Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2018/0328(COD)	Procédure terminée
Centre européen de compétences en matière de cybersécurité Sujet 3.30.07 Cybersécurité, politique cyberespace 3.50.20 Coopération et accords scientifiques et technologiques 8.40.08 Agences et organes de l'Union Priorités législatives Déclaration commune 2021		

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	ITRE Industrie, recherche et énergie		02/09/2019
		ANDRESEN Rasmus	
		Rapporteur(e) fictif/fictive	
		DEL CASTILLO VERA Pilar	
		GEIER Jens	
		GAMON Claudia	
		TOŠENOVSKÝ Evžen	
	Commission au fond précédente		
	ITRE Industrie, recherche et énergie		07/11/2018
		REDA Felix	
	Commission pour avis précédente		
	BUDG Budgets	La commission a décidé de ne pas donner d'avis.	
	IMCO Marché intérieur et protection des consommateurs		24/09/2018
		KOHN Arndt	
Conseil de l'Union européenne			
Commission européenne	DG de la Commission	Commissaire	

Comité économique et social européen Comité européen des régions	Secrétariat général	JUNCKER Jean-Claude

Evénements clés

12/09/2018	Publication de la proposition législative	COM(2018)0630	Résumé
01/10/2018	Annonce en plénière de la saisine de la commission, 1ère lecture		
19/02/2019	Vote en commission,1ère lecture		
22/02/2019	Dépôt du rapport de la commission, 1ère lecture	A8-0084/2019	Résumé
11/03/2019	Débat en plénière		
13/03/2019	Résultat du vote au parlement		
13/03/2019	Décision du Parlement, 1ère lecture	T8-0189/2019	Résumé
13/03/2019	Dossier renvoyé a la commission compétente		
17/04/2019	Décision du Parlement, 1ère lecture	T8-0419/2019	Résumé
25/09/2019	Ouverture des négociations interinstitutionnelles après 1ère lecture par la commission parlementaire		
09/10/2019	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles annoncée en plénière (Article 72)		
14/01/2021	Approbation en commission du texte accordé aux négociations interinstitutionnelles en 2ème lecture précoce	PE662.119 PE662.120	
23/04/2021	Publication de la position du Conseil	05628/2/2021	Résumé
26/04/2021	Vote en commission, 2ème lecture		
17/05/2021	Annonce en plénière de la saisine de la commission, 2ème lecture		
17/05/2021	Dépôt de la recommandation de la commission, 2ème lecture	A9-0166/2021	
19/05/2021	Débat en plénière		
19/05/2021	Décision du Parlement, 2ème lecture	T9-0246/2021	Résumé
20/05/2021	Signature de l'acte final		
20/05/2021	Fin de la procédure au Parlement		
08/06/2021	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de procédure	2018/0328(COD)

Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
Base juridique	Traité sur le fonctionnement de l'UE TFEU 188 -a1; Traité sur le fonctionnement de l'UE TFEU 173-p3; Règlement du Parlement EP 59-p4
Autre base juridique	Règlement du Parlement EP 159
Consultation obligatoire d'autres institutions	Comité économique et social européen Comité européen des régions
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	ITRE/9/01206

Portail de documentation

Document de base législatif		COM(2018)0630	12/09/2018	EC	Résumé
Document annexé à la procédure		SWD(2018)0403	12/09/2018	EC	Résumé
Document annexé à la procédure		SWD(2018)0404	12/09/2018	EC	Résumé
Projet de rapport de la commission		PE631.940	07/12/2018	EP	
Comité économique et social: avis, rapport		CES5208/2018	12/12/2018	ESC	
Amendements déposés en commission		PE632.973	17/01/2019	EP	
Comité économique et social: avis, rapport		CES4805/2018	23/01/2019	ESC	
Avis de la commission	IMCO	PE630.409	31/01/2019	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A8-0084/2019	22/02/2019	EP	Résumé
Texte adopté du Parlement, vote partiel en 1ère lecture/lecture unique		T8-0189/2019	13/03/2019	EP	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T8-0419/2019	17/04/2019	EP	Résumé
Réaction de la Commission sur le texte adopté en plénière		SP(2019)440	08/08/2019	EC	
Projet de rapport de la commission		PE689.669	30/03/2021	EP	
Position du Conseil		05628/2/2021	23/04/2021	CSL	Résumé
Communication de la Commission sur la position du Conseil		COM(2021)0225	03/05/2021	EC	
Recommandation déposée de la commission, 2e lecture		A9-0166/2021	17/05/2021	EP	
Texte adopté du Parlement, 2ème lecture		T9-0246/2021	19/05/2021	EP	Résumé
Projet d'acte final		00028/2021/LEX	20/05/2021	CSL	

Informations complémentaires

Document de recherche	Briefing

Acte final

Règlement 2021/887
JO L 202 08.06.2021, p. 0001

Acte législatif final contenant des dispositions relatives aux actes délégués

Centre européen de compétences en matière de cybersécurité

OBJECTIF: regrouper les ressources et l'expertise dans le domaine des technologies de cybersécurité.

ACTE PROPOSÉ: Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN: le Parlement européen décide conformément à la procédure législative ordinaire sur un pied dégalité avec le Conseil.

CONTEXTE: la cybersécurité est une question dintérêt commun de lUnion. La sécurité future dépend, entre autres, du renforcement de la capacité technologique et industrielle à protéger lUnion contre les cybermenaces, car tant les infrastructures civiles que les capacités militaires reposent sur des systèmes numériques sûrs.

À la suite de la stratégie de cybersécurité de 2013, lUnion na cessé daccroître ses activités pour relever les défis croissants en matière de cybersécurité:

- en 2016, lUnion a adopté les premières mesures dans le domaine de la cybersécurité par lintermédiaire de la directive (UE) 2016/1148 du Parlement européen et du Conseil relative à la sécurité des réseaux et des systèmes dinformation;
- la création, en 2016, du partenariat public-privé sur la cybersécurité (PPPc) dans lUE a constitué une première étape rassemblant les communautés de la recherche, de lindustrie et du secteur public afin de faciliter la recherche et linnovation dans le domaine de la cybersécurité; il aura généré jusquà 1,8 milliard dEUR dinvestissements dici à 2020;
- en septembre 2017, la Commission et la haute représentante de lUnion pour les affaires étrangères et la politique de sécurité ont présenté une communication conjointe intitulée «Résilience, dissuasion et défense: doter lUE dune cybersécurité solide» afin de renforcer encore la résilience, la dissuasion et la capacité de réaction de lUnion face aux cyberattaques;
- lors du sommet numérique de Tallinn, en septembre 2017, les chefs dÉtat et de gouvernement ont enjoint lUnion de devenir «un acteur mondial de premier plan dans le domaine de la cybersécurité dici à 2025».

Avec plus de 660 centres de compétences en matière de cybersécurité répartis dans lensemble de lUE, celle-ci dispose déjà dune expertise considérable en la matière. Toutefois, les efforts des communautés de la recherche et de l'industrie sont fragmentés, non harmonisés et caractérisés par labsence dune mission commune, ce qui entrave la compétitivité de lUE dans ce domaine.

La Commission estime que 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 lUnion et au niveau national.

ANALYSE DIMPACT: parmi les principaux arguments en faveur de loption retenue figuraient :

- 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 lessor du marché;
- la flexibilité permettant de recourir à différents modèles de coopération avec le Réseau de centres de compétences afin doptimiser lutilisation 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.

CONTENU: le présent règlement propose la création dun Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, associé à un Réseau des 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.

Le Centre de compétences: son rôle serait de faciliter les travaux du Réseau des centres nationaux de coordination et de dynamiser la communauté des compétences en matière de cybersécurité, en faisant progresser lagenda technologique et en facilitant laccès à lexpertise ainsi acquise. À cet effet, il coordonnerait lutilisation des fonds consacrés à la cybersécurité dans le cadre du prochain budget à long terme de lUE pour la période 2021-2027 au titre du programme pour une Europe numérique et du programme «Horizon Europe». Ses objectifs seraient:

- de renforcer les capacités, les connaissances et les infrastructures en matière de cybersécurité au service des industries, du secteur public et des communautés scientifiques;
- de contribuer au déploiement à grande échelle de produits et de solutions de pointe en matière de cybersécurité dans l'ensemble de léconomie;
- daméliorer la compréhension de la cybersécurité et contribuer à réduire les déficits de compétences dans lUnion en matière de cybersécurité;
- de contribuer au renforcement de la recherche et du développement dans le domaine de la cybersécurité dans lUnion;
- de renforcer les synergies entre les dimensions civile et militaire de la cybersécurité.

Le Centre de compétences serait mis sur pied sous la forme dun partenariat européen de façon à faciliter des investissements conjoints de la part de lUnion, des États membres et/ou de lindustrie. Par conséquent, la proposition prévoit que les États membres contribuent de manière proportionnée aux actions du Centre de compétences et du Réseau. Lorgane décisionnel principal serait le conseil de direction, où tous les États membres sont représentés. Cependant, seuls les États membres qui participent financièrement disposeraient du droit de vote.

Le Réseau des centres nationaux de coordination: chaque État membre désignerait un centre national de coordination pour piloter le Réseau, qui sattellerait au développement de nouvelles capacités et de compétences plus étendues dans le domaine de la cybersécurité. Le Réseau permettrait de recenser et de soutenir les projets les plus pertinents en matière de cybersécurité dans les États membres.

La communauté des compétences en matière de cybersécurité: celle-ci contribuerait à la mission du Centre de compétences en améliorant et en diffusant lexpertise en matière de cybersécurité dans toute lUnion. Elle ferait intervenir un groupe important et varié dacteurs associés au

développement des technologies de cybersécurité, tels que les entités de recherche, les secteurs de loffre, les secteurs de la demande et le secteur public.

INCIDENCE BUDGÉTAIRE: la contribution de lUnion au Centre de compétences pour couvrir les coûts administratifs et les frais de fonctionnement comprend les éléments suivants:

- 1.981.668.000 EUR provenant du programme pour une Europe numérique, dont jusqu'à 23.746.000 EUR pour les coûts administratifs;
- un montant de 2,8 milliards dEUR provenant du programme «Horizon Europe», y compris pour les coûts administratifs; cette contribution sera proposée par la Commission au cours du processus législatif et, en tout état de cause, avant la conclusion dun accord politique.

Centre européen de compétences en matière de cybersécurité

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

Nécessité dune action : linitiative proposée a pour objectif :

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

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

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

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

3) le fait que les résultats européens de la recherche et de linnovation dans le domaine de la cybersécurité ne sont que rarement convertis en solutions commercialisables ou déployés dans lensemble de léconomie.

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

Loption retenue est la création dun Réseau de centres de compétences en cybersécurité avec un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité habilité à prendre des mesures en faveur des technologies industrielles ainsi que dans le domaine de la recherche et de linnovation.

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

Lanalyse a montré que cette option est la plus appropriée pour atteindre les objectifs de linitiative, tout en assurant les meilleures retombées économiques, sociétales et environnementales et en préservant au mieux les intérêts de lUnion. Linitiative apporterait une valeur ajoutée aux efforts actuels déployés au niveau national :

- en contribuant à créer un écosystème industriel et de recherche en matière de cybersécurité à léchelle européenne;
- en encourageant une meilleure coopération entre les parties prenantes (notamment entre les secteurs civil et militaire de la cybersécurité) afin dutiliser au mieux les ressources et lexpertise existantes réparties dans toute lEurope.

Incidences de loption privilégiée: les avantages escomptés seraient les suivants :

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

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

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

Centre européen de compétences en matière de cybersécurité

Le document de travail des services de la Commission présente l'analyse d'impact qui accompagne la proposition de règlement du Parlement européen et du Conseil portant création du Centre européen de compétences industriel, technologique et de recherche en matière de cybersécurité et du Réseau des centres nationaux de coordination.

L'Union européenne a déjà mis en place un certain nombre d'instruments politiques et réglementaires pour faire face à l'évolution rapide des cybermenaces et pour protéger sa société, son économie et sa démocratie contre celles-ci.

Toutefois, à l'heure actuelle, l'UE ne dispose toujours pas des capacités technologiques et industrielles suffisantes pour sécuriser de manière autonome son économie et ses infrastructures critiques et pour devenir un leader mondial dans le domaine de la cybersécurité. L'insuffisance des capacités technologiques et industrielles de l'UE en matière de cybersécurité continue de poser des problèmes.

Plusieurs problèmes doivent être résolus :

- un niveau insuffisant de coordination et de coopération stratégiques et durables entre les industries, les communautés de recherche sur la cybersécurité et les gouvernements pour protéger l'économie, la société et la démocratie avec des solutions européennes de pointe en matière de cybersécurité;
- un accès limité au savoir-faire, aux compétences et aux installations en matière de cybersécurité dans toute l'Europe ;
- peu de résultats européens en matière de recherche et d'innovation dans le domaine de la cybersécurité se sont traduits par des solutions commercialisables et largement déployés dans l'ensemble de l'économie.

Les options suivantes ont été examinées :

- 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 dun double mandat pour poursuivre les mesures en faveur des technologies industrielles ainsi que dans le domaine de la recherche et de linnovation.
- 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 dinnovation.

Option privilégiée: l'option retenue (option 1) est la création d'un réseau de centres de compétences en matière de cybersécurité avec un centre européen de compétences en matière de cybersécurité industrielle, technologique et de recherche habilité à agir en faveur des technologies industrielles ainsi que dans le domaine de la recherche et de l'innovation. Selon la Commission, cette option était la plus appropriée pour atteindre les objectifs de linitiative, tout en assurant les meilleures retombées économiques, sociétales et environnementales et en préservant aux mieux les intérêts de lUnion.

Les principaux arguments en faveur de la création d'un centre européen de compétences en matière de cybersécurité industrielle et de recherche soutenant le réseau en tant qu'entité européenne fondée sur l'art. 173 et 187 TFUE (entité juridique autonome de l'UE, dotée de son propre budget, personnel, structure, règles et gouvernance) étaient les suivants:

- garantir la flexibilité nécessaire pour permettre aux différents modèles de coopération avec le réseau de centres de compétence d'optimiser l'utilisation des connaissances et des ressources existantes, y compris les outils financiers et autres incitations destinées à soutenir les membres du réseau;
- fournir un cadre juridique, contractuel et organisationnel commun et visible pour structurer les engagements communs des acteurs publics et privés issus de tous les secteurs concernés, y compris la défense;
- permettre la création d'une véritable politique industrielle de cybersécurité en soutenant des activités liées non seulement à la recherche et au développement mais aussi au déploiement sur le marché;
- agir en tant que mécanisme de mise en uvre pour différents volets de financement de l'UE en matière de cybersécurité au titre du prochain cadre financier pluriannuel (programme Europe numérique, Horizon Europe) et renforcer les synergies entre les dimensions civile et militaire de la cybersécurité en rapport avec le Fonds européen de défense.

Centre européen de compétences en matière de cybersécurité

La commission de lindustrie, de la recherche et de lénergie a adopté le rapport de Julia REDA (Verts/ ALE, DE) sur la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition de la Commission comme suit :

Objectifs et missions du Centre de compétences

Le Centre de compétence et le Réseau établis par le règlement devraient contribuer à la résilience globale et à la prise de conscience, dans lUnion, des menaces en matière de cybersécurité, en tenant compte des implications pour la société.

Les députés ont précisé les missions et tâches du Centre de compétences, à savoir notamment:

- contribuer à accroître la résilience et la fiabilité des infrastructures des réseaux et des systèmes dinformation, y compris linternet et les autres infrastructures critiques pour le fonctionnement de la société, telles que les transports, la santé et les systèmes bancaires ;
- sensibiliser aux menaces en matière de cybersécurité et aux implications et préoccupations dordre sociétal et éthique, et à réduire le déficit de compétence en matière de cybersécurité dans lUnion;

- développer le leadership européen en matière de cybersécurité en vue de garantir les normes de cybersécurité les plus élevées dans lensemble de lUnion;
- renforcer la compétitivité et les capacités de lUnion tout en réduisant sa dépendance numérique en améliorant ladoption des produits, processus et services de cybersécurité développés au sein de lUnion ;
- renforcer la confiance des citoyens, des consommateurs et des entreprises dans le monde numérique ;
- fournir un soutien financier et une assistance technique aux jeunes entreprises, aux PME, aux microentreprises, aux associations, aux experts individuels et aux projets de technologie civile dans le domaine de la cybersécurité;
- financer des contrôles des codes de sécurité des logiciels et des améliorations connexes des projets de logiciels libres et ouverts, couramment utilisés pour les infrastructures, les produits et les processus;
- faciliter le partage des connaissances en matière de cybersécurité et de lassistance technique entre autres à la société civile, à lindustrie et aux autorités publiques, ainsi quà la communauté universitaire et la communauté scientifique ;
- promouvoir la «sécurité dès la conception» en tant que principe dans le processus de développement, de maintenance, dexploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres les plus récentes, des essais de sécurité appropriés et des audits de sécurité ;
- garantir le respect des droits fondamentaux et dun comportement éthique dans les projets de recherche sur la cybersécurité soutenus par le Centre de compétences ;
- contrôler les rapports de vulnérabilité signalés par la communauté des compétences et faciliter la divulgation de vulnérabilités, le développement et la diffusion des correctifs et des solutions ;
- soutenir la recherche dans le domaine de la cybercriminalité ainsi que le développement de produits et de processus pouvant être librement étudiés, partagés et développés ;
- contribuer aux efforts de lUnion visant à renforcer la coopération internationale en matière de cybersécurité.

Centres nationaux de coordination

Un centre national de coordination devrait être mis en place dans chaque État membre.

Les relations entre le Centre de compétences et les centres nationaux de coordination devraient se fonder sur un accord contractuel type signé entre le Centre de compétences et chacun des centres nationaux de coordination. Laccord devrait contenir un ensemble de conditions générales harmonisées établissant les règles régissant les relations et la répartition des tâches entre le Centre de compétences et chaque centre national de coordination, et de conditions spéciales adaptées à chaque centre national de coordination.

Les centres nationaux devraient coopérer étroitement avec les organismes nationaux de normalisation afin de promouvoir ladoption des normes existantes et dassocier toutes les parties prenantes concernées, en particulier les PME, à la définition de nouvelles normes. Ils devraient également promouvoir et diffuser un programme denseignement commun minimal en matière de cybersécurité.

Communauté des compétences en matière de cybersécurité

Celle-ci contribuerait à la mission du Centre de compétences et améliorerait et diffuserait lexpertise en matière de cybersécurité dans toute lUnion.

La communauté des compétences devrait se composer de la société civile, de lindustrie, tant du côté de la demande que de loffre, y compris les PME, du monde universitaire et scientifique, dassociations dutilisateurs, dexperts individuels, des organismes européens de normalisation concernés et dautres associations, ainsi que dentités publiques et dautres entités traitant de questions opérationnelles et techniques dans le domaine de la cybersécurité.

Structure de gouvernance

Le conseil de direction se composerait dun représentant de chaque État membre, dun représentant nommé par le Parlement européen en tant quobservateur, et de quatre représentants de la Commission, au nom de lUnion, et viserait la parité hommes-femmes entre les membres du conseil de direction et leurs suppléants.

Le Centre et ses organes devraient veiller à ce que les conflits dintérêts soient non seulement identifiés, mais résolus et traités de manière transparente et responsable. Les États membres devraient veiller à ce quil en soit de même pour les centres nationaux de coordination.

Le comité consultatif industriel et scientifique conseillerait régulièrement le Centre de compétences sur lexécution de ses activités.

Contribution financière de lUnion

Celle-ci sélèverait à 1.780.954.875 EUR en prix de 2018 (1.998.696.000 EUR en prix courants) provenant du programme pour une Europe numérique, dont jusquà 21.385.465 EUR en prix de 2018 (23.746.000 EUR en prix courants) pour les coûts administratifs. Elle comprendrait également un montant du Fonds européen de la défense pour les actions liées à la défense du Centre de compétences.

Centre européen de compétences en matière de cybersécurité

Le Parlement européen a adopté par 489 voix pour, 73 contre et 56 abstentions, des amendements à la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

La question a été renvoyée à la commission compétente pour négociations interinstitutonnelles.

Les principaux amendements adoptés en plénière portent sur les points suivants :

Objectifs et missions du Centre de compétences

Le Parlement a rappelé quen 2017, 80 % des entreprises européennes ont été confrontées à au moins un incident de cybersécurité, doù la nécessité nécessaire dadopter les normes les plus élevées et des solutions globales en matière de cybersécurité en mobilisant les personnes, les produits, les processus et la technologie au niveau de lUnion.

Le Centre européen de compétences et le réseau de centres nationaux de coordination établis par le règlement devraient contribuer à la

résilience globale et à la prise de conscience, dans lUnion, des menaces en matière de cybersécurité, en tenant compte des implications pour la société.

Les députés ont précisé les missions et tâches du Centre de compétences, à savoir notamment:

- contribuer à accroître la résilience et la fiabilité des infrastructures des réseaux et des systèmes dinformation, y compris linternet et les autres infrastructures critiques pour le fonctionnement de la société, telles que les transports, la santé et les systèmes bancaires ;
- développer les compétences et les capacités dexpertise technologique, industrielle, sociétale, universitaire et de recherche en matière de cybersécurité ;
- sensibiliser aux menaces en matière de cybersécurité et aux implications et préoccupations dordre sociétal et éthique, et réduire le déficit de compétence en matière de cybersécurité dans lUnion;
- développer le leadership européen en matière de cybersécurité en vue de garantir les normes de cybersécurité les plus élevées dans lensemble de lUnion;
- renforcer la compétitivité et les capacités de lUnion tout en réduisant sa dépendance numérique en améliorant ladoption des produits, processus et services de cybersécurité développés au sein de lUnion ;
- renforcer la confiance des citoyens, des consommateurs et des entreprises dans le monde numérique ;
- fournir un soutien financier et une assistance technique aux jeunes entreprises, aux PME, aux microentreprises, aux associations, aux experts individuels et aux projets de technologie civile dans le domaine de la cybersécurité;
- financer des contrôles des codes de sécurité des logiciels et des améliorations connexes des projets de logiciels libres et ouverts, couramment utilisés pour les infrastructures, les produits et les processus;
- faciliter le partage des connaissances en matière de cybersécurité et de lassistance technique entre autres à la société civile, à lindustrie et aux autorités publiques, ainsi quà la communauté universitaire et la communauté scientifique ;
- promouvoir la «sécurité dès la conception» en tant que principe dans le processus de développement, de maintenance, dexploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres les plus récentes, des essais de sécurité appropriés et des audits de sécurité ;
- garantir le respect des droits fondamentaux et dun comportement éthique dans les projets de recherche sur la cybersécurité soutenus par le Centre de compétences ;
- contrôler les rapports de vulnérabilité signalés par la communauté des compétences et faciliter la divulgation de vulnérabilités, le développement et la diffusion des correctifs et des solutions ;
- soutenir la recherche dans le domaine de la cybercriminalité ainsi que le développement de produits et de processus pouvant être librement étudiés, partagés et développés ;
- renforcer la coopération entre les sphères civile et militaire en accomplissant des tâches liées à la technologie, aux applications et aux services de cyberdéfense réactive et défensive ;
- contribuer aux efforts de lUnion visant à renforcer la coopération internationale en matière de cybersécurité.

Centres nationaux de coordination

Un centre national de coordination devrait être mis en place dans chaque État membre.

Les relations entre le Centre de compétences et les centres nationaux de coordination devraient se fonder sur un accord contractuel type signé entre le Centre de compétences et chacun des centres nationaux de coordination.

Les centres nationaux devraient coopérer étroitement avec les organismes nationaux de normalisation afin de promouvoir ladoption des normes existantes et dassocier toutes les parties prenantes concernées, en particulier les PME, à la définition de nouvelles normes. Ils devraient également servir de guichet unique pour les produits et processus financés par dautres programmes de lUnion et diffuser un programme denseignement commun minimal en matière de cybersécurité.

Communauté des compétences en matière de cybersécurité

Celle-ci contribuerait à la mission du Centre de compétences et améliorerait et diffuserait lexpertise en matière de cybersécurité dans toute lUnion.

La communauté des compétences devrait se composer de la société civile, de lindustrie, tant du côté de la demande que de loffre, y compris les PME, du monde universitaire et scientifique, dassociations dutilisateurs, dexperts individuels, des organismes européens de normalisation concernés et dautres associations, ainsi que dentités publiques et dautres entités traitant de questions opérationnelles et techniques dans le domaine de la cybersécurité.

Structure de gouvernance

Le conseil de direction se composerait dun représentant de chaque État membre, dun représentant nommé par le Parlement européen en tant quobservateur, et de quatre représentants de la Commission, au nom de lUnion, et viserait la parité hommes-femmes entre les membres du conseil de direction et leurs suppléants.

Le Centre et ses organes devraient veiller à ce que les conflits dintérêts soient non seulement identifiés, mais résolus et traités de manière transparente et responsable. Les États membres devraient veiller à ce quil en soit de même pour les centres nationaux de coordination.

Le comité consultatif industriel et scientifique, composé de 25 membres au maximum, conseillerait régulièrement le Centre de compétences sur lexécution de ses activités.

Contribution financière de lUnion

Celle-ci sélèverait à 1.780.954.875 EUR en prix de 2018 (1.998.696.000 EUR en prix courants) provenant du programme pour une Europe numérique, dont jusquà 21.385.465 EUR en prix de 2018 (23.746.000 EUR en prix courants) pour les coûts administratifs. Elle comprendrait également un montant du Fonds européen de la défense pour les actions liées à la défense du Centre de compétences.

Centre européen de compétences en matière de cybersécurité

Le Parlement européen a adopté par 480 voix pour, 70 contre et 60 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.
La position du Parlement européen arrêtée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Objectifs et missions du Centre de compétences

Le Parlement a rappelé quen 2017, 80 % des entreprises européennes ont été confrontées à au moins un incident de cybersécurité, doù la nécessité dadopter les normes les plus élevées et des solutions globales en matière de cybersécurité.
Les objectifs du règlement proposé seraient de renforcer la compétitivité et les capacités de lUnion en matière de cybersécurité, et la réduction de sa dépendance numérique en améliorant ladoption des produits, processus et services de cybersécurité développés au sein lUnion.
Le Centre européen de compétences et le réseau de centres nationaux de coordination établis par le règlement devraient contribuer à la résilience globale et à la prise de conscience, dans lUnion, des menaces en matière de cybersécurité, en tenant compte des implications pour la société.
Les députés ont précisé les missions et tâches du Centre de compétences, à savoir notamment:

- développer les compétences et les capacités dexpertise technologique, industrielle, sociétale, universitaire et de recherche en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique et renforcer la protection des données des citoyens, des entreprises et des administrations publiques de lUnion;
- contribuer à accroître la résilience et la fiabilité des infrastructures des réseaux et des systèmes dinformation, y compris linternet et les autres infrastructures critiques pour le fonctionnement de la société, telles que les transports, la santé et les systèmes bancaires ;
- développer les compétences et les capacités dexpertise technologique, industrielle, sociétale, universitaire et de recherche en matière de cybersécurité ;
- sensibiliser aux menaces en matière de cybersécurité et aux implications et préoccupations dordre sociétal et éthique, et réduire le déficit de compétence en matière de cybersécurité dans lUnion;
- développer le leadership européen en matière de cybersécurité en vue de garantir les normes de cybersécurité les plus élevées dans lensemble de lUnion;
- renforcer la confiance des citoyens, des consommateurs et des entreprises dans le monde numérique ;
- fournir un soutien financier et une assistance technique aux jeunes entreprises, aux PME, aux microentreprises, aux associations, aux experts individuels et aux projets de technologie civile dans le domaine de la cybersécurité;
- financer des contrôles des codes de sécurité des logiciels et des améliorations connexes des projets de logiciels libres et ouverts, couramment utilisés pour les infrastructures, les produits et les processus;
- faciliter le partage des connaissances en matière de cybersécurité et de lassistance technique entre autres à la société civile, à lindustrie et aux autorités publiques, ainsi quà la communauté universitaire et la communauté scientifique ;
- promouvoir la «sécurité dès la conception» en tant que principe dans le processus de développement, de maintenance, dexploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres les plus récentes, des essais de sécurité appropriés et des audits de sécurité ;
- soutenir le développement, la mise en commun et le partage des aptitudes et des compétences en matière de cybersécurité à tous les niveaux déducation pertinents ;
- garantir le respect des droits fondamentaux et dun comportement éthique dans les projets de recherche sur la cybersécurité soutenus par le Centre de compétences ;
- contrôler les rapports de vulnérabilité signalés par la communauté des compétences et faciliter la divulgation de vulnérabilités, le développement et la diffusion des correctifs et des solutions ;
- soutenir la recherche dans le domaine de la cybercriminalité ainsi que le développement de produits et de processus pouvant être librement étudiés, partagés et développés ;
- apporter un soutien spécifique aux PME en facilitant leur accès sur mesure aux connaissances et à la formation ;
- renforcer la coopération entre les sphères civile et militaire en accomplissant des tâches liées à la technologie, aux applications et aux services de cyberdéfense réactive et défensive ;
- contribuer aux efforts de lUnion visant à renforcer la coopération internationale en matière de cybersécurité.

Centres nationaux de coordination

Un centre national de coordination devrait être mis en place dans chaque État membre.

Les relations entre le Centre de compétences et les centres nationaux de coordination devraient se fonder sur un accord contractuel type signé entre le Centre de compétences et chacun des centres nationaux de coordination.
Les centres nationaux devraient coopérer étroitement avec les organismes nationaux de normalisation afin de promouvoir ladoption des normes existantes et dassocier toutes les parties prenantes concernées, en particulier les PME, à la définition de nouvelles normes. Ils devraient également servir de guichet unique pour les produits et processus financés par dautres programmes de lUnion et diffuser un programme denseignement commun minimal en matière de cybersécurité.
Communauté des compétences en matière de cybersécurité
Celle-ci contribuerait à la mission du Centre de compétences et améliorerait et diffuserait lexpertise en matière de cybersécurité dans toute lUnion.
La communauté des compétences devrait se composer de la société civile, de lindustrie, tant du côté de la demande que de loffre, y compris les PME, du monde universitaire et scientifique, dassociations dutilisateurs, dexperts individuels, des organismes européens de normalisation concernés et dautres associations, ainsi que dentités publiques et dautres entités traitant de questions opérationnelles et techniques dans le domaine de la cybersécurité.
Structure de gouvernance
Le conseil de direction se composerait dun représentant de chaque État membre, dun représentant nommé par le Parlement européen en tant quobservateur, et de quatre représentants de la Commission, au nom de lUnion, et viserait la parité hommes-femmes entre les membres du conseil de direction et leurs suppléants.
Le Centre et ses organes devraient veiller à ce que les conflits dintérêts soient non seulement identifiés, mais résolus et traités de manière transparente et responsable. Les États membres devraient veiller à ce quil en soit de même pour les centres nationaux de coordination.
Le comité consultatif industriel et scientifique, composé de 25 membres au maximum, conseillerait régulièrement le Centre de compétences sur lexécution de ses activités.
Contribution financière de lUnion
Celle-ci sélèverait à 1.780.954.875 EUR en prix de 2018 (1.998.696.000 EUR en prix courants) provenant du programme pour une Europe numérique, dont jusquà 21.385.465 EUR en prix de 2018 (23.746.000 EUR en prix courants) pour les coûts administratifs. Elle comprendrait également un montant du Fonds européen de la défense pour les actions liées à la défense du Centre de compétences.

Centre européen de compétences en matière de cybersécurité

Le Conseil a adopté sa position en première lecture en vue de l'adoption d'un 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.

Le règlement proposé vise à aider l'UE à maintenir et à développer les capacités technologiques et industrielles en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique. Il prévoit la création de structures à trois niveaux institutionnels:

1) un Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (au niveau de l'UE),

2) un Réseau de centres nationaux de coordination (niveau national), et

3) une communauté de compétences en matière de cybersécurité (au niveau des parties prenantes).

Mission du Centre de compétences et du Réseau

La mission du Centre de compétences et du Réseau consiste à aider l'Union à:

- renforcer son leadership et son autonomie stratégique dans le domaine de la cybersécurité en maintenant et développant les moyens et capacités de l'Union nécessaires pour améliorer la confiance et la sécurité, y compris la confidentialité, l'intégrité et l'accessibilité des données, au sein du marché unique numérique;

- soutenir les moyens, capacités, et compétences technologiques de l'Union en ce qui concerne la résilience et la fiabilité des infrastructures des réseaux et des systèmes d'information, y compris des infrastructures critiques ainsi que du matériel et des logiciels couramment utilisés dans l'Union; et

- accroître la compétitivité du secteur de la cybersécurité de l'Union au niveau mondial, à garantir des normes de cybersécurité élevées dans l'ensemble de l'Union et à transformer la cybersécurité en un avantage concurrentiel pour d'autres industries de l'Union.

Centre de compétences

L'objectif du Centre sera d'assurer une coordination plus étroite entre la recherche et l'innovation ainsi que le déploiement de stratégies au niveau tant national que de l'UE, et de permettre aux États membres de prendre des décisions concernant leur contribution financière aux actions conjointes.

Le Centre de compétences sera en mesure:

- de mettre en uvre des actions de recherche et d'innovation (soutenues par le programme «Horizon Europe») ainsi que des actions de renforcement des capacités (soutenues par le programme pour une Europe numérique);

- de soutenir, en liaison avec les États membres, le développement et l'acquisition d'équipements, d'outils et d'infrastructures de données de cybersécurité avancés en Europe et d'assurer un large déploiement des dernières solutions de cybersécurité dans l'ensemble des secteurs économiques; à cette fin, le Centre de compétences sera également en mesure de faciliter l'acquisition partagée de capacités pour le compte des États membres.

Organisation du Centre de compétences

Le Centre de compétences aura son siège à Bucarest et sera doté d'un conseil de direction composé de représentants des États membres et de la Commission, chargé de définir l'orientation générale des activités du Centre de compétences et de veiller à ce que celui-ci s'acquitte de ses tâches conformément au règlement.

Le groupe consultatif stratégique - composé de 20 membres au maximum - fournira des conseils sur la base d'un dialogue régulier entre le Centre de compétences et la communauté de compétences en matière de cybersécurité.

L'Agence de l'Union européenne pour la cybersécurité (ENISA) sera observateur permanent au sein du conseil de direction du Centre de compétences et pourra fournir des avis et des contributions sur la rédaction de la stratégie et des programmes de travail annuel et pluriannuel.

La position du Conseil inclut de nouveaux articles sur l'équilibre entre les hommes et les femmes et sur la personnalité juridique du Centre de compétences.

Règles de vote

Le conseil de direction adoptera une approche consensuelle lors des discussions menées en son sein. Un vote sera organisé si les membres du conseil de direction ne parviennent pas à un consensus.

Pour certaines décisions liées à l'exécution du budget de l'Union, ainsi qu'en ce qui concerne le programme de travail annuel, le programme de travail pluriannuel et la méthode de calcul des contributions des États membres, la Commission disposera de 26 % des droits de vote. Le conseil de direction adoptera ses décisions à la majorité d'au moins 75 % des votes de l'ensemble de ses membres.

Centres nationaux de coordination

Au plus tard six mois après la date d'entrée en vigueur du règlement, chaque État membre désignera une entité pour agir comme son centre national de coordination.

Les centres nationaux de coordination feront office de points de contact au niveau national pour la communauté afin d'aider le Centre de compétences à remplir sa mission et ses objectifs, en particulier, à coordonner la communauté au moyen d'une coordination entre ses membres dans leur État membre.

Communauté de compétences en matière de cybersécurité

La communauté contribuera à la mission du Centre de compétences et du Réseau et améliorera, partagera et diffusera l'expertise en matière de cybersécurité dans toute l'Union.

La communauté sera composée d'organismes/organisations collectifs et n'inclura pas de personnes. Le Centre de compétences et ses organes pourront recourir à l'expertise de particuliers et de personnes physiques en tant qu'experts ad hoc.

Centre européen de compétences en matière de cybersécurité

Le Parlement européen a adopté une résolution législative approuvant la position du Conseil en première lecture en vue de l?adoption du 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.

Le règlement proposé vise à aider l'UE à maintenir et à développer les capacités technologiques et industrielles en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique. Le règlement :

- établit le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et 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 de compétences en matière de cybersécurité.

Le Centre de compétences, dont le siège sera situé à Bucarest, affectera notamment les financements liés à la cybersécurité issus du programme Horizon Europe et du programme pour une Europe numérique. Il sera en mesure de soutenir, en liaison avec les États membres, le développement et l'acquisition d'équipements, d'outils et d'infrastructures de données de cybersécurité avancés en Europe et d'assurer un large déploiement des dernières solutions de cybersécurité dans l'ensemble des secteurs économiques.

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité travaillera en coopération avec un réseau de centres nationaux de coordination désignés par les États membres.

Le Centre réunira également les principales parties prenantes européennes, notamment des entreprises, des organisations universitaires et de recherche et d'autres associations de la société civile concernées, afin de constituer une communauté de compétences en matière de cybersécurité destinée à renforcer et diffuser l'expertise en matière de cybersécurité dans toute l'Union.