Informations de base

2017/0225(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	Procédure terminée
Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act") Abrogation Règlement (EU) 526/2013 2010/0275(COD) Modification 2023/0108(COD) **Subject** 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet 8.40.08 Agences et organes de l'Union	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ITRE Industrie, recherche et énergie	NIEBLER Angelika (PPE)	27/10/2017
	Rapporteur(e) fictif/fictive KOUROUMBASHEV Peter (S&D) TOŠENOVSKÝ Evžen (ECR) TELIČKA Pavel (ALDE) MATIAS Marisa (GUE/NGL) DALUNDE Jakop G. (Verts/ALE) TAMBURRANO Dario (EFDD) LETARD-LECHEVALIER Christelle (ENF)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	La commission a décidé de ne pas donner d'avis.	
BUDG Budgets	GEIER Jens (S&D)	26/09/2017

	IMCO Marché intérieur et protection des consommateurs (Commission associée)	DANTI Nicola (S&D)	25/09/2017
	LIBE Libertés civiles, justice et affaires intérieures	FRANZ Romeo (Verts/ALE)	11/03/2019

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Affaires générales	3578	2017-11-20
Affaires générales	3685	2019-04-09

Commission européenne

DG de la Commission	Commissaire
Réseaux de communication, contenu et technologies	KING Julian

Comité économique et social européen

Comité européen des régions

Evénements clés

Date	Evénement	Référence	Résumé
13/09/2017	Publication de la proposition législative	COM(2017)0477	Résumé
23/10/2017	Annonce en plénière de la saisine de la commission, 1ère lecture		
20/11/2017	Adoption de résolution/conclusions par le Conseil		
18/01/2018	Annonce en plénière de la saisine des commissions associées		
10/07/2018	Vote en commission,1ère lecture		
10/07/2018	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
30/07/2018	Dépôt du rapport de la commission, 1ère lecture	A8-0264/2018	Résumé
10/09/2018	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
12/09/2018	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
14/01/2019	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture		
11/03/2019	Débat en plénière		
12/03/2019	Décision du Parlement, 1ère lecture	T8-0151/2019	Résumé
12/03/2019	Résultat du vote au parlement		
09/04/2019	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
17/04/2019	Signature de l'acte final		

17/04/2019	Fin de la procédure au Parlement		
07/06/2019	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2017/0225(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Règlement
Modifications et abrogations	Abrogation Règlement (EU) 526/2013 2010/0275(COD) Modification 2023/0108(COD)
Base juridique	Traité sur le fonctionnement de l'Union européenne TFEU 114
Autre base juridique	Règlement du Parlement EP 165
Consultation obligatoire d'autres institutions	Comité économique et social européen Comité européen des régions
État de la procédure	Procédure terminée
Dossier de la commission	ITRE/8/11042

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Avis de la commission	LIBE	PE615.394	16/03/2018	
Projet de rapport de la commission		PE619.373	27/03/2018	
Avis de la commission	BUDG	PE619.094	23/04/2018	
Amendements déposés en commission		PE621.015	30/04/2018	
Amendements déposés en commission		PE621.098	30/04/2018	
Avis de la commission	IMCO	PE616.831	22/05/2018	
Rapport déposé de la commission, 1ère lecture/lecture unique		A8-0264/2018	30/07/2018	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T8-0151/2019	12/03/2019	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Projet d'acte final	00086/2018/LEX	17/04/2019	

Commission Européenne

Type de document	Référence	Date	Résumé
	COM(2017)0477		

Document de base législatif		13/09/2017	Résumé
Document annexé à la procédure	SWD(2017)0500	13/09/2017	
Document annexé à la procédure	SWD(2017)0501	13/09/2017	
Document annexé à la procédure	SWD(2017)0502	13/09/2017	
Réaction de la Commission sur le texte adopté en plénière	SP(2019)393	30/04/2019	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	ES_PARLIAMENT	COM(2017)0477	21/11/2017	
Contribution	PT_PARLIAMENT	COM(2017)0477	07/12/2017	
Avis motivé	FR_SENATE	PE615.375	12/12/2017	
Contribution	CZ_SENATE	COM(2017)0477	14/12/2017	
Contribution	DE_BUNDESRAT	COM(2017)0477	19/12/2017	
Contribution	RO_SENATE	COM(2017)0477	20/12/2017	
Contribution	CZ_CHAMBER	COM(2017)0477	05/02/2018	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EESC	Comité économique et social: avis, rapport	CES4390/2017	14/02/2018	

Informations complémentaires

Source	Document	Date
Commission européenne	EUR-Lex	

Acte final

Règlement 2019/0881
JO L 151 07.06.2019, p. 0015 Résumé

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 30/07/2018 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport d'Angelika NIEBLER (PPE, DE) sur la 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) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité).

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.

Rôle et le mandat de l'Agence: l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information devrait être renforcée afin i) d' atteindre un niveau élevé de cybersécurité, ii) d'éviter les **cyberattaques** dans l'Union; iii) de **réduire la fragmentation du marché intérieur** et d'améliorer son fonctionnement; et iv) d'assurer la cohérence en tenant compte des résultats obtenus par les États membres en matière de coopération dans le cadre de la directive relative à la cybersécurité («directive SRI»).

L'Agence devrait **respecter les compétences des États membres** en ce qui concerne la cybersécurité, en particulier les compétences relatives à la sécurité publique, à la défense et à la sûreté de l'État, et les activités de l'État dans les domaines du droit pénal.

Les principales missions de Agence consisteraient, entre autres, à:

- soutenir **la coopération, la coordination et le partage d'informations** au niveau de l'Union entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées, sur les questions liées à la cybersécurité;
- promouvoir des projets contribuant à un **niveau élevé d'hygiène informatique et d'habileté numérique** des particuliers et des entreprises aux questions liées à la cybersécurité;
- **sensibiliser en permanence le public** aux risques liés à la cybersécurité, y compris en favorisant l'éducation, et fournir, à l'intention des particuliers, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs;
- aider les États membres et les institutions de l'Union à mettre en place de **politiques de divulgation coordonnée des vulnérabilités** et des procédures d'examen des divulgations de vulnérabilités par les acteurs gouvernementaux, dont les pratiques et les conclusions devraient être transparentes et soumises à un contrôle indépendant;
- faciliter la mise en place et le lancement d'un **projet européen à long terme** sur la sécurité des technologies de l'information afin de soutenir le développement d'une industrie de la sécurité informatique indépendante à l'échelle de l'Union;
- soutenir la **coopération opérationnelle** entre les États membres, les institutions, les agences et organes de l'Union et entre les parties prenantes en évaluant les systèmes nationaux existants, en élaborant et en mettant en œuvre un plan et en utilisant les instruments appropriés pour atteindre le niveau le plus élevé de certification en matière de cybersécurité dans l'Union et dans les États membres;
- contribuer à l'élaboration d'une **réaction concertée au niveau de l'UE** en cas d'incidents ou de crises transfrontières de cybersécurité majeurs, principalement en soutenant la gestion technique des incidents ou des crises à l'aide de son expertise indépendante et de ses propres ressources;
- organiser au moins **une fois par an**, des exercices de cybersécurité à l'échelle de l'Union.

Organisation et capacités: les députés suggèrent que l'ENISA renforce davantage ses propres capacités et compétences techniques pour être en mesure d'apporter un soutien adéquat à la coopération opérationnelle avec les États membres. À cette fin, l'Agence devrait **renforcer progressivement son personnel** afin de pouvoir collecter et analyser de manière autonome les différents types d'un large éventail de menaces en matière de cybersécurité, procéder à des analyses scientifiques et aider les États membres à réagir aux incidents de grande ampleur. Elle devrait accroître ses capacités sur la base des ressources existantes dans les États membres, notamment en détachant des experts nationaux auprès de l'Agence, en créant des groupes d'experts ou encore des programmes d'échanges de personnel.

L'Agence devrait disposer d'un **groupe consultatif de l'ENISA** composé d'experts en sécurité reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des technologies de l'information des communications (y compris les PME), les opérateurs de services essentiels, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de cybersécurité, les **organisations européennes de normalisation** (OEN) et les organes de l'Union.

Le groupe consultatif de l'ENISA devrait fixer les objectifs de son **programme de travail** et le rendre public tous les six mois pour en garantir la transparence.

L'Agence disposerait également d'un **groupe des parties prenantes pour la certification** pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs, le monde universitaire et les autres parties prenantes.

Système européen de certification de cybersécurité: les députés estiment que ce ne sont pas seulement les produits et services qui devraient être couverts par le règlement, mais **l'ensemble du cycle de vie**. Ainsi, les **processus** devraient également être inclus dans le champ d'application.

La certification devrait permettre:

- d'assurer la confidentialité, l'intégrité, la disponibilité et la confidentialité des services, des fonctions et des données;
- de veiller à ce que les services, fonctions et données puissent être consultés et utilisés uniquement par les personnes, systèmes et programmes autorisés;
- d'assurer que des processus soient mis en place pour identifier toutes les vulnérabilités connues et traiter les nouvelles;
- de faire en sorte que les produits, processus et services TIC soient sûrs par défaut et dès la conception;
- de réduire au maximum les autres risques liés aux incidents de cybersécurité, tels que les risques pour la vie humaine, la santé, l' environnement et d'autres intérêts juridiques importants.

Les députés ont suggéré une participation plus forte des États membres et de l'industrie au processus de certification.

L'Agence devrait tenir à jour un **site Web spécifique** fournissant des informations sur les systèmes européens de certification de cybersécurité, notamment les certificats retirés et expirés et les certifications nationales couvertes, et leur assurant une publicité.

Enfin, pour promouvoir l'acceptation généralisée des certificats et des résultats d'évaluation de la conformité délivrés par les organismes d'évaluation de la conformité, les députés ont proposé que les autorités nationales de contrôle de la certification fassent régulièrement l'objet d'un **examen par les pairs** rigoureux et transparent.

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 07/06/2019 - Acte final

OBJECTIF : réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place d'un système européen de certification en matière cybersécurité.

ACTE LÉGISLATIF : Règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

CONTENU : en vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyber-résilience et de confiance au sein de l'Union, le règlement fixe:

- les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l' Union européenne pour la cybersécurité); et
- un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l' Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

Agence de l'Union européenne pour la cybersécurité (ENISA)

Le règlement renforce l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire un organe permanent, l'Agence de l'UE pour la cybersécurité.

L'ENISA exécutera les tâches qui lui sont assignées par le règlement dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union. Elle servira de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de l' Union ainsi que pour les autres parties prenantes concernées de l'Union.

Les tâches de l'ENISA consisteront entre autres à :

- assister les institutions, organes et organismes de l'Union, ainsi que les États membres, dans l' élaboration et la mise en œuvre des politiques de l'Union liées à la cybersécurité et à les aider à accroître la protection de leurs réseaux et systèmes d'information, à améliorer les capacités de cyber-résilience et de cyber-réaction, et à développer des aptitudes et des compétences dans le domaine de la cybersécurité ;
- soutenir la politique de l'UE en matière de certification de la cybersécurité, par exemple en jouant un rôle central dans l'élaboration des systèmes de certification ;
- promouvoir l'utilisation du nouveau système de certification, par exemple en créant un site web fournissant des informations sur les certificats ;
- favoriser la coopération, notamment le partage d'informations et la coordination au niveau de l' Union ;

- soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci, notamment en cas d'incidents transfrontières ;
- promouvoir un niveau élevé de sensibilisation des citoyens, des organisations et des entreprises aux questions liées à la cybersécurité, y compris en matière d'hygiène informatique et d'habileté numérique ;
- organiser des exercices réguliers de cybersécurité à l'échelle de l'UE, y compris un exercice global à grande échelle une fois tous les deux ans ;
- produire des analyses stratégiques à long terme des cybermenaces et des incidents afin d'identifier les tendances émergentes et contribuer à prévenir les incidents.

Le mandat prévoit aussi un réseau d'agents de liaison nationaux afin de faciliter l'échange d'informations entre l'ENISA et les États membres.

Un groupe consultatif de l'ENISA composé d'experts reconnus représentant les parties prenantes concernées, ainsi qu'un groupe des parties prenantes pour la certification de cybersécurité seront établis.

Cadre européen de certification de cybersécurité

Le règlement crée un mécanisme pour l'établissement de systèmes européens de certification de cybersécurité afin de garantir que les produits, les processus et les services TIC vendus dans les pays de l' UE soient conformes aux normes de cybersécurité. Les certificats délivrés dans le cadre de ces systèmes seront valables dans tous les pays de l'UE.

La Commission devra publier un programme de travail de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Elle devra tenir à jour un site internet dédié fournissant des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE.

Les systèmes de certification eux-mêmes s'appuieront sur ce qui existe déjà aux niveaux international, européen et national. Les systèmes seront adoptés par la Commission et mis en œuvre et contrôlés par des autorités nationales de certification de cybersécurité.

La certification sera volontaire, sauf disposition contraire dans le droit de l'UE ou des États membres. La Commission surveillera régulièrement l'impact des systèmes de certification et évaluera leur niveau d'utilisation par les fabricants et les fournisseurs de services.

Il existera trois niveaux d'assurance différents, selon le niveau de risque associé à l'utilisation prévue du produit, à savoir «élémentaire», «substantiel» ou «élevé». Au niveau le plus élémentaire, les fabricants ou les fournisseurs de services pourront effectuer eux-mêmes l'évaluation de conformité.

Dans un souci d'équivalence des normes, dans l'ensemble de l'Union, en ce qui concerne les certificats de cybersécurité européens, les autorités nationales de certification de cybersécurité feront l'objet d'un examen par les pairs.

ENTRÉE EN VIGUEUR : 27.6.2019. Certaines dispositions s'appliqueront à partir du 28.6.2021.

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 12/03/2019 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 586 voix pour, 44 contre et 36 abstentions, une résolution législative sur la 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) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité).

La position du Parlement européen arrêtée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Pouvoirs renforcés pour l'Agence de l'UE pour la cybersécurité (ENISA)

En vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, le règlement proposé fixerait les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l'Union européenne pour la cybersécurité).

L'ENISA exécuterait ses tâches dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité. Elle servirait de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de l'Union ainsi que pour les autres parties prenantes concernées de l'Union. À cette fin, elle devrait développer ses ressources propres, y compris ses capacités et aptitudes techniques.

L'ENISA devrait, entre autres :

- assister les États membres et les institutions, organes et organismes de l'Union i) à mettre en place les capacités et la préparation requises pour prévenir et détecter les cybermenaces et incidents et y réagir ; ii) à élaborer et à promouvoir des politiques en matière de cybersécurité visant à soutenir la disponibilité ou l'intégrité générales du noyau public de l'internet ouvert; iii) à mettre en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités;
- favoriser le partage d'informations et la coordination au niveau de l'Union, entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées des secteurs public et privé en ce qui concerne les questions liées à la cybersécurité ;
- favoriser le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur ;
- soutenir les États membres dans le domaine de la sensibilisation et de l'éducation à la cybersécurité en favorisant une coordination plus étroite et l'échange de bonnes pratiques entre les États membres. Un tel soutien pourrait consister à développer un réseau de points de contact nationaux en matière d'éducation ainsi qu'une plateforme de formation à la cybersécurité ;
- sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des citoyens, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels, y compris en matière d'hygiène informatique et d'habileté numérique;
- faciliter la gestion technique des incidents ayant un impact significatif ou substantiel, en particulier en soutenant le partage volontaire de solutions techniques entre États membres ou en produisant des informations techniques combinées, telles que des solutions techniques partagées volontairement par les États membres ;
- promouvoir les concepts de sécurité dès la conception et de protection de la vie privée dès la conception au niveau de l'Union ;
- contribuer, s'il y a lieu, à une coopération avec des organisations telles que l'OCDE, l'OSCE et l'OTAN par exemple au moyen d'exercices conjoints dans le domaine de la cybersécurité.

L'ENISA devrait tenir le Parlement européen régulièrement informé de ses activités.

Réseau des agents de liaison nationaux

Le conseil d'administration devrait créer, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux composé de représentants de tous les États membres (les agents de liaison nationaux). Ce réseau faciliterait l'échange d'informations entre l'ENISA et les États membres et aiderait l'ENISA à faire connaître ses activités et à diffuser les résultats de ses travaux et ses recommandations auprès des parties prenantes concernées dans l'ensemble de l'Union.

Cadre européen de certification de cybersécurité

Le texte amendé crée le premier dispositif européen de certification en matière de cybersécurité afin de garantir que les produits, les processus et les services vendus dans les pays de l'UE soient conformes aux normes de cybersécurité.

La Commission devrait publier, au plus tard un an après l'entrée en vigueur du règlement, un programme de travail glissant de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Elle devrait tenir à jour un site internet dédié fournissant des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE.

Dans un souci d'équivalence des normes, dans l'ensemble de l'Union, en ce qui concerne les certificats de cybersécurité européens et les déclarations de conformité de l'UE, les autorités nationales de certification de cybersécurité feraient l'objet d'un examen par les pairs.

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 13/09/2017 - Document de base législatif

OBJECTIF: réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place d'un système européen de certification en matière cybersécurité.

ACTE PROPOSÉ: Règlement du Parlement européen et du Conseil.

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

CONTEXTE: l'Union européenne a déjà pris un certain nombre de mesures pour accroître la résilience face aux cyberattaques. Depuis la première stratégie européenne de cybersécurité adoptée en 2013, des développements importants ont eu lieu, y compris le deuxième mandat de l'Agence européenne pour la sécurité des réseaux et de l'information (**ENISA**) et l'adoption de la directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) qui constituent la base de la présente proposition.

En 2016, la Commission européenne a adopté une communication **sur le renforcement du système européen de cyber-résilience**, dans laquelle d'autres mesures ont été annoncées pour mieux protéger l'UE.

Le Conseil a rappelé que le règlement (UE) n° 526/2013 sur l'ENISA était l'un des éléments essentiels d'un cadre de résilience informatique de l'UE et a demandé à la Commission de prendre d'autres mesures pour aborder la question de la certification au niveau européen. En 2017, il s'est félicité de l'intention de la Commission d'examiner la stratégie de la cybersécurité en septembre et de proposer d'autres actions ciblées avant la fin de 2017.

ANALYSE D'IMPACT: l'analyse d'impact a identifié plusieurs problèmes tels que: la fragmentation des politiques et des approches de la cybersécurité dans les États membres; des ressources dispersées et des approches disparates au sein des institutions, organismes et organes de l'UE; une sensibilisation et une information insuffisantes des citoyens et des entreprises, conjuguée à l'émergence croissante de multiples systèmes nationaux et sectoriels de certification.

L'analyse a permis de conclure qu'une **ENISA réformée combinée à un cadre général de certification de la cybersécurité de l'UE** en matière de technologies de l'information des communications (TIC) était l'option privilégiée.

CONTENU: la proposition vise à **réviser le mandat actuel de l'ENISA** et à définir un ensemble renouvelé de tâches et de fonctions, en vue de soutenir efficacement les États membres, les institutions de l'UE et les efforts des autres parties prenantes dans l'objectif d'assurer un cyberespace sécurisé dans l'Union européenne.

Le nouveau mandat proposé vise à donner à l'Agence **un rôle plus important et plus central**, notamment en contribuant à la mise en œuvre de la directive SRI, et en devenant un centre d'expertise pour aider les États membres et la Commission à créer et à appliquer le cadre de certification à l'échelle de l'UE.

En particulier, la proposition vise à:

- **transformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en une Agence européenne de la cybersécurité**, qui améliorera la coordination et la coopération entre les États membres et les institutions, organismes et organes de l'UE;
- **établir un cadre de certification à l'échelle l'UE** qui assurera la fiabilité de milliards de dispositifs («Internet des objets») qui pilotent dorénavant les infrastructures critiques, telles que les réseaux d'énergie et de transport, mais aussi de nouveaux équipements grand public, tels que les voitures connectées.

Une Agence européenne pour la cybersécurité: l'Agence disposerait d'un **mandat permanent** pour aider les États membres à prévenir efficacement les cyberattaques et à y répondre.

En vue d'améliorer la préparation de l'UE en cas d'attaques, elle organiserait chaque année des **exercices de cybersécurité paneuropéens** et assurerait un meilleur partage des connaissances et des informations sur les menaces par la création de **centres de partage et d'analyse de l'information**.

Elle contribuerait aussi à la mise en œuvre de la directive SRI, qui impose des obligations de signalement des incidents graves aux autorités nationales.

L'Agence aiderait en outre à créer et à appliquer le cadre de certification à l'échelle de l'UE proposé par la Commission pour garantir que les produits et les services répondent à toutes les exigences de cybersécurité applicables.

La proposition comprend également les dispositions visant à faciliter la **lutte contre la fraude, la corruption et d'autres activités illégales**, ainsi que des dispositions en matière de dotation en personnel et de budget.

Un cadre de certification de la cybersécurité de l'UE: actuellement, il existe différents systèmes de certification de sécurité pour les produits TIC dans l'UE. L'Agence mettra en place un processus de certification. Le cadre de certification proposé à l'échelle de l'UE crée un **ensemble complet de règles, d'exigences techniques, de normes et de procédures** destiné à convenir à chaque système. Chaque système de certification serait basé sur un accord au niveau de l'UE pour l'évaluation des propriétés de sécurité d'un produit TIC spécifique (par exemple : carte à puce).

La proposition établit les **principaux effets juridiques** des systèmes européens de certification de la cybersécurité, à savoir: i) l'obligation de mettre en œuvre le régime au niveau national et le **caractère volontaire** de la certification; ii) l'effet invalidant des systèmes de certification de la cybersécurité européenne sur les régimes nationaux pour les mêmes produits ou services. Elle définit également la procédure d'adoption des systèmes européens de certification ainsi que les rôles respectifs de la Commission, de l'Agence et du Groupe européen de certification de la cybersécurité.

INCIDENCE BUDGÉTAIRE: le total des crédits, y compris les dépenses administratives, de 2019 à 2022 est estimé à **86,038 millions d'EUR**.