcer d'améliorer les synergies entre les dimensions civile et militaire de la cybersécurité. Il devrait apporter un soutien aux États membres et aux autres acteurs concernés en fournissant des conseils, en partageant les compétences et en facilitant la collaboration en ce qui concerne les projets et les actions. À la demande des États membres, il pourrait également jouer le rôle de gestionnaire de projet, notamment en ce qui concerne le Fonds européen de la défense. La présente initiative vise à contribuer à résoudre les problèmes suivants:

- **Coopération insuffisante entre les secteurs de la demande et de l'offre de cybersécurité.** Les entreprises européennes doivent relever le défi de la sécurité et de l'offre de produits et de services sûrs à leurs clients. Pourtant, elles ne sont bien souvent pas en mesure d'assurer une protection appropriée de leurs produits, services et actifs existants ou de concevoir des produits et des services innovants et sûrs. Les principaux actifs dans le domaine de la cybersécurité sont souvent trop coûteux pour être développés et mis en place par des acteurs individuels, dont l'activité principale n'est pas liée à la cybersécurité. Dans le même temps, les liens entre la demande et l'offre sur le marché de la cybersécurité ne sont pas suffisamment développés, ce qui se traduit par une offre non

optimale de produits et de solutions européens adaptés aux besoins de différents secteurs, ainsi que par un manque de confiance parmi les acteurs du marché.

- **Absence de mécanisme de coopération efficace entre les États membres pour le renforcement des capacités industrielles.** À l'heure actuelle, il n'existe pas non plus de mécanisme de coopération efficace permettant aux États membres de travailler ensemble au renforcement des capacités nécessaires pour soutenir l'innovation en matière de cybersécurité dans tous les secteurs industriels et le déploiement de solutions européennes de pointe en matière de cybersécurité. Les mécanismes de coopération existants pour les États membres dans le domaine de la cybersécurité établis au titre de la directive (UE) 2016/1148 ne prévoient pas ce type d'activités dans le cadre de leur mandat.
- **Coopération insuffisante au sein des communautés de la recherche et de l'industrie et entre celles-ci.** Malgré la capacité théorique de l'Europe de couvrir l'ensemble de la chaîne de valeur de la cybersécurité, certains secteurs (par exemple, l'énergie, l'espace, la défense, les transports) et sous-domaines pertinents de la cybersécurité sont aujourd'hui insuffisamment soutenus par la communauté scientifique, ou uniquement soutenus par un nombre limité de centres (par exemple, la cryptographie quantique et post-quantique, la confiance et la cybersécurité en ce qui concerne l'intelligence artificielle). Bien que cette collaboration existe manifestement, il s'agit très souvent d'un arrangement à court terme de type consultation, qui ne permet pas de s'engager dans des projets de recherche à long terme pour résoudre les problèmes industriels liés à la cybersécurité.
- **Coopération insuffisante entre les communautés civile et militaire dans le domaine de la recherche et de l'innovation en matière de cybersécurité.** Le problème du niveau insuffisant de coopération concerne également les communautés civile et militaire. Les synergies existantes ne sont pas pleinement exploitées en raison du manque de mécanismes efficaces permettant à ces communautés de coopérer efficacement et d'instaurer un climat de confiance qui, même plus que dans d'autres domaines, est une condition préalable à une coopération fructueuse. Cette situation s'accompagne de capacités financières limitées sur le marché européen de la cybersécurité, notamment de fonds insuffisants pour soutenir l'innovation.
- **Cohérence avec les dispositions existantes dans le domaine d'action**

Le Réseau de compétences en cybersécurité et le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité apporteront un soutien supplémentaire aux dispositions et aux acteurs existants en matière de politique de cybersécurité. Le mandat du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité complétera les efforts déployés par l'ENISA, mais il a une orientation différente et fait appel à un autre ensemble de compétences. Bien que le mandat de l'ENISA prévoie un rôle de conseil en matière de recherche et d'innovation dans le domaine de la cybersécurité dans l'Union européenne, le mandat proposé se concentre avant tout sur d'autres tâches essentielles au renforcement de la résilience en matière de cybersécurité dans l'Union. En outre, le mandat de l'ENISA ne prévoit pas les types d'activités qui seraient les tâches essentielles du Centre et du Réseau, à savoir stimuler le développement et le déploiement des technologies en matière de cybersécurité et compléter les efforts de renforcement des capacités dans ce domaine au niveau de l'Union et au niveau national.

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, ainsi que le Réseau de compétences en cybersécurité, œuvreront également à soutenir la recherche pour faciliter et accélérer les processus de normalisation et de

certification, en particulier ceux liés aux systèmes de certification de cybersécurité au sens de la proposition de législation sur la cybersécurité[13] [14].

La présente initiative renforce de facto le partenariat public-privé en matière de cybersécurité (PPPc), qui était la première tentative, à l'échelle de l'UE, de réunir le secteur de la cybersécurité, le côté de la demande (acheteurs de produits et de solutions de cybersécurité, y compris l'administration publique et les secteurs critiques tels que les transports, la santé, l'énergie, les services financiers) et la communauté scientifique, afin de créer une plateforme de dialogue durable et de créer les conditions d'un co-investissement volontaire. Le PPPc a été créé en 2016 et aura généré jusqu'à 1,8 milliard d'EUR d'investissements d'ici à 2020. Toutefois, l'ampleur des investissements en cours dans d'autres parties du monde (par exemple, les États-Unis ont investi 19 milliards de dollars dans la cybersécurité rien qu'en 2017) montre que l'Union européenne doit redoubler d'efforts pour atteindre une masse critique d'investissement et surmonter la fragmentation des capacités réparties dans l'ensemble de l'Union.

- **Cohérence avec les autres politiques de l'Union**

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité agira en tant qu'organe unique de mise en œuvre pour divers programmes de l'Union en faveur de la cybersécurité (programme pour une Europe numérique et programme «Horizon Europe») et renforcera la cohérence et les synergies entre eux.

La présente initiative permettra également de compléter les efforts des États membres en apportant une contribution appropriée aux décideurs en matière d'éducation afin d'améliorer les compétences en cybersécurité (par exemple, en élaborant des programmes de formation en matière de cybersécurité dans les systèmes éducatifs civils et militaires) afin de contribuer au développement d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité au niveau de l'Union, un atout majeur pour les entreprises de cybersécurité ainsi que pour d'autres secteurs concernés par la cybersécurité. En ce qui concerne la formation et l'éducation à la cyberdéfense, la présente initiative sera compatible avec les travaux qui se déroulent actuellement sur la plateforme d'éducation, de formation et d'exercices dans le domaine de la cyberdéfense créée dans le cadre du Collège européen de sécurité et de défense.

La présente initiative complétera et soutiendra les efforts déployés par les pôles d'innovation numérique dans le cadre du programme pour une Europe numérique. Les pôles d'innovation numérique sont des organisations sans but lucratif qui aident les entreprises, en particulier les jeunes entreprises, les PME et les entreprises à capitalisation moyenne, à devenir plus compétitives en améliorant leurs processus d'entreprise/de production, ainsi que leurs produits et leurs services grâce à une innovation intelligente favorisée par la technologie numérique. Les pôles d'innovation numérique offrent des services d'innovation axés sur les entreprises,

---

[13] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité [règlement sur la cybersécurité, COM(2017) 477 final/3].

[14] Cela est sans préjudice des mécanismes de certification prévus par le règlement général sur la protection des données, dans le cadre desquels les autorités chargées de la protection des données ont un rôle à jouer, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE («règlement général sur la protection des données»).

tels que des services de connaissance du marché, des conseils financiers, un accès aux infrastructures d'essai et d'expérimentation pertinentes, la formation et le développement des compétences, pour permettre à de nouveaux produits ou services d'atteindre avec succès le marché ou pour introduire de meilleurs procédés de production. Certains pôles d'innovation numérique, dotés d'une expertise spécifique en matière de cybersécurité, pourraient être directement associés à la communauté des compétences en cybersécurité instituée par la présente initiative. Dans la plupart des cas, toutefois, les pôles d'innovation numérique, qui n'ont pas un profil de cybersécurité particulier, faciliteraient l'accès de leur groupe cible à l'expertise, aux connaissances et aux capacités en matière de cybersécurité accessibles à la communauté des compétences cybersécurité en coopérant étroitement avec le Réseau des centres nationaux de coordination et avec le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité. Les pôles d'innovation numérique soutiendraient également le déploiement de produits et de solutions innovants en matière de cybersécurité correspondant aux besoins des entreprises et des autres utilisateurs finals qu'ils desservent. Dernier point, et non des moindres, des pôles d'innovation numérique sectoriels spécifiques pourraient partager leurs connaissances sur les besoins sectoriels réels avec le Réseau et le Centre pour alimenter la réflexion sur le programme de recherche et d'innovation dans le respect des exigences industrielles.

Des synergies avec les communautés de la connaissance et de l'innovation concernées de l'Institut européen d'innovation et de technologie, et en particulier avec l'EIT Digital, seront recherchées.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

Il convient d'instituer le Centre de compétences sur une double base juridique en raison de sa nature et de ses objectifs spécifiques. L'article 187 du traité sur le fonctionnement de l'Union européenne, qui établit les structures nécessaires à l'exécution efficace des programmes de recherche, de développement technologique et de démonstration de l'Union, permet au Centre de compétences de créer des synergies et de mettre en commun des ressources afin d'investir dans les capacités nécessaires au niveau des États membres et de développer des actifs partagés européens (par exemple, en acquérant conjointement les infrastructures nécessaires pour les essais et l'expérimentation en matière de cybersécurité). L'article 188, premier alinéa, prévoit l'adoption de telles mesures. Néanmoins, l'article 188, premier alinéa, en tant que seule base juridique ne permettrait pas aux activités d'aller au-delà du domaine de la recherche et du développement, dans la mesure nécessaire pour atteindre tous les objectifs du Centre de compétences énoncés dans le présent règlement, à savoir soutenir le déploiement commercial de produits et de solutions de cybersécurité, aider le secteur européen de la cybersécurité à devenir plus compétitif et à accroître sa part de marché et apporter une valeur ajoutée aux efforts nationaux visant à combler l'écart de compétences en cybersécurité. Par conséquent, pour atteindre ces objectifs, il est nécessaire d'ajouter l'article 173, paragraphe 3, en tant que base juridique permettant à l'Union de prévoir des mesures destinées à soutenir la compétitivité de l'industrie.

• Justification de la proposition au regard des principes de subsidiarité et de proportionnalité

La cybersécurité est une question d'intérêt commun de l'Union, comme le confirment les conclusions du Conseil mentionnées ci-dessus. L'ampleur et le caractère transfrontalier d'incidents tels que *WannaCry* ou *NonPetya* en sont un bon exemple. La nature et l'ampleur

des défis technologiques liés à la cybersécurité, ainsi que la coordination insuffisante des efforts déployés au sein de l'industrie, du secteur public et des communautés scientifiques et entre ceux-ci, imposent à l'Union de continuer de soutenir les efforts de coordination afin de mettre en commun une masse critique de ressources et de garantir une meilleure gestion des connaissances et des actifs. Cela est nécessaire compte tenu des besoins en ressources liés à certaines capacités en matière de recherche, de développement et de déploiement dans le domaine de la cybersécurité; la nécessité de fournir un accès à un savoir-faire interdisciplinaire en matière de cybersécurité entre différentes disciplines (souvent partiellement disponible au niveau national); la nature mondiale des chaînes de valeur industrielles, ainsi que l'activité des concurrents mondiaux opérant sur les marchés.

Cela nécessite des ressources et une expertise à une échelle qui peut difficilement être égalée par l'action individuelle d'un État membre quel qu'il soit. Par exemple, un réseau paneuropéen de communication quantique pourrait nécessiter un investissement de l'Union d'environ 900 millions d'EUR, en fonction des investissements réalisés par les États membres (à interconnecter/compléter) et de la mesure dans laquelle la technologie permettra la réutilisation des infrastructures existantes. La présente initiative contribuera à la mise en commun des financements et permettra la réalisation de ce type d'investissement dans l'Union.

Les objectifs de la présente initiative ne peuvent pas être pleinement atteints par les seuls États membres. Comme indiqué ci-dessus, ils peuvent être mieux réalisés au niveau de l'Union en mettant en commun les efforts et en évitant les doubles emplois inutiles, en contribuant à atteindre une masse critique d'investissements et en veillant à ce que les fonds publics soient utilisés de manière optimale. Dans le même temps, conformément au principe de proportionnalité, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs. L'action de l'Union se justifie pour des raisons de subsidiarité et de proportionnalité.

Le présent instrument ne prévoit pas de nouvelles obligations réglementaires pour les entreprises. Dans le même temps, les entreprises, et en particulier les PME, sont susceptibles de réduire les coûts liés à leurs efforts de conception de cyberproduits sûrs et innovants, étant donné que l'initiative permet de mettre en commun des ressources pour investir dans les capacités nécessaires au niveau des États membres ou développer des actifs partagés européens (par exemple, en acquérant conjointement les infrastructures nécessaires pour les essais et l'expérimentation en matière de cybersécurité). Ces actifs pourraient être utilisés par les industries et les PME de différents secteurs afin de garantir la cybersécurité de leurs produits et de faire de la cybersécurité un avantage concurrentiel.

- **Choix de l'instrument**

L'instrument proposé crée un organe chargé de mettre en œuvre des actions en matière de cybersécurité dans le cadre du programme pour une Europe numérique et du programme «Horizon Europe». Il décrit le mandat, les tâches ainsi que la structure de gouvernance de l'organe. La création d'un tel organe de l'Union nécessite l'adoption d'un règlement.

3. CONSULTATION DES PARTIES INTÉRESSÉES ET ANALYSES D'IMPACT

La proposition de créer un Réseau de compétences en cybersécurité avec un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité est une nouvelle initiative. Elle s'inscrit dans la continuité et l'extension du partenariat public-privé contractuel en matière de cybersécurité créé en 2016.

- **Consultation des parties intéressées**

La cybersécurité est un sujet vaste et intersectoriel. La Commission a eu recours à différentes méthodes de consultation afin de veiller à ce que l'intérêt public général de l'Union, par opposition aux intérêts particuliers d'un éventail restreint de groupes de parties prenantes, soit bien pris en considération dans la présente initiative. Cette méthode garantit la transparence et la responsabilité dans les travaux de la Commission. Aucune consultation publique ouverte n'a été menée spécifiquement pour la présente initiative, compte tenu de son public cible (communauté de l'industrie et de la recherche et États membres), mais la thématique a déjà été couverte par plusieurs autres consultations publiques ouvertes:

- une consultation publique générale ouverte, réalisée en 2018, sur le thème de l'investissement, de la recherche et de l'innovation, des PME et du marché unique;
- une consultation publique en ligne de 12 semaines lancée en 2017 afin de recueillir l'avis du grand public (environ 90 répondants) sur l'évaluation et le réexamen de l'ENISA;
- une consultation publique en ligne de 12 semaines réalisée en 2016 à l'occasion du lancement du partenariat public-privé contractuel en matière de cybersécurité (environ 240 répondants).

La Commission a également organisé des consultations ciblées sur la présente initiative, notamment des ateliers, des réunions et des demandes ciblées de contribution (de l'ENISA et de l'Agence européenne de défense). La période de consultation s'est étendue sur six mois, de novembre 2017 à mars 2018. La Commission a également procédé à une cartographie des centres d'expertise, qui a permis de recueillir les contributions de 665 centres d'expertise en matière de cybersécurité sur leur savoir-faire, leurs activités, leurs domaines de travail, la coopération internationale. L'enquête a été lancée en janvier et les enquêtes soumises jusqu'au 8 mars 2018 ont été prises en considération pour l'analyse du rapport.

Les parties prenantes des milieux de l'industrie et de la recherche ont estimé que le Centre de compétences et le Réseau pourraient apporter une valeur ajoutée aux efforts actuellement déployés au niveau national en contribuant à la création d'un écosystème européen de cybersécurité permettant une meilleure coopération entre lesdits milieux. Elles ont également estimé qu'il était nécessaire que l'Union européenne et les États membres adoptent une démarche proactive, stratégique et à plus long terme en ce qui concerne la politique industrielle de cybersécurité, allant au-delà de la recherche et de l'innovation. Les parties prenantes ont exprimé le besoin d'avoir accès à des capacités essentielles, telles que des infrastructures d'essai et d'expérimentation, et d'être plus ambitieuses pour combler le manque de compétences en cybersécurité, par exemple au moyen de projets européens à grande échelle attirant les meilleurs talents. Tous les éléments ci-dessus ont également été jugés nécessaires pour que l'Union soit reconnue au niveau mondial comme un acteur de premier plan en matière de cybersécurité.

Les États membres, dans le cadre des activités de consultation entreprises depuis septembre dernier[15] et dans des conclusions spécifiques du Conseil[16], ont salué l'intention de mettre en place un Réseau de compétences en cybersécurité pour stimuler le développement et le déploiement des technologies de cybersécurité, en soulignant la nécessité d'inclure tous les États membres et leurs centres d'excellence et de compétences existants et de prêter une

[15] Par exemple, table ronde de haut niveau avec les États membres, M. Ansip, vice-président de la Commission, et Mme Gabriel, commissaire européenne, le 5 décembre 2017.

[16] Conseil «Affaires générales»: Conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» (20 novembre 2017).

attention particulière à la complémentarité. En ce qui concerne plus particulièrement le futur Centre de compétences, les États membres ont souligné l'importance de son rôle de coordination dans le soutien du Réseau. Pour ce qui est, en particulier, des activités et des besoins nationaux de cyberdéfense, l'exercice visant à recenser les besoins des États membres en matière de cyberdéfense organisé par le Service européen pour l'action extérieure en mars 2018 a montré que la plupart des États membres perçoivent la valeur ajoutée européenne dans les domaines du soutien à la formation et à l'éducation à la cyberdéfense et du soutien aux entreprises du secteur à travers la recherche et le développement[17]. L'initiative serait effectivement mise en œuvre conjointement avec les États membres ou les entités qu'ils soutiennent. Les collaborations entre les communautés de l'industrie, de la recherche et/ou du secteur public permettraient de réunir et de renforcer les efforts réalisés et les entités existantes en vue d'éviter les doubles emplois. Les États membres participeraient également à la définition d'actions spécifiques ciblant le secteur public en tant qu'utilisateur direct de technologie et de savoir-faire en matière de cybersécurité.

- **Analyse d'impact**

Une analyse d'impact à l'appui de la présente initiative a été soumise le 11 avril 2017 au comité d'examen de la réglementation et a reçu un avis favorable assorti de réserves. L'analyse d'impact a ensuite été revue à la lumière des observations formulées par le comité. L'avis du comité et l'annexe expliquant comment les observations de celui-ci ont été prises en considération sont publiés en même temps que la présente proposition.

Plusieurs options stratégiques, tant législatives que non législatives, ont été envisagées dans l'analyse d'impact. Les options suivantes ont été retenues pour une évaluation approfondie:

- 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'Union en soutenant la recherche et l'innovation et les mécanismes de collaboration qui s'y rapportent dans le cadre du 9e PC.
- Option 1: création d'un Réseau de compétences en cybersécurité avec un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité doté d'un double mandat pour poursuivre les mesures en faveur des technologies industrielles ainsi que dans le domaine de la recherche et de l'innovation.
- Option 2: création d'un Réseau de compétences en cybersécurité avec un Centre européen de recherche et de compétences en matière de cybersécurité, axé sur les activités de recherche et d'innovation.

Les options écartées à un stade précoce incluaient 1) l'option consistant à ne rien faire du tout, 2) l'option de créer uniquement un Réseau de compétences en cybersécurité, 3) l'option de créer uniquement une structure centralisée et 4) l'option de recourir à une agence existante [Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), Agence exécutive pour la recherche (REA), Agence exécutive pour l'innovation et les réseaux (INEA)].

L'analyse a conclu que l'option 1 était la plus appropriée pour atteindre les objectifs de l'initiative, tout en assurant les meilleures retombées économiques, sociétales et

[17] SEAE, mars 2018.

environnementales et en préservant aux mieux les intérêts de l'Union. Parmi les principaux arguments en faveur de cette option figurait la capacité de créer une véritable politique industrielle en matière de cybersécurité en soutenant des activités liées non seulement à la recherche et au développement, mais aussi à l'essor du marché; la flexibilité permettant de recourir à différents modèles de coopération avec le Réseau de centres de compétences afin d'optimiser l'utilisation des connaissances et des ressources existantes; la capacité à structurer la coopération et les engagements conjoints des parties prenantes publiques et privées provenant de tous les secteurs concernés, y compris la défense. Dernier point, mais non des moindres, l'option 1 permet également d'accroître les synergies et peut servir de mécanisme de mise en œuvre pour deux volets de financement différents de l'Union dans le domaine de la cybersécurité au titre du prochain cadre financier pluriannuel (programme pour une Europe numérique, programme «Horizon Europe»).

- **Droits fondamentaux**

La présente initiative permettra aux autorités publiques et aux industries dans tous les États membres de prévenir plus efficacement les cybermenaces et de mieux y répondre en proposant et en se dotant de produits et solutions plus sûrs. Cela vaut en particulier pour la protection de l'accès aux services essentiels (par exemple, les transports, la santé, les services bancaires et financiers).

Le renforcement de la capacité de l'Union européenne à sécuriser de manière autonome ses produits et ses services devrait également aider les citoyens à jouir de leurs droits et valeurs démocratiques (par exemple, mieux protéger les droits liés à l'information consacrés par la Charte des droits fondamentaux, notamment le droit à la protection des données à caractère personnel et à la vie privée) et, par conséquent, à renforcer leur confiance dans la société et l'économie numériques.

4. INCIDENCE BUDGÉTAIRE

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, en coopération avec le Réseau des compétences en cybersécurité, sera le principal organe de mise en œuvre des ressources financières de l'Union consacrées à la cybersécurité dans le cadre du programme pour une Europe numérique et du programme «Horizon Europe».

Les incidences budgétaires liées à la mise en œuvre de l'Europe numérique sont énumérées en détail dans la fiche financière législative annexée à la présente proposition. La contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b), sera proposée par la Commission au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique. La proposition sera fondée sur les résultats du processus de planification stratégique défini à l'article 6, paragraphe 6, du règlement XXX [programme-cadre «Horizon Europe»].

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La présente proposition prévoit une clause d'évaluation explicite, par laquelle la Commission procédera à une évaluation indépendante (article 38). La Commission transmettra ensuite au Parlement européen et au Conseil un rapport sur son évaluation, accompagné le cas échéant

d’une proposition en vue de sa révision, afin de mesurer l’impact de l’instrument et sa valeur ajoutée. La Commission appliquera ses méthodes d’évaluation figurant dans l’initiative «Mieux légiférer».

Le directeur exécutif devrait présenter au conseil de direction une évaluation ex post des activités du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et des activités du Réseau tous les deux ans, comme le prévoit l’article 17 de la présente proposition. Le directeur exécutif devrait également élaborer un plan d’action de suivi concernant les conclusions des évaluations rétrospectives et faire rapport deux fois par an à la Commission sur les progrès accomplis. Le conseil de direction devrait être chargé de veiller au suivi adéquat de ces conclusions, conformément à l’article 16 de la présente proposition.

Les cas présumés de mauvaise administration dans les activités de l’entité juridique peuvent faire l’objet d’enquêtes du Médiateur européen conformément aux dispositions de l’article 228 du traité.

2018/0328 (COD)

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

Contribution de la Commission européenne à la réunion des dirigeants des 19 et 20 septembre 2018 à Salzbourg

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 173, paragraphe 3, et son article 188, premier alinéa,

vu la proposition de la Commission européenne,

vu l'avis du Comité économique et social européen[18],

vu l'avis du Comité des régions[19],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) À mesure que la vie quotidienne et les économies deviennent de plus en plus tributaires des technologies numériques, les citoyens sont de plus en plus exposés à des cyberincidents graves. La sécurité future dépend, entre autres, du renforcement de la capacité technologique et industrielle à protéger l'Union contre les cybermenaces, car tant les infrastructures civiles que les capacités militaires reposent sur des systèmes numériques sûrs.

(2) L'Union n'a cessé d'accroître ses activités pour relever les défis croissants en matière de cybersécurité à la suite de la stratégie de cybersécurité de 2013[20] visant à favoriser un cyberécosystème fiable, sûr et ouvert. En 2016, l'Union a adopté les premières mesures dans le domaine de la cybersécurité par l'intermédiaire de la directive (UE) 2016/1148 du Parlement européen et du Conseil[21] relative à la sécurité des réseaux et des systèmes d'information.

(3) En septembre 2017, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont présenté une communication

---

18 JO C du , p.

19 JO C du , p. .

20 Communication conjointe au Parlement européen et au Conseil: Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, JOIN(2013) 1 final.

21 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

conjointe[22] intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» afin de renforcer encore la résilience, la dissuasion et la capacité de réaction de l'Union face aux cyberattaques.

(4) Lors du sommet numérique de Tallinn, en septembre 2017, les chefs d'État et de gouvernement ont enjoint l'Union de devenir «un acteur mondial de premier plan dans le domaine de la cybersécurité d'ici à 2025, afin de s'assurer de la confiance de nos citoyens, consommateurs et entreprises, d'assurer leur protection en ligne et de permettre un internet libre et réglementé».

(5) Une perturbation substantielle des réseaux et des systèmes d'information peut affecter les différents États membres et l'Union dans son ensemble. La sécurité des réseaux et des systèmes d'information est donc essentielle au fonctionnement harmonieux du marché intérieur. Actuellement, l'Union dépend de fournisseurs de services de cybersécurité non européens. Cependant, il est dans l'intérêt stratégique de l'Union de veiller à maintenir et à développer des capacités technologiques essentielles en matière de cybersécurité pour consolider son marché unique numérique, et notamment pour protéger les réseaux et les systèmes d'information critiques et pour fournir des services clés de cybersécurité.

(6) L'Union dispose d'une expertise et d'une expérience considérables en matière de recherche, de technologies et de développement industriel dans le domaine de la cybersécurité, mais les efforts des communautés de la recherche et de l'industrie sont fragmentés, non harmonisés et caractérisés par l'absence d'une mission commune, ce qui entrave la compétitivité de l'UE dans ce domaine. Ces efforts et cette expertise doivent être mis en commun, mis en réseau et utilisés de manière efficace afin de renforcer et de compléter les capacités de recherche, technologiques et industrielles existantes au niveau de l'Union et au niveau national.

(7) Dans ses conclusions adoptées en novembre 2017, le Conseil a invité la Commission à fournir rapidement une analyse d'impact sur les options possibles pour créer un Réseau de centres de compétences en cybersécurité ayant comme pierre angulaire un Centre européen de recherche et de compétences, ainsi qu'à proposer, d'ici la mi-2018, l'instrument juridique pertinent.

(8) Le Centre de compétences devrait être le principal instrument de l'Union pour mettre en commun les investissements dans la recherche, le développement technologique et industriel en matière de cybersécurité et pour mettre en œuvre les projets et initiatives pertinents, en collaboration avec le Réseau de compétences en cybersécurité. Il devrait permettre de fournir un soutien financier en matière de cybersécurité au titre du programme «Horizon Europe» et du programme pour une Europe numérique, et devrait être ouvert, le cas échéant, au Fonds européen de développement régional et à d'autres programmes. Cette approche devrait contribuer à créer des synergies et à coordonner l'aide financière liée à la recherche, à l'innovation, et au développement industriel et technologique dans le domaine de la cybersécurité, tout en évitant les doubles emplois.

(9) Compte tenu du fait que les objectifs de la présente initiative peuvent être mieux réalisés si tous les États membres, ou autant d'États membres que possible, y

[22] COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL: Communication conjointe au Parlement européen et au Conseil «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» (JOIN(2017) 450 final).

participent, et pour inciter les États membres à y prendre part, seuls les États membres qui contribuent financièrement aux coûts administratifs et aux frais de fonctionnement du Centre de compétences devraient détenir un droit de vote.

(10) La participation financière des États membres participants devrait être proportionnelle à la contribution financière de l'Union à la présente initiative.

(11) Le Centre de compétences devrait faciliter et contribuer à coordonner les travaux du Réseau des compétences en cybersécurité (ci-après le «Réseau»), composé de centres nationaux de coordination dans chaque État membre. Les centres nationaux de coordination devraient bénéficier d'un soutien financier direct de l'Union, y compris de subventions octroyées sans appel à propositions, pour mener à bien les activités liées au présent règlement.

(12) Les centres nationaux de coordination devraient être sélectionnés par les États membres. Outre les capacités administratives nécessaires, les centres devraient soit posséder, soit avoir un accès direct à une expertise technologique en matière de cybersécurité, notamment dans des domaines tels que la cryptographie, les services de sécurité des TIC, la détection d'intrusion, la sécurité des systèmes, la sécurité des réseaux, la sécurité des logiciels et des applications, ou les aspects humains et sociétaux de la sécurité et de la protection de la vie privée. Ils devraient également être en mesure d'assurer un dialogue et une coordination efficaces avec l'industrie, le secteur public, et notamment les autorités désignées en vertu de la directive (UE) 2016/1148 du Parlement européen et du Conseil[23], ainsi qu'avec la communauté scientifique.

(13) Lorsqu'une aide financière est fournie à des centres nationaux de coordination afin de soutenir des tiers au niveau national, cela est répercuté sur les parties prenantes concernées au travers d'accords de subvention en cascade.

(14) Les technologies émergentes, telles que l'intelligence artificielle, l'internet des objets, le calcul à haute performance (CHP) et l'informatique quantique, les chaînes de blocs et les concepts tels que les identités numériques sûres, posent à la fois de nouveaux défis en matière de cybersécurité et offrent des solutions. L'évaluation et la validation de la robustesse des systèmes TIC existants ou futurs nécessiteront la mise à l'essai de solutions de sécurité contre les attaques exécutées sur des machines CHP et quantiques. Le Centre de compétences, le Réseau et la communauté des compétences en matière de cybersécurité devraient contribuer à faire progresser et à diffuser les solutions les plus récentes en matière de cybersécurité. Parallèlement, le Réseau et le Centre de compétences devraient être au service des développeurs et des opérateurs dans des secteurs critiques tels que les transports, l'énergie, la santé, les services financiers, l'administration, les télécommunications, l'industrie manufacturière, la défense et l'espace pour les aider à résoudre leurs problèmes de cybersécurité.

(15) Le Centre de compétences devrait avoir plusieurs fonctions clés. Premièrement, le Centre de compétences devrait faciliter et contribuer à coordonner les travaux du Réseau européen de compétences en matière de cybersécurité, ainsi qu'à favoriser le développement de la communauté des compétences en matière de cybersécurité. Il devrait faire progresser l'agenda technologique en matière de cybersécurité et faciliter

[23] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

l'accès à l'expertise acquise au sein du Réseau et de la communauté des compétences en matière de cybersécurité. Deuxièmement, il devrait mettre en œuvre les parties pertinentes du programme pour une Europe numérique et du programme «Horizon Europe» en attribuant des subventions, en général à la suite d'un appel à propositions concurrentiel. Troisièmement, le Centre de compétences devrait faciliter les investissements conjoints de l'Union, des États membres et/ou de l'industrie.

(16) Le Centre de compétences devrait encourager et soutenir la coopération et la coordination des activités de la communauté des compétences en matière de cybersécurité, qui associerait un groupe important, ouvert et varié d'acteurs concernés par les technologies de la cybersécurité. Il convient que cette communauté inclue notamment les entités de recherche, les secteurs du côté de l'offre, les secteurs du côté de la demande et le secteur public. La communauté des compétences en matière de cybersécurité devrait contribuer aux activités et au plan de travail du Centre de compétences, et elle devrait également bénéficier des activités de renforcement des communautés du Centre de compétences et du Réseau, mais ne devrait pas être privilégiée en ce qui concerne les appels à propositions ou les appels d'offres.

(17) Afin de répondre aux besoins de l'offre et de la demande, la tâche du Centre de compétences consistant à fournir aux différents secteurs des connaissances et une assistance technique en matière de cybersécurité devrait porter à la fois sur les produits et services TIC et sur tous les autres produits et solutions industriels et technologiques dans lesquels la cybersécurité doit être intégrée.

(18) Alors que le Centre de compétences et le Réseau devraient s'efforcer de créer des synergies entre les sphères civile et militaire dans le domaine de la cybersécurité, les projets financés par le programme «Horizon Europe» seront mis en œuvre conformément au règlement XXX [règlement «Horizon Europe»], qui prévoit que les activités de recherche et d'innovation menées au titre du programme «Horizon Europe» sont axées sur les applications civiles.

(19) Afin de garantir une collaboration structurée et durable, la relation entre le Centre de compétences et les centres nationaux de coordination devrait reposer sur un accord contractuel.

(20) Des dispositions appropriées devraient être prises pour garantir la responsabilité et la transparence du Centre de compétences.

(21) Compte tenu de leurs compétences respectives en matière de cybersécurité, le Centre commun de recherche de la Commission ainsi que l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) devraient jouer un rôle actif au sein de la communauté des compétences en matière de cybersécurité et du comité consultatif industriel et scientifique.

(22) Lorsqu'ils reçoivent une contribution financière du budget général de l'Union, les centres nationaux de coordination et les entités qui font partie de la communauté des compétences en matière de cybersécurité devraient rendre public le fait que les activités respectives sont menées dans le cadre de la présente initiative.

(23) La contribution de l'Union au Centre de compétences devrait financer la moitié des coûts résultant des activités d'établissement, d'administration et de coordination du Centre de compétences. Afin d'éviter un double financement, ces activités ne devraient pas bénéficier simultanément d'une contribution d'autres programmes de l'Union.

(24) Le conseil de direction du Centre de compétences, composé des États membres et de la Commission, devrait définir l'orientation générale des activités du Centre de compétences et veiller à ce que celui-ci s'acquitte de ses tâches conformément au présent règlement. Le conseil de direction devrait être investi des pouvoirs nécessaires pour établir le budget, vérifier son exécution, adopter les règles financières appropriées, établir des procédures de travail transparentes pour la prise de décision par le Centre de compétences, adopter le plan de travail et le plan stratégique pluriannuel du Centre de compétences en tenant compte des priorités dans la réalisation des objectifs et des tâches de celui-ci, adopter son règlement intérieur, nommer le directeur exécutif et décider de la prorogation du mandat du directeur exécutif et de sa cessation.

(25) Afin que le Centre de compétences fonctionne de manière appropriée et efficace, la Commission et les États membres devraient veiller à ce que les personnes désignées au conseil de direction disposent d'une expertise et d'une expérience professionnelles appropriées dans les domaines fonctionnels. La Commission et les États membres devraient s'efforcer de limiter le roulement de leurs représentants respectifs dans le conseil de direction, afin de garantir la continuité des travaux de ce dernier.

(26) Le bon fonctionnement du Centre de compétences exige que son directeur exécutif soit nommé sur la base du mérite, de ses capacités attestées en matière d'administration et de gestion, de ses compétences et de son expérience pertinentes en matière de cybersécurité, et que les fonctions du directeur exécutif soient exercées en toute indépendance.

(27) Le Centre de compétences devrait être doté d'un comité consultatif industriel et scientifique tenant lieu d'instance consultative pour assurer un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties prenantes concernées. Le comité consultatif industriel et scientifique devrait se concentrer sur les questions intéressant les parties prenantes et les porter à l'attention du conseil de direction du Centre de compétences. La composition du comité consultatif industriel et scientifique et les tâches qui lui sont assignées, telles que sa consultation sur le plan de travail, devraient assurer une représentation suffisante des parties prenantes dans les travaux du Centre de compétences.

(28) Le Centre de compétences devrait bénéficier de l'expertise particulière et de la représentation large et pertinente des parties prenantes, grâce au partenariat public-privé contractuel en matière de cybersécurité pendant la durée du programme Horizon 2020, par l'intermédiaire de son comité consultatif industriel et scientifique.

(29) Le Centre de compétences devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. Le Centre de compétences devrait également appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil[24]. Les opérations de traitement de données à caractère personnel effectuées par le Centre de compétences sont soumises au règlement (UE) nº XXX/2018 du Parlement européen et du Conseil. Le Centre de compétences devrait respecter les dispositions applicables aux institutions de l'Union et la législation nationale

[24] Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

concernant le traitement des informations, notamment des informations non classifiées sensibles et des informations classifiées de l'UE.

(30) Les intérêts financiers de l'Union et des États membres devraient être protégés par des mesures proportionnées tout au long du cycle des dépenses, notamment la prévention, la détection et la recherche des irrégularités, le recouvrement des fonds perdus, indûment versés ou mal employés et, s'il y a lieu, l'application de sanctions administratives et financières conformément au règlement XXX (UE, Euratom) du Parlement européen et du Conseil[25] (ci-après le «règlement financier»).

(31) Le Centre de compétences devrait fonctionner de manière ouverte et transparente en fournissant en temps voulu toutes les informations utiles et en assurant la promotion de ses activités, notamment des activités d'information et de diffusion à l'intention du grand public. Le règlement intérieur des organes du Centre de compétences devrait être rendu public.

(32) L'auditeur interne de la Commission devrait exercer à l'égard du Centre de compétences les mêmes compétences que celles qu'il exerce à l'égard de la Commission.

(33) La Commission, le Centre de compétences, la Cour des comptes et l'Office européen de lutte antifraude devraient avoir accès à toutes les informations nécessaires et aux locaux pour mener à bien les audits et les enquêtes concernant les subventions, contrats et accords signés par le Centre de compétences.

(34) Étant donné que les objectifs du présent règlement, à savoir le maintien et le développement des capacités technologiques et industrielles de l'Union en matière de cybersécurité, le renforcement de la compétitivité du secteur de la cybersécurité de l'Union et la transformation de la cybersécurité en avantage concurrentiel pour d'autres secteurs de l'Union, ne peuvent pas être réalisés de manière suffisante par les États membres compte tenu du fait que les ressources existantes sont limitées et dispersées ainsi qu'en raison de l'ampleur des investissements nécessaires, mais peuvent plutôt, pour éviter les doubles emplois inutiles, contribuer à atteindre une masse critique d'investissement et garantir l'utilisation optimale des fonds publics au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS ET PRINCIPES GÉNÉRAUX DU CENTRE DE COMPÉTENCES ET DU RÉSEAU

Article premier

Objet

[25] [ajouter le titre et la référence du JO].

1. Le présent règlement établit le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité (ci-après le «Centre de compétences»), ainsi que le Réseau de centres nationaux de coordination, et fixe les règles applicables à la désignation des centres nationaux de coordination et à la création de la communauté des compétences en matière de cybersécurité.

2. Le Centre de compétences contribue à la mise en œuvre du volet «cybersécurité» du programme pour une Europe numérique établi par le règlement nº XXX et, en particulier, des actions se rapportant à l'article 6 du règlement (UE) nº XXX [programme pour une Europe numérique] et au programme «Horizon Europe» établi par le règlement nº XXX, et notamment à la section 2.2.6 du pilier II de l'annexe I de la décision nº XXX établissant le programme spécifique d'exécution du programme-cadre pour la recherche et l'innovation «Horizon Europe» [numéro de réf. du programme spécifique].

3. Le siège du Centre de compétences est situé à [Bruxelles, en Belgique].

4. Le Centre de compétences est doté de la personnalité juridique. Dans chaque État membre, il jouit de la capacité juridique la plus large reconnue aux personnes morales par la législation de cet État. Il peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et ester en justice.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

(1) «cybersécurité», la protection des réseaux et des systèmes d'information, de leurs utilisateurs et d'autres personnes contre les cybermenaces;

(2) «produits et solutions de cybersécurité», les produits, services ou processus TIC ayant pour objet spécifique la protection des réseaux et des systèmes d'information, de leurs utilisateurs et des personnes exposées contre les cybermenaces;

(3) «autorité publique»: tout gouvernement ou toute autre administration publique, y compris les organismes consultatifs publics, au niveau national, régional ou local, ou toute personne physique ou morale exerçant, en vertu du droit national, des fonctions administratives publiques, y compris des tâches spécifiques;

(4) «État membre participant»: un État membre qui, sur une base volontaire, contribue financièrement à couvrir les coûts administratifs et les frais de fonctionnement du Centre de compétences.

Article 3

Tâche du Centre et du Réseau

1. Le Centre de compétences et le Réseau aident l'Union:

   (a) à maintenir et à développer les capacités technologiques et industrielles en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique;

   (b) à accroître la compétitivité du secteur de la cybersécurité de l'Union et à faire de la cybersécurité un avantage concurrentiel pour les autres secteurs de l'Union.

2. Le Centre de compétences s'acquitte de ses tâches, le cas échéant, en collaboration avec le Réseau des centres nationaux de coordination et la communauté des compétences en matière de cybersécurité.

Article 4

Objectifs et tâches du Centre

Les objectifs et les missions connexes du Centre de compétences sont les suivants:

1. faciliter et contribuer à coordonner les travaux du Réseau des centres nationaux de coordination (ci-après le «Réseau») visé à l'article 6 et de la communauté des compétences en matière de cybersécurité visée à l'article 8;

2. contribuer à la mise en œuvre du volet «cybersécurité» du programme pour une Europe numérique établi par le règlement nº XXX[26] et, en particulier, des actions se rapportant à l'article 6 du règlement (UE) nº XXX [programme pour une Europe numérique] et au programme «Horizon Europe» établi par le règlement nº XXX[27], et notamment à la section 2.2.6 du pilier II de l'annexe I de la décision nº XXX établissant le programme spécifique d'exécution du programme-cadre pour la recherche et l'innovation «Horizon Europe» [numéro de réf. du programme spécifique] et d'autres programmes de l'Union, lorsque cela est prévu dans des actes juridiques de l'Union;

3. renforcer les capacités, les connaissances et les infrastructures en matière de cybersécurité au service des industries, du secteur public et des communautés scientifiques, en accomplissant les tâches suivantes:

   (a) compte tenu des infrastructures industrielles et de recherche de pointe en matière de cybersécurité et des services connexes, acquérir, mettre à niveau, exploiter et mettre ces infrastructures et services connexes à la disposition d'un large éventail d'utilisateurs dans l'ensemble de l'Union issus de l'industrie, y compris des PME, du secteur public, du milieu de la recherche et de la communauté scientifique;

   (b) compte tenu des infrastructures industrielles et de recherche de pointe en matière de cybersécurité et des services connexes, fournir un soutien à d'autres entités, y compris financièrement, pour l'acquisition, la mise à niveau, l'exploitation et la mise à disposition de ces infrastructures et services connexes à un large éventail d'utilisateurs dans l'ensemble de l'Union issus de l'industrie, y compris des PME, du secteur public, du milieu de la recherche et de la communauté scientifique;

   (c) fournir des connaissances en matière de cybersécurité et une assistance technique à l'industrie et aux autorités publiques, notamment en soutenant des actions visant à faciliter l'accès à l'expertise disponible au sein du Réseau et de la communauté des compétences en matière de cybersécurité;

4. contribuer au déploiement à grande échelle de produits et de solutions de pointe en matière de cybersécurité dans l'ensemble de l'économie, en accomplissant les tâches suivantes:

---

26 [ajouter le titre complet et la référence du JO].

27 [ajouter le titre complet et la référence du JO].

(a) encourager la recherche et le développement en matière de cybersécurité, ainsi que l'adoption de produits et de solutions de cybersécurité de l'Union par les autorités publiques et les industries utilisatrices;

(b) aider les autorités publiques, les secteurs du côté de la demande et d'autres utilisateurs à adopter et à intégrer les dernières solutions en matière de cybersécurité;

(c) soutenir, en particulier, les autorités publiques dans l'organisation de leurs marchés publics, ou acquérir des produits et des solutions de pointe en matière de cybersécurité pour le compte des autorités publiques;

(d) fournir un soutien financier et une assistance technique aux jeunes entreprises et aux PME dans le domaine de la cybersécurité afin de les connecter à des marchés potentiels et d'attirer les investissements;

5. améliorer la compréhension de la cybersécurité et contribuer à réduire les déficits de compétences dans l'Union en matière de cybersécurité en accomplissant les tâches suivantes:

(a) soutenir le développement des compétences en matière de cybersécurité, le cas échéant en collaboration avec les agences et organes compétents de l'Union européenne, y compris l'ENISA;

6. contribuer au renforcement de la recherche et du développement dans le domaine de la cybersécurité dans l'Union:

(a) en apportant un soutien financier aux efforts de recherche en matière de cybersécurité sur la base d'un programme commun pluriannuel, évalué et amélioré en permanence, dans les domaines stratégique, industriel, technologique et de la recherche;

(b) en soutenant des projets de recherche et de démonstration à grande échelle sur les capacités technologiques de la prochaine génération en matière de cybersécurité, en collaboration avec l'industrie et le Réseau;

(c) en soutenant la recherche et l'innovation en matière de normalisation dans le domaine des technologies de cybersécurité;

7. renforcer la coopération entre les sphères civile et militaire en ce qui concerne les technologies et les applications à double usage dans le domaine de la cybersécurité, en accomplissant les tâches suivantes:

(a) soutenir les États membres et les acteurs de l'industrie et de la recherche en ce qui concerne la recherche, le développement et le déploiement;

(b) contribuer à la coopération entre les États membres en soutenant l'éducation, la formation et les exercices;

(c) réunir les parties prenantes, afin de favoriser les synergies entre la recherche et les marchés en matière de cybersécurité civile et militaire;

8. renforcer les synergies entre les dimensions civile et militaire de la cybersécurité en ce qui concerne le Fonds européen de la défense, en accomplissant les tâches suivantes:

(a) fournir des conseils, partager l'expertise et faciliter la collaboration entre les parties prenantes concernées;

(b) gérer des projets multinationaux de cyberdéfense, à la demande des États membres, et donc agir en tant que gestionnaire de projet au sens du règlement XXX [règlement instituant le Fonds européen de la défense].

Article 5

Investissements dans les infrastructures, capacités, produits ou solutions et recours à ceux-ci

1. Lorsque le Centre de compétences finance des infrastructures, des capacités, des produits ou des solutions, conformément à l'article 4, paragraphes 3 et 4, sous la forme d'une subvention ou d'un prix, le plan de travail du Centre de compétences peut préciser notamment:

   (a) les règles régissant l'exploitation d'une infrastructure ou d'une capacité, y compris, le cas échéant, le fait de confier l'exploitation à une entité d'accueil, sur la base de critères que le Centre de compétences définit;

   (b) les règles régissant l'accès et le recours à une infrastructure ou à une capacité.

2. Le Centre de compétences peut être chargé de l'exécution générale des actions d'acquisition conjointes pertinentes, y compris des achats publics avant commercialisation pour le compte de membres du Réseau, de membres de la communauté des compétences en matière de cybersécurité, ou d'autres tierces parties représentant les utilisateurs de produits et de solutions de cybersécurité. À cette fin, le Centre de compétences peut être assisté par un ou plusieurs centres nationaux de coordination ou par des membres de la communauté des compétences en matière de cybersécurité.

Article 6

Désignation des centres nationaux de coordination

1. Au plus tard le [date], chaque État membre désigne l'entité qui fera office de centre national de coordination aux fins du présent règlement et le notifie à la Commission.

2. Sur la base d'une évaluation du respect, par cette entité, des critères énoncés au paragraphe 4, la Commission prend une décision dans un délai de six mois à compter de la désignation transmise par l'État membre, prononçant l'accréditation de l'entité en tant que centre national de coordination ou rejetant la désignation. La liste des centres nationaux de coordination est publiée par la Commission.

3. Les États membres peuvent désigner à tout moment une nouvelle entité en tant que centre national de coordination aux fins du présent règlement. Les paragraphes 1 et 2 s'appliquent à la désignation de toute nouvelle entité.

4. Les centres nationaux de coordination désignés ont la capacité d'aider le Centre de compétences et le Réseau à remplir la mission qui leur est confiée en vertu de l'article 3 du présent règlement. Ils possèdent ou ont un accès direct à l'expertise technologique en matière de cybersécurité et sont en mesure d'établir des relations et d'assurer une coordination efficace avec l'industrie, le secteur public et la communauté scientifique.

5. Les relations entre le Centre de compétences et les centres nationaux de coordination sont fondées sur un accord contractuel signé entre le Centre de compétences et chacun des centres nationaux de coordination. L'accord définit les règles régissant

les relations et la répartition des tâches entre le Centre de compétences et chaque centre national de coordination.

6. Le Réseau des centres nationaux de coordination se compose de tous les centres nationaux de coordination désignés par les États membres.

Article 7

Tâches des centres nationaux de coordination

1. Les centres nationaux de coordination s'acquittent des tâches suivantes:

   (a) aider le Centre de compétences à atteindre ses objectifs et, en particulier, à coordonner la communauté des compétences en matière de cybersécurité;

   (b) favoriser la participation de l'industrie et d'autres acteurs au niveau des États membres à des projets transfrontaliers;

   (c) contribuer, avec le Centre de compétences, à recenser et à relever les défis industriels qui se posent dans chaque secteur en matière de cybersécurité;

   (d) faire office de point de contact au niveau national pour la communauté des compétences en matière de cybersécurité et le Centre de compétences;

   (e) s'efforcer de créer des synergies avec les activités pertinentes aux niveaux national et régional;

   (f) mettre en œuvre des actions spécifiques pour lesquelles des subventions ont été accordées par le Centre de compétences, y compris à travers la fourniture d'un soutien financier à des tiers conformément à l'article 204 du règlement XXX [nouveau règlement financier], dans les conditions spécifiées dans les conventions de subvention concernées;

   (g) promouvoir et diffuser les résultats pertinents des travaux du Réseau, de la communauté des compétences en matière de cybersécurité et du Centre de compétences aux niveaux national ou régional;

   (h) évaluer les demandes présentées par des entités établies dans le même État membre que le Centre de coordination en vue de faire partie de la communauté des compétences en matière de cybersécurité.

2. Aux fins du point f), le soutien financier à des tiers peut être fourni sous l'une des formes spécifiées à l'article 125 du règlement XXX [nouveau règlement financier], y compris sous la forme de montants forfaitaires.

3. Les centres nationaux de coordination peuvent recevoir une subvention de l'Union conformément à l'article 195, point d), du règlement XXX [nouveau règlement financier] pour l'exécution des tâches définies dans le présent article.

4. Les centres nationaux de coordination coopèrent, le cas échéant, par l'intermédiaire du Réseau aux fins de l'exécution des tâches visées au paragraphe 1, points a), b), c), e) et g).

Article 8

Communauté des compétences en matière de cybersécurité

1. La communauté des compétences en matière de cybersécurité contribue à la mission du Centre de compétences telle qu'elle est définie à l'article 3, et améliore et diffuse l'expertise en matière de cybersécurité dans toute l'Union.

2. La communauté des compétences en matière de cybersécurité se compose de l'industrie, d'organismes universitaires et d'organisations de recherche sans but lucratif, ainsi que d'associations, d'entités publiques et d'autres entités traitant de questions opérationnelles et techniques. Elle réunit les principales parties prenantes en ce qui concerne les capacités technologiques et industrielles en matière de cybersécurité dans l'Union. Elle associe les centres nationaux de coordination ainsi que les institutions et organes de l'Union disposant de l'expertise nécessaire.

3. Seules les entités établies au sein de l'Union peuvent être accréditées en tant que membres de la communauté des compétences en matière de cybersécurité. Elles doivent démontrer qu'elles possèdent des compétences spécialisées en matière de cybersécurité dans au moins l'un des domaines suivants:

   (a) recherche;

   (b) développement industriel;

   (c) formation et éducation.

4. Le Centre de compétences accrédite les entités établies en vertu du droit national en tant que membres de la communauté des compétences en matière de cybersécurité après une évaluation effectuée par le centre national de coordination de l'État membre dans lequel l'entité est établie, afin de déterminer si cette entité remplit les critères prévus au paragraphe 3. Une accréditation n'est pas limitée dans le temps, mais peut être révoquée à tout moment par le Centre de compétences si ce dernier ou le centre national de coordination compétent estime que l'entité ne remplit pas les critères énoncés au paragraphe 3 ou qu'elle relève des dispositions pertinentes énoncées à l'article 136 du règlement XXX [nouveau règlement financier].

5. Le Centre de compétences accrédite les organes et organismes pertinents de l'Union en tant que membres de la communauté des compétences en matière de cybersécurité, après avoir vérifié si cette entité satisfait aux critères énoncés au paragraphe 3. Une accréditation n'est pas limitée dans le temps, mais peut être révoquée à tout moment par le Centre de compétences si ce dernier estime que l'entité ne remplit pas les critères énoncés au paragraphe 3 ou qu'elle relève des dispositions pertinentes énoncées à l'article 136 du règlement XXX [nouveau règlement financier].

6. Les représentants de la Commission peuvent participer aux travaux de la communauté.

Article 9

Tâches des membres de la communauté des compétences en matière de cybersécurité

Les membres de la communauté des compétences en matière de cybersécurité:

(1) aident le Centre de compétences à réaliser la mission et les objectifs visés aux articles 3 et 4 et, à cette fin, travaillent en étroite collaboration avec le Centre de compétences et les centres nationaux de coordination concernés;

(2) participent aux activités promues par le Centre de compétences et les centres nationaux de coordination;

(3) le cas échéant, participent aux groupes de travail établis par le conseil de direction du Centre de compétences pour mener à bien les activités spécifiques prévues dans le plan de travail du Centre de compétences;

(4) le cas échéant, aident le Centre de compétences et les centres nationaux de coordination à promouvoir des projets spécifiques;

(5) promeuvent et diffusent les résultats pertinents des activités et des projets réalisés au sein de la communauté.

Article 10

Coopération entre le Centre de compétences et les institutions, organes et organismes de l'Union

1. Le Centre de compétences coopère avec les institutions, organes et organismes de l'Union concernés, notamment l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, l'équipe d'intervention en cas d'urgence informatique (CERT-UE), le Service européen pour l'action extérieure, le Centre commun de recherche de la Commission, l'Agence exécutive pour la recherche, l'Agence exécutive pour l'innovation et les réseaux, le Centre européen de lutte contre la cybercriminalité au sein d'Europol ainsi que l'Agence européenne de défense.

2. Cette coopération s'inscrit dans le cadre d'arrangements de travail. Ces arrangements sont soumis à l'approbation préalable de la Commission.

CHAPITRE II

ORGANISATION DU CENTRE DE COMPÉTENCES

Article 11

Composition et structure

1. Les membres du Centre de compétences sont l'Union, représentée par la Commission, et les États membres.

2. La structure du Centre de compétences se compose:

(a) d'un conseil de direction, qui exerce les tâches définies à l'article 13;

(b) d'un directeur exécutif, qui exerce les tâches définies à l'article 16;

(c) d'un comité consultatif industriel et scientifique, qui exerce les fonctions définies à l'article 20.

SECTION I

CONSEIL DE DIRECTION

Article 12

Composition du conseil de direction

1. Le conseil de direction se compose d'un représentant de chaque État membre et de cinq représentants de la Commission, au nom de l'Union.

2. Chaque membre du conseil de direction dispose d'un suppléant, qui le représente en cas d'absence.

3. Les membres du conseil de direction et leurs suppléants sont nommés sur la base de leurs connaissances dans le domaine de la technologie, ainsi que de leurs compétences pertinentes en matière de gestion, d'administration et de budget. La Commission et les États membres s'efforcent de limiter le roulement de leurs représentants au sein du conseil de direction, afin de garantir la continuité des travaux de celui-ci. La Commission et les États membres visent à atteindre une représentation équilibrée entre hommes et femmes au sein du conseil de direction.

4. Le mandat des membres du conseil de direction et de leurs suppléants a une durée de quatre ans. Ce mandat est renouvelable.

5. Les membres du conseil de direction agissent dans l'intérêt du Centre de compétences, en défendant ses objectifs et sa mission, son identité, son autonomie et sa cohérence, en toute indépendance et transparence.

6. La Commission peut inviter des observateurs, notamment des représentants d'organes et organismes compétents de l'Union, à prendre part, le cas échéant, aux réunions du conseil de direction.

7. L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) est un observateur permanent au sein du conseil de direction.

Article 13

Tâches du conseil de direction

1. Le conseil de direction a la responsabilité globale de l'orientation stratégique et du fonctionnement du Centre de compétences et supervise la mise en œuvre de ses activités.

2. Le conseil de direction arrête son règlement intérieur. Ces règles comprennent des procédures spécifiques visant à détecter et prévenir les conflits d'intérêts et à garantir la confidentialité de toutes les informations sensibles.

3. Le conseil de direction prend les décisions stratégiques nécessaires, notamment, il:

   (a) adopte un plan stratégique pluriannuel, contenant un exposé des principales priorités et initiatives prévues du Centre de compétences, y compris une estimation des besoins et des sources de financement;

   (b) adopte le plan de travail, les comptes annuels, le bilan et le rapport annuel d'activités du Centre de compétences, sur la base d'une proposition du directeur exécutif;

   (c) adopte les règles financières spécifiques du Centre de compétences conformément à [l'article 70 du RF];

   (d) adopte une procédure de nomination du directeur exécutif;

   (e) adopte les critères et les procédures d'évaluation et d'accréditation des entités en tant que membres de la communauté des compétences en matière de cybersécurité;

   (f) nomme le directeur exécutif, le révoque, prolonge son mandat, lui fournit des orientations et contrôle ses résultats, et nomme le comptable;

(g) adopte le budget annuel du Centre de compétences, y compris le tableau correspondant des effectifs indiquant le nombre de postes temporaires par groupe de fonctions et par grade ainsi que le nombre d'agents contractuels et d'experts nationaux détachés, exprimé en équivalent temps plein;

(h) adopte des règles concernant les conflits d'intérêts;

(i) constitue des groupes de travail composés de membres de la communauté des compétences en matière de cybersécurité;

(j) nomme les membres du comité consultatif industriel et scientifique;

(k) met en place une fonction d'audit interne conformément au règlement délégué (UE) nº 1271/2013 de la Commission[28];

(l) promeut le Centre de compétences à l'échelle mondiale, afin d'accroître son attractivité et d'en faire un organisme d'excellence de classe mondiale en matière de cybersécurité;

(m) élabore la politique de communication du Centre de compétences sur recommandation du directeur exécutif;

(n) est responsable du suivi adéquat des conclusions des évaluations rétrospectives;

(o) arrête, le cas échéant, les modalités d'application du statut et du régime conformément à l'article 31, paragraphe 3;

(p) établit, le cas échéant, les règles applicables au détachement d'experts nationaux auprès du Centre de compétences et à l'emploi de stagiaires, conformément à l'article 32, paragraphe 2;

(q) adopte des règles de sécurité pour le Centre de compétences;

(r) adopte une stratégie antifraude qui est proportionnée aux risques de fraude compte tenu de l'analyse coût-bénéfice des mesures à mettre en œuvre;

(s) adopte la méthode de calcul de la contribution financière des États membres;

(t) assume la responsabilité de toute tâche qui n'est pas spécifiquement attribuée à un organe donné du Centre de compétences; il peut confier ces tâches à l'un ou l'autre membre du Centre de compétences.

Article 14

Président et réunions du conseil de direction

1. Le conseil de direction élit un président et un vice-président parmi les membres disposant du droit de vote, pour une période de deux ans. Le mandat du président et du vice-président peut être prorogé une fois, sur décision du conseil de direction. Cependant, si le président ou le vice-président perd sa qualité de membre du conseil de direction à un moment quelconque de son mandat, ledit mandat expire automatiquement à la même date. Le vice-président remplace d'office le président

[28] Règlement délégué (UE) nº 1271/2013 de la Commission du 30 septembre 2013 portant règlement financier-cadre des organismes visés à l'article 208 du règlement (UE, Euratom) nº 966/2012 du Parlement européen et du Conseil (JO L 328 du 7.12.2013, p. 42).

lorsque celui-ci n'est pas en mesure d'assumer ses fonctions. Le président participe au vote.

2. Le conseil de direction tient ses réunions ordinaires au moins trois fois par an. Il peut tenir des réunions extraordinaires à la demande de la Commission, à la demande d'un tiers de tous ses membres, à la demande du président, ou à la demande du directeur exécutif dans l'accomplissement de ses tâches.

3. Le directeur exécutif prend part aux délibérations, à moins que le conseil de direction n'en décide autrement, mais il n'a pas de droit de vote. Le conseil de direction peut inviter au cas par cas d'autres personnes à assister à ses réunions en qualité d'observateurs.

4. Les membres du comité consultatif industriel et scientifique peuvent participer, sur invitation du président, aux réunions du conseil de direction, sans droit de vote.

5. Les membres du conseil de direction et leurs suppléants peuvent, sous réserve du règlement intérieur, être assistés par des conseillers ou des experts lors des réunions.

6. Le Centre de compétences assure le secrétariat du conseil de direction.

Article 15

Modalités de vote du conseil de direction

1. L'Union détient 50 % des droits de vote. Les droits de vote de l'Union sont indivisibles.

2. Chaque État membre participant dispose d'une voix.

3. Le conseil de direction prend ses décisions à la majorité d'au moins 75 % de l'ensemble des voix, y compris celles des membres absents, représentant au moins 75 % du total des contributions financières au Centre de compétences. La contribution financière sera calculée sur la base des estimations des dépenses proposées par les États membres visées à l'article 17, paragraphe 2, point c), et sur la base du rapport sur la valeur des contributions des États membres participants visée à l'article 22, paragraphe 5.

4. Seuls les représentants de la Commission et les représentants des États membres participants disposent du droit de vote.

5. Le président participe au vote.

SECTION II

DIRECTEUR EXÉCUTIF

Article 16

Nomination, révocation et prorogation du mandat du directeur exécutif

1. Le directeur exécutif est une personne possédant une grande compétence et jouissant d'une haute réputation dans les domaines d'activité du Centre de compétence.

2. Le directeur exécutif est engagé en tant qu'agent temporaire du Centre de compétences conformément à l'article 2, point a), du régime applicable aux autres agents.

3. Le directeur exécutif est nommé par le conseil de direction à partir d'une liste de candidats proposés par la Commission à la suite d'une procédure de sélection ouverte et transparente.

4. Aux fins de la conclusion du contrat du directeur exécutif, le Centre de compétences est représenté par le président du conseil de direction.

5. Le mandat du directeur exécutif est de quatre ans. Avant la fin de cette période, la Commission procède à une évaluation qui tient compte de l'évaluation du travail accompli par le directeur exécutif et des tâches et défis futurs du Centre de compétences.

6. Le conseil de direction, sur proposition de la Commission tenant compte de l'examen visé au paragraphe 5, peut proroger une fois le mandat du directeur exécutif, pour une durée n'excédant pas quatre ans.

7. Un directeur exécutif dont le mandat a été prolongé ne peut pas participer à une nouvelle procédure de sélection pour le même poste.

8. Le directeur exécutif n'est démis de ses fonctions que sur décision du conseil de direction, statuant sur proposition de la Commission.

Article 17

Tâches du directeur exécutif

1. Le directeur exécutif est chargé des opérations et de la gestion quotidienne du Centre de compétences, dont il est le représentant légal. Il rend compte de sa gestion au conseil de direction et exerce ses fonctions en toute indépendance, dans les limites des pouvoirs qui lui sont dévolus.

2. En particulier, le directeur exécutif exerce les tâches suivantes de manière indépendante:

   (a) mettre en œuvre les décisions adoptées par le conseil de direction;

   (b) assister le conseil de direction dans ses travaux, assurer le secrétariat de ses réunions et fournir toutes les informations nécessaires à l'exercice de ses fonctions;

   (c) après consultation du conseil de direction et de la Commission, préparer et soumettre pour adoption au conseil de direction le projet de plan stratégique pluriannuel et le projet de plan de travail annuel du Centre de compétences, y compris la portée des appels à propositions, des appels à manifestation d'intérêt et des appels d'offres nécessaires à la mise en œuvre du plan de travail et les estimations de dépenses correspondantes, comme proposé par les États membres et la Commission;

   (d) préparer et soumettre pour adoption au comité directeur le projet de budget annuel, y compris le tableau des effectifs correspondant indiquant le nombre d'emplois temporaires dans chaque grade et chaque groupe de fonctions et le nombre d'agents contractuels et d'experts nationaux détachés, exprimés en équivalents temps plein;

   (e) mettre en œuvre le plan de travail et en rendre compte au conseil de direction;

   (f) élaborer le projet de rapport annuel d'activités du Centre de compétences, y compris les informations sur les dépenses correspondantes;

(g) assurer la mise en œuvre de procédures efficaces de suivi et d'évaluation des résultats du Centre de compétences;

(h) préparer un plan d'action faisant suite aux conclusions des évaluations rétrospectives et de faire rapport tous les deux ans à la Commission sur les progrès accomplis;

(i) préparer, négocier et conclure les accords avec les centres nationaux de coordination;

(j) assumer les responsabilités des questions administratives, financières et de personnel, y compris de l'exécution du budget du Centre de compétences, en tenant dûment compte des avis reçus de la fonction d'audit interne, dans les limites de la délégation par le conseil de direction;

(k) approuver et gérer le lancement des appels à propositions, conformément au plan de travail et gérer les conventions et les décisions de subvention;

(l) approuver la liste des actions sélectionnées en vue d'un financement sur la base du classement établi par un groupe d'experts indépendants;

(m) approuver et gérer le lancement des appels d'offres, conformément au plan de travail, et gérer les contrats;

(n) approuver les offres retenues en vue d'un financement;

(o) soumettre les projets de comptes annuels et de bilan à la fonction d'audit interne et, par la suite, au conseil de direction;

(p) s'assurer de la bonne exécution de l'évaluation et de la gestion des risques;

(q) signer les conventions, décisions et contrats de subvention;

(r) signer les contrats de passation de marché;

(s) préparer un plan d'action donnant suite aux conclusions des rapports d'audit internes ou externes, ainsi qu'aux enquêtes de l'Office européen de lutte antifraude (OLAF), et présenter des rapports semestriels à la Commission et des rapports réguliers au conseil de direction sur les progrès accomplis;

(t) préparer un projet de règles financières applicables au Centre de compétences;

(u) mettre en place un système de contrôle interne efficace et efficient et en assurer le fonctionnement, et faire rapport au conseil de direction de tout changement important qui y serait apporté;

(v) assurer une communication efficace avec les institutions de l'Union;

(w) prendre toute autre mesure nécessaire pour évaluer les progrès accomplis par le Centre de compétences dans la réalisation de sa mission et de ses objectifs, tels qu'énoncés aux articles 3 et 4 du présent règlement;

(x) exécuter toutes les autres tâches qui lui sont confiées ou déléguées par le conseil de direction.

SECTION III

COMITÉ CONSULTATIF INDUSTRIEL ET SCIENTIFIQUE

Article 18

Composition du comité consultatif industriel et scientifique

1. Le comité consultatif industriel et scientifique se compose de seize membres au maximum. Les membres sont nommés par le conseil de direction parmi les représentants des entités de la communauté des compétences en matière de cybersécurité.

2. Les membres du comité consultatif industriel et scientifique possèdent une expertise en matière de recherche sur la cybersécurité, de développement industriel, de services professionnels ou de leur déploiement. Les exigences relatives à cette expertise sont précisées par le conseil de direction.

3. Les procédures relatives à la nomination de ses membres par le conseil de direction et à son fonctionnement sont précisées dans le règlement intérieur du Centre de compétences et sont rendues publiques.

4. La durée du mandat des membres du comité consultatif industriel et scientifique est de trois ans. Ce mandat est renouvelable.

5. Des représentants de la Commission et de l'Agence européenne chargée de la sécurité des réseaux et de l'information peuvent participer aux travaux du comité consultatif industriel et scientifique et les appuyer.

Article 19

Fonctionnement du comité consultatif industriel et scientifique

1. Le comité consultatif industriel et scientifique se réunit au moins deux fois par an.

2. Le comité consultatif industriel et scientifique peut conseiller le conseil de direction sur la création de groupes de travail sur des questions spécifiques en rapport avec les travaux du Centre de compétences, le cas échéant sous la coordination générale d'un ou de plusieurs membres du comité consultatif industriel et scientifique.

3. Le comité consultatif industriel et scientifique élit son président.

4. Le comité consultatif industriel et scientifique adopte son règlement intérieur, lequel inclut la nomination des représentants qui représentent le comité consultatif, le cas échéant, et la durée de leur nomination.

Article 20

Tâches du comité consultatif industriel et scientifique

Le comité consultatif industriel et scientifique conseille le Centre de compétences sur l'exécution de ses activités et:

(1) fournit au directeur exécutif et au conseil de direction des conseils et des avis stratégiques en vue de l'élaboration du plan de travail et du plan stratégique pluriannuel dans les délais fixés par le conseil de direction;

(2) organise des consultations publiques ouvertes à toutes les parties prenantes publiques et privées ayant un intérêt dans le domaine de la cybersécurité, afin de recueillir des contributions pour les conseils stratégiques visés au paragraphe 1;

(3) encourage et recueille tout retour d'information sur le plan de travail et le plan stratégique pluriannuel du Centre de compétences.

CHAPITRE III

DISPOSITIONS FINANCIÈRES

Article 21

Contribution financière de l'Union

1. La contribution de l'Union au Centre de compétences pour couvrir les coûts administratifs et les frais de fonctionnement comprend les éléments suivants:

   (a) 1 981 668 000 EUR provenant du programme pour une Europe numérique, dont jusqu'à 23 746 000 EUR pour les coûts administratifs;

   (b) un montant provenant du programme «Horizon Europe», y compris pour les coûts administratifs, à déterminer en tenant compte du processus de planification stratégique à mettre en œuvre conformément à l'article 6, paragraphe 6, du règlement XXX [règlement «Horizon Europe»].

2. La contribution maximale de l'Union est prélevée sur les crédits du budget général de l'Union alloués au [programme pour une Europe numérique] et au programme spécifique d'exécution du programme «Horizon Europe», établi par la décision XXX.

3. Le Centre de compétences met en œuvre les actions de cybersécurité du [programme pour une Europe numérique] et du [programme «Horizon Europe»] conformément à l'article 62, point c) iv), du règlement (UE, Euratom) XXX[29] [le règlement financier].

4. La contribution financière de l'Union ne couvre pas les tâches visées à l'article 4, paragraphe 8, point b).

Article 22

Contributions des États membres participants

1. Les États membres participants apportent une contribution totale aux frais de fonctionnement et aux coûts administratifs du Centre de compétences d'un montant au moins équivalent à celui visé à l'article 21, paragraphe 1, du présent règlement.

2. Aux fins de l'évaluation des contributions visées au paragraphe 1 et à l'article 23, paragraphe 3, point b) ii), les coûts sont déterminés conformément aux pratiques comptables habituelles des États membres concernés, aux normes comptables applicables de l'État membre, ainsi qu'aux normes comptables internationales et aux normes internationales d'information financière applicables. Les coûts sont certifiés par un auditeur externe indépendant désigné par l'État membre concerné. La méthode d'évaluation peut être vérifiée par le Centre de compétences en cas de doute quant à la certification.

3. Si l'un des États membres participants se trouve en situation de défaut d'exécution de ses engagements en matière de contribution financière, le directeur exécutif le consigne par écrit et fixe un délai raisonnable pour remédier à la situation. S'il n'est pas remédié à la situation dans ce délai, le directeur exécutif convoque une réunion du conseil de direction pour décider si le droit de vote de l'État membre participant défaillant doit être révoqué ou si d'autres mesures doivent être prises jusqu'à ce que ses obligations soient remplies. Les droits de vote de l'État membre défaillant sont suspendus jusqu'à ce qu'il soit remédié au défaut d'exécution de ses engagements.

[29] [ajouter le titre complet et la référence du JO].

4. La Commission peut mettre un terme, réduire proportionnellement ou suspendre la contribution financière de l'Union au Centre de compétences si les États membres participants ne contribuent pas ou n'apportent que partiellement ou tardivement les contributions visées au paragraphe 1.

5. Les États membres participants communiquent au conseil de direction, au plus tard le 31 janvier de chaque année, la valeur des contributions visées au paragraphe 1 versées au cours de chacun des exercices précédents.

Article 23

Coûts et ressources du Centre de compétences

1. Le Centre de compétences est financé conjointement par l'Union et les États membres au moyen de contributions financières versées par tranches et de contributions correspondant aux coûts supportés par les centres nationaux de coordination et les bénéficiaires pour la mise en œuvre d'actions qui ne sont pas remboursées par le Centre de compétences.

2. Les coûts administratifs du Centre de compétences ne dépassent pas [nombre] EUR et sont couverts par des contributions financières réparties à parts égales sur une base annuelle entre l'Union et les États membres participants. Si une partie des contributions aux coûts administratifs n'est pas utilisée, elle peut être mise à disposition pour couvrir les frais de fonctionnement du Centre de compétences.

3. Les frais de fonctionnement du Centre de compétences sont couverts par les moyens suivants:

   (a) la contribution financière de l'Union;

   (b) les contributions des États membres participants sous la forme:

      (i) de contributions financières; et

      ii) le cas échéant, de contributions en nature des États membres participants aux coûts supportés par les centres nationaux de coordination et les bénéficiaires pour la mise en œuvre des actions indirectes, déduction faite de la contribution du Centre de compétences et de toute autre contribution de l'Union à ces coûts;

4. Les ressources du Centre de compétences inscrites à son budget proviennent des contributions suivantes:

   (a) les contributions financières des États membres participants aux coûts administratifs;

   (b) les contributions financières des États membres participants aux frais de fonctionnement;

   (c) toute recette générée par le Centre de compétences;

   (d) toutes autres recettes, ressources et contributions financières.

5. Les intérêts produits par les contributions versées au Centre de compétences par les États membres participants sont considérés comme une recette de celui-ci.

6. Toutes les ressources du Centre de compétences et ses activités visent à atteindre les objectifs fixés à l'article 4.

7. Le Centre de compétences est propriétaire de tous les actifs qu'il génère ou qui lui sont transférés aux fins de la réalisation de ses objectifs.

8. Sauf en cas de liquidation du Centre de compétences, les excédents de recettes éventuels ne sont pas reversés aux membres participants du Centre de compétences.

Article 24

Engagements financiers

Les engagements financiers du Centre de compétences n'excèdent pas le montant des ressources financières disponibles ou inscrites à son budget par ses membres.

Article 25

Exercice financier

L'exercice budgétaire commence le 1er janvier et s'achève le 31 décembre.

Article 26

Établissement du budget

1. Chaque année, le directeur exécutif établit un projet d'état prévisionnel des recettes et des dépenses du Centre de compétences pour l'exercice budgétaire suivant et le transmet au conseil de direction avec un projet de tableau des effectifs. Les recettes et les dépenses sont équilibrées. Les dépenses du Centre de compétences comprennent les dépenses de personnel, d'administration, d'infrastructure et de fonctionnement. Les dépenses administratives sont réduites au minimum.

2. Le conseil de direction établit chaque année, sur la base du projet d'état prévisionnel des recettes et des dépenses visé au paragraphe 1, un état prévisionnel des recettes et des dépenses du Centre de compétences pour l'exercice budgétaire suivant.

3. Le conseil de direction transmet à la Commission, au plus tard le 31 janvier de chaque année, l'état prévisionnel visé au paragraphe 2, qui fait partie du projet de document unique de programmation.

4. Sur la base de cet état prévisionnel, la Commission inscrit dans le projet de budget général de l'Union les prévisions qu'elle estime nécessaires en ce qui concerne le tableau des effectifs et le montant de la contribution à la charge du budget général et le soumet au Parlement européen et au Conseil conformément aux articles 313 et 314 du traité sur le fonctionnement de l'Union européenne.

5. Le Parlement européen et le Conseil autorisent les crédits au titre de la contribution destinée au Centre de compétences.

6. Le Parlement européen et le Conseil adoptent le tableau des effectifs du Centre de compétences.

7. En même temps que le plan de travail, le conseil de direction adopte le budget du Centre. Ce budget devient définitif après l'adoption définitive du budget général de l'Union. Le cas échéant, le conseil de direction adapte le budget et le plan de travail du Centre de compétences en fonction du budget général de l'Union.

Article 27

Présentation des comptes du Centre de compétences et décharge

La présentation des comptes provisoires et définitifs du Centre de compétences ainsi que la décharge suivent les règles et le calendrier du règlement financier et de ses règles financières adoptées conformément à l'article 29.

Article 28

Rapports opérationnels et financiers

1. Le directeur exécutif présente chaque année au conseil de direction un rapport sur l'exécution de ses tâches conformément aux règles financières du Centre de compétences.

2. Dans un délai de deux mois à compter de la fin de chaque exercice financier, le directeur exécutif soumet au conseil de direction, pour approbation, un rapport d'activité annuel sur les progrès accomplis par le Centre de compétences au cours de l'année civile précédente, au regard notamment du plan de travail adopté pour l'année en question. Ce rapport comprend, entre autres, des informations sur les points suivants:

   (a) les actions opérationnelles qui ont été réalisées, ainsi que les dépenses correspondantes;

   (b) les actions proposées, incluant une ventilation par type de participants, y compris les PME, ainsi que par État membre;

   (c) les actions sélectionnées en vue d'un financement, avec une ventilation par type de participant, y compris les PME, et par État membre, indiquant les contributions versées par le Centre de compétences à chaque participant et pour chaque action;

   (d) les progrès accomplis en vue de la réalisation des objectifs, tels qu'ils sont énoncés à l'article 4, et les propositions concernant d'autres initiatives nécessaires pour atteindre lesdits objectifs.

3. Une fois approuvé par le conseil de direction, le rapport d'activité annuel est rendu public.

Article 29

Règles financières

Le Centre de compétences adopte ses règles financières spécifiques conformément à l'article 70 du règlement XXX [nouveau règlement financier].

Article 30

Protection des intérêts financiers

1. Le Centre de compétences prend les mesures appropriées pour garantir la protection des intérêts financiers de l'Union lors de la mise en œuvre d'actions financées au titre du présent règlement, par l'application de mesures préventives contre la fraude, la corruption et toute autre activité illégale, par des contrôles efficaces et, si des irrégularités sont décelées, par le recouvrement des montants indûment versés et, s'il y a lieu, par des sanctions administratives effectives, proportionnées et dissuasives.

2. Le Centre de compétences accorde au personnel de la Commission et aux autres personnes autorisées par celle-ci, ainsi qu'à la Cour des comptes, un droit d'accès à ses sites et locaux, ainsi qu'à toutes les informations, y compris sous forme électronique, qui sont nécessaires pour mener à bien leurs audits.

3. L'Office européen de lutte antifraude (OLAF) peut mener des enquêtes, y compris des contrôles et vérifications sur place, conformément aux dispositions et procédures prévues par le règlement (Euratom, CE) nº 2185/96 du Conseil[30] et le règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil[31] en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, en rapport avec une convention de subvention ou un contrat bénéficiant d'un financement direct ou indirect au titre du présent règlement.

4. Sans préjudice des paragraphes 1, 2 et 3 du présent article, les contrats et les conventions de subvention résultant de la mise en œuvre du présent règlement contiennent des dispositions habilitant expressément la Commission, le Centre de compétences, la Cour des comptes et l'OLAF à procéder à ces audits et enquêtes en conformité avec leurs compétences respectives. Lorsque la mise en œuvre d'une action est externalisée ou sous-traitée en tout ou partie, ou lorsqu'elle nécessite l'attribution d'un marché ou un soutien financier à un tiers, le contrat ou la convention de subvention prévoit l'obligation, pour le contractant ou le bénéficiaire, d'imposer à tout tiers concerné l'acceptation explicite de ces pouvoirs de la Commission, du Centre de compétences, de la Cour des comptes et de l'OLAF.

CHAPITRE IV

PERSONNEL DU CENTRE DE COMPÉTENCES

Article 31

Personnel

1. Le statut des fonctionnaires et le régime applicable aux autres agents de l'Union européenne, fixés par le règlement (CEE, Euratom, CECA) nº 259/68 du Conseil[32] (ci-après le «statut» et le «régime»), ainsi que les règles adoptées conjointement par les institutions de l'Union aux fins de l'application du statut et du régime, s'appliquent au personnel du Centre de compétences.

2. Le conseil de direction exerce, à l'égard du personnel du Centre de compétences, les compétences conférées par le statut à l'autorité investie du pouvoir de nomination et

---

30 Règlement (Euratom, CE) nº 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2).

31 Règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) nº 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) nº 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

32 Règlement (CEE, Euratom, CECA) nº 259/68 du Conseil du 29 février 1968 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (JO L 56 du 4.3.1968, p. 1).

les compétences conférées par le régime à l'autorité habilitée à conclure les contrats (les «compétences relevant de l'autorité investie du pouvoir de nomination»).

3. Le conseil de direction adopte, conformément à l'article 110 du statut des fonctionnaires, une décision fondée sur l'article 2, paragraphe 1, du statut et sur l'article 6 du régime, déléguant au directeur exécutif les compétences correspondantes de l'autorité investie du pouvoir de nomination et définissant les conditions dans lesquelles cette délégation peut être suspendue. Le directeur exécutif est autorisé à subdéléguer ces compétences.

4. Lorsque des circonstances exceptionnelles l'exigent, le conseil de direction peut, par voie de décision, suspendre temporairement la délégation au directeur exécutif des compétences relevant de l'autorité investie du pouvoir de nomination et toute subdélégation de ces compétences par ce dernier. Dans ce cas, le conseil de direction exerce lui-même les compétences relevant de l'autorité investie du pouvoir de nomination ou les délègue à l'un de ses membres ou à un membre du personnel du Centre de compétences autre que le directeur exécutif.

5. Le conseil de direction arrête les modalités de mise en œuvre en ce qui concerne le statut et le régime conformément à l'article 110 du statut.

6. Les effectifs sont déterminés par le tableau des effectifs du Centre de compétences indiquant le nombre d'emplois temporaires par groupe de fonctions et par grade et les effectifs en personnel contractuel exprimés en équivalents temps plein, conformément à son budget annuel.

7. Le personnel du Centre de compétences se compose d'agents temporaires et d'agents contractuels.

8. Toutes les dépenses de personnel sont à la charge du Centre de compétences.

Article 32

Experts nationaux détachés et autre personnel

1. Le Centre de compétences peut recourir à des experts nationaux détachés ou à d'autres membres du personnel qui ne sont pas employés par le Centre de compétences.

2. Le conseil de direction adopte une décision fixant les règles applicables au détachement d'experts nationaux auprès du Centre de compétences, en accord avec la Commission.

Article 33

Privilèges et immunités

Le protocole nº 7 sur les privilèges et immunités de l'Union européenne annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne s'applique au Centre de compétences et à son personnel.

CHAPITRE V
DISPOSITIONS COMMUNES

Article 34

Règles de sécurité

1. L'article 12, paragraphe 7, du règlement (UE) nº XXX [programme pour une Europe numérique] s'applique à la participation à toutes les actions financées par le Centre de compétences.

2. Les règles de sécurité spécifiques suivantes s'appliquent aux actions financées par le programme «Horizon Europe»:

   (a) aux fins de l'article 34, paragraphe 1 [Propriété et protection], du règlement (UE) nº XXX [programme «Horizon Europe»], lorsque le plan de travail le prévoit, l'octroi de licences non exclusives peut être limité à des tiers établis ou réputés établis dans des États membres et contrôlés par des États membres et/ou des ressortissants d'États membres;

   (b) aux fins de l'article 36, paragraphe 4, point b) [Transfert et octroi de licences], du règlement (UE) nº XXX [programme «Horizon Europe»], le transfert ou la concession d'une licence à une entité juridique établie dans un pays associé ou établie dans l'Union, mais contrôlée depuis des pays tiers, constitue également un motif d'objection aux transferts de propriété des résultats ou à l'octroi d'une licence exclusive en ce qui concerne les résultats;

   (c) aux fins de l'article 37, paragraphe 3, point a) [Droits d'accès], du règlement (UE) nº XXX [programme «Horizon Europe»], lorsque le plan de travail le prévoit, l'octroi de l'accès aux résultats et à l'historique peut être limité uniquement à une entité juridique établie ou réputée établie dans des États membres et contrôlée par des États membres et/ou des ressortissants des États membres.

Article 35

Transparence

1. Le Centre de compétences mène ses activités dans une large transparence.

2. Le Centre de compétences veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux. Il rend également publiques les déclarations d'intérêt faites conformément à l'article 41.

3. Le conseil de direction peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités du Centre de compétences.

4. Le Centre de compétences fixe dans son règlement intérieur les modalités pratiques assurant l'application des règles de transparence visées aux paragraphes 1 et 2. S'agissant des actions financées au titre du programme «Horizon Europe», il sera dûment tenu compte des dispositions de l'annexe III du règlement «Horizon Europe».

Article 36

Règles de sécurité en matière de protection des informations classifiées et des informations sensibles non classifiées

1. Sans préjudice de l'article 35, le Centre de compétences ne divulgue pas à des tiers les informations qu'il traite ou qu'il reçoit et pour lesquelles une demande motivée de traitement confidentiel, en tout ou en partie, a été faite.

2. Les membres du conseil de direction, le directeur exécutif, les membres du comité consultatif industriel et scientifique, les experts externes participant aux groupes de travail ad hoc et les membres du personnel du Centre de compétences se conforment aux exigences de confidentialité prévues à l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions.

3. Le conseil de direction du Centre de compétences adopte les règles de sécurité du Centre de compétences, après approbation par la Commission, sur la base des principes et des règles établis dans les règles de sécurité de la Commission pour la protection des informations classifiées de l'Union européenne (ICUE) et des informations sensibles non classifiées, y compris, entre autres, des dispositions relatives au traitement et au stockage de ces informations telles que définies dans les décisions de la Commission (UE, Euratom) 2015/443[33] et 2015/444[34].

4. Le Centre de compétences peut prendre toutes les mesures nécessaires pour faciliter l'échange, avec la Commission et les États membres et, le cas échéant, les agences et organes de l'Union concernés, d'informations utiles à l'exécution de ses tâches. Tout arrangement administratif conclu à cette fin concernant le partage d'ICUE ou, en l'absence d'un tel arrangement, toute communication ad hoc exceptionnelle d'ICUE doit avoir reçu l'accord préalable de la Commission.

Article 37

Accès aux documents

1. Le règlement (CE) nº 1049/2001 s'applique aux documents détenus par le Centre de compétences.

2. Le conseil de direction adopte des dispositions pour la mise en œuvre du règlement (CE) nº 1049/2001 dans les six mois suivant la création du Centre de compétences.

3. Les décisions prises par le Centre de compétences en application de l'article 8 du règlement (CE) nº 1049/2001 peuvent faire l'objet d'une plainte auprès du médiateur au titre de l'article 228 du traité sur le fonctionnement de l'Union européenne ou d'un recours devant la Cour de justice de l'Union européenne au titre de l'article 263 du traité sur le fonctionnement de l'Union européenne.

Article 38

Suivi, évaluation et réexamen

[33] Décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41).

[34] Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

1. Le Centre de compétences veille à ce que ses activités, y compris celles qui sont gérées par l'intermédiaire des centres nationaux de coordination et du Réseau, fassent l'objet d'un suivi continu et systématique et d'une évaluation périodique. Le Centre de compétences veille à ce que les données nécessaires au suivi de la mise en œuvre et des résultats du programme soient collectées de manière efficace, effective et en temps utile, et à ce que les bénéficiaires de fonds de l'Union et les États membres soient soumis à des exigences proportionnées en matière de rapports. Les résultats des évaluations sont rendus publics.

2. Dès qu'elle dispose d'informations suffisantes sur la mise en œuvre du présent règlement, et au plus tard trois ans et demi après le début de la mise en œuvre du présent règlement, la Commission procède à une évaluation intermédiaire du Centre de compétences. La Commission établit un rapport sur cette évaluation et soumet ce rapport au Parlement européen et au Conseil au plus tard le 31 décembre 2024. Le Centre de compétences et les États membres fournissent à la Commission les informations nécessaires à l'établissement de ce rapport.

3. L'évaluation visée au paragraphe 2 examine les résultats obtenus par le Centre de compétences, à la lumière de ses objectifs, de son mandat et de ses tâches. Si la Commission estime que le maintien du Centre de compétences est justifié au regard des objectifs, du mandat et des tâches qui lui ont été assignés, elle peut proposer le prolongement de la durée du mandat du Centre de compétences énoncée à l'article 46.

4. Sur la base des conclusions de l'évaluation intermédiaire visée au paragraphe 2, la Commission peut agir conformément à [l'article 22, paragraphe 5], ou prendre toute autre mesure appropriée.

5. Le suivi, l'évaluation, la suppression progressive et le renouvellement de la contribution au titre du programme «Horizon Europe» se baseront sur les dispositions des articles 8, 45 et 47 et de l'annexe III du règlement «Horizon Europe», ainsi que les modalités de mise en œuvre convenues.

6. Le suivi, l'établissement de rapports et l'évaluation de la contribution du programme pour une Europe numérique se baseront sur les dispositions des articles 24 et 25 du programme pour une Europe numérique.

7. En cas de liquidation du Centre de compétences, la Commission procède à une évaluation finale du Centre de compétences dans les six mois suivant sa liquidation, et au plus tard deux ans après le déclenchement de la procédure de liquidation visée à l'article 46 du présent règlement. Les résultats de cette évaluation finale sont présentés au Parlement européen et au Conseil.

Article 39

Responsabilité du Centre de compétences

1. La responsabilité contractuelle du Centre de compétences est régie par le droit applicable à l'accord, à la décision ou au contrat en cause.

2. En matière de responsabilité non contractuelle, le Centre de compétences doit réparer, conformément aux principes généraux communs aux droits des États membres, les dommages causés par ses agents dans l'exercice de leurs fonctions.

3. Tout paiement du Centre de compétences relatif à la responsabilité mentionnée aux paragraphes 1 et 2, ainsi que les frais et dépenses exposés en relation avec celle-ci,

sont considérés comme dépenses du Centre de compétences et sont couverts par ses ressources.

4. Le Centre de compétences répond seul de ses obligations.

Article 40

Compétence de la Cour de justice de l'Union européenne et droit applicable

1. La Cour de justice de l'Union européenne est compétente:

   (1) en vertu des clauses compromissoires contenues dans les conventions ou contrats passés ou dans les décisions adoptées par le Centre de compétences;

   (2) sur les litiges concernant la réparation des dommages causés par les agents du Centre de compétences dans l'exercice de leurs fonctions;

   (3) pour tout litige entre le Centre de compétences et son personnel dans les limites et dans les conditions prévues par le statut des fonctionnaires.

2. Le droit de l'État membre où se trouve le siège du Centre de compétences est applicable à toute matière non couverte par le présent règlement ou par d'autres actes juridiques de l'Union.

Article 41

Responsabilité des membres et assurance

1. La responsabilité financière des membres en ce qui concerne les dettes du Centre de compétences est limitée à la contribution qu'ils ont déjà versée pour couvrir les coûts administratifs.

2. Le Centre de compétences contracte et acquitte les assurances nécessaires.

Article 42

Conflits d'intérêts

Le conseil de direction du Centre de compétences adopte des règles en matière de prévention et de gestion des conflits d'intérêts qui s'appliquent à ses membres, à ses organes et à son personnel. Ces règles contiennent des dispositions visant à éviter tout conflit d'intérêts impliquant des représentants des membres siégeant au conseil de direction ainsi qu'au comité consultatif industriel et scientifique, conformément au règlement XXX [nouveau règlement financier].

Article 43

Protection des données à caractère personnel

1. Les opérations de traitement de données à caractère personnel effectuées par le Centre de compétences sont soumises au règlement (UE) XXX/2018 du Parlement européen et du Conseil.

2. Le conseil de direction adopte les dispositions d'application visées à l'article xx, paragraphe 3, du règlement (UE) xxx/2018. Le conseil de direction peut adopter les mesures supplémentaires nécessaires à l'application du règlement (UE) nº xxx/2018 par le Centre de compétences.

Article 44

Soutien apporté par l'État membre d'accueil

Un accord administratif peut être conclu entre le Centre de compétences et l'État membre [la Belgique] où se trouve son siège en ce qui concerne les privilèges et immunités et les autres formes de soutien à fournir par cet État membre au Centre de compétences.

CHAPITRE VII

DISPOSITIONS FINALES

Article 45

Mesures initiales

1. La Commission est chargée de la création et de l'exploitation initiale du Centre de compétences jusqu'à ce que celui-ci dispose de la capacité opérationnelle pour exécuter son propre budget. La Commission prend, conformément au droit de l'Union, toutes les dispositions nécessaires en association avec les organes compétents du Centre de compétences.

2. Aux fins du paragraphe 1, en attendant que le directeur exécutif prenne ses fonctions une fois nommé par le conseil de direction conformément à l'article 16, la Commission peut désigner un directeur exécutif par intérim chargé d'exercer les tâches attribuées au directeur exécutif, avec l'aide, le cas échéant, d'un nombre limité de fonctionnaires de la Commission; La Commission peut détacher, à titre provisoire, un nombre limité de ses fonctionnaires.

3. Le directeur exécutif par intérim peut autoriser tous les paiements couverts par les crédits prévus au budget annuel du Centre de compétences après approbation par le conseil de direction, et il peut prendre des décisions et conclure des conventions, des décisions et des contrats, y compris des contrats d'engagement lorsque le tableau des effectifs du Centre de compétences a été adopté.

4. Le directeur exécutif par intérim détermine, d'un commun accord avec le directeur exécutif du Centre de compétences et sous réserve de l'approbation du conseil de direction, la date à laquelle le Centre de compétences aura la capacité d'exécuter son propre budget. À compter de cette date, la Commission s'abstient de procéder à des engagements et d'exécuter des paiements pour les activités du Centre de compétences.

Article 46

Durée

1. Le Centre de compétences est établi pour la période allant du 1er janvier 2021 au 31 décembre 2029.
2. Au terme de cette période, sauf décision contraire dans le cadre d'un réexamen du présent règlement, la procédure de liquidation est déclenchée. La procédure de liquidation est déclenchée automatiquement si l'Union ou tous les États membres participants se retirent du Centre de compétences.
3. Pour les besoins de la procédure de liquidation du Centre de compétences, le conseil de direction nomme un ou plusieurs liquidateurs, qui se conforment à ses décisions.
4. Lors de la liquidation du Centre de compétences, ses actifs sont utilisés pour couvrir ses dettes et les dépenses liées à sa liquidation. Tout excédent est réparti entre l'Union et les États membres participants, au prorata de leur contribution financière au Centre de compétences. Tout excédent de ce type attribué à l'Union est reversé au budget de l'Union.

Article 47

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

3.2.2. Incidence estimée sur les crédits opérationnels

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Règlement établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB[35]

Recherche et innovation

Investissements stratégiques européens

1.3. Nature de la proposition/de l'initiative

☒La proposition/l'initiative porte sur **une action nouvelle**

☐ La proposition/l'initiative porte sur **une action nouvelle suite à un projet pilote/une action préparatoire**[36]

☐ La proposition/l'initiative est relative à **la prolongation d'une action existante**

☐ La proposition/l'initiative porte sur **une action réorientée vers une nouvelle action**

1.4. Objectif(s)

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative

1. Un marché unique numérique connecté

2. Un nouvel élan pour l'emploi, la croissance et l'investissement

1.4.2. Objectif(s) spécifique(s) concerné(s)

Objectifs spécifiques

1.3 Aider l'économie numérique à réaliser tout son potentiel par des initiatives permettant aux technologies numériques et fondées sur les données de se développer pleinement;

2.1 L'Europe conserve sa position de leader mondial dans le domaine de l'économie numérique, où les entreprises européennes peuvent se développer à l'échelle mondiale, en s'appuyant sur un fort esprit d'entreprise numérique et sur de jeunes entreprises performantes et où les entreprises et les services publics maîtrisent la transformation numérique.

2.2. La recherche européenne trouve des possibilités d'investissement dans des avancées technologiques et des initiatives phares, en particulier les programmes «Horizon 2020» et «Horizon Europe» et le recours à des partenariats public-privé.

[35] ABM: activity-based management; ABB: activity-based budgeting.

[36] Tel(le) que visé(e) à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Le Centre de compétences, conjointement avec le Réseau et la communauté, s'efforcera d'atteindre les objectifs suivants:

(1) contribuer à la mise en œuvre du volet «cybersécurité» du programme pour une Europe numérique établi par le règlement nº XXX et, en particulier, des actions se rapportant à l'article 6 du règlement (UE) nº XXX [programme pour une Europe numérique] et au programme «Horizon Europe» établi par le règlement nº XXX, et notamment à la section 2.2.6 de l'annexe I de la décision nº XXX établissant le programme spécifique d'exécution du programme-cadre pour la recherche et l'innovation «Horizon Europe» et d'autres programmes de l'Union lorsque cela est prévu dans des actes juridiques de l'Union;

(2) renforcer les capacités, les connaissances et les infrastructures en matière de cybersécurité au service des industries, du secteur public et des communautés scientifiques;

(3) contribuer au déploiement à grande échelle de produits et de solutions de pointe en matière de cybersécurité dans l'ensemble de l'économie;

(4) améliorer la compréhension de la cybersécurité et contribuer à réduire les déficits de compétences dans l'Union en matière de cybersécurité;

(5) contribuer au renforcement de la recherche et du développement dans le domaine de la cybersécurité dans l'Union;

(6) renforcer la collaboration entre les sphères civile et militaire en ce qui concerne les technologies et les applications à double usage;

(7) renforcer les synergies entre les dimensions civile et militaire de la cybersécurité;

(8) aider à coordonner et à faciliter les travaux du Réseau des centres nationaux de coordination (ci-après le «Réseau») visé à l'article 10 et de la communauté des compétences en matière de cybersécurité visée à l'article 12.

1.4.4. Indicateurs de résultats et d'incidences

Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.

· Nombre d'infrastructures/outils de cybersécurité faisant l'objet de marchés publics conjoints.

· Disponibilité de temps d'essai et d'expérimentation pour les chercheurs européens et les entreprises européennes dans l'ensemble du Réseau et au sein du Centre. Lorsque les infrastructures existent déjà, le nombre d'heures supplémentaires disponibles pour ces communautés par rapport aux heures actuellement disponibles.

· Le nombre de communautés d'utilisateurs servies et le nombre de chercheurs ayant accès aux installations européennes en matière de cybersécurité augmente par rapport au nombre de ces communautés et chercheurs qui doivent chercher de telles ressources en dehors de l'Europe.

· Compétitivité accrue des fournisseurs européens, mesurée du point de vue de la part du marché mondial (objectif: 25 % de part de marché d'ici à 2027), ainsi que de la part des résultats de R&D européens obtenus par l'industrie.

· Contribution aux prochaines technologies de cybersécurité, mesurée du point de vue des droits d'auteur, des brevets, des publications scientifiques et des produits commerciaux.

· Nombre de programmes de compétences en matière de cybersécurité évalués et harmonisés, nombre de programmes de certification professionnelle évalués dans le domaine de la cybersécurité.

· Nombre de chercheurs, d'étudiants, d'utilisateurs (entreprises et administrations publiques) formés.

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

Atteindre une masse critique d'investissements dans le développement technologique et industriel en matière de cybersécurité et remédier à la fragmentation des capacités pertinentes réparties dans l'ensemble de l'Union.

1.5.2. Valeur ajoutée de l'intervention de l'UE

La cybersécurité est une question d'intérêt commun de l'Union, comme le confirment les conclusions du Conseil mentionnées ci-dessus. L'ampleur et le caractère transfrontalier d'incidents tels que WannaCry ou NonPetya en sont un bon exemple. La nature et l'ampleur des défis technologiques liés à la cybersécurité, ainsi que la coordination insuffisante des efforts déployés au sein de l'industrie, du secteur public et des communautés scientifiques et entre ceux-ci, imposent à l'Union de continuer de soutenir les efforts de coordination afin de mettre en commun une masse critique de ressources et de garantir une meilleure gestion des connaissances et des actifs. Cela est nécessaire compte tenu des besoins en ressources liés à certaines capacités en matière de recherche, de développement et de déploiement dans le domaine de la cybersécurité; la nécessité de fournir un accès à un savoir-faire interdisciplinaire en matière de cybersécurité entre différentes disciplines (souvent partiellement disponible au niveau national); la nature mondiale des chaînes de valeur industrielles, ainsi que l'activité des concurrents mondiaux opérant sur les marchés.

Cela nécessite des ressources et une expertise à une échelle qui peut difficilement être égalée par l'action individuelle d'un État membre quel qu'il soit. Par exemple, un réseau paneuropéen de communication quantique pourrait nécessiter un investissement de l'Union d'environ 900 millions d'EUR, en fonction des investissements réalisés par les États membres (à interconnecter/compléter) et de la mesure dans laquelle la technologie permettra la réutilisation des infrastructures existantes.

1.5.3. Leçons tirées d'expériences similaires

L'évaluation intermédiaire d'Horizon 2020 a, entre autres, confirmé la pertinence constante du soutien de l'Union en faveur de la recherche et du développement et des enjeux de société (parmi lesquels les «sociétés sûres», à partir desquelles la R&D en matière de cybersécurité est soutenue). Dans le même temps, l'évaluation confirme que le renforcement du leadership industriel reste un défi et qu'il subsiste un fossé en matière d'innovation, l'Union européenne étant à la traîne en ce qui concerne l'innovation révolutionnaire et créatrice de marché.

L'évaluation à mi-parcours du mécanisme pour l'interconnexion en Europe (MIE) semble confirmer la valeur ajoutée de l'intervention de l'Union au-delà de la recherche et du développement, même si la cybersécurité dans le cadre du MIE avait une orientation (sur la sécurité opérationnelle) et une logique d'intervention quelque peu différentes. Dans le même temps, la majorité des bénéficiaires de subventions en faveur de la cybersécurité au titre du MIE – la communauté des CSIRT nationaux – ont exprimé le souhait d'un programme d'aide sur mesure au titre du prochain CFP.

La création, en 2016, du partenariat public-privé sur la cybersécurité (PPPc) dans l'UE a constitué une première étape solide rassemblant les communautés de la recherche, de l'industrie et du secteur public afin de faciliter la recherche et l'innovation dans le domaine de la cybersécurité et, dans les limites du cadre financier 2014-2020, les résultats obtenus dans le domaine de la recherche et de l'innovation devraient être plus ciblés. Le PPPc a permis aux partenaires industriels de prendre des engagements à l'égard de leurs dépenses individuelles dans les domaines définis dans le programme stratégique de recherche et d'innovation du partenariat.

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés

Le Réseau de compétences en cybersécurité et le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité apporteront un soutien supplémentaire aux dispositions et aux acteurs existants en matière de politique de cybersécurité. Le mandat du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité complétera les efforts déployés par l'ENISA, mais il a une orientation différente et fait appel à un autre ensemble de compétences. Bien que l'ENISA ait un rôle de conseil à jouer en matière de recherche et d'innovation dans le domaine de la cybersécurité dans l'Union européenne, le mandat proposé se concentre avant tout sur d'autres tâches essentielles au renforcement de la résilience en matière de cybersécurité dans l'Union. Le Centre devrait stimuler la mise au point et le déploiement de technologies dans le domaine de la cybersécurité et compléter les efforts de renforcement des capacités dans ce domaine au niveau national et de l'Union.

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, ainsi que le Réseau de compétences en cybersécurité, œuvreront également à soutenir la recherche pour faciliter et accélérer les processus de normalisation et de certification, en particulier ceux liés aux systèmes de certification de cybersécurité au sens de la législation sur la cybersécurité.

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité agira en tant que mécanisme de mise en œuvre unique pour deux programmes de l'Union en faveur de la cybersécurité (le programme pour une Europe numérique et le programme «Horizon Europe») et renforcera la cohérence et les synergies entre eux.

La présente initiative permet de compléter les efforts des États membres en apportant une contribution adéquate aux responsables des politiques éducatives afin d'améliorer l'éducation à la cybersécurité (par exemple, en élaborant des programmes de formation dans le domaine de la cybersécurité dans les systèmes éducatifs civils et militaires, mais aussi en contribuant à l'éducation de base en matière de cybersécurité). Elle permettrait également de soutenir l'harmonisation et l'évaluation continue des programmes professionnels de certification de

cybersécurité – toutes les activités nécessaires pour contribuer à combler le déficit de compétences en cybersécurité et pour faciliter l'accès des industries et d'autres communautés aux spécialistes de la cybersécurité. L'harmonisation de l'éducation et des compétences contribuera au développement d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité au niveau de l'Union, un atout majeur pour les entreprises de cybersécurité ainsi que pour d'autres industries concernées par la cybersécurité.

1.6. Durée et incidence financière

☒ Proposition/initiative à **durée limitée**

– ☒ Proposition/initiative en vigueur du 01/01/2021 au 31/12/2029

– ☒ Incidence financière de 2021 jusqu'en 2027 pour les crédits d'engagement et de 2021 jusqu'en 2031 pour les crédits de paiement.

☐ Proposition/initiative à **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de AAAA jusqu'en AAAA,

– puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[37]

☐ **Gestion directe** par la Commission

– ☐ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

☒

Gestion indirecte en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☒ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

[37] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

L'article 28 contient des dispositions détaillées sur le suivi et l'établissement de rapports.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Afin d'atténuer les risques liés au fonctionnement du Centre de compétences après sa mise en place et les retards qu'elle entraîne, la Commission soutiendra le Centre de compétences au cours de cette phase afin de garantir un recrutement rapide du personnel clé et la mise en place d'un système de contrôle interne efficace et de procédures appropriées.

2.2.2. Informations concernant le système de contrôle interne mis en place

Le directeur exécutif est chargé des opérations et de la gestion quotidienne du Centre de compétences, dont il est le représentant légal. Le directeur est responsable devant le conseil de direction et lui rend compte en permanence de l'évolution des activités du Centre de compétences.

Le conseil de direction a la responsabilité globale de l'orientation stratégique et du fonctionnement du Centre de compétences et supervise la mise en œuvre de ses activités.

Les règles financières applicables au Centre de compétences sont adoptées par le conseil de direction après consultation de la Commission. Elles ne peuvent s'écarter du règlement (UE) nº 1271/2013 que si les exigences spécifiques du fonctionnement du Centre de compétences le nécessitent et moyennant l'accord préalable de la Commission.

L'auditeur interne de la Commission exerce, à l'égard du Centre de compétences, les mêmes compétences que celles exercées à l'égard de la Commission. La Cour des comptes dispose d'un pouvoir d'audit, sur pièces et sur place, à l'égard de tous les bénéficiaires de subventions, contractants et sous-traitants qui ont reçu des fonds de l'Union en provenance du Centre de compétences.

2.2.3. Estimation du coût et des avantages des contrôles et évaluation du niveau attendu de risque d'erreur

Coût et avantages des contrôles

Le coût des contrôles du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité est réparti entre le coût de la surveillance au niveau de la Commission et le coût des contrôles opérationnels au niveau de l'organisme d'exécution.

Le coût des contrôles au niveau du Centre de compétences est estimé à environ 1,19 % des crédits de paiement opérationnels exécutés au niveau du Centre de compétences.

Le coût de la surveillance au niveau de la Commission est estimé à 1,20 % des crédits de paiement opérationnels exécutés au niveau du Centre de compétences.

Dans l'hypothèse où les activités seraient entièrement gérées par la Commission sans le soutien de l'organisme d'exécution, le coût des contrôles serait sensiblement plus élevé et pourrait représenter environ 7,7 % des crédits de paiement.

Les contrôles prévus visent à garantir, d'une part, une surveillance harmonieuse et efficace des entités de mise en œuvre par la Commission et, d'autre part, le degré d'assurance nécessaire au niveau de la Commission.

Les avantages des contrôles sont les suivants:

- éviter que des propositions plus faibles ou inadéquates ne soient sélectionnées;
- optimiser la planification et l'utilisation des fonds de l'UE de manière à préserver la valeur ajoutée de l'UE;
- garantir la qualité des conventions de subvention, éviter les erreurs dans l'identification des entités juridiques, assurer le calcul correct des contributions de l'UE et prendre les garanties nécessaires à la bonne utilisation des subventions;
- détecter les coûts inéligibles au stade du paiement
- détecter les erreurs concernant la légalité et la régularité des opérations au stade de l'audit.

Niveau d'erreur estimatif

Le but est de maintenir le taux d'erreur résiduel sous le seuil de 2 % pour l'ensemble du programme tout en limitant la charge du contrôle pour les bénéficiaires de façon à assurer le juste équilibre entre l'objectif de légalité et régularité et les autres objectifs comme l'attractivité du programme, en particulier pour les PME, et le coût des contrôles.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées.

L'OLAF peut effectuer des enquêtes, y compris des contrôles et vérifications sur place, selon les dispositions et modalités prévues par le règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil et le règlement (Euratom, CE) nº 2185/9640 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités, en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, dans le cadre d'une subvention ou d'un contrat financés par le Centre de compétences.

Les conventions, décisions et contrats résultant de la mise en œuvre du présent règlement contiennent des dispositions habilitant expressément la Commission, le Centre de compétences, la Cour des comptes et l'OLAF à procéder à des audits et des enquêtes, en fonction de leurs compétences respectives.

Le Centre de compétences veille à ce que les intérêts financiers de ses membres soient correctement protégés en procédant ou en faisant procéder aux contrôles internes et externes appropriés.

Le Centre de compétences adhère à l'accord interinstitutionnel du 25 mai 1999 entre le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF). Le Centre de compétences adopte les mesures nécessaires pour faciliter la conduite des enquêtes internes effectuées par l'OLAF.

Le Centre de compétences adoptera une stratégie antifraude reposant sur une analyse des risques de fraude et des considérations relatives au rapport coûts-avantages. Il protège les intérêts financiers de l'Union par l'application de mesures préventives contre la fraude, la corruption et d'autres activités illégales, par des contrôles efficaces et, si des irrégularités sont constatées, par le recouvrement des montants indûment payés et, le cas échéant, par des sanctions administratives et financières efficaces, proportionnées et dissuasives.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique du cadre financier pluriannuel et nouvelle(s) ligne(s) budgétaire(s) de dépenses proposée(s)

- Nouvelles lignes budgétaires, dont la création est demandée

  Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépenses	Participation			
	Numéro	CD/CND[38]	de pays AELE[39]	de pays candidats[40]	de pays tiers	au sens de l'article [21, paragraphe 2, point b)] du règlement financier
Rubrique 1: Marché unique, innovation et numérique	01 02 XX XX Horizon Europe – Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité – Dépenses d'appui 01 02 XX XX Horizon Europe – Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité 02 06 01 XX Programme pour une Europe numérique – Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité – Dépenses d'appui 02 06 01 XX Programme pour une Europe numérique – Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité	Diss.	OUI	OUI (si spécifié dans le programme de travail annuel)	OUI (limité à certaines parties du programme)	NON

[38] CD = crédits dissociés / CND = crédits non dissociés.

[39] AELE: Association européenne de libre-échange.

[40] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

- Les contributions à ces lignes budgétaires devraient provenir de:

En Mio EUR (à la 3e décimale)

Ligne budgétaire	Année 2021	Année 2022	Année 2023	Année 2024	Année 2025	Année 2026	Année 2027	**Total**
01 01 01 01 Dépenses relatives aux fonctionnaires et aux agents temporaires recherche – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Personnel externe mettant en œuvre les programmes de recherche – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Autres dépenses de gestion pour la recherche – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Problématiques mondiales et compétitivité industrielle	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Assistance administrative – Programme pour une Europe numérique	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cybersécurité – Programme pour une Europe numérique	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Total des dépenses	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

La contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b), sera proposée par la Commission au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique. La proposition sera fondée sur les résultats du processus de planification stratégique défini à l'article 6, paragraphe 6, du règlement XXX [programme-cadre «Horizon Europe»].

Les montants susmentionnés n'incluent pas la contribution des États membres aux frais de fonctionnement et aux coûts administratifs du Centre de compétences, proportionnelle à la contribution financière de l'Union.

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	**1**	Marché unique, innovation et numérique

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Après 2027***	**TOTAL**
Titre 1 (Dépenses en personnel)	Engagements = Paiements	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titre 2 (Dépenses d'infrastructure et de fonctionnement)	Engagements = Paiements	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titre 3 (Dépenses opérationnelles)	Engagements	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Paiements	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTAL des crédits pour l'enveloppe des	Engagements	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] Les crédits de personnel ne sont comptabilisés que pour un semestre en 2021

programmes[42]	Paiements	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] Le total des crédits indiqués se rapporte uniquement aux ressources financières de l'Union consacrées à la cybersécurité dans le cadre du programme pour une Europe numérique. La contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 5, paragraphe 1, point b), sera proposée par la Commission au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique. La proposition sera fondée sur les résultats du processus de planification stratégique défini à l'article 6, paragraphe 6, du règlement XXX [programme-cadre «Horizon Europe»].

Rubrique du cadre financier pluriannuel	7	«Dépenses administratives»

En Mio EUR (à la 3e décimale)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Après 2027***	**TOTAL**
Ressources humaines		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Autres dépenses administratives		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

En Mio EUR (à la 3e décimale)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Après 2027***	**TOTAL**
TOTAL des crédits des diverses RUBRIQUES du cadre financier pluriannuel	Engagements	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Paiements	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 ²061,715**	**2 005,637**

3.2.2. Synthèse de l'incidence estimée sur les crédits de nature administrative

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

Années	2021	2022	2023	2024	2025	2026	2027	TOTAL
RUBRIQUE 7 du cadre financier pluriannuel								
Ressources humaines	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Autres dépenses administratives	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Hors RUBRIQUE 7[43] du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses de nature administrative	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Sous-total Hors RUBRIQUE 7 du cadre financier pluriannuel	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

TOTAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Les crédits susmentionnés nécessaires pour les ressources humaines et les autres dépenses de nature administrative hors rubrique 7 correspondent aux montants couverts par la contribution financière de l'Union au titre du programme pour une Europe numérique.

Les crédits nécessaires pour les ressources humaines et les autres dépenses de nature administrative hors rubrique 7 seront augmentés des montants couverts par la contribution financière de l'Union au titre du programme «Horizon Europe», une fois que la Commission proposera, au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique, la contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales

[43] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b).

Les montants susmentionnés des crédits nécessaires pour les ressources humaines et les autres dépenses de nature administrative hors rubrique 7 ne comprennent pas la contribution des États membres aux coûts administratifs du Centre de compétences, proportionnelle à la contribution financière de l'Union.

3.2.2.1. Besoins estimés en ressources humaines pour la Commission

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ■ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

Années		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
•Emplois du tableau des effectifs (fonctionnaires et d'agents temporaires)								
Siège et bureaux de représentation de la Commission		20	21	21	21	21	21	22
Délégations								
Recherche								
•Personnel externe (en équivalents temps plein: ETP) - AC, AL, END, INT et JPD [44] Rubrique 7								
Financés au titre de la RUBRIQUE 7 du cadre financier pluriannuel	- au siège	3	3	3	3	3	3	3
	- en délégation							
Financés par l'enveloppe du programme [45]	- au siège							
	- en délégation							
Recherche								
Autres (préciser)								
TOTAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Coordination, suivi et pilotage des tâches confiées au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, y compris les coûts de soutien et de coordination. Élaboration et coordination des politiques dans le domaine de la cybersécurité en fonction des missions confiées au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, par exemple en ce qui concerne l'établissement des priorités pour la politique industrielle et de recherche, la coopération générale entre les États membres et les opérateurs économiques, la cohérence avec le futur cadre de certification de l'Union en matière de cybersécurité, les travaux en matière de responsabilité et de devoir de vigilance, ou la coordination avec les politiques en matière de CHP, d'IA et de compétences numériques. .
Personnel externe	Coordination, suivi et pilotage des tâches confiées au Centre européen de compétences

[44] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[45] Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

	industrielles, technologiques et de recherche en matière de cybersécurité, y compris les coûts de soutien et de coordination. Élaboration et coordination des politiques dans le domaine de la cybersécurité en fonction des missions confiées au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, par exemple en ce qui concerne l'établissement des priorités pour la politique industrielle et de recherche, la coopération générale entre les États membres et les opérateurs économiques, la cohérence avec le futur cadre de certification de l'Union en matière de cybersécurité, les travaux en matière de responsabilité et de devoir de vigilance, ou la coordination avec les politiques en matière de CHP, d'IA et de compétences numériques. .

3.2.2.2. Besoins estimés en ressources humaines au sein du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité

	2021	2022	2023	2024	2025	2026	2027
Fonctionnaires de la Commission							
dont AD							
dont AST							
dont AST-SC							
Agents temporaires							
dont AD	10	11	13	13	13	13	13
dont AST							
dont AST-SC							
Agents contractuels	26	32	39	39	39	39	39
END	1	1	1	1	1	1	1
Total	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Mise en œuvre opérationnelle des tâches confiées au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité conformément à l'article 4 du présent règlement, y compris les coûts de soutien et de coordination.
Personnel externe	Mise en œuvre opérationnelle des tâches confiées au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité conformément à l'article 4 du présent règlement, y compris les coûts de soutien et de coordination.

L'estimation ci-dessus des besoins en ressources humaines au sein du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité correspond aux besoins estimés pour mettre en œuvre la contribution financière de l'Union au titre du programme pour une Europe numérique.

L'estimation ci-dessus des besoins en ressources humaines au sein du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité sera augmentée des besoins estimés pour la mise en œuvre de la contribution financière de l'Union au titre du programme «Horizon Europe», une fois que la Commission proposera, au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique, la contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b).

3.2.2.3. Tableau des effectifs du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité

Groupe de fonctions et grade	2021	2022	2023	2024	2025	2025	2025

AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Total AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
Total AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							

AST/SC 3							
AST/SC 2							
AST/SC 1							
Total AST/SC							
TOTAL GÉNÉRAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Incidence estimée sur le personnel (supplémentaire) – personnel externe du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité

Agents contractuels	2021	2022	2023	2024	2025	2026	2027
Groupe de fonctions IV	20	22	29	29	29	29	29
Groupe de fonctions III	2	4	4	4	4	4	4
Groupe de fonctions II	4	6	6	6	6	6	6
Groupe de fonctions I							
Total	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Afin d'assurer la neutralité en termes d'effectif, la dotation supplémentaire en effectifs du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité sera partiellement compensée par la réduction du nombre de fonctionnaires et d'agents externes (c'est-à-dire le tableau des effectifs et le personnel externe actuellement en place) dans les services concernés de la Commission.
Le nombre de membres du personnel du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité figurant aux points 3.2.2.2 à 3.2.2.4 sera compensé de la manière suivante[46]:

TOTAL	2021	2022	2023	2024	2025	2026	2027
Fonctionnaires de la Commission	5	5	6	6	6	6	6
Agents temporaires							
Agents contractuels	14	17	20	20	20	20	20
END							
Total ETP	19	22	26	26	26	26	26

[46] Sous réserve du montant final du budget dont la mise en œuvre sera déléguée au Centre de compétences

Effectifs	19	22	26	26	26	26	26

La compensation des ressources humaines du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité sera proportionnelle à la part de la contribution financière de l'Union, c'est-à-dire 50 %.

La compensation susmentionnée est liée aux besoins estimés en ressources humaines du Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité pour mettre en œuvre la contribution financière de l'Union au titre du programme pour une Europe numérique.

La compensation susmentionnée sera augmentée des besoins estimés pour mettre en œuvre la contribution financière de l'Union au titre du programme «Horizon Europe», une fois que la Commission proposera, au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique, la contribution de l'enveloppe financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b).

3.2.3. Participation de tiers au financement

La proposition/L'initiative:

– ☐ ne prévoit pas de cofinancement par des tierces parties

– ☒ prévoit le cofinancement par des tierces parties[47] estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

Années	2021	2022	2023	2024	2025	2026	2027	TOTAL
États membres – contribution aux dépenses de personnel	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
États membres – contribution aux dépenses d'infrastructure et de fonctionnement	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
États membres – contribution aux dépenses opérationnelles	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTAL crédits cofinancés	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

La contribution susmentionnée des tierces parties concerne uniquement le cofinancement proportionnel aux ressources financières de l'Union consacrées à la cybersécurité au titre du programme pour une Europe numérique. La contribution susmentionnée des tierces parties sera augmentée une fois que la Commission proposera, au cours du processus législatif et, en tout état de cause, avant la conclusion d'un accord politique, la contribution financière du pôle «Société inclusive et sûre» du pilier II «Problématiques mondiales et compétitivité industrielle» du programme «Horizon Europe» (enveloppe totale de 2 800 000 000 EUR) visée à l'article 21, paragraphe 1, point b). La proposition sera fondée sur les résultats du processus de planification stratégique défini à l'article 6, paragraphe 6, du règlement XXX [programme-cadre «Horizon Europe»].

3.3. Incidence estimée sur les recettes

– ☒ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐

En Mio EUR (à la 3e décimale)

Ligne budgétaire de	Incidence de la proposition/de l'initiative[48]

[47] Estimation de la contribution en nature des États membres

[48] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

recettes:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Article …….							

Pour les recettes qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).