COMMISSION
EUROPÉENNE

Bruxelles, le 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

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)

(Texte présentant de l'intérêt pour l'EEE)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

L'Union européenne a pris un certain nombre de mesures pour être plus résiliente et mieux préparée en ce qui concerne la cybersécurité. Au titre de sa première stratégie de cybersécurité[1] adoptée en 2013, l'UE a défini des objectifs stratégiques et des actions concrètes pour parvenir à la résilience, faire reculer la cybercriminalité, développer une politique et des moyens de cyberdéfense, développer les ressources industrielles et technologiques correspondantes et instaurer une politique internationale de l'UE cohérente en matière de cyberespace. Dans ce domaine, des événements importants se sont produits depuis lors, notamment le commencement du deuxième mandat de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[2] et l'adoption de la **directive sur la sécurité des réseaux et des systèmes d'information**[3] (directive SRI), qui constitue la base de la présente proposition.

De plus, en 2016, la Commission européenne a adopté une **communication intitulée «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité»**[4] dans laquelle elle annonçait de nouvelles mesures pour intensifier la coopération, l'échange d'informations et le partage des connaissances et pour accroître la résilience et améliorer la préparation de l'UE, compte tenu également de l'éventualité d'incidents de grande ampleur et de la possibilité d'une crise paneuropéenne en matière de cybersécurité. À cet égard, la Commission a annoncé qu'elle procéderait à l'**évaluation** et au **réexamen** du règlement (UE) n° 526/2013 du Parlement européen et du Conseil concernant l'ENISA et abrogeant le règlement (CE) n° 460/2004 (règlement ENISA). Le processus d'évaluation pourrait conduire à une éventuelle réforme de l'Agence et à un renforcement de ses capacités et de ses moyens pour apporter un soutien durable aux États membres. Il s'agirait donc de donner à l'Agence un rôle plus opérationnel et plus central pour ce qui est de parvenir à la résilience en matière de cybersécurité et de reconnaître, dans son nouveau mandat, les nouvelles responsabilités de l'Agence en vertu de la directive SRI.

La directive SRI, en imposant des exigences de sécurité comme obligations légales aux principaux acteurs économiques, notamment aux opérateurs fournissant des services essentiels (opérateurs de services essentiels – OSE) et aux fournisseurs de certains services numériques clés (fournisseurs de services numériques – FSN), constitue une première étape capitale en vue de promouvoir une culture de gestion des risques. Les exigences de sécurité étant considérées comme essentielles pour préserver les avantages procurés par la numérisation en cours de la société, et compte tenu de la multiplication des dispositifs

---

1 Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé», JOIN(2013) 1.

2 Règlement (UE) n° 526/2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004.

3 Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

4 Communication de la Commission européenne «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», COM(2016) 410 final.

connectés (Internet des objets – IdO), la Commission, dans sa communication de 2016, a également avancé l'idée d'instaurer un cadre concernant la certification de sécurité des produits et services TIC afin de susciter davantage la confiance et d'accroître la sécurité dans le marché unique numérique. La certification de cybersécurité en matière de TIC revêt une importance particulière vu l'utilisation accrue de technologies qui exigent un niveau élevé de cybersécurité, comme les voitures connectées et automatisées, la santé électronique ou les systèmes de contrôle-commande industriels (IACS).

Ces mesures et annonces politiques ont également été étayées par les conclusions du Conseil de 2016, dans lesquelles il a été reconnu que «les cybermenaces et les vulnérabilités continuent d'évoluer et de s'aggraver, ce qui nécessitera de poursuivre et d'intensifier la coopération, en particulier pour répondre aux cyberincidents transfrontières majeurs». Le Conseil y a réaffirmé que le règlement ENISA constitue l'un des «éléments essentiels d'un cadre de cyberrésilience de l'UE»[5] et invité la Commission à prendre de nouvelles mesures pour traiter la question de la certification au niveau européen.

L'instauration d'un système de certification exigerait la mise en place d'un système approprié de gouvernance au niveau de l'UE et, notamment, une solide expertise fournie par une agence de l'UE indépendante. À cet égard, dans la présente proposition, l'ENISA est désignée comme l'organisme, au niveau de l'UE, naturellement compétent en matière de cybersécurité, qui devrait remplir la fonction consistant à rassembler les organismes nationaux compétents dans ce domaine et à en coordonner les travaux.

Dans sa communication sur l'**examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique** de mai 2017, la Commission a encore précisé qu'elle réviserait le mandat de l'ENISA avant septembre 2017. Il s'agit de définir son rôle dans le nouvel écosystème de la cybersécurité et d'élaborer des mesures concernant les normes, la certification et l'étiquetage en matière de cybersécurité afin de sécuriser davantage les systèmes fondés sur les TIC, notamment les objets connectés[6]. Dans ses **conclusions** de juin 2017[7], le Conseil européen a salué l'intention de la Commission de réexaminer en septembre la stratégie de cybersécurité et de proposer avant la fin de 2017 de nouvelles actions ciblées.

Le règlement proposé prévoit un ensemble complet de mesures s'inspirant d'actions antérieures et fixe des objectifs précis se renforçant mutuellement:

- développer **les moyens et la préparation** des États membres et des entreprises;
- améliorer **la coopération et la coordination** entre les États membres et les institutions, organes et organismes de l'UE;
- accroître **les moyens au niveau de l'UE pour compléter l'action des États membres**, notamment en cas de crise transfrontière;
- davantage **sensibiliser** les particuliers et les entreprises aux questions de cybersécurité;

[5] Conclusions du Conseil intitulées «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», 15 novembre 2016.

[6] Communication de la Commission sur l'examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique, COM(2017) 228.

[7] Conclusions du Conseil européen des 22 et 23 juin 2017, EUCO 8/17.

- accroître globalement **la transparence de l'assurance de la cybersécurité**[8] des produits et services TIC pour susciter une plus grande confiance dans le marché unique numérique et l'innovation numérique; et
- éviter **la multiplication des systèmes de certification** dans l'UE, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres et secteurs d'activité.

La partie suivante du présent exposé des motifs fournit une justification plus détaillée de l'initiative relativement aux actions proposées pour l'ENISA et à la certification de cybersécurité.

[8] Par transparence de l'assurance de la cybersécurité, on entend le fait de fournir aux utilisateurs suffisamment d'informations sur les caractéristiques de cybersécurité pour leur permettre de déterminer, de façon objective, le niveau de sécurité offert par un produit, service ou processus TIC donné.

ENISA

L'ENISA fait office de centre d'expertise chargé de renforcer la sécurité des réseaux et de l'information dans l'Union et d'aider les États membres à se doter de moyens.

L'ENISA a été instituée en 2004[9] en vue de contribuer à la réalisation de l'objectif global consistant à assurer un niveau élevé de sécurité des réseaux et de l'information au sein de l'UE. En 2013, le règlement (UE) n° 526/2013 a défini le nouveau mandat de l'Agence pour une période de sept ans, jusqu'en 2020. L'Agence a ses bureaux en Grèce, notamment son siège administratif à Heraklion (Crète) et son centre opérationnel à Athènes.

En comparaison des autres organes de l'UE, l'ENISA est une petite agence dotée d'un budget peu élevé et d'un effectif réduit. Son mandat est à durée déterminée.

L'ENISA apporte son soutien aux institutions européennes, aux États membres et aux entreprises **en traitant les problèmes de sécurité des réseaux et de l'information, en y réagissant et, surtout, en les prévenant**. Pour ce faire, elle exerce une série d'activités dans les cinq domaines définis dans sa stratégie[10]:

- Expertise: fournir des informations et une expertise sur des questions essentielles en matière de sécurité des réseaux et de l'information.
- Politiques: contribuer à l'élaboration des politiques et à leur mise en œuvre dans l'Union.
- Moyens: aider à se doter de moyens dans toute l'Union (p. ex. par des formations, recommandations, activités de sensibilisation).
- Communauté: promouvoir la communauté de la sécurité des réseaux et de l'information [p. ex. soutien aux équipes d'intervention en cas d'urgence informatique (CERT), coordination d'exercices paneuropéens de cybersécurité].
- Facilitation (p. ex. collaboration avec les parties intéressées et relations internationales).

Au cours des négociations relatives à la directive SRI, les colégislateurs de l'UE ont décidé de confier des missions importantes à l'ENISA en vue de la mise en œuvre de cette directive. En particulier, l'Agence assure le secrétariat du réseau des CSIRT (mis en place pour promouvoir une coopération rapide et effective, au niveau opérationnel, entre les États membres en cas d'incidents de cybersécurité spécifiques et pour échanger des informations sur les risques) et elle est aussi appelée à assister le groupe de coopération dans l'exécution de ses tâches. En outre, la directive exige de l'ENISA qu'elle assiste les États membres et la Commission en fournissant son expertise et ses conseils et en facilitant l'échange de bonnes pratiques.

Conformément au règlement ENISA, la Commission a procédé à une évaluation de l'Agence, qui comprenait une étude indépendante ainsi qu'une consultation publique. L'évaluation a consisté à déterminer la pertinence, l'incidence, l'efficacité, l'efficience, la cohérence et la valeur ajoutée européenne de l'Agence en ce qui concerne son fonctionnement, sa

9 Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JO L 77 du 13.3.2004, p. 1.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

gouvernance, sa structure organisationnelle interne et ses méthodes de travail au cours de la période 2013-2016.

Le fonctionnement global de l'ENISA a été jugé satisfaisant par une majorité de participants[11] (74 %) à la consultation publique. Une majorité de participants a également estimé que l'ENISA atteignait ses différents objectifs (au moins 63 % pour chacun des objectifs). Les services et produits de l'ENISA sont régulièrement (chaque mois ou plus souvent) utilisés par près de la moitié des participants (46 %) et sont appréciés parce qu'ils proviennent d'un organisme au niveau de l'UE (83 %) et pour leur qualité (62 %).

Toutefois, une grande majorité (88 %) de participants a estimé que les instruments et mécanismes actuellement disponibles au niveau de l'UE n'étaient pas suffisants ou que partiellement adaptés pour traiter les problèmes que pose la cybersécurité aujourd'hui. Dans leur grande majorité (98 %), les participants ont déclaré qu'il fallait un organisme de l'UE pour répondre à ces besoins, et 99 % d'entre eux ont estimé que l'ENISA était l'organisation appropriée à cette fin. En outre, 67,5 % des participants étaient d'avis que l'ENISA pourrait jouer un rôle dans l'établissement d'un cadre harmonisé pour la certification de sécurité des produits et services informatiques.

L'évaluation globale (basée non seulement sur la consultation publique, mais aussi sur plusieurs entretiens individuels, enquêtes ciblées et ateliers supplémentaires) a permis de tirer les conclusions suivantes:

- Les objectifs de l'ENISA restent pertinents aujourd'hui. Dans un contexte de progrès technologiques rapides et de menaces changeantes et vu les risques croissants pour la cybersécurité au niveau mondial, le besoin se fait clairement sentir, dans l'UE, de promouvoir et de développer davantage l'expertise technique de haut niveau en la matière. Il faut se doter de moyens, dans les États membres, pour appréhender les menaces et y répondre, et les parties intéressées doivent coopérer dans tous les champs thématiques et toutes les institutions.
- Malgré son budget limité, l'Agence a été efficiente, du point de vue opérationnel, dans l'utilisation de ses ressources et dans l'accomplissement de ses missions. Le dédoublement de l'implantation entre Athènes et Heraklion a, cependant, engendré des coûts administratifs supplémentaires.
- Du point de vue de l'efficacité, l'ENISA a partiellement atteint ses objectifs. L'Agence a contribué avec succès à améliorer la sécurité des réseaux et de l'information en Europe en aidant à se doter de moyens dans les 28 États membres[12],

[11] Ont participé à la consultation 90 parties intéressées de 19 États membres (88 réponses et 2 documents de synthèse), dont des autorités nationales de 15 États membres et 8 organisations faîtières représentant un nombre significatif d'entreprises européennes.

[12] Il a été demandé aux participants à la consultation publique d'indiquer ce qu'ils considéraient comme les principales réalisations de l'ENISA sur la période 2013-2016. Des participants de tous les groupes (55 au total, dont 13 du groupe des autorités nationales, 20 du secteur privé et 22 du groupe «Autres») ont considéré ce qui suit comme les principales réalisations de l'ENISA: 1) la coordination des exercices Cyber Europe; 2) l'apport d'un soutien aux CERT/CSIRT par la formation et les ateliers permettant de promouvoir la coordination et les échanges; 3) les publications de l'ENISA (lignes directrices et recommandations, rapports sur la nature des menaces, stratégies de signalement des incidents et de gestion des crises, etc.) ont été jugées utiles pour créer et actualiser les cadres nationaux de sécurité, ainsi que comme référence pour les décideurs et les professionnels de la cybersécurité; 4) la contribution à la promotion de la directive SRI; 5) les efforts pour sensibiliser davantage à la cybersécurité par l'organisation du «mois de la cybersécurité».

en intensifiant la coopération entre les États membres et les parties intéressées par la sécurité des réseaux et de l'information, et en fournissant une expertise, la possibilité de nouer des relations et un soutien à l'élaboration de politiques. Globalement, l'ENISA s'est consacrée avec diligence à la réalisation de son programme de travail et s'est comportée en partenaire de confiance pour ses interlocuteurs, dans un domaine dont on n'a pris conscience que récemment qu'il avait une telle dimension transfrontière.

- L'ENISA est parvenue à avoir une influence, au moins relative, dans le vaste domaine de la sécurité des réseaux et de l'information, mais elle n'a pas vraiment réussi à se forger une réputation solide et à acquérir assez de visibilité pour être reconnue comme «le» centre d'expertise en Europe. Cela s'explique par le large mandat de l'ENISA, laquelle n'a pas été dotée de ressources suffisantes en proportion. De plus, l'ENISA reste la seule agence de l'UE dont le mandat est à durée déterminée, ce qui limite sa capacité à élaborer une vision à long terme et à apporter un soutien durable aux parties intéressées. Cela contredit aussi les dispositions de la directive SRI, en vertu de laquelle l'ENISA se voit confier des missions sans date de fin. Enfin, il est ressorti de l'évaluation que cette efficacité limitée peut s'expliquer en partie par le recours important à des experts externes plutôt qu'aux experts internes, et par les difficultés à recruter et retenir du personnel spécialisé.
- Enfin, et surtout, il a été conclu de l'évaluation que la valeur ajoutée de l'ENISA réside d'abord dans la capacité de l'Agence à intensifier la coopération entre les États membres principalement, et en particulier avec les communautés de la sécurité des réseaux et de l'information correspondantes (notamment entre les CSIRT). Il n'y a aucune autre entité au niveau de l'UE qui prenne en charge autant de parties intéressées par la sécurité des réseaux et de l'information. Toutefois, du fait de la nécessité de hiérarchiser les activités de l'Agence de façon stricte, le programme de travail de l'ENISA est largement dicté par les besoins des États membres. En conséquence, il ne répond pas suffisamment à ceux des autres parties intéressées, en particulier des entreprises. Cela a aussi incité l'Agence à satisfaire les besoins des principales parties intéressées, l'empêchant ainsi d'avoir une plus grande influence. Aussi la valeur ajoutée procurée par l'Agence varie-t-elle en fonction des besoins des parties intéressées et de la mesure dans laquelle l'Agence a pu y répondre (p. ex. grands États membres par opposition aux petits États membres; États membres par opposition aux entreprises).

En somme, les résultats de la consultation des parties intéressées et de l'évaluation ont fait apparaître que les ressources et le mandat de l'ENISA doivent être adaptés de sorte qu'elle puisse jouer un rôle adéquat dans la résolution des problèmes actuels et futurs.

Ce constat étant établi, il est ici proposé de revoir le mandat actuel de l'ENISA et de définir un ensemble renouvelé de missions et de fonctions en vue de soutenir, de façon efficace et efficiente, les efforts déployés par les États membres, les institutions de l'UE et d'autres parties intéressées pour assurer la sécurité du cyberespace dans l'Union européenne. Le nouveau mandat proposé vise à donner un rôle plus important et plus central à l'Agence qui, en particulier, est appelée à aider aussi les États membres à mettre en œuvre la directive SRI et à réagir plus activement aux menaces particulières (capacité opérationnelle), et à devenir un centre d'expertise apportant un soutien aux États membres et à la Commission en matière de certification de cybersécurité. En vertu de la présente proposition:

- Il serait accordé un mandat permanent à l'ENISA qui verrait ainsi sa stabilité assurée à l'avenir. Le mandat, les objectifs et les missions feraient toujours l'objet d'un réexamen périodique.
- Le mandat proposé définit plus précisément le rôle de l'ENISA en tant qu'agence de l'UE pour la cybersécurité et comme point de référence dans l'écosystème de cybersécurité de l'UE, œuvrant en étroite coopération avec tous les autres organismes compétents dudit écosystème.
- L'organisation et la gouvernance de l'Agence, qui ont été jugées satisfaisantes lors de l'évaluation, seraient légèrement revues, en particulier pour faire en sorte que les besoins de la communauté des parties intéressées, au sens large, soient mieux pris en compte dans les travaux de l'Agence.
- Le mandat suggéré prévoit des domaines d'action bien délimités. Sont renforcés les domaines où l'Agence apporte une valeur ajoutée avérée, et sont ajoutés les nouveaux domaines où un soutien s'impose vu les priorités et instruments politiques nouveaux, en particulier la directive SRI, le réexamen de la stratégie de cybersécurité de l'UE, le prochain plan de l'UE en matière de cybersécurité pour la coopération en cas de crise et la certification de sécurité en matière de TIC:
    - **Élaboration et mise en œuvre de la politique de l'UE:** l'ENISA serait chargée de contribuer de façon proactive à l'élaboration de la politique dans le domaine de la sécurité des réseaux et de l'information, ainsi qu'à d'autres initiatives politiques dans différents secteurs (p. ex. énergie, transports, finance) présentant des aspects de cybersécurité. À cette fin, elle aurait une fonction consultative importante, qu'elle pourrait remplir en émettant des avis indépendants et en réalisant des travaux préparatoires à l'élaboration et à l'actualisation de la politique et de la législation. L'ENISA aurait aussi une fonction de soutien de la politique et de la législation de l'UE dans les domaines des communications électroniques, de l'identification électronique et des services de confiance en vue de promouvoir un niveau de cybersécurité plus élevé. En phase de mise en œuvre, notamment dans le cadre du groupe de coopération SRI, l'ENISA aiderait les États membres à définir une approche cohérente de l'application de la directive SRI à travers les frontières et dans tous les secteurs, ainsi que d'autres politiques et législations pertinentes. Afin de permettre le réexamen périodique des politiques et législations dans le domaine de la cybersécurité, l'ENISA fournirait aussi des rapports réguliers sur l'avancement de la mise en œuvre du cadre juridique de l'UE.
    - **Dotation de moyens:** l'ENISA devrait contribuer à perfectionner les moyens et les compétences dont disposent les autorités publiques nationales et de l'UE, y compris en matière de réponse aux incidents et de supervision des mesures réglementaires relatives à la cybersécurité. Il serait également demandé à l'Agence de contribuer à la mise en place de centres d'échange et d'analyse d'informations (ISAC) dans divers secteurs, en proposant de bonnes pratiques et des orientations sur les outils et procédures disponibles et en traitant de façon adéquate les questions réglementaires relatives à l'échange d'informations.
    - **Partage des connaissances et informations, sensibilisation:** l'ENISA deviendrait le pôle d'information de l'UE. Cela impliquerait de promouvoir l'échange de bonnes pratiques et d'initiatives dans toute l'UE en mettant en

commun les informations sur la cybersécurité provenant des institutions, organes et organismes nationaux et de l'UE. L'Agence fournirait aussi des conseils, des orientations et de bonnes pratiques sur la sécurité des infrastructures critiques. De plus, au lendemain de cyberincidents transfrontières significatifs, l'ENISA établirait des rapports afin de donner des orientations aux entreprises et aux particuliers dans toute l'UE. Cette partie du travail impliquerait également d'organiser régulièrement des activités de sensibilisation en coordination avec les autorités des États membres.

- **Missions relatives au marché (normalisation, certification de cybersécurité):** l'ENISA remplirait un certain nombre de fonctions afin de soutenir spécifiquement le marché intérieur et constituer un «observatoire du marché» de la cybersécurité, en analysant les tendances pertinentes sur ledit marché pour mieux faire correspondre l'offre et la demande, et en contribuant à l'élaboration de la politique de l'UE dans les domaines de la normalisation et de la certification de cybersécurité en matière de TIC. En ce qui concerne plus particulièrement la normalisation, elle faciliterait l'instauration et l'adoption de normes de cybersécurité. L'ENISA accomplirait aussi les missions prévues au titre du futur cadre de certification (voir ci-après).

- **Recherche et innovation:** l'ENISA apporterait son expertise en conseillant les autorités nationales et de l'UE sur la fixation des priorités de recherche et développement, y compris dans le cadre du partenariat public-privé contractuel sur la cybersécurité (PPPc). Les conseils de l'ENISA sur la recherche seraient mis à profit par le nouveau Centre européen de recherche et de compétences en matière de cybersécurité au titre du prochain cadre financier pluriannuel. L'ENISA prendrait également part, lorsque la Commission le lui demanderait, à la réalisation des programmes européens de financement de la recherche et de l'innovation.

- **Coopération opérationnelle et gestion des crises:** cette partie du travail consisterait à renforcer les moyens opérationnels de prévention existants, notamment par la mise à niveau des exercices de cybersécurité paneuropéens (Cyber Europe) en les organisant tous les ans, et à remplir une fonction de soutien à la coopération opérationnelle, en tant que secrétariat du réseau des CSIRT (conformément aux dispositions de la directive SRI), en assurant, entre autres, le bon fonctionnement de l'infrastructure informatique et des moyens de communication dudit réseau. Dans ce contexte, il serait nécessaire d'instaurer une coopération structurée avec la CERT-UE, le Centre européen de lutte contre la cybercriminalité (EC3) et d'autres organismes compétents de l'UE. De plus, cette coopération structurée avec la CERT-UE, à proximité géographique immédiate, permettrait d'assurer une fonction d'assistance technique en cas d'incidents significatifs et de soutien à leur analyse. Les États membres qui en feraient la demande bénéficieraient d'une assistance pour gérer les incidents et d'un soutien pour l'analyse des vulnérabilités, artefacts et incidents afin de renforcer leur propre capacité de prévention et de réaction.

- L'ENISA jouerait aussi un rôle dans **le plan de l'UE en matière de cybersécurité** présenté comme élément du présent paquet législatif et constituant la recommandation de la Commission aux États membres pour la coordination, au niveau de l'UE, des réactions aux incidents et crises de

cybersécurité transfrontières majeurs[13]. L'ENISA faciliterait la coopération entre les différents États membres en matière d'intervention en cas d'urgence en analysant et en agrégeant les rapports de situation nationaux établis à partir des informations fournies à l'Agence, sur une base volontaire, par les États membres et d'autres entités.

- **Certification de cybersécurité des produits et services TIC**

Pour susciter la confiance dans les produits et services TIC et en assurer la sécurité, leurs caractéristiques de sécurité doivent être définies dès les premières phases de conception technique et de développement (sécurité dès la conception). De plus, les clients et utilisateurs doivent pouvoir vérifier le niveau d'assurance de la sécurité des produits et services qu'ils acquièrent ou achètent.

La certification, qui consiste en l'évaluation formelle des produits, services et processus par un organisme indépendant et agréé, selon un ensemble défini de critères ou de normes, et en la délivrance d'un certificat attestant la conformité, contribue grandement à susciter davantage la confiance dans les produits et services et en accroître la sécurité. Si les évaluations de sécurité relèvent assurément de la technique, la certification a pour finalité d'informer et de rassurer les acheteurs et utilisateurs en ce qui concerne les propriétés des produits et services TIC en matière de sécurité. Comme indiqué plus haut, cela vaut en particulier pour les nouveaux systèmes qui utilisent abondamment les technologies numériques et nécessitent un niveau de sécurité élevé, tels que les voitures connectées et automatisées, la santé électronique, les systèmes de contrôle-commande industriels (IACS)[14] ou les réseaux intelligents.

Actuellement, la certification de cybersécurité des produits et services TIC dans l'UE offre un paysage assez contrasté. Plusieurs initiatives internationales ont été prises, comme les Critères communs (CC) d'évaluation de la sécurité des technologies de l'information (norme ISO 15408) qui constituent une norme internationale d'évaluation de la sécurité informatique. Elle repose sur une évaluation par des tiers et prévoit sept niveaux d'assurance de l'évaluation (EAL). Les CC et la Méthodologie commune d'évaluation de la sécurité des technologies de l'information (CEM), qui les accompagne, forment la base technique d'un accord international, l'Accord de reconnaissance des critères communs (CCRA), qui garantit que les certificats CC sont reconnus par tous ses signataires. Toutefois, selon la version actuelle du CCRA, seules les évaluations jusqu'à EAL 2 sont mutuellement reconnues. De plus, l'accord n'a été signé que par 13 États membres.

Les autorités de certification de 12 États membres ont conclu un accord de reconnaissance mutuelle concernant les certificats délivrés conformément à l'accord sur la base des CC[15]. En

---

13 Le «plan» concernera les incidents de cybersécurité provoquant une perturbation dont l'ampleur dépasse ce qu'un État membre peut gérer seul ou qui touche au moins deux États membres avec une incidence ou une importance politique telle qu'ils exigent une coordination et une réaction rapides au niveau politique de l'UE.

14 La DG JRC a publié un rapport dans lequel elle propose un premier ensemble d'exigences européennes communes et de grandes lignes directrices relatives à la certification de cybersécurité des composants IACS. Il est disponible à l'adresse suivante: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

15 Le Groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS) comprend des représentants de 12 États membres et de la Norvège et a élaboré quelques profils de protection pour un nombre limité de produits comme la signature numérique, le tachygraphe numérique et les cartes à

outre, plusieurs initiatives en matière de certification des TIC existent déjà, ou sont à l'étude, dans des États membres. Aussi importantes soient-elles, ces initiatives risquent de morceler le marché et de créer des problèmes d'interopérabilité. Par conséquent, il n'est pas exclu qu'une entreprise, pour pouvoir proposer ses produits sur plusieurs marchés, doive se soumettre à de multiples procédures dans différents États membres. Par exemple, un fabricant de compteurs intelligents qui souhaite vendre ses produits dans trois États membres, disons le Royaume-Uni, la France et l'Allemagne, doit aujourd'hui se conformer à trois systèmes de certification différents: la CPA (*Commercial Product Assurance*) au Royaume-Uni, la Certification de Sécurité de Premier Niveau (CSPN) en France et un profil de protection spécifique basé sur les CC en Allemagne.

Cette situation entraîne des coûts élevés et une charge administrative considérable pour les entreprises exerçant leur activité dans plusieurs États membres. Si le coût de la certification peut varier de façon significative en fonction du produit/service concerné, du niveau d'assurance de l'évaluation recherché et/ou d'autres éléments, il est en général assez important pour les entreprises. Le certificat «Passerelle pour compteur intelligent» du BSI, par exemple, coûte plus d'un million d'euros (niveau d'essai et d'assurance le plus élevé, concerne non seulement un produit, mais aussi l'ensemble de l'infrastructure environnante). Le coût de la certification des compteurs intelligents au Royaume-Uni est d'environ 150 000 euros. En France, le coût est du même ordre qu'au Royaume -Uni, de 150 000 euros au moins.

Les principaux acteurs publics et privés ont reconnu que, faute de système de certification de cybersécurité à l'échelle de l'UE, les entreprises doivent, dans de nombreux cas, se faire certifier dans chaque État membre, ce qui entraîne un morcellement du marché. Qui plus est, faute de législation européenne sur l'harmonisation des produits et services TIC, les différences de normes et de pratiques de certification de cybersécurité entre les États membres risquent de créer, dans les faits, 28 marchés de la sécurité distincts au sein de l'UE, chacun ayant ses propres exigences techniques, méthodes d'essai et procédures de certification. Si aucune mesure appropriée n'est prise au niveau de l'UE, ces approches nationales divergentes sont susceptibles de compromettre gravement la réalisation du marché unique numérique et d'en ralentir ou annuler les effets positifs en termes de croissance et d'emploi.

Compte tenu de la situation exposée ci-dessus, le règlement proposé vise à instaurer un Cadre européen de certification de cybersécurité (le «**Cadre**») des produits et services TIC, et précise les fonctions et missions essentielles de l'ENISA dans ce domaine. La présente proposition définit le cadre global des règles régissant les systèmes européens de certification de cybersécurité. Elle ne vise pas à instaurer des systèmes de certification immédiatement opérationnels, mais plutôt à créer un système (cadre) pour l'instauration de systèmes de certification spécifiques à certains produits/services TIC (les «systèmes européens de certification de cybersécurité»). La création de systèmes européens de certification de cybersécurité conformément au Cadre permettra de faire en sorte que les certificats délivrés en vertu de ces systèmes soient valables et reconnus dans tous les États membres et de remédier ainsi au morcellement actuel du marché.

La finalité générale d'un système européen de certification de cybersécurité est d'attester que les produits et services TIC qui ont été certifiés conformément au système satisfont à des exigences de cybersécurité précises. Il pourrait s'agir, par exemple, de leur capacité à protéger

puce. Les participants collaborent pour coordonner la normalisation des profils de protection CC et coordonnent l'élaboration des profils de protection. Les États membres demandent souvent la certification SOG-IS pour les appels d'offres publics nationaux.

les données (stockées, transmises ou traitées d'une autre façon) contre le stockage, le traitement, l'accès, la diffusion, la destruction, la perte ou l'altération accidentels ou non autorisés. En ce qui concerne les exigences techniques et procédures d'évaluation auxquelles les produits doivent satisfaire, les responsables des systèmes européens de certification de cybersécurité utiliseraient les normes existantes et n'élaboreraient pas de normes techniques eux-mêmes[16]. Par exemple, la certification UE de produits comme les cartes à puce, qui sont aujourd'hui mises à l'essai selon des normes CC internationales dans le cadre du système multilatéral SOG-IS (décrit plus haut), équivaudrait à rendre ce système valable dans toute l'UE.

En plus de décrire un ensemble précis d'objectifs de sécurité à prendre en compte dans la conception d'un système européen de certification de cybersécurité spécifique, la proposition prévoit ce que devrait être le contenu minimal de tels systèmes. Ceux-ci devront définir, entre autres choses, un certain nombre d'éléments spécifiques établissant le champ d'application et l'objet de la certification de cybersécurité. Cela comprend notamment l'indication des catégories de produits et services couverts, la description détaillée des exigences de cybersécurité (par exemple par référence aux normes ou spécifications techniques pertinentes), les critères et méthodes d'évaluation spécifiques, et le niveau d'assurance qu'ils entendent garantir (c.-à-d. élémentaire, substantiel ou élevé).

Les systèmes européens de certification de cybersécurité seront préparés par l'ENISA, avec l'aide et les conseils d'experts du Groupe européen de certification de cybersécurité (voir ci-après) et en étroite coopération avec lui, et seront adoptés par la Commission au moyen d'actes d'exécution. Lorsque le besoin d'un système de certification de sécurité se fera sentir, la Commission demandera à l'ENISA de préparer un système spécifique à certains produits ou services TIC. L'ENISA s'y attellera en étroite coopération avec les autorités nationales de contrôle de la certification représentées au sein du Groupe. Les États membres et le Groupe peuvent aussi proposer à la Commission de demander à l'ENISA de préparer un système particulier.

La certification peut constituer un processus très onéreux, et donc entraîner un prix élevé pour les clients et les consommateurs. De plus, le besoin de certification peut varier considérablement en fonction du contexte d'utilisation spécifique des produits et services et de la rapidité des progrès technologiques. Le recours à la certification européenne de cybersécurité devrait donc rester facultatif, à moins qu'il n'en soit prévu autrement dans une législation de l'Union définissant les exigences de sécurité de certains produits et services TIC.

Afin d'assurer l'harmonisation et d'éviter le morcellement, les systèmes et procédures nationaux de certification de cybersécurité des produits et services TIC couverts par un système européen de certification de cybersécurité cesseront de s'appliquer à partir de la date fixée dans l'acte d'exécution portant adoption du système européen. De plus, les États membres devraient s'abstenir d'instaurer de nouveaux systèmes nationaux de certification de cybersécurité des produits et services TIC couverts par un système européen de certification de cybersécurité existant.

Une fois qu'un système européen de certification de cybersécurité aura été adopté, les fabricants de produits TIC ou les fournisseurs de services TIC pourront soumettre une demande de certification de leurs produits ou services à l'organisme d'évaluation de la

[16] Dans le cas des normes européennes, elles sont élaborées par les organisations européennes de normalisation et approuvées par la Commission européenne lors de leur publication au Journal officiel [voir règlement (UE) n° 1025/2012].

conformité de leur choix. Les organismes d'évaluation de la conformité devront être agréés par un organisme d'accréditation s'ils satisfont à certaines exigences spécifiées. L'accréditation sera accordée pour une durée maximale de cinq ans et pourra être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle sera révoquée si les conditions de l'accréditation ne sont pas ou plus remplies ou si des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.

En vertu de la proposition, les fonctions de suivi, de contrôle et d'exécution incombent aux États membres. Ceux-ci devront prévoir une autorité de contrôle de la certification, laquelle aura pour mission de contrôler que les organismes d'évaluation de la conformité, ainsi que les certificats délivrés par ceux qui sont établis sur son territoire, satisfont aux exigences du présent règlement et des systèmes européens de certification de cybersécurité pertinents. Les autorités nationales de contrôle de la certification seront compétentes pour traiter les plaintes déposées par des personnes physiques ou morales concernant les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire. Dans la mesure appropriée, elles examineront l'objet de la plainte et informeront le plaignant de l'avancement et des résultats de leur examen dans un délai raisonnable. De plus, elles coopéreront avec d'autres autorités de contrôle de la certification ou d'autres autorités publiques, par exemple en s'échangeant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou aux systèmes européens de certification de cybersécurité correspondants.

Enfin, la proposition consiste à instituer le Groupe européen de certification de cybersécurité (le «Groupe») composé d'autorités nationales de contrôle de la certification de tous les États membres. Il a pour mission principale de conseiller la Commission sur des questions concernant la politique de certification de cybersécurité et de travailler avec l'ENISA à l'élaboration de projets de systèmes européens de certification de cybersécurité. L'ENISA aidera la Commission à assurer le secrétariat du Groupe et tiendra à jour un recueil public des systèmes approuvés en vertu du Cadre européen de certification de cybersécurité. L'ENISA coopérerait aussi avec les organismes de normalisation afin de veiller à l'adéquation des normes utilisées dans les systèmes approuvés et de recenser les domaines nécessitant des normes de cybersécurité.

Le Cadre européen de certification de cybersécurité procurera divers avantages aux particuliers et aux entreprises. En particulier:

- Avec la création de systèmes de certification de cybersécurité de produits ou services spécifiques à l'échelle de l'UE, un guichet unique sera mis à la disposition des entreprises pour la certification de cybersécurité dans l'UE. Ces entreprises pourront ainsi ne faire certifier leurs produits qu'une seule fois et obtenir un certificat valable dans tous les États membres. Elles ne seront plus tenues de faire recertifier leurs produits par différents organismes nationaux de certification. Cela réduira considérablement les coûts des entreprises, facilitera les opérations transfrontières et, en fin de compte, limitera ou évitera le morcellement du marché intérieur des produits concernés.
- Le Cadre établit la primauté des systèmes européens de certification de cybersécurité sur les systèmes nationaux: en vertu de cette règle, l'adoption d'un système européen de certification de cybersécurité aura pour effet de remplacer tous les systèmes nationaux applicables parallèlement aux mêmes produits ou services TIC à un niveau d'assurance donné. Cela contribuera à une plus grande clarté en limitant la

multiplication de systèmes nationaux de certification de cybersécurité qui, aujourd'hui, font double emploi ou sont parfois contradictoires.

- La proposition vient en soutien et en complément de la mise en œuvre de la directive SRI en fournissant aux entreprises visées par celle-ci un moyen très pratique de prouver qu'elles satisfont aux exigences SRI dans l'ensemble de l'Union. Lors de l'élaboration de nouveaux systèmes de certification de cybersécurité, la Commission et l'ENISA veilleront en particulier à ce que les exigences SRI soient reprises dans lesdits systèmes.
- La proposition soutiendra et facilitera l'élaboration d'une politique européenne de cybersécurité en harmonisant les conditions et exigences fondamentales de la certification de cybersécurité des produits et services TIC dans l'UE. Les systèmes européens de certification de cybersécurité feront référence à des normes ou des critères d'évaluation et méthodes d'essai communs. Cela contribuera grandement, quoique indirectement, à l'adoption de solutions de sécurité communes dans l'UE et, ainsi, à la levée des obstacles au marché intérieur également.
- Le Cadre est conçu de façon à garantir la souplesse nécessaire aux systèmes de certification de cybersécurité. En fonction des besoins de cybersécurité spécifiques, un produit ou service peut être certifié à un niveau de sécurité plus ou moins élevé. Les systèmes européens de certification de cybersécurité seront conçus en tenant compte de cette souplesse et offriront donc plusieurs niveaux d'assurance (c.-à-d. élémentaire, substantiel ou élevé) de façon à pouvoir être utilisés à diverses fins ou dans différents contextes.
- Tous les éléments ci-dessus feront que les entreprises voient davantage la certification comme un moyen efficace de communiquer le niveau d'assurance de la cybersécurité de leurs produits ou services TIC. Dans la mesure où la certification de cybersécurité devient moins onéreuse, plus efficace et commercialement attrayante, les entreprises seront plus enclines à certifier leurs produits concernant les risques en la matière et contribueront ainsi à la diffusion de bonnes pratiques lors de la conception des produits et services TIC (cybersécurité dès la conception).

- **Cohérence avec les dispositions existantes dans le domaine d'action**

En vertu de la directive SRI, les opérateurs des secteurs d'activité vitaux pour l'économie et la société, comme l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé et les infrastructures numériques ainsi que les fournisseurs de services numériques (moteurs de recherche, services d'informatique en nuage et places de marché en ligne) sont tenus de prendre des mesures pour gérer correctement les risques pour la sécurité. Les nouvelles règles de la présente proposition sont conformes aux dispositions de la directive SRI et les complètent afin de perfectionner encore la cyberrésilience de l'UE par un renforcement des moyens, de la coopération, de la gestion des risques et de la sensibilisation.

De plus, les règles relatives à la certification de cybersécurité fournissent aux entreprises visées par la directive SRI un outil indispensable qui leur permettra de certifier leurs produits et services TIC concernant les risques en la matière sur la base de systèmes valables et

reconnus dans toute l'UE. Elles compléteront aussi les exigences de sécurité énoncées dans le règlement eIDAS[17] et la directive sur les équipements radioélectriques[18].

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

Le règlement (UE) n° 2016/679 (règlement général sur la protection des données ou «**RGPD**»)[19] contient des dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données afin de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Le présent règlement est sans préjudice de la certification des opérations de traitement de données, y compris lorsque ces opérations sont intégrées dans des produits et services, en vertu du RGPD.

Le règlement proposé garantira la compatibilité avec le règlement (CE) n° 765/2008 sur les prescriptions relatives à l'accréditation et à la surveillance du marché[20] en renvoyant aux règles de ce cadre sur les organismes nationaux d'accréditation et les organismes d'évaluation de la conformité. En ce qui concerne les autorités de contrôle, le règlement proposé exigera des États membres qu'ils désignent des autorités nationales de contrôle de la certification chargées du contrôle, du suivi et de l'application des règles. Ces organismes seront distincts des organismes d'évaluation de la conformité, comme prévu par le règlement (CE) n° 765/2008.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La base juridique de l'action de l'UE est l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), qui concerne le rapprochement des législations des États membres aux fins de la réalisation des objectifs énoncés à l'article 26 TFUE, à savoir le fonctionnement du marché intérieur.

La base juridique du marché intérieur, sur laquelle repose le règlement instituant l'ENISA, a été confirmée par la Cour de justice (dans l'affaire C-217/04 *Royaume-Uni contre Parlement européen et Conseil*), puis par le règlement de 2013 qui définit le mandat actuel de l'Agence. En outre, les activités ayant pour objectif d'intensifier la coopération et la coordination entre les États membres et celles visant à accroître les moyens au niveau de l'UE pour compléter l'action des États membres relèveraient de la «coopération opérationnelle». Celle-ci est expressément définie par la directive SRI (dont la base juridique est l'article 114 TFUE)

---

17 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

18 Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE.

19 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), JO L 119 du 4.5.2016, p. 1.

20 Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93.

comme un objectif à atteindre dans le cadre du réseau des CSIRT dont «[l]'ENISA assure le secrétariat et soutient activement la coopération» (article 12, paragraphe 2). En particulier, l'article 12, paragraphe 3, point f), précise les autres formes de coopération opérationnelle constituant des tâches du réseau des CSIRT, notamment en rapport avec: i) les catégories de risques et d'incidents; ii) les alertes précoces; iii) l'assistance mutuelle; et iv) les principes et modalités d'une coordination lorsque les États membres réagissent à des risques et incidents transfrontaliers.

- La multiplicité actuelle des systèmes de certification des produits et services TIC s'explique aussi par l'absence de réel cadre commun juridiquement contraignant pour les États membres. Cela empêche de créer un marché intérieur des produits et services TIC et nuit à la compétitivité des entreprises européennes dans ce secteur. La présente proposition vise à remédier au morcellement actuel du marché intérieur et à lever les obstacles qui s'opposent à celui-ci en fournissant un cadre commun pour l'instauration de systèmes de certification de cybersécurité valables dans toute l'UE.

Subsidiarité (en cas de compétence non exclusive)

Le principe de subsidiarité suppose d'évaluer la nécessité et la valeur ajoutée de l'action de l'UE. Le respect dudit principe dans ce domaine a déjà été reconnu lors de l'adoption de l'actuel règlement ENISA[21].

La cybersécurité est un sujet présentant un intérêt commun pour l'Union. Les interdépendances entre les réseaux et systèmes d'information sont telles que les acteurs à titre individuel (publics et privés, y compris les particuliers) sont très souvent incapables, isolément, de réagir aux menaces et de gérer les risques et les éventuelles conséquences de cyberincidents. D'une part, compte tenu des interdépendances entre les États membres, notamment en matière d'exploitation des infrastructures critiques (énergie, transports, eau, pour n'en citer que quelques-unes), l'intervention des pouvoirs publics au niveau européen est non seulement profitable, mais aussi nécessaire. D'autre part, l'intervention de l'UE peut avoir un effet positif d'entraînement dû à l'échange de bonnes pratiques entre les États membres avec, pour résultat, une cybersécurité accrue de l'Union.

En résumé, dans le contexte actuel et vu les scénarios futurs, il semble que, pour **accroître la cyberrésilience collective** de l'Union, **les actions individuelles des États membres de l'UE et une approche parcellaire de la cybersécurité** ne soient pas suffisantes.

Une action de l'UE est également jugée nécessaire pour remédier à la multiplicité des systèmes de certification de cybersécurité actuels. Elle permettrait aux fabricants de bénéficier pleinement d'un marché intérieur et de réaliser des économies substantielles sur les coûts d'expérimentation et de reconception. L'accord de reconnaissance mutuelle (ARM) du Groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS), par exemple, a donné des résultats importants à cet égard, mais il présente aussi de sérieuses lacunes qui le rendent inapte à fournir des solutions durables pour tirer pleinement parti du marché intérieur.

[21] Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004.

La valeur ajoutée d'une action au niveau de l'UE, notamment afin d'intensifier la coopération entre les États membres mais aussi entre les communautés de la sécurité des réseaux et de l'information, a été reconnue dans les conclusions du Conseil de 2016[22] et transparaît clairement dans l'évaluation de l'ENISA.

- **Proportionnalité**

Les mesures proposées n'excèdent pas ce qui est nécessaire pour atteindre les objectifs politiques envisagés. De plus, la portée de l'intervention de l'UE n'interdit aucune mesure nationale relative à des questions touchant à la sûreté de l'État. L'action de l'UE est donc justifiée pour des raisons de subsidiarité et de proportionnalité.

- **Choix de l'instrument**

La présente proposition prévoit le réexamen du règlement (UE) n° 526/2013 qui définit le mandat actuel et les missions de l'ENISA. De plus, étant donné le rôle important de l'ENISA dans la mise en place et la gestion d'un Cadre européen de certification de cybersécurité, mieux vaut établir le nouveau mandat de l'ENISA et ledit Cadre en vertu d'un seul instrument juridique, en l'occurrence un règlement.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

Évaluations ex post/bilans de qualité de la législation existante

La Commission, conformément à la feuille de route de l'évaluation[23], a apprécié **la pertinence, l'incidence, l'efficacité, l'efficience, la cohérence et la valeur ajoutée** de l'Agence en ce qui concerne son fonctionnement, sa gouvernance, sa structure organisationnelle interne et ses méthodes de travail au cours de la période 2013-2016. Les principales conclusions peuvent être résumées comme suit (pour plus de détails, consulter le document de travail des services de la Commission sur le sujet, qui accompagne l'analyse d'impact).

- **Pertinence:** compte tenu de l'évolution des technologies et des menaces et du besoin pressant d'accroître la cybersécurité dans l'UE, les objectifs de l'ENISA se sont avérés pertinents. De fait, les États membres et les organismes de l'UE comptent sur la grande expertise de l'Agence en matière de cybersécurité. De plus, il faut se doter de moyens, dans les États membres, pour mieux appréhender les menaces et y répondre, et les parties intéressées doivent coopérer dans tous les champs thématiques et toutes les institutions. La cybersécurité reste une priorité politique absolue de l'UE à laquelle l'ENISA est censée répondre. Toutefois, le fait que l'ENISA ait été créée en tant qu'agence de l'UE avec un mandat à durée déterminée: i) ne permet aucune planification à long terme et empêche d'apporter un soutien durable aux États membres et aux institutions de l'UE; ii) peut créer un vide juridique car les dispositions de la directive SRI confiant des missions à l'ENISA

[22] Conclusions du Conseil intitulées «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», 15 novembre 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

sont de nature permanente[24]; iii) n'est pas compatible avec une vision intégrant l'ENISA dans un écosystème européen de cybersécurité renforcé.

- **Efficacité**: l'ENISA a globalement atteint ses objectifs et accompli ses missions. Elle a contribué à accroître la sécurité des réseaux et de l'information en Europe par ses principales activités (dotation de moyens, fourniture d'expertise, création de communautés et soutien aux politiques). Concernant chacune d'elles, des possibilités d'amélioration ont cependant été recensées. Il est ressorti de l'évaluation que l'ENISA a effectivement permis de créer de solides relations de confiance avec certaines parties intéressées, notamment les États membres et la communauté des CSIRT. Les interventions concernant la dotation de moyens ont été jugées efficaces, en particulier pour les États membres ayant le moins de ressources. L'action en faveur d'une coopération étendue a été l'une des plus remarquables et les parties intéressées s'accordent à dire que l'ENISA a joué un rôle fédérateur utile. Néanmoins, l'ENISA a eu du mal à exercer son influence dans le vaste domaine de la sécurité des réseaux et de l'information. Cela tient aussi au fait qu'elle disposait de ressources humaines et financières assez limitées pour s'acquitter d'un mandat très large. Il a également été conclu de l'évaluation que l'ENISA avait en partie atteint l'objectif de fournir une expertise, cela étant lié aux problèmes pour recruter des experts (voir aussi ci-après la partie «Efficience»).

- **Efficience**: malgré son budget limité – l'un des moins élevés de tous les organes de l'UE –, l'Agence a été capable de poursuivre les objectifs fixés, en se montrant globalement efficiente dans l'utilisation de ses ressources. Il est ressorti de l'évaluation que les processus étaient généralement efficients et que le partage clair des responsabilités au sein de l'organisation a permis une exécution satisfaisante des tâches. L'un des principaux problèmes de l'Agence en matière d'efficience tient aux difficultés rencontrées par l'ENISA pour recruter et retenir des experts hautement qualifiés. D'après les conclusions, cela peut s'expliquer par une combinaison de facteurs: la difficulté du secteur public, en général, à concurrencer le secteur privé lorsqu'il s'agit d'embaucher des experts hautement spécialisés; le type de contrats (à durée déterminée) que l'Agence pouvait surtout proposer; et le degré d'attractivité relativement faible de l'ENISA dû à sa localisation et, notamment, aux problèmes rencontrés par les conjoints pour trouver du travail. Le dédoublement de l'implantation entre Athènes et Heraklion a exigé des efforts de coordination et engendré des coûts administratifs supplémentaires, mais le déménagement à Athènes, en 2013, du centre opérationnel a permis d'accroître l'efficacité opérationnelle de l'Agence.

- **Cohérence**: la cohérence entre les activités de l'ENISA et les politiques et activités des parties intéressées a été généralement assurée, aux niveaux national et de l'UE, mais une approche plus coordonnée de la cybersécurité est nécessaire au niveau de l'UE. Les possibilités de coopération entre l'ENISA et d'autres organismes de l'UE n'ont pas été pleinement exploitées. L'évolution de l'environnement juridique et politique de l'UE rend le mandat actuel de l'Agence moins cohérent.

- **Valeur ajoutée européenne**: la valeur ajoutée de l'ENISA réside d'abord dans la capacité de l'Agence à intensifier la coopération entre les États membres principalement, mais aussi avec les communautés de la sécurité des réseaux et de

[24] Référence aux articles 7, 9, 11, 12 et 19 de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI).

l'information correspondantes. Il n'y a aucune autre entité au niveau de l'UE qui favorise la coopération d'autant de parties intéressées par la sécurité des réseaux et de l'information. La valeur ajoutée procurée par l'Agence varie en fonction des besoins et des ressources des parties intéressées (p. ex. grands États membres par opposition aux petits États membres; États membres par opposition aux entreprises) et de la nécessité de l'Agence de hiérarchiser ses activités selon le programme de travail. Il est ressorti de l'évaluation qu'une éventuelle disparition de l'ENISA constituerait une occasion manquée pour tous les États membres. Il serait dès lors impossible d'assurer la création de communautés et une coopération aussi poussée de tous les États membres en matière de cybersécurité. Sans une agence de l'UE centralisée, la situation serait plus diverse et des formes de coopération bilatérale ou régionale feraient leur apparition pour combler le vide laissé par l'ENISA.

En ce qui concerne plus particulièrement le fonctionnement de l'ENISA jusqu'à maintenant et à l'avenir, les grandes tendances qui se dégagent de la consultation de 2017 sont les suivantes[25]:

- Le fonctionnement global de l'ENISA au cours de la période 2013-2016 a été jugé satisfaisant par une majorité de participants (74 %). Une majorité de participants a également estimé que l'ENISA atteignait ses différents objectifs (au moins 63 % pour chacun des objectifs). Les services et produits de l'ENISA sont régulièrement (chaque mois ou plus souvent) utilisés par près de la moitié des participants (46 %) et sont appréciés parce qu'ils proviennent d'un organisme au niveau de l'UE (83 %) et pour leur qualité (62 %).
- Les participants ont recensé un certain nombre de lacunes et de problèmes concernant l'avenir de la cybersécurité dans l'UE, parmi lesquels les cinq principaux (sur une liste de 16) étaient: la coopération de tous les États membres; la capacité à prévenir et détecter les cyberattaques de grande ampleur et à y réagir; la coopération entre les États membres en ce qui concerne la cybersécurité; la coopération et l'échange d'informations entre les différentes parties intéressées, y compris entre secteur public et secteur privé; la protection des infrastructures critiques contre les cyberattaques.
- Une grande majorité (88 %) de participants a estimé que les instruments et mécanismes actuellement disponibles au niveau de l'UE n'étaient pas suffisants ou que partiellement adaptés pour traiter ces problèmes. Dans leur grande majorité (98 %), les participants ont déclaré qu'il fallait un organisme de l'UE pour répondre à ces besoins, et 99 % d'entre eux ont estimé que l'ENISA était l'organisation appropriée à cette fin.

[25] Ont participé à la consultation 90 parties intéressées de 19 États membres (88 réponses et 2 documents de synthèse), dont des autorités nationales de 15 États membres, parmi lesquels la France, l'Italie, l'Irlande et la Grèce, et 8 organisations faîtières représentant un nombre significatif d'entreprises européennes, par exemple la Fédération bancaire de l'Union européenne, Digital Europe (représentant le secteur des technologies numériques en Europe) et l'Association européenne des exploitants de réseaux de télécommunications (ETNO). La consultation publique sur l'ENISA a été complétée par plusieurs autres sources telles que: i) entretiens approfondis avec quelque 50 acteurs clés du secteur de la cybersécurité; ii) enquête auprès du réseau des CSIRT; iii) enquête auprès du conseil d'administration, du conseil exécutif et du groupe permanent des parties prenantes de l'ENISA.

Consultation des parties intéressées

- La Commission a organisé, du 12 avril au 5 juillet 2016, une consultation publique sur le réexamen de l'ENISA et a reçu 421 contributions[26]. D'après les résultats, 67,5 % des participants étaient d'avis que l'ENISA pourrait jouer un rôle dans l'établissement d'un cadre harmonisé pour la certification de sécurité des produits et services informatiques.

Les résultats de la consultation de 2016 concernant le PPPc sur la cybersécurité[27] révèlent, à la partie consacrée à la certification, que:

- 50,4 % des participants (121 sur 240) ne savent pas si les systèmes nationaux de certification sont mutuellement reconnus dans tous les États membres de l'UE. 25,8 % (62 sur 240) ont répondu «Non» tandis que 23,8 % (57 sur 240) ont répondu «Oui».
- 37,9 % des participants (91 sur 240) pensent que les systèmes de certification existants ne répondent pas aux besoins des entreprises en Europe. Par ailleurs, 17,5 % (42 sur 240), principalement des entreprises multinationales présentes sur le marché européen, étaient d'avis contraire.
- 49,6 % des participants (119 sur 240) déclarent qu'il n'est pas facile de démontrer l'équivalence entre les normes, les systèmes de certification et les étiquettes. 37,9 % (91 sur 240) ont répondu «Je ne sais pas» tandis que 12,5 % (30 sur 240) ont répondu «Oui».

Obtention et utilisation d'expertise

La Commission s'est appuyée sur les conseils d'experts externes suivants:

- étude sur l'évaluation de l'ENISA (Ramboll/Carsa 2017; SMART n° 2016/0077),
- étude sur la certification et l'étiquetage de sécurité en matière de TIC – collecte de données et analyse d'impact (PriceWaterhouseCoopers 2017; SMART n° 2016/0029).

Analyse d'impact

- Dans le rapport d'analyse d'impact de cette initiative, sont recensés les principaux problèmes à traiter:
- multiplicité des politiques et approches en matière de cybersécurité dans les États membres;
- dispersion des ressources et multiplicité des approches de la cybersécurité dans les institutions, organes et organismes de l'UE; et

[26] 162 contributions de la part de particuliers, 33 de représentants de la société civile et d'associations de consommateurs, 186 d'entreprises et 40 d'autorités publiques, y compris d'autorités responsables de l'application de la directive «vie privée et communications électroniques».

[27] 240 parties intéressées, représentant des administrations publiques nationales, des grandes entreprises, des PME, des micro-entreprises et des organismes de recherche, ont répondu à la partie consacrée à la certification.

- insuffisance de la sensibilisation et de l'information des particuliers et des entreprises, associée à la multiplication des systèmes de certification nationaux et sectoriels.

Dans le rapport, sont examinées les possibilités suivantes concernant le mandat de l'ENISA:

- le maintien du statu quo, c'est-à-dire renouvellement d'un mandat toujours limité dans le temps (scénario de référence);
- l'expiration du mandat actuel de l'ENISA sans renouvellement et disparition de l'ENISA (aucune intervention);
- une «ENISA réformée»; et
- une agence de l'UE pour la cybersécurité disposant de moyens opérationnels complets.

Dans le rapport, sont examinées les possibilités suivantes concernant la certification de sécurité:

- aucune intervention (scénario de référence);
- des mesures non législatives (non contraignantes);
- un acte législatif de l'UE portant création d'un système obligatoire pour tous les États membres et fondé sur le système SOG-IS; et
- un cadre européen général de certification de cybersécurité en matière de TIC.

L'analyse a permis de conclure qu'une «ENISA réformée», combinée à un cadre européen général de certification de cybersécurité en matière de TIC, est l'option privilégiée.

L'option privilégiée a été jugée la plus susceptible de permettre à l'UE d'atteindre les objectifs suivants: accroître les moyens de cybersécurité, la préparation, la coopération et la transparence; et éviter le morcellement du marché. Elle a également été jugée la plus conforme aux priorités de la stratégie de cybersécurité de l'UE et des politiques qui s'y rapportent (p. ex. directive SRI), et à la stratégie pour le marché unique numérique. En outre, il est ressorti du processus de consultation que l'option privilégiée bénéficie du soutien de la majorité des parties intéressées. De plus, l'analyse d'impact a montré que l'option privilégiée permettrait d'atteindre les objectifs fixés grâce à une utilisation raisonnable des ressources.

Le comité d'examen de la réglementation de la Commission a rendu, le 24 juillet, un premier avis défavorable puis, le 25 août 2017, un avis favorable sur une nouvelle version. Le rapport d'analyse d'impact modifié fournissait de nouveaux éléments justificatifs, les conclusions finales de l'évaluation de l'ENISA et des explications supplémentaires sur les options stratégiques et leur incidence. L'annexe 1 du rapport d'analyse d'impact final indique succinctement comment ont été prises en compte les observations du comité dans son second avis. Le rapport a notamment été mis à jour de façon à décrire plus en détail la situation en matière de cybersécurité dans l'UE, y compris les mesures figurant dans la communication conjointe «*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*», [JOIN(2017) 450] et présentant un intérêt particulier pour l'ENISA: le plan de l'UE en matière de cybersécurité et le Centre européen de recherche et de compétences en matière de cybersécurité auquel l'Agence fournirait ses conseils sur les besoins de recherche de l'UE.

Le rapport explique comment la réforme de l'Agence, notamment ses nouvelles missions, les meilleures conditions d'emploi et la coopération structurelle avec les organismes de l'UE actifs dans ce domaine, rendraient l'ENISA plus attrayante comme employeur et permettraient de traiter les problèmes liés au recrutement d'experts. L'annexe 6 du rapport

fournit aussi une estimation révisée des coûts associés aux options stratégiques concernant l'ENISA. S'agissant de la certification, le rapport a été revu de façon à fournir une explication plus détaillée de l'option privilégiée, y compris par une présentation graphique, ainsi que des estimations des coûts liés au nouveau cadre de certification pour les États membres et la Commission. Le choix de l'ENISA comme principal intervenant en la matière a été justifié avec plus de clarté par son expertise dans le domaine et par le fait que c'est la seule agence pour la cybersécurité au niveau de l'UE. Enfin, les parties sur la certification ont été revues afin d'en éclaircir certains aspects comme la différence avec le système SOG-IS actuel et les avantages procurés par les différentes options stratégiques, et de préciser que le type de produit ou service TIC couvert par un système européen de certification sera défini dans le système approuvé même.

Réglementation affûtée et simplification

Sans objet.

Incidence sur les droits fondamentaux

La cybersécurité est essentielle pour protéger la vie privée et les données à caractère personnel des individus conformément aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE. Or, en cas de cyberincidents, le respect de la vie privée et la protection de nos données à caractère personnel sont incontestablement compromis. La cybersécurité est donc une condition nécessaire au respect de la vie privée et à la confidentialité de nos données à caractère personnel. Dans cette perspective, la présente proposition, en visant à renforcer la cybersécurité en Europe, constitue un complément important de la législation protégeant actuellement le droit fondamental au respect de la vie privée et des données à caractère personnel. La cybersécurité est également essentielle pour préserver la confidentialité de nos communications électroniques et donc à l'exercice de la liberté d'expression et d'information et d'autres droits apparentés tels que la liberté de pensée, de conscience et de religion.

4. INCIDENCE BUDGÉTAIRE

Voir la fiche financière.

5. AUTRES ÉLÉMENTS

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

La Commission contrôlera l'application du règlement et présentera, tous les cinq ans, un rapport sur son évaluation au Parlement européen, au Conseil et au Comité économique et social européen. Ces rapports seront publics et rendront compte en détail de l'application et de l'exécution effectives du présent règlement.

- **Explication détaillée des différentes dispositions de la proposition**

Le titre I du règlement contient les dispositions générales: l'objet (article 1er), les définitions (article 2), y compris les références aux définitions applicables tirées d'autres instruments de l'UE comme la directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI), le règlement (CE) n° 765/2008 du

Parlement européen et du Conseil fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, et le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil relatif à la normalisation européenne.

Le titre II du règlement contient les principales dispositions relatives à l'ENISA, agence de l'UE pour la cybersécurité.

Le chapitre I sous ce titre définit le mandat (article 3), les objectifs (article 4) et les missions (articles 5 à 11) de l'Agence.

Le chapitre II précise l'organisation de l'ENISA et comprend des dispositions sur sa structure (article 12). Il indique la composition, les règles de vote et les fonctions du conseil d'administration (section 1, articles 13 à 17) et du conseil exécutif (section 2, article 18) et les fonctions du directeur exécutif (section 3, article 19). Il comprend aussi des dispositions sur la composition et le rôle du groupe permanent des parties prenantes (section 4, article 20). Enfin, la section 5 de ce chapitre détaille les règles de fonctionnement de l'Agence, notamment en ce qui concerne la programmation de ses opérations, les conflits d'intérêts, la transparence, la confidentialité et l'accès aux documents (articles 21 à 25).

Le chapitre III concerne l'établissement et la structure du budget de l'Agence (articles 26 et 27) ainsi que les règles régissant sa mise en œuvre (articles 28 et 29). Il comprend aussi les dispositions visant à faciliter la lutte contre la fraude, la corruption et les autres activités illicites (article 30).

Le chapitre IV porte sur la dotation en personnel de l'Agence. Il comprend des dispositions générales sur le statut et le régime applicable au personnel, et des règles régissant les privilèges et immunités (articles 31 et 32). Il détaille également les règles d'embauche et de nomination du directeur exécutif de l'Agence (article 33). Enfin, il comprend des dispositions régissant le recours à des experts nationaux détachés ou à tout autre personnel non employé par l'Agence (article 34).

En dernier lieu, le chapitre V contient les dispositions générales relatives à l'Agence. Il définit le statut juridique (article 35) et comprend des dispositions concernant les questions de responsabilité, de régime linguistique et de protection des données à caractère personnel (articles 36 à 38) ainsi que les règles de sécurité en matière de protection des informations classifiées et des informations sensibles non classifiées (article 40). Il décrit les règles régissant la coopération de l'Agence avec des pays tiers et les organisations internationales (article 39). Enfin, il contient aussi des dispositions concernant le siège de l'Agence et ses conditions de fonctionnement, ainsi que le contrôle administratif exercé par le médiateur (articles 41 et 42).

Le titre III du règlement instaure le Cadre européen de certification de cybersécurité (le «**Cadre**») des produits et services TIC en tant qu'entité relevant de la *lex generalis* (article 1er). Il établit la finalité générale des systèmes européens de certification de cybersécurité, c'est-à-dire garantir que les produits et services TIC satisfont à des exigences de cybersécurité spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à une action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés (article 43). De plus, il énumère les objectifs de sécurité que les systèmes européens de certification de cybersécurité doivent poursuivre (article 45), comme par exemple protéger les données contre l'accès, la diffusion, la destruction ou l'altération accidentels ou non autorisés, et précise le contenu (c.-à-d. les éléments) des systèmes européens de certification de cybersécurité,

comme la spécification détaillée de leur champ d'application, les objectifs de sécurité, les critères d'évaluation, etc. (article 47).

Le titre III définit aussi les principaux effets juridiques des systèmes européens de certification de cybersécurité, à savoir: i) l'obligation de mettre en œuvre le système au niveau national et le caractère facultatif de la certification; ii) l'invalidation des systèmes nationaux de certification de cybersécurité des mêmes produits et services (articles 48 et 49).

Ce titre précise la procédure d'adoption des systèmes européens de certification de cybersécurité et les rôles respectifs de la Commission, de l'ENISA et du Groupe européen de certification de cybersécurité (le «Groupe») (article 44). Enfin, ce titre établit les dispositions régissant les organismes d'évaluation de la conformité, notamment leurs exigences, pouvoirs et missions, les autorités nationales de contrôle de la certification ainsi que les sanctions.

Le Groupe est également institué en tant qu'organisme essentiel, composé de représentants des autorités nationales de contrôle de la certification, dont la principale fonction est de travailler avec l'ENISA à la préparation de systèmes européens de certification de cybersécurité et de conseiller la Commission sur des questions générales ou particulières concernant la politique en la matière.

Le titre IV du règlement comprend les dispositions finales concernant l'exercice de la délégation, les exigences en matière d'évaluation, l'abrogation et la succession, ainsi que l'entrée en vigueur.

2017/0225 (COD)

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)

(Texte présentant de l'intérêt pour l'EEE)

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[28],

vu l'avis du Comité des régions[29],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Les réseaux et systèmes d'information et les réseaux et services de télécommunications remplissent une fonction essentielle pour la société et sont devenus le nerf de la croissance économique. Les technologies de l'information et des communications sont le fondement des systèmes complexes qui rendent possibles les activités sociales; elles permettent à nos économies de fonctionner dans des secteurs clés comme la santé, l'énergie, la finance et les transports, et soutiennent en particulier le fonctionnement du marché intérieur.

(2) L'utilisation des réseaux et des systèmes d'information par les particuliers, les entreprises et les pouvoirs publics s'est généralisée dans l'Union tout entière. La numérisation et la connectivité caractérisent un nombre toujours croissant de produits et de services; avec l'avènement de l'internet des objets (IdO), ce sont des millions, sinon des milliards, de dispositifs numériques connectés qui devraient être mis en service dans l'UE au cours de la prochaine décennie. Alors qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment les impératifs de sécurité et de résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification entraîne un manque d'information des utilisateurs, qu'il s'agisse de particuliers ou d'organisations, sur les caractéristiques des produits et services TIC en matière de cybersécurité, sapant ainsi la confiance dans les solutions numériques.

[28] JO C du , p. .
[29] JO C du , p. .

(3) Une numérisation et une connectivité accrues entraînent une augmentation des risques en matière de cybersécurité, ce qui rend ainsi l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. Afin d'atténuer ce risque pour la société, il convient de prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin de mieux protéger les réseaux et systèmes d'information, les réseaux de télécommunication, les produits, services et appareils numériques utilisés par les particuliers, les pouvoirs publics et les entreprises — depuis les PME jusqu'aux opérateurs d'infrastructures critiques — contre les cybermenaces.

(4) Les cyberattaques sont en augmentation; une économie et une société connectées, qui sont plus vulnérables aux cybermenaces et aux cyberattaques, ont donc besoin de dispositifs de défense renforcés. Cependant, alors que les cyberattaques sont souvent de nature transnationale, les réponses apportées par les autorités chargées de la cybersécurité et les compétences en matière de répression sont surtout nationales. Des incidents de cybersécurité majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'UE. Il est donc indispensable de mettre sur pied une capacité de réaction et de gestion des crises à l'échelon de l'UE, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée à partir de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs tant au niveau de l'Union qu'au niveau mondial.

(5) Compte tenu de l'augmentation des enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'une panoplie de mesures qui développent les actions déjà menées par l'Union et promeuvent des objectifs se renforçant mutuellement. Ces objectifs sont notamment la nécessité de continuer à renforcer les capacités et l'état de préparation des États membres et des entreprises, ainsi que d'améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE. En outre, étant donné la nature universelle des cybermenaces, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et crises transfrontières de cybersécurité majeurs. Des efforts supplémentaires sont également requis pour sensibiliser davantage les particuliers et les entreprises aux questions de cybersécurité. En outre, une information transparente sur le niveau de sécurité qui caractérise les produits et services TIC permettrait de renforcer la confiance dans le marché unique numérique. Une certification mise en œuvre à l'échelle de l'UE, prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs, peut faciliter cette transparence.

(6) En 2004, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 460/2004[30] instituant l'ENISA en vue de contribuer à la réalisation des objectifs visant à assurer un niveau élevé de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de

[30] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. En 2008, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 1007/2008[31] prolongeant le mandat de l'Agence jusqu'en mars 2012. Le règlement (CE) n° 580/2011[32] a prolongé le mandat de l'Agence une nouvelle fois jusqu'au 13 septembre 2013. En 2013, le Parlement européen et le Conseil ont adopté le règlement (UE) n° 526/2013[33] concernant l'ENISA et abrogeant le règlement (CE) n° 460/2004, qui a prolongé le mandat de l'Agence jusqu'en juin 2020.

(7) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et renforcer la confiance dans les technologies numériques. En 2013, l'UE s'est dotée d'une stratégie de cybersécurité afin d'orienter la politique qu'elle entendait mener en réaction aux menaces et aux risques qui pèsent sur la cybersécurité. Dans le cadre de ses efforts pour mieux protéger les Européens en ligne, l'Union a adopté en 2016 le premier acte législatif dans le domaine de la cybersécurité, la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (la «directive SRI»). La directive SRI a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, établi le premier mécanisme destiné à améliorer la coopération stratégique et opérationnelle entre les États membres, et introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société, tels que l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne). L'ENISA s'est vu attribuer un rôle essentiel d'appui à la mise en œuvre de cette directive. En outre, lutter efficacement contre la cybercriminalité est l'une des principales priorités du programme européen en matière de sécurité et contribue à l'objectif global consistant à atteindre un niveau élevé de cybersécurité.

(8) Il est reconnu que, depuis l'adoption de la stratégie de cybersécurité de l'UE en 2013 et la dernière révision du mandat de l'Agence, le cadre d'action général a considérablement évolué, compte tenu notamment d'un environnement mondial plus incertain et moins sûr. Dans ce contexte, et dans le cadre de la nouvelle politique de cybersécurité de l'Union, il est nécessaire de réviser le mandat de l'ENISA pour définir son rôle dans le nouvel écosystème de la cybersécurité et faire en sorte qu'elle contribue efficacement à la réponse apportée par l'Union aux défis en matière de cybersécurité qui résultent de cette transformation radicale de la nature des menaces. L'évaluation de l'Agence a en effet conclu à une insuffisance du mandat actuel à cet égard.

---

31 Règlement (CE) n° 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) no 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 293 du 31.10.2008, p. 1).

32 Règlement (UE) n° 580/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) no 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 165 du 24.6.2011, p. 3).

33 Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) no 460/2004 (JO L 165 du 18.6.2013, p. 41).

(9) L'Agence établie par le présent règlement devrait succéder à l'ENISA telle qu'instituée par le règlement (UE) n° 526/2013. L'Agence devrait remplir les missions qui lui sont confiées par le présent règlement et par les actes législatifs de l'Union dans le domaine de la cybersécurité notamment en fournissant une expertise et des conseils et en jouant le rôle de centre d'information et de connaissance au niveau de l'Union. Elle devrait promouvoir l'échange des meilleures pratiques entre les États membres et les parties prenantes du secteur privé en proposant des mesures à la Commission européenne et aux États membres, en jouant le rôle de point de référence pour les initiatives politiques sectorielles au niveau de l'Union en ce qui concerne la cybersécurité, en favorisant la coopération opérationnelle entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union.

(10) Dans le cadre de la décision 2004/97/CE, Euratom adoptée lors de la réunion du Conseil européen du 13 décembre 2003, les représentants des États membres ont décidé que l'Agence aurait son siège dans une ville en Grèce que le gouvernement grec déterminerait. L'État membre d'accueil de l'Agence devrait offrir les meilleures conditions possibles pour un fonctionnement harmonieux et efficace de l'Agence. Il est impératif, pour l'accomplissement correct et efficace de ses missions, pour le recrutement et la fidélisation du personnel et pour une plus grande efficacité des activités de mise en réseau, que l'Agence soit établie dans un lieu approprié, offrant, entre autres, des liaisons de transport et des aménagements appropriés pour les conjoints et enfants accompagnant les membres du personnel de l'Agence. Les dispositions nécessaires devraient être arrêtées dans un accord conclu, après approbation du conseil d'administration de l'Agence, entre l'Agence et l'État membre d'accueil.

(11) Étant donné l'aggravation des défis en matière de cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'Agence pour tenir compte du renforcement de son rôle et de ses missions, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique européen.

(12) L'Agence devrait acquérir et maintenir un niveau élevé d'expertise et servir de point de référence, en instaurant la confiance dans le marché intérieur du fait de son indépendance, de la qualité des conseils fournis et des informations diffusées, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à exécuter ses missions. L'Agence devrait contribuer de manière dynamique aux efforts consentis aux niveaux national et de l'Union, tout en s'acquittant de ses missions en totale coopération avec les institutions, organes et organismes de l'Union et les États membres. De plus, l'Agence devrait s'appuyer sur les informations fournies par le secteur privé et travailler en coopération avec celui-ci, ainsi qu'avec d'autres parties prenantes. Un ensemble de missions devrait déterminer la manière dont l'Agence doit atteindre ses objectifs tout en lui laissant une certaine souplesse de fonctionnement.

(13) L'Agence devrait assister la Commission sous la forme de conseils, d'avis et d'analyses sur toutes les questions européennes liées à l'élaboration, l'actualisation et la révision des politiques et de la législation dans le domaine de la cybersécurité, y compris la protection des infrastructures critiques et la cyberrésilience. L'Agence devrait être un point de référence, par ses conseils et son expertise, pour les initiatives politiques et législatives sectorielles au niveau de l'Union dans tous les cas où la cybersécurité est en jeu.

(14) La mission fondamentale de l'Agence consiste à promouvoir la mise en œuvre cohérente du cadre législatif applicable, et notamment la mise en œuvre effective de la directive SRI, essentielle pour renforcer la cyberrésilience. Compte tenu de l'évolution rapide de l'éventail des menaces en matière de cybersécurité, il est clair que les États membres ont besoin de s'appuyer sur une approche plus globale, transsectorielle, du développement de la cyberrésilience.

(15) L'Agence devrait assister les États membres et les institutions, organes et organismes de l'Union dans leurs efforts pour mettre en place et développer les capacités et la préparation requises pour prévenir et détecter les problèmes et incidents de cybersécurité et y réagir, et en ce qui concerne la sécurité des réseaux et des systèmes d'information. L'Agence devrait notamment soutenir le développement et l'amélioration des CSIRT nationaux, afin qu'ils atteignent un niveau de maturité commun élevé dans l'ensemble de l'Union. L'Agence devrait également contribuer à l'élaboration et à la mise à jour des stratégies de l'Union et des États membres en matière de sécurité des réseaux et systèmes d'information, notamment en matière de cybersécurité, promouvoir leur diffusion et suivre l'avancement de leur mise en œuvre. L'Agence devrait enfin proposer des formations et du matériel pédagogique aux organismes publics et, le cas échéant, «former les formateurs» en vue d'aider les États membres à mettre en place leurs propres capacités de formation.

(16) L'Agence devrait aider le groupe de coopération établi par la directive SRI à accomplir ses tâches, notamment en le faisant bénéficier de ses conseils et de son expertise, et en facilitant l'échange de bonnes pratiques en matière de risques et d'incidents, en particulier en ce qui concerne l'identification des opérateurs de services essentiels par les États membres, y compris au regard des dépendances transfrontalières.

(17) Afin de stimuler la coopération entre le secteur public et le secteur privé et au sein de ce dernier, notamment pour favoriser la protection des infrastructures critiques, l'Agence devrait faciliter la mise en place de centres sectoriels d'échange et d'analyse d'informations (ISAC), en proposant des bonnes pratiques et des orientations sur les outils disponibles, des procédures, et en fournissant des orientations sur la manière de traiter les questions de réglementation liées au partage d'informations.

(18) L'Agence devrait agréger et analyser les rapports nationaux émanant des CSIRT et des CERT-UE, en établissant des règles, un langage et une terminologie communs pour l'échange d'informations. L'Agence devrait également assurer la participation du secteur privé, dans le cadre de la directive SRI, qui a fixé les bases d'un échange volontaire d'informations techniques à l'échelon opérationnel avec la création du réseau des CSIRT.

(19) L'Agence devrait contribuer à l'élaboration d'une réaction au niveau de l'UE en cas d'incidents ou de crises transfrontières de cybersécurité majeurs. Cette fonction devrait comprendre la collecte d'informations pertinentes et un rôle de facilitateur entre le réseau des CSIRT et la communauté technique ainsi que les décideurs chargés de la gestion des crises. En outre, l'Agence pourrait soutenir le traitement des incidents sur le plan technique, en facilitant l'échange de solutions techniques pertinentes entre les États membres et en contribuant à l'élaboration des communications au public. L'Agence devrait soutenir le processus en testant les modalités de cette coopération grâce à des exercices de cybersécurité annuels.

(20) Pour s'acquitter de ses missions opérationnelles, l'Agence devrait recourir à l'expertise disponible de la CERT-UE, grâce à une coopération structurée, dans un

contexte de proximité physique. La coopération structurée facilitera les synergies nécessaires et le renforcement des compétences de l'ENISA. Le cas échéant, des accords spécifiques entre les deux organisations devraient être conclus afin de définir les modalités pratiques de la mise en œuvre de cette coopération.

(21) Dans le cadre de ses missions opérationnelles, l'Agence devrait être en mesure de fournir un appui aux États membres, par exemple sous la forme de conseils ou d'assistance technique, ou encore en assurant l'analyse des menaces et incidents. La recommandation de la Commission sur la coordination des réactions aux incidents et crises de cybersécurité majeurs invite les États membres à coopérer de bonne foi et à partager dans les meilleurs délais, entre eux et avec l'ENISA, les informations relatives aux crises et incidents de cybersécurité majeurs. Ces informations devraient apporter une aide supplémentaire à l'ENISA pour l'accomplissement de ses missions opérationnelles.

(22) Dans le cadre de la coopération technique régulière menée pour étayer l'appréciation de la situation au niveau de l'Union, l'Agence devrait, à intervalle régulier, préparer le rapport de situation technique sur les incidents et menaces de cybersécurité dans l'UE, sur la base d'informations du domaine public, de sa propre analyse et de rapports que lui communiquent les CSIRT des États membres (sur une base volontaire) ou les points de contact uniques au titre de la directive SRI, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE et, le cas échéant, le Centre de l'UE pour l'analyse des renseignements (INTCEN) au sein du Service européen pour l'action extérieure (SEAE). Le rapport devrait être mis à la disposition des instances compétentes du Conseil, de la Commission, de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et du réseau des CSIRT.

(23) Les enquêtes techniques ex post sur les incidents ayant un impact significatif dans plusieurs États membres, lancées ou soutenues par l'Agence sur demande des États membres concernés ou avec leur accord, devraient être axées sur la prévention des incidents futurs et être exécutées sans préjudice de toute action judiciaire ou administrative visant à déterminer des fautes ou des responsabilités.

(24) Les États membres concernés devraient fournir à l'Agence les renseignements et l'assistance requis aux fins de l'enquête, sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne ou d'autres raisons d'ordre public.

(25) Les États membres peuvent inviter les entreprises concernées par l'incident à coopérer en fournissant les renseignements et l'assistance nécessaires à l'Agence, sans préjudice de leur droit de protéger les informations commercialement sensibles.

(26) Pour mieux comprendre les défis dans le domaine de la cybersécurité et en vue de fournir aux États membres et aux institutions de l'Union des conseils stratégiques à long terme, l'Agence devrait analyser les risques actuels et émergents. À cet effet, l'Agence devrait, en coopération avec les États membres et, le cas échéant, avec des instituts de statistique et d'autres organismes, recueillir des informations pertinentes sur les technologies émergentes, les soumettre à des analyses et fournir des évaluations thématiques spécifiques sur les effets sociétaux, juridiques, économiques et réglementaires à attendre des innovations technologiques sur la sécurité des réseaux et de l'information, et notamment sur la cybersécurité. L'Agence devrait en outre aider les États membres et les institutions, organes et organismes de l'Union à déceler les tendances nouvelles et à prévenir les problèmes liés à la cybersécurité, en procédant à l'analyse des menaces et incidents.

(27) Afin de renforcer la résilience de l'Union, l'Agence devrait développer l'excellence en matière de sécurité des infrastructures internet et des infrastructures critiques en fournissant des conseils, des orientations ou des bonnes pratiques. En vue de faciliter l'accès à des informations mieux structurées sur les risques de cybersécurité et les solutions possibles, l'Agence devrait mettre sur pied et gérer le «pôle d'information» de l'Union, un portail servant de guichet unique pour l'obtention d'informations sur la cybersécurité en provenance des institutions, organes et organismes de l'UE et nationaux.

(28) L'Agence devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs. L'Agence devrait également contribuer à promouvoir les meilleures pratiques et solutions pour les particuliers et les organisations en collectant et en analysant des informations du domaine public sur les incidents significatifs, et en rédigeant des rapports en vue de fournir des orientations aux entreprises et aux particuliers, et d'améliorer le niveau global de préparation et de résilience. L'Agence devrait en outre organiser, en coopération avec les membres et les institutions, organes et organismes de l'Union, des campagnes d'information régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finaux, en vue de promouvoir une navigation en ligne plus sûre pour tous et de sensibiliser aux dangers potentiels du cyberespace, y compris la cybercriminalité notamment sous forme de hameçonnages, réseaux zombies, fraudes financières et bancaires, et de donner des conseils de base en matière d'authentification et de protection des données. L'Agence devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finaux à la sécurité des appareils.

(29) Afin de soutenir les entreprises actives dans le secteur de la cybersécurité, ainsi que les utilisateurs qui recourent aux solutions de cybersécurité, l'Agence devrait mettre sur pied et gérer un «observatoire du marché» en procédant à des analyses régulières des principales tendances observées sur le marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, et en diffusant ses observations.

(30) Pour réaliser pleinement ses objectifs, l'Agence devrait se concerter avec les institutions, organes et organismes compétents, notamment la CERT-UE, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, l'Agence européenne de défense (EDA), l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), l'Agence européenne de la sécurité aérienne (AESA) et toute autre agence de l'UE jouant un rôle en matière de cybersécurité. Elle devrait aussi coopérer avec les autorités chargées de la protection des données en vue de procéder à des échanges de savoir-faire et de bonnes pratiques et de leur fournir des conseils sur les aspects liés à la cybersécurité susceptibles d'avoir une incidence sur leurs activités. Les représentants des autorités répressives et des autorités chargées de la protection des données aux échelons national et de l'Union devraient pouvoir être représentés au sein du groupe permanent des parties prenantes de l'Agence. Dans ses relations avec les organismes chargés de l'application de la loi concernant les questions de sécurité des réseaux et de l'information susceptibles d'avoir une incidence sur leurs activités, l'Agence devrait utiliser les canaux d'information existants et les réseaux établis.

(31) L'Agence, en tant que membre du réseau des CSIRT chargé en outre d'en assurer le secrétariat, devrait soutenir les CSIRT des États membres et la CERT-UE dans leur coopération opérationnelle ainsi que dans toutes les tâches pertinentes du réseau des CSIRT, telles que définies par la directive SRI. En outre, l'Agence devrait promouvoir

et soutenir la coopération entre les CSIRT concernés en cas d'incidents, d'attaques ou de perturbations sur les réseaux ou infrastructures dont les CSIRT assurent la gestion ou la protection et impliquant, ou susceptibles d'impliquer, au moins deux CERT, tout en tenant dûment compte des procédures opératoires standard du réseau des CSIRT.

(32) Afin que l'Union soit mieux préparée pour réagir aux incidents de cybersécurité, l'Agence devrait organiser des exercices annuels de cybersécurité au niveau de l'Union et aider les États membres et les institutions, organes et organismes de l'UE à organiser des exercices s'ils en font la demande.

(33) L'Agence devrait continuer à développer et maintenir son expertise en matière de certification de cybersécurité en vue de soutenir la politique de l'Union dans ce domaine. L'Agence devrait promouvoir le recours à la certification de cybersécurité dans l'Union, notamment en contribuant à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de rehausser la confiance dans le marché intérieur numérique.

(34) Des politiques de cybersécurité efficaces devraient reposer sur des méthodes d'évaluation des risques bien élaborées, dans le secteur public comme dans le secteur privé. Les méthodes d'évaluation des risques sont utilisées à différents niveaux et il n'existe pas de pratiques communes en ce qui concerne leur application efficace. La promotion et le développement des meilleures pratiques en matière d'évaluation des risques et de solutions interopérables de gestion des risques dans les organisations des secteurs public et privé relèveront le niveau de cybersécurité dans l'Union. À cette fin, l'Agence devrait favoriser la coopération entre parties prenantes au niveau de l'Union, en contribuant à leurs efforts concernant l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité mesurable des produits, systèmes, réseaux et services électroniques, lesquels, conjointement avec les logiciels, constituent les réseaux et systèmes d'information.

(35) L'Agence devrait encourager les États membres et les fournisseurs de services à renforcer leurs normes de sécurité générales, de manière que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité. En particulier, les fournisseurs de services et les fabricants de produits devraient retirer ou recycler les produits et services qui ne satisfont pas aux normes de cybersécurité. En coopération avec les autorités compétentes, l'ENISA peut diffuser des informations sur le niveau de cybersécurité des produits et services offerts sur le marché intérieur, et émettre des alertes visant des fournisseurs et des fabricants et les contraignant à améliorer la sécurité de leurs produits et services, y compris leur cybersécurité.

(36) L'Agence devrait prendre pleinement en compte les activités en cours en matière de recherche, de développement et d'évaluation technologique, et plus particulièrement celles menées dans le cadre des différentes initiatives de recherche de l'Union, pour fournir des conseils aux institutions, organes et organismes de l'Union et, le cas échéant, à leur demande, aux États membres sur les besoins en matière de recherche dans le domaine de la sécurité des réseaux et de l'information, et en particulier de la cybersécurité.

(37) Les problèmes de cybersécurité sont des enjeux mondiaux. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de sécurité, y compris en définissant des normes de comportement communes, et le partage des informations, en encourageant une collaboration internationale plus prompte en

réponse aux problèmes de sécurité des réseaux et de l'information ainsi qu'une approche globale commune de ces problèmes. À cette fin, l'Agence devrait aider l'Union à poursuivre son engagement et sa coopération avec les pays tiers et les organisations internationales en mettant, le cas échéant, les compétences et l'analyse nécessaires au service des institutions, organes et organismes de l'Union concernés.

(38) L'Agence devrait être en mesure de réagir aux demandes de conseil et d'assistance ad hoc qui sont formulées par les États membres et les institutions, organes et organismes de l'UE et qui relèvent des objectifs de l'Agence.

(39) Il convient de mettre en œuvre certains principes en ce qui concerne la gouvernance de l'Agence afin de se conformer à la déclaration conjointe et à l'approche commune adoptées par le groupe de travail interinstitutionnel sur les agences décentralisées de l'Union en juillet 2012, le but de cette déclaration et de cette approche étant de rationaliser les activités des agences et d'améliorer leur efficacité. La déclaration conjointe et l'approche commune devraient également se refléter, le cas échéant, dans les programmes de travail, les évaluations, ainsi que les pratiques en matière d'établissement des rapports et les pratiques administratives de l'Agence.

(40) Le conseil d'administration, composé de représentants des États membres et de la Commission, devrait fixer l'orientation générale du fonctionnement de l'Agence et veiller à ce qu'elle exécute ses missions conformément au présent règlement. Le conseil d'administration devrait être doté des pouvoirs nécessaires pour établir le budget, vérifier son exécution, adopter les règles financières appropriées, instaurer des procédures de travail transparentes pour la prise de décisions par l'Agence, adopter le document unique de programmation de l'Agence, adopter son propre règlement intérieur, nommer le directeur exécutif et statuer sur la prolongation du mandat du directeur exécutif et sur l'expiration dudit mandat.

(41) Pour assurer le fonctionnement approprié et efficace de l'Agence, la Commission et les États membres devraient veiller à ce que les personnes désignées au conseil d'administration soient dotées de compétences professionnelles et d'une expérience appropriées dans des domaines opérationnels. La Commission et les États membres devraient s'efforcer de limiter le roulement de leurs représentants respectifs au sein du conseil d'administration, afin de garantir la continuité des travaux de ce dernier.

(42) Le bon fonctionnement de l'Agence exige que le directeur exécutif de celle-ci soit nommé sur la base de son mérite et de ses capacités attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes en matière de cybersécurité, et qu'il exerce ses fonctions en toute indépendance. Le directeur exécutif devrait élaborer une proposition de programme de travail pour l'Agence, après consultation de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne exécution de ce programme de travail. Le directeur exécutif devrait préparer un rapport annuel à soumettre au conseil d'administration, établir un projet d'état prévisionnel des recettes et des dépenses de l'Agence et exécuter le budget. Le directeur exécutif devrait en outre avoir la possibilité de créer des groupes de travail ad hoc pour traiter de questions spécifiques, en particulier de nature scientifique, technique, juridique ou socio-économique. Le directeur exécutif devrait veiller à ce que les membres des groupes de travail ad hoc soient sélectionnés aux niveaux d'expertise les plus élevés, compte dûment tenu de la nécessité d'assurer une représentation équilibrée, en fonction des questions spécifiques concernées, des administrations publiques des États membres, des institutions de

l'Union et du secteur privé, y compris des entreprises, des utilisateurs et des experts universitaires en matière de sécurité des réseaux et de l'information.

(43) Le conseil exécutif devrait contribuer au fonctionnement efficace du conseil d'administration. Dans le cadre de ses travaux préparatoires liés aux décisions du conseil d'administration, il devrait examiner de manière approfondie les informations pertinentes, étudier les options disponibles et proposer des conseils et des solutions.

(44) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe permanent des parties prenantes pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties prenantes. Le groupe permanent des parties prenantes, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et à les porter à l'attention de l'Agence. La composition du groupe permanent des parties prenantes et les tâches assignées à ce groupe, qui doit être consulté en particulier sur le projet de programme de travail, devraient assurer une représentation suffisante des parties prenantes dans le travail de l'Agence.

(45) L'Agence devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. L'Agence devrait aussi appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil[34]. Le traitement des données à caractère personnel devrait être régi par le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[35]. L'Agence devrait respecter les dispositions applicables aux institutions de l'Union et la législation nationale concernant le traitement des informations, notamment les informations non classifiées sensibles et les informations classifiées de l'UE.

(46) Pour garantir l'autonomie et l'indépendance complètes de l'Agence et lui permettre d'effectuer des missions nouvelles et supplémentaires, y compris des missions urgentes imprévues, il conviendrait de la doter d'un budget suffisant et autonome dont l'essentiel des recettes provienne d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'Agence. La plus grande partie des effectifs de l'Agence devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'Agence. L'État membre d'accueil ou tout autre État membre devrait être autorisé à apporter des contributions volontaires aux recettes de l'Agence. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'Agence afin de garantir la transparence et la responsabilité.

(47) L'évaluation de la conformité est le processus destiné à établir si les exigences spécifiées relatives à un produit, à un processus, à un service, à un système, à une personne ou à un organisme ont été respectées. Aux fins du présent règlement, il y a lieu de considérer la certification comme un type d'évaluation de la conformité portant sur les caractéristiques de cybersécurité d'un produit, processus, service, système, ou

---

34 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).

35 JO L 8 du 12.1.2001, p. 1.

d'une combinaison de ceux-ci («produits et services TIC») effectuée par un tiers indépendant, distinct du fabricant du produit ou du fournisseur du service. En soi, la certification ne peut garantir que les produits et services TIC certifiés sont fiables du point de vue de la cybersécurité. Il s'agit plutôt d'une procédure et d'une méthodologie technique visant à attester que des produits et services TIC ont été soumis à des essais et qu'ils sont conformes à certaines exigences de cybersécurité définies par ailleurs, par exemple dans des normes techniques.

(48) La certification de cybersécurité est importante pour accroître la sécurité des produits et services et renforcer la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'internet des objets, ne peuvent prospérer que si le grand public est convaincu que ces produits et services offrent un certain niveau d'assurance de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels ou les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive SRI sont également des secteurs où la certification de cybersécurité joue un rôle critique.

(49) Dans la communication de 2016 intitulée «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et la cybersécurité», la Commission a souligné le besoin de produits et de solutions de très bonne qualité, abordables et interopérables en matière de cybersécurité. L'offre de produits et services TIC au sein du marché unique reste très dispersée sur le plan géographique. Cela est dû au fait que le secteur de la cybersécurité en Europe s'est développé principalement en fonction de la demande des pouvoirs publics nationaux. Le manque de solutions interopérables (normes techniques), de pratiques et de mécanismes de certification à l'échelle de l'UE est l'une des autres lacunes affectant le marché unique dans le domaine de la cybersécurité. Il en résulte, d'une part, qu'il est difficile pour les entreprises européennes d'être concurrentielles aux niveaux national, européen et mondial, et, d'autre part, que le choix des technologies viables et utilisables en matière de cybersécurité qui s'offre aux particuliers et aux entreprises est restreint. Dans le même ordre d'idées, dans son examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique, la Commission a insisté sur le besoin de produits et systèmes connectés qui soient sûrs, et a indiqué que la création d'un cadre européen de la sécurité des TIC fixant des règles sur les modalités d'organisation de la certification de sécurité des TIC dans l'UE pourrait à la fois préserver la confiance dans l'internet et lutter contre la fragmentation du marché de la cybersécurité.

(50) Actuellement, la certification de cybersécurité des produits et services TIC n'est utilisée que de façon limitée. Lorsqu'elle existe, elle intervient généralement au niveau des États membres ou dans le cadre de systèmes pilotés par l'industrie. Dans ce contexte, un certificat délivré par une autorité nationale de cybersécurité n'est pas, en principe, reconnu par d'autres États membres. Il arrive donc que les entreprises doivent certifier leurs produits et services dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passation de marchés. En outre, alors que de nouveaux systèmes voient le jour, il ne semble pas exister d'approche cohérente et globale des questions de cybersécurité transversales, par exemple dans le domaine de l'internet des objets. Les systèmes existants présentent des lacunes importantes et des différences en termes de couverture des produits, de niveau d'assurance, de critères de fond et d'utilisation effective.

(51) Des efforts ont été réalisés dans le passé pour parvenir à une reconnaissance mutuelle des certificats en Europe, mais ils n'ont que partiellement abouti. L'exemple le plus marquant à cet égard est l'accord de reconnaissance mutuelle (ARM) du SOG-IS (groupe de hauts fonctionnaires pour la sécurité des systèmes d'information). Même s'il est le modèle le plus remarquable en ce qui concerne la coopération et la reconnaissance mutuelle en matière de certification de sécurité, l'ARM du SOG-IS présente certaines faiblesses importantes liées à ses coûts élevés et à son champ d'application limité. Jusqu'à présent, seuls quelques profils de protection relatifs à des produits numériques ont été élaborés, par exemple pour la signature numérique, les tachygraphes numériques et les cartes à puce. Qui plus est, le SOG-IS ne réunit qu'une partie des États membres de l'Union. De ce fait, son ARM n'a eu qu'une efficacité limitée dans la perspective du marché intérieur.

(52) Compte tenu de ce qui précède, il est nécessaire d'établir un cadre européen de certification de cybersécurité définissant les principales exigences horizontales pour les systèmes de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats applicables aux produits et services TIC. Le cadre européen devrait poursuivre un double objectif. D'une part, il devrait contribuer à rehausser la confiance dans les produits et services TIC qui ont été certifiés conformément à de tels systèmes. D'autre part, il devrait éviter la multiplication de certifications de cybersécurité nationales contradictoires ou faisant double emploi, ce qui réduirait les coûts à charge des entreprises opérant dans le marché unique numérique. Les systèmes devraient être non discriminatoires et fondés sur des normes internationales et/ou européennes, sauf si ces normes sont inefficaces ou inappropriées pour remplir les objectifs légitimes de l'UE à cet égard.

(53) La Commission devrait être habilitée à adopter des systèmes européens de certification de cybersécurité concernant des groupes spécifiques de produits et services TIC. Ces systèmes devraient être mis en œuvre et contrôlés par des autorités nationales de contrôle de la certification, et les certificats délivrés au titre de ces systèmes devraient être valables et reconnus sur tout le territoire de l'Union. Les systèmes de certification gérés par l'industrie ou d'autres organismes privés devraient être exclus du champ d'application du présent règlement. Toutefois, les organismes qui gèrent un système de ce type peuvent proposer à la Commission de le prendre pour base en vue de l'approuver en tant que système européen.

(54) Les dispositions du présent règlement devraient être sans préjudice de la législation de l'Union prévoyant des règles spécifiques concernant la certification des produits et services TIC. En particulier, le règlement général sur la protection des données (RGPD) contient des dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données afin de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Ces mécanismes de certification et ces labels et marques en matière de protection des données devraient permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question. Le présent règlement est sans préjudice de la certification des opérations de traitement des données au titre du RGPD, y compris lorsque ces opérations sont intégrées dans des produits et services.

(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits et services TIC certifiés selon un tel système sont conformes aux exigences spécifiées. Ces exigences concernent l'aptitude à résister, à un niveau d'assurance donné, aux actions qui visent à compromettre la disponibilité,

l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises ou traitées, ou les fonctions connexes des produits, processus, services et systèmes au sens du présent règlement, ou les services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail dans le présent règlement les exigences de cybersécurité se rapportant à tous les produits et services TIC. Les produits et services TIC et les besoins de cybersécurité correspondants sont si diversifiés qu'il est très difficile d'établir des exigences de cybersécurité d'application universelle. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, complétée par une série d'objectifs spécifiques en matière de cybersécurité qui devraient être pris en compte lors de la conception de systèmes européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs seront atteints pour des produits et services TIC spécifiques devraient ensuite être précisées en détail au niveau des différents systèmes de certification adoptés par la Commission, par exemple, en faisant référence à des normes ou à des spécifications techniques.

(56) La Commission devrait être habilitée à demander à l'ENISA de préparer des systèmes candidats pour des produits ou services TIC spécifiques. Sur la base du système candidat que propose l'ENISA, la Commission devrait alors être habilitée à adopter le système européen de certification de cybersécurité par voie d'actes d'exécution. Compte tenu de la finalité générale du présent règlement et des objectifs de sécurité qui y sont définis, tout système européen de certification de cybersécurité adopté par la Commission devrait préciser un ensemble minimal d'éléments relatifs à l'objet, au champ d'application et au fonctionnement du système considéré. Ces éléments devraient comprendre notamment le champ d'application et l'objet de la certification de cybersécurité, notamment l'indication des catégories de produits et services TIC couverts, la description détaillée des exigences de cybersécurité (par exemple par référence à des normes ou spécifications techniques), les critères et méthodes d'évaluation spécifiques, ainsi que le niveau d'assurance visé, c.-à-d. élémentaire, substantiel ou supérieur.

(57) Le recours à la certification européenne de cybersécurité devrait rester volontaire, sauf disposition contraire dans la législation de l'Union ou la législation nationale. Toutefois, en vue de réaliser les objectifs du présent règlement et d'éviter la fragmentation du marché intérieur, les systèmes ou procédures nationaux de certification de cybersécurité applicables aux produits et services TIC couverts par un système européen de certification de cybersécurité devraient cesser de produire des effets à compter de la date arrêtée par la Commission par voie d'acte d'exécution. De plus, les États membres devraient s'abstenir d'instaurer de nouveaux systèmes de certification nationaux portant sur la cybersécurité de produits et services TIC déjà couverts par un système européen de certification de cybersécurité existant.

(58) Une fois un système européen de certification de cybersécurité adopté, les fabricants de produits TIC ou les fournisseurs de services TIC devraient être en mesure de soumettre une demande de certification de leurs produits ou services à l'organisme d'évaluation de la conformité de leur choix. Les organismes d'évaluation de la conformité devraient être agréés par un organisme d'accréditation s'ils satisfont à certaines exigences précises énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et pouvoir être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle devrait être révoquée si les conditions de l'accréditation

ne sont pas ou plus remplies ou si des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.

(59) Il est nécessaire d'exiger que tous les États membres désignent une autorité de contrôle de la certification de cybersécurité afin de contrôler que les organismes d'évaluation de la conformité et les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire respectent les exigences du présent règlement et des systèmes de certification de cybersécurité pertinents. Les autorités nationales de contrôle de la certification devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, examiner l'objet de la réclamation dans la mesure nécessaire et informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable. De plus, elles devraient coopérer avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en s'échangeant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques.

(60) Afin d'assurer l'application cohérente du cadre européen de certification de cybersécurité, un Groupe européen de certification de cybersécurité (ci-après le «groupe»), constitué des autorités nationales de contrôle de la certification, devrait être mis en place. Les tâches principales du groupe devraient consister à conseiller et assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes du cadre européen de certification de cybersécurité; à assister l'Agence et à coopérer étroitement avec elle dans la préparation des systèmes de certification de cybersécurité candidats; à recommander à la Commission qu'elle demande à l'Agence d'élaborer un système européen de certification de cybersécurité candidat; et à adopter des avis adressés à la Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants.

(61) Dans une optique de sensibilisation et pour faciliter l'acceptation de futurs systèmes européens de certification de cybersécurité, la Commission européenne peut publier des lignes directrices générales ou sectorielles dans le domaine de la cybersécurité, par exemple sur les bonnes pratiques ou les comportements responsables en matière de cybersécurité, en soulignant les effets positifs de l'utilisation de produits et services TIC certifiés.

(62) Le soutien apporté par l'Agence à la certification de cybersécurité devrait également inclure les contacts avec le Comité de sécurité du Conseil et l'organe national compétent, en ce qui concerne l'approbation des produits cryptographiques à utiliser dans les réseaux classifiés.

(63) Afin de préciser les critères d'accréditation des organismes d'évaluation de la conformité, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Il convient que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Ces consultations devraient être menées conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts avoir systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(64) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission lorsque le présent règlement le prévoit. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011.

(65) La procédure d'examen devrait être utilisée pour l'adoption d'actes d'exécution concernant les systèmes européens de certification de cybersécurité applicables à des produits et services TIC; concernant les modalités d'exécution des enquêtes menées par l'Agence; et concernant les circonstances, les formats et les procédures de notification à la Commission, par les autorités nationales de contrôle de la certification, des organismes d'évaluation de la conformité accrédités.

(66) Le fonctionnement de l'Agence devrait faire l'objet d'une évaluation indépendante. Cette évaluation devrait s'intéresser à la réalisation des objectifs, aux méthodes de travail et à la pertinence des missions de l'Agence. L'évaluation devrait également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité.

(67) Il y a lieu d'abroger le règlement (UE) n° 526/2013.

(68) Étant donné que les objectifs du présent règlement ne peuvent pas être réalisés de manière suffisante par les États membres, mais peuvent l'être mieux 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 ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet et champ d'application

En vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, le présent règlement:

(a) fixe les objectifs, les missions et les aspects organisationnels de l'ENISA, Agence de l'Union européenne pour la cybersécurité, ci-après dénommée l'«Agence»; et

(b) instaure un cadre pour la mise en place de systèmes européens de certification de cybersécurité dans le but de garantir un niveau suffisant de cybersécurité des produits et services TIC dans l'Union. Ce cadre s'applique sans préjudice des dispositions spécifiques d'autres actes de l'Union en matière de certification volontaire ou obligatoire.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

(1) «cybersécurité», toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les personnes exposées contre les cybermenaces;

(2) «réseau et système d'information», un réseau et système d'information au sens de l'article 4, point 1), de la directive (UE) 2016/1148;

(3) «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information», un cadre au sens de l'article 4, point 3), de la directive (UE) 2016/1148;

(4) «opérateur de services essentiels», une entité publique ou privée telle que définie à l'article 4, point 4), de la directive (UE) 2016/1148;

(5) «fournisseur de service numérique», toute personne morale qui fournit un service numérique, tel que défini à l'article 4, point 6), de la directive (UE) 2016/1148;

(6) «incident», tout événement tel que défini à l'article 4, point 7), de la directive (UE) 2016/1148;

(7) «gestion d'incident», toute procédure telle que définie à l'article 4, point 8), de la directive (UE) 2016/1148;

(8) «cybermenace», toute circonstance ou tout événement potentiels susceptibles de porter atteinte aux réseaux et systèmes d'information, à leurs utilisateurs et aux personnes exposées;

(9) «système européen de certification de cybersécurité», l'ensemble complet de règles, d'exigences techniques, de normes et de procédures définies à l'échelon de l'Union, qui s'appliquent à la certification des produits et services des technologies de l'information et des communications (TIC) relevant de ce système spécifique;

(10) «certificat européen de cybersécurité», un document délivré par un organisme d'évaluation de la conformité attestant qu'un produit ou service TIC donné satisfait aux exigences spécifiques énoncées dans un système européen de certification de cybersécurité;

(11) «produit ou service TIC», tout élément ou groupe d'éléments appartenant aux réseaux et systèmes d'information;

(12) «accréditation», l'accréditation telle que définie à l'article 2, point 10), du règlement (CE) n° 765/2008;

(13) «organisme national d'accréditation», un organisme national d'accréditation tel que défini à l'article 2, point 11), du règlement (CE) n° 765/2008;

(14) «évaluation de la conformité», l'évaluation de la conformité telle que définie à l'article 2, point 12), du règlement (CE) n° 765/2008;

(15) «organisme d'évaluation de la conformité», un organisme d'évaluation de la conformité tel que défini à l'article 2, point 13), du règlement (CE) n° 765/2008;

(16) «norme», une norme telle que définie à l'article 2, point 1), du règlement (UE) n° 1025/2012.

TITRE II
ENISA, l'Agence de l'Union européenne pour la cybersécurité

CHAPITRE I
MANDAT, OBJECTIFS ET MISSIONS

Article 3
Mandat

1. L'Agence exécute les missions qui lui sont assignées par le présent règlement dans le but de contribuer à assurer un niveau élevé de cybersécurité dans l'Union.

2. L'Agence exécute les missions qui lui sont confiées par des actes de l'Union établissant des mesures destinées à rapprocher les dispositions législatives, réglementaires et administratives des États membres relatives à la cybersécurité.

3. Les objectifs et les missions de l'Agence s'entendent sans préjudice des compétences des États membres en ce qui concerne la cybersécurité et, en tout état de cause, sans préjudice des activités relatives à la sécurité publique, à la défense et à la sûreté de l'État, et des activités de l'État dans les domaines du droit pénal.

Article 4
Objectifs

1. L'Agence est un centre d'expertise en matière de cybersécurité du fait de son indépendance, de la qualité scientifique et technique des conseils et de l'assistance qu'elle dispense et des informations qu'elle fournit, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à exécuter ses missions.

2. L'Agence assiste les institutions, organes et organismes de l'Union, ainsi que les États membres, dans l'élaboration et la mise en œuvre de politiques liées à la cybersécurité.

3. L'Agence soutient le renforcement des capacités et contribue à l'état de préparation au sein de l'Union en aidant l'Union, les États membres et les parties prenantes des secteurs public et privé à accroître la protection de leurs réseaux et systèmes d'information, à développer des aptitudes et des compétences dans le domaine de la cybersécurité et à parvenir à la cyberrésilience.

4. L'Agence promeut la coopération 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, y compris le secteur privé, sur les questions liées à la cybersécurité.

5. L'Agence accroît les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de compléter l'action des États membres en matière de prévention des cybermenaces et de réaction à celles-ci, notamment en cas d'incidents transfrontières.

6. L'Agence promeut le recours à la certification, notamment en contribuant à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau

de l'Union, conformément au titre III du présent règlement, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de rehausser la confiance dans le marché intérieur numérique.

7. L'Agence promeut un niveau élevé de sensibilisation des particuliers et des entreprises aux questions liées à la cybersécurité.

Article 5

Missions liées à l'élaboration et à la mise en œuvre de la politique et du droit de l'Union

L'Agence contribue à l'élaboration et à la mise en œuvre de la politique et du droit de l'Union:

1. en apportant son concours et ses conseils, en particulier sous la forme d'avis indépendants et de travaux préparatoires, concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, ainsi que les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité;
2. en aidant les États membres à mettre en œuvre de manière cohérente la politique et le droit de l'Union en matière de cybersécurité, notamment en ce qui concerne la directive (UE) 2016/1148, y compris au moyen d'avis, de lignes directrices, de conseils et de bonnes pratiques sur des thèmes tels que la gestion des risques, le signalement des incidents et le partage d'informations, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes à cet égard;
3. en contribuant, par son expertise et son concours, aux travaux du groupe de coopération institué en application de l'article 11 de la directive (UE) 2016/1148;
4. en soutenant:
    (1) l'élaboration et la mise en œuvre de la politique de l'Union dans le domaine de l'identification électronique et des services de confiance, en particulier en fournissant des conseils et des lignes directrices techniques, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;
    (2) l'amélioration du niveau de sécurité des communications électroniques, y compris en fournissant une expertise et des conseils, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;
5. en facilitant le réexamen périodique des activités liées aux politiques de l'Union, au moyen d'un rapport annuel sur l'avancement de la mise en œuvre du cadre juridique applicable en ce qui concerne:
    (a) les notifications d'incidents transmises par le point de contact unique de chaque État membre au groupe de coopération conformément à l'article 10, paragraphe 3, de la directive (UE) 2016/1148;
    (b) les notifications d'atteinte à la sécurité et de perte d'intégrité reçues des prestataires de services de confiance et transmises à l'Agence par les organes de contrôle, conformément à l'article 19, paragraphe 3, du règlement (UE) n° 910/2014;

(c) les notifications d'atteinte à la sécurité reçues des entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public et transmises à l'Agence par les autorités compétentes, conformément à l'article 40, de la [directive établissant le code des communications électroniques européen].

Article 6

Missions liées au renforcement des capacités

1. L'Agence assiste:

(a) les États membres dans leurs efforts pour améliorer la prévention, la détection et l'analyse des problèmes et incidents de cybersécurité, et la capacité d'y réagir, en leur fournissant les connaissances et l'expertise nécessaires;

(b) les institutions, organes et organismes de l'Union dans leurs efforts pour améliorer la prévention, la détection et l'analyse des problèmes et incidents de cybersécurité, et la capacité d'y réagir, en apportant un soutien adapté à l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union européenne (CERT-UE);

(c) les États membres, à leur demande, dans la mise en place de centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux, conformément à l'article 9, paragraphe 5, de la directive (UE) 2016/1148;

(d) les États membres, à leur demande, dans l'élaboration de leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/1148; en outre, l'Agence favorise la diffusion et suit l'avancement de la mise en œuvre de ces stratégies dans l'Union afin de promouvoir les bonnes pratiques;

(e) les institutions de l'Union dans l'élaboration et la révision des stratégies de l'Union en matière de cybersécurité, la promotion de leur diffusion et le suivi de l'avancement de leur mise en œuvre;

(f) les CERT nationales et de l'UE dans le relèvement du niveau de leurs capacités, y compris en favorisant le dialogue et l'échange d'informations, pour faire en sorte que, en ce qui concerne l'état de la technologie, chaque CERT satisfasse à un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;

(g) les États membres en organisant chaque année les exercices de cybersécurité à grande échelle au niveau de l'Union visés à l'article 7, paragraphe 6, et en formulant des recommandations en vue d'actions sur la base de l'évaluation de ces exercices et des enseignements qui en ont été tirés;

(h) les organismes publics concernés en proposant des formations sur la cybersécurité, le cas échéant en coopération avec des parties prenantes;

(i) le groupe de coopération en échangeant des bonnes pratiques, notamment en ce qui concerne l'identification, par les États membres, des opérateurs de services essentiels, y compris au regard des dépendances transfrontalières, en matière de risques et d'incidents, conformément à l'article 11, paragraphe 3, point l), de la directive (UE) 2016/1148.

2. L'Agence facilite la mise en place de centres d'échange et d'analyse d'informations (ISAC) sectoriels et leur apporte un soutien continu, en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant de bonnes pratiques et des orientations sur les outils disponibles, les procédures et sur la manière d'aborder les questions réglementaires relatives au partage d'informations.

Article 7

Missions liées à la coopération opérationnelle au niveau de l'Union

1. L'Agence apporte son soutien à la coopération opérationnelle entre les organismes publics compétents, et entre les parties prenantes.

2. L'Agence coopère sur le plan opérationnel et crée des synergies avec les institutions, organes et organismes de l'Union, y compris la CERT-UE, les services traitant de la cybercriminalité et les autorités de contrôle responsables de la protection de la vie privée et des données à caractère personnel, en vue de traiter des questions d'intérêt commun, y compris:

   (a) en échangeant savoir-faire et bonnes pratiques;

   (b) en fournissant des conseils et des lignes directrices sur des questions pertinentes liées à la cybersécurité;

   (c) en établissant, après consultation de la Commission, des arrangements pratiques pour l'exécution de missions spécifiques.

3. L'Agence assure le secrétariat du réseau des CSIRT, conformément à l'article 12, paragraphe 2, de la directive (UE) 2016/1148, et facilite activement le partage d'informations et la coopération entre les membres du réseau.

4. L'Agence contribue à la coopération sur le plan opérationnel au sein du réseau des CSIRT par le soutien qu'elle apporte aux États membres:

   (a) en prodiguant des conseils sur la façon d'améliorer leur capacité à prévenir et détecter les incidents, et à y réagir;

   (b) en fournissant, à leur demande, une assistance technique en cas d'incidents ayant un impact important ou significatif;

   (c) en analysant les vulnérabilités, les artéfacts et les incidents.

Dans l'accomplissement de ces missions, l'Agence pratique avec la CERT-UE une coopération structurée afin de tirer avantage des synergies, notamment en ce qui concerne les aspects opérationnels.

5. À la demande d'au moins deux États membres concernés et dans le seul but de fournir des conseils sur la prévention des incidents, l'Agence apporte son concours ou procède elle-même à une enquête technique ex post à la suite de la notification, par les entreprises exposées, d'incidents ayant un impact important ou significatif conformément à la directive (UE) 2016/1148. L'Agence procède également à une enquête de ce type à la demande dûment justifiée de la Commission, en accord avec les États membres concernés, lorsque les incidents atteignent plus de deux États membres.

La portée de l'enquête et la procédure à suivre pour la conduite de cette enquête sont définies d'un commun accord par les États membres concernés et l'Agence, et ne préjugent pas de l'issue de toute enquête pénale en cours concernant le même incident. L'enquête se conclut par un rapport technique final élaboré par l'Agence, notamment sur la base des informations et des commentaires fournis par les États membres et les entreprises concernés, et approuvé par les États membres concernés. Une synthèse du rapport mettant en évidence les recommandations formulées en vue de la prévention des incidents est communiquée au réseau des CSIRT.

6. L'Agence organise des exercices de cybersécurité annuels à l'échelle de l'Union, et aide, à leur demande, les États membres et les institutions, organes et organismes de l'UE à organiser de tels exercices. Les exercices annuels à l'échelle de l'Union comportent des aspects techniques, opérationnels et stratégiques, et contribuent à la préparation de la réaction concertée à l'échelle de l'Union en cas d'incidents transfrontières de cybersécurité majeurs. En outre, l'Agence contribue à des exercices de cybersécurité sectoriels, qu'elle aide à organiser le cas échéant, en collaboration avec les ISAC compétents, et permet à des ISAC de participer également à des exercices de cybersécurité au niveau de l'Union.

7. L'Agence prépare, à intervalle régulier, un rapport de situation technique sur les incidents et menaces de cybersécurité dans l'UE, sur la base d'informations provenant de sources ouvertes, de ses propres analyses et des rapports que lui communiquent notamment: les CSIRT des États membres (sur une base volontaire) ou les points de contact uniques au titre de la directive SRI (conformément à l'article 14, paragraphe 5, de la directive SRI), le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE.

8. L'Agence contribue 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:

   (a) agrégeant des rapports provenant de sources nationales en vue de contribuer à former une appréciation commune de la situation;

   (b) assurant une circulation efficace de l'information et en proposant des mécanismes de remontée des décisions entre le réseau des CSIRT et les décideurs techniques et politiques au niveau de l'Union;

   (c) soutenant la gestion technique des incidents ou des crises, y compris en facilitant le partage de solutions techniques entre les États membres;

   (d) encourageant la communication publique autour des incidents ou des crises;

   (e) mettant à l'épreuve les plans de coopération destinés à réagir à ces incidents ou crises.

Article 8

Missions liées au marché, à la certification de cybersécurité et à la normalisation

L'Agence:

(a) soutient et promeut l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits et services TIC, telle que décrite au titre III du présent règlement, en:

(1) préparant des systèmes européens de certification de cybersécurité candidats pour des produits et services TIC, conformément à l'article 44 du présent règlement;

(2) aidant la Commission à assurer le secrétariat du Groupe européen de certification de cybersécurité, conformément à l'article 53 du présent règlement;

(3) établissant et publiant des lignes directrices, ainsi qu'en mettant au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits et services TIC, en coopération avec les autorités nationales de contrôle de la certification et l'industrie;

(b) facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits et services TIC; formule, en collaboration avec les États membres, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de service numérique, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148;

(c) effectue et diffuse, à intervalle régulier, des analyses des principales tendances du marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, en vue de stimuler le marché de la cybersécurité dans l'Union.

Article 9

Missions liées à la connaissance, à l'information et à la sensibilisation

L'Agence:

(a) analyse les technologies émergentes et fournit des évaluations thématiques sur les incidences escomptées des innovations technologiques en matière de cybersécurité du point de vue sociétal, juridique, économique et réglementaire;

(b) produit des analyses stratégiques à long terme des menaces et des incidents de cybersécurité afin d'identifier les tendances émergentes et de contribuer à prévenir les problèmes liés à la cybersécurité;

(c) fournit, en coopération avec des experts des États membres, des avis, des orientations et des bonnes pratiques en matière de sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité de l'infrastructure internet et des infrastructures sur lesquelles s'appuient les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148;

(d) regroupe, organise et met à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la cybersécurité, fournies par les institutions, organes et organismes de l'Union;

(e) sensibilise le public sur les risques liés à la cybersécurité et fournit, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs;

(f) collecte et analyse des informations du domaine public sur les incidents significatifs, et rédige des rapports en vue de fournir des orientations aux entreprises et aux particuliers dans toute l'Union;

(g) organise à intervalle régulier, en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes d'information afin de relever le niveau de la cybersécurité et d'accroître sa visibilité dans l'Union.

Article 10
Missions liées à la recherche et à l'innovation

En ce qui concerne la recherche et l'innovation, l'Agence:

(a) conseille l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité, afin que des réponses efficaces puissent être apportées face aux risques et aux menaces actuels et émergents, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et afin que les technologies de prévention des risques soient utilisées d'une manière efficace;

(b) participe, lorsque la Commission lui a délégué les pouvoirs correspondants, à la phase de mise en œuvre des programmes de financement de la recherche et de l'innovation, ou est bénéficiaire de ces programmes.

Article 11
Missions liées à la coopération internationale

L'Agence contribue aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, afin de promouvoir une coopération internationale sur les problèmes de cybersécurité, en:

(a) s'impliquant, le cas échéant, en tant qu'observateur dans l'organisation d'exercices internationaux, ainsi qu'en analysant les résultats de ces exercices et en en rendant compte au conseil d'administration;

(b) facilitant, à la demande de la Commission, l'échange de bonnes pratiques entre les organisations internationales compétentes;

(c) mettant son expertise à la disposition de la Commission si elle en fait la demande.

CHAPITRE II
ORGANISATION DE L'AGENCE

Article 12
Structure

La structure administrative et de gestion de l'Agence comprend:

(a) un conseil d'administration, qui exerce les fonctions définies à l'article 14;

(b) un conseil exécutif, qui exerce les fonctions définies à l'article 18;

(c) un directeur exécutif, qui assume les responsabilités définies à l'article 19;

(d) un groupe permanent des parties prenantes, qui exerce les fonctions définies à l'article 20.

SECTION 1
CONSEIL D'ADMINISTRATION

Article 13
Composition du conseil d'administration

1. Le conseil d'administration est composé d'un représentant de chaque État membre, et de deux représentants nommés par la Commission. Tous les représentants disposent du droit de vote.

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

3. Les membres du conseil d'administration et leurs suppléants sont nommés sur la base de leurs connaissances dans le domaine de la cybersécurité, compte tenu des compétences managériales, administratives et budgétaires requises. La Commission et les États membres s'efforcent de limiter le roulement de leurs représentants au sein du conseil d'administration, 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 d'administration.

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

Article 14
Fonctions du conseil d'administration

1. Le conseil d'administration:

   (a) fixe l'orientation générale du fonctionnement de l'Agence et veille à ce que l'Agence travaille conformément aux règles et principes énoncés dans le présent règlement. Il assure aussi la cohérence des travaux de l'Agence avec les activités menées par les États membres ainsi qu'au niveau de l'Union;

   (b) adopte le projet de document unique de programmation de l'Agence visé à l'article 21, avant de le soumettre pour avis à la Commission;

   (c) adopte, en tenant compte de l'avis de la Commission, le document unique de programmation de l'Agence, à la majorité des deux tiers des membres et conformément à l'article 17;

   (d) adopte le budget annuel de l'Agence à la majorité des deux tiers des membres et exerce d'autres fonctions liées au budget de l'Agence en application du chapitre III;

   (e) évalue et adopte le rapport annuel consolidé sur les activités de l'Agence et transmet, au plus tard le 1er juillet de l'année suivante, le rapport et son évaluation au Parlement européen, au Conseil, à la Commission et à la Cour des comptes. Le rapport annuel inclut les comptes et décrit la

manière dont l'Agence atteint ses indicateurs de performance. Le rapport annuel est rendu public;

(f) adopte les règles financières applicables à l'Agence, conformément à l'article 29;

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

(h) adopte des règles en matière de prévention et de gestion des conflits d'intérêts concernant ses membres;

(i) assure le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'Office européen de lutte antifraude (OLAF) et des divers rapports d'audit et évaluations internes ou externes;

(j) adopte son règlement intérieur;

(k) conformément au paragraphe 2, exerce, à l'égard du personnel de l'Agence, les compétences qui sont dévolues, par le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, respectivement à l'autorité investie du pouvoir de nomination et à l'autorité habilitée à conclure les contrats d'engagement («compétences de l'autorité investie du pouvoir de nomination»);

(l) arrête les modalités d'application du statut et du régime applicable aux autres agents conformément à la procédure prévue à l'article 110 du statut;

(m) nomme le directeur exécutif et, le cas échéant, prolonge son mandat ou le démet de ses fonctions conformément à l'article 33 du présent règlement;

(n) nomme un comptable, qui peut être le comptable de la Commission, qui est totalement indépendant dans l'exercice de ses fonctions;

(o) prend toutes les décisions relatives à la mise en place des structures internes de l'Agence et, le cas échéant, à leur modification, en tenant compte des besoins liés à l'activité de l'Agence et en respectant le principe d'une gestion budgétaire saine;

(p) autorise la conclusion d'arrangements de travail conformément aux articles 7 et 39.

2. Le conseil d'administration adopte, conformément à la procédure prévue à l'article 110 du statut, une décision fondée sur l'article 2, paragraphe 1, du statut et sur l'article 6 du régime applicable aux autres agents, déléguant au directeur exécutif les compétences correspondantes dévolues à l'autorité investie du pouvoir de nomination et définissant les conditions dans lesquelles cette délégation de compétences peut être suspendue. Le directeur exécutif est autorisé à sous-déléguer ces compétences.

3. Lorsque des circonstances exceptionnelles l'exigent, le conseil d'administration peut, par voie de décision, suspendre temporairement la délégation au directeur exécutif des compétences dévolues à l'autorité investie du pouvoir de nomination ainsi que de celles sous-déléguées par le directeur exécutif, pour les exercer lui-même ou les

déléguer à un de ses membres ou à un membre du personnel autre que le directeur exécutif.

Article 15
Présidence du conseil d'administration

Le conseil d'administration élit, à la majorité des deux tiers des membres, son président et un vice-président parmi ses membres, pour une durée de quatre ans renouvelable une fois. Cependant, si le président ou le vice-président perd sa qualité de membre du conseil d'administration à un moment quelconque de son mandat, ledit mandat expire automatiquement à la même date. Le vice-président remplace d'office le président lorsque celui-ci n'est pas en mesure d'assumer ses fonctions.

Article 16
Réunions du conseil d'administration

1. Les réunions du conseil d'administration sont convoquées par son président.
2. Le conseil d'administration tient une réunion ordinaire au moins deux fois par an. Il tient aussi des réunions extraordinaires à l'initiative du président, à la demande de la Commission ou à la demande d'au moins un tiers de ses membres.
3. Le directeur exécutif participe sans droit de vote aux réunions du conseil d'administration.
4. Sur invitation du président, des membres du groupe permanent des parties prenantes peuvent participer sans droit de vote aux réunions du conseil d'administration.
5. Les membres du conseil d'administration et leurs suppléants peuvent, dans le respect du règlement intérieur, être assistés au cours des réunions par des conseillers ou des experts.
6. L'Agence assure le secrétariat du conseil d'administration.

Article 17
Règles de vote du conseil d'administration

1. Les décisions du conseil d'administration sont prises à la majorité de ses membres.
2. Une majorité des deux tiers de tous les membres du conseil d'administration est nécessaire pour adopter le document unique de programmation et le budget annuel, pour nommer le directeur exécutif, prolonger son mandat ou le révoquer.
3. Chaque membre dispose d'une voix. En l'absence d'un membre, son suppléant peut exercer son droit de vote.
4. Le président prend part au vote.
5. Le directeur exécutif ne prend pas part au vote.
6. Le règlement intérieur du conseil d'administration fixe les modalités détaillées du vote, notamment les conditions dans lesquelles un membre peut agir au nom d'un autre membre.

SECTION 2
CONSEIL EXÉCUTIF

Article 18
Conseil exécutif

1. Le conseil d'administration est assisté d'un conseil exécutif.

2. Le conseil exécutif:

   (a) prépare les décisions qui doivent être adoptées par le conseil d'administration;

   (b) assure, avec le conseil d'administration, le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'OLAF ainsi que des divers rapports d'audit interne ou externe et des évaluations;

   (c) sans préjudice des responsabilités du directeur exécutif définies à l'article 19, assiste et conseille celui-ci dans la mise en œuvre des décisions du conseil d'administration relatives à des questions administratives et budgétaires, conformément à l'article 19.

3. Le conseil exécutif est composé de cinq membres nommés parmi les membres du conseil d'administration, dont le président du conseil d'administration, qui peut également présider le conseil exécutif, et un des représentants de la Commission. Le directeur exécutif participe aux réunions du conseil exécutif, mais sans droit de vote.

4. La durée du mandat des membres du conseil exécutif est de quatre ans. Ce mandat est renouvelable.

5. Le conseil exécutif se réunit au moins une fois par trimestre. Le président du conseil exécutif convoque des réunions supplémentaires à la demande de ses membres.

6. Le conseil d'administration établit le règlement intérieur du conseil exécutif.

7. Lorsque l'urgence le justifie, le conseil exécutif peut prendre certaines décisions provisoires au nom du conseil d'administration, en particulier sur des questions de gestion administrative, comme la suspension de la délégation des compétences dévolues à l'autorité investie du pouvoir de nomination, et sur des questions budgétaires.

SECTION 3
DIRECTEUR EXÉCUTIF

Article 19
Responsabilités du directeur exécutif

1. L'Agence est gérée par son directeur exécutif, qui est indépendant dans l'exécution de ses tâches. Le directeur exécutif rend compte de ses activités au conseil d'administration.

2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.

3. Le directeur exécutif est chargé:

(a) d’assurer l’administration courante de l’Agence;

(b) de mettre en œuvre les décisions adoptées par le conseil d’administration;

(c) de préparer le projet de document unique de programmation et de le soumettre au conseil d’administration pour approbation, avant qu'il ne soit soumis à la Commission;

(d) de mettre en œuvre le document unique de programmation et d’en faire rapport au conseil d’administration;

(e) de préparer le rapport annuel consolidé sur les activités de l’Agence et de le présenter au conseil d’administration pour évaluation et adoption;

(f) de 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;

(g) de 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 d’administration sur les progrès accomplis;

(h) d’élaborer le projet de règles financières applicables à l’Agence;

(i) d’établir le projet d’état prévisionnel des recettes et dépenses de l’Agence et d’exécuter son budget;

(j) de protéger 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;

(k) de préparer une stratégie antifraude pour l’Agence et de la présenter au conseil d’administration pour approbation;

(l) d’établir et de maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d’assurer un dialogue régulier avec les parties prenantes concernées;

(m) d’exécuter les autres tâches qui lui sont confiées par le présent règlement.

4. En tant que de besoin, dans le cadre du mandat de l’Agence et conformément aux objectifs et aux missions de l’Agence, le directeur exécutif peut créer des groupes de travail ad hoc composés d’experts, y compris des experts des autorités compétentes des États membres. Le conseil d’administration en est préalablement informé. Les modalités concernant en particulier la composition des groupes de travail, la nomination par le directeur exécutif des experts qui les composent et le fonctionnement de ces groupes sont précisées dans les règles internes de fonctionnement de l’Agence.

5. Le directeur exécutif décide s'il est nécessaire que les membres du personnel soient situés dans un ou dans plusieurs États membres à l'effet d'exécuter les missions de l'Agence de manière efficiente et efficace. Avant d'arrêter une décision sur l'établissement d'un bureau local, le directeur exécutif doit obtenir le consentement préalable de la Commission, du conseil d'administration et du ou des États membres concernés. La décision précise la portée des activités confiées à ce bureau local de manière à éviter les coûts inutiles et les doubles emplois dans les fonctions administratives de l'Agence. L'accord de l'État ou des États membre(s) concerné(s) est obtenu, si cela est approprié ou nécessaire.

SECTION 4
GROUPE PERMANENT DES PARTIES PRENANTES

Article 20
Groupe permanent des parties prenantes

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de cybersécurité et les représentants des autorités compétentes notifiées au titre de la [directive établissant le code des communications électroniques européen], ainsi que les autorités chargées du respect de la loi et de la protection des données.

2. Les procédures applicables au groupe permanent des parties prenantes, notamment en ce qui concerne le nombre de membres, la composition du groupe, la nomination des membres par le conseil d'administration, la proposition par le directeur exécutif et le fonctionnement du groupe sont précisées dans les règles internes de fonctionnement de l'Agence et sont rendues publiques.

3. Le groupe permanent des parties prenantes est présidé par le directeur exécutif ou par toute personne qu'il désigne à cet effet au cas par cas.

4. La durée du mandat des membres du groupe permanent des parties prenantes est de deux ans et demi. Les membres du conseil d'administration ne peuvent pas être membres du groupe permanent des parties prenantes. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe permanent des parties prenantes. Des représentants d'autres organismes jugés intéressants par le directeur exécutif, qui ne sont pas membres du groupe permanent des parties prenantes, peuvent être invités à assister aux réunions du groupe permanent des parties prenantes et à prendre part à ses travaux.

5. Le groupe permanent des parties prenantes conseille l'Agence dans l'exercice de ses activités. Il conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour la communication avec les parties prenantes concernées sur toutes les questions liées au programme de travail.

SECTION 5
FONCTIONNEMENT

Article 21
Document unique de programmation

1. L'Agence exécute ses tâches conformément à un document unique de programmation qui décrit sa programmation annuelle et pluriannuelle, et qui contient l'ensemble de ses activités planifiées.

2. Le directeur exécutif établit, chaque année, un projet de document unique de programmation contenant la programmation annuelle et pluriannuelle, ainsi que les ressources humaines et financières correspondantes, conformément à l'article 32 du règlement délégué (UE) n° 1271/2013 de la Commission[36], et tenant compte des lignes directrices fixées par la Commission.

3. Le Conseil d'administration adopte, au plus tard le 30 novembre de chaque année, le document unique de programmation visé au paragraphe 1 et le transmet au Parlement européen, au Conseil et à la Commission au plus tard le 31 janvier de l'année suivante, ainsi que toute version de ce document actualisée ultérieurement.

4. Le document unique de programmation devient définitif après l'adoption définitive du budget général de l'Union et, si nécessaire, il est adapté en conséquence.

5. Le programme de travail annuel expose des objectifs détaillés et les résultats escomptés, notamment des indicateurs de performance. Il contient, en outre, une description des actions à financer et une indication des ressources financières et humaines allouées à chaque action, conformément aux principes d'établissement du budget par activités et de la gestion fondée sur les activités. Le programme de travail annuel s'inscrit dans la logique du programme de travail pluriannuel visé au paragraphe 7. Il indique clairement les tâches qui ont été ajoutées, modifiées ou supprimées par rapport à l'exercice précédent.

6. Le conseil d'administration modifie le programme de travail annuel adopté lorsqu'une nouvelle tâche est confiée à l'Agence. Toute modification substantielle du programme de travail annuel est soumise à une procédure d'adoption identique à celle applicable au programme de travail annuel initial. Le conseil d'administration peut déléguer au directeur exécutif le pouvoir d'apporter des modifications non substantielles au programme de travail annuel.

7. Le programme de travail pluriannuel expose la programmation stratégique globale comprenant les objectifs, les résultats escomptés et les indicateurs de performance. Il définit également la programmation des ressources, notamment le budget pluriannuel et les effectifs.

8. La programmation des ressources est actualisée chaque année. La programmation stratégique est actualisée en tant que de besoin, notamment pour tenir compte des résultats de l'évaluation visée à l'article 56.

---

36 Règlement délégué (UE) n° 1271/2013 de la Commission du 30 septembre 2013 portant règlement financier-cadre des organismes visés à l'article 208 du règlement (UE, Euratom) n° 966/2012 du Parlement européen et du Conseil (JO L 328 du 7.12.2013, p. 42).

Article 22

Déclaration d'intérêt

1. Les membres du conseil d'administration, le directeur exécutif et les fonctionnaires détachés par les États membres à titre temporaire font chacun une déclaration d'engagements et une déclaration indiquant l'absence ou la présence de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance. Les déclarations sont exactes et complètes, faites par écrit sur une base annuelle et actualisées si nécessaire.
2. Les membres du conseil d'administration, le directeur exécutif et les experts externes participant aux groupes de travail ad hoc déclarent chacun de manière exacte et complète, au plus tard au début de chaque réunion, les intérêts qui pourraient être considérés comme préjudiciables à leur indépendance eu égard aux points inscrits à l'ordre du jour, et s'abstiennent de prendre part aux discussions et de voter sur ces points.
3. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques concernant les règles relatives aux déclarations d'intérêt visées aux paragraphes 1 et 2.

Article 23

Transparence

1. L'Agence exerce ses activités avec un niveau élevé de transparence et conformément aux dispositions de l'article 25.
2. L'Agence 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. Elle rend également publiques les déclarations d'intérêt faites conformément à l'article 22.
3. Le conseil d'administration peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités de l'Agence.
4. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de transparence visées aux paragraphes 1 et 2.

Article 24

Confidentialité

1. Sans préjudice de l'article 25, l'Agence ne divulgue pas à des tiers les informations qu'elle traite ou qu'elle reçoit et pour lesquelles une demande motivée de traitement confidentiel, en tout ou en partie, a été faite.
2. Les membres du conseil d'administration, le directeur exécutif, les membres du groupe permanent des parties prenantes, les experts externes participant aux groupes de travail ad hoc et les membres du personnel de l'Agence, y compris les fonctionnaires détachés par les États membres à titre temporaire, respectent l'obligation de confidentialité visée à l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions.

3. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de confidentialité visées aux paragraphes 1 et 2.

4. Si l'exécution des missions de l'Agence l'exige, le conseil d'administration décide d'autoriser l'Agence à traiter des informations classifiées. Dans ce cas, le conseil d'administration, en accord avec les services de la Commission, adopte des règles internes de fonctionnement respectant les principes de sécurité énoncés dans les décisions (UE, Euratom) 2015/443[37] et 2015/444[38]. Ces règles comprennent des dispositions relatives à l'échange, au traitement et à l'archivage des informations classifiées.

Article 25
Accès aux documents

1. Le règlement (CE) n° 1049/2001 s'applique aux documents détenus par l'Agence.

2. Le conseil d'administration adopte des dispositions pour la mise en œuvre du règlement (CE) n° 1049/2001 dans les six mois suivant la création de l'Agence.

3. Les décisions prises par l'Agence en application de l'article 8 du règlement (CE) n° 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.

CHAPITRE III
ÉTABLISSEMENT ET STRUCTURE DU BUDGET

Article 26
Établissement du budget

1. Chaque année, le directeur exécutif établit un projet d'état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant et le transmet au conseil d'administration avec un projet de tableau des effectifs. Les recettes et les dépenses sont équilibrées.

2. Le conseil d'administration 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 de l'Agence pour l'exercice budgétaire suivant.

3. Le conseil d'administration transmet, 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, à la Commission et aux pays tiers avec lesquels l'Union européenne a conclu des accords conformément à l'article 39.

---

37 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).

38 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).

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 à l'Agence.

6. Le Parlement européen et le Conseil adoptent le tableau des effectifs de l'Agence.

7. Le conseil d'administration adopte le budget de l'Agence en même temps que le document unique de programmation. Ce budget devient définitif après l'adoption définitive du budget général de l'Union. Le cas échéant, le conseil d'administration ajuste le budget de l'Agence et le document unique de programmation conformément au budget général de l'Union.

Article 27
Structure du budget

1. Sans préjudice d'autres ressources, les recettes de l'Agence sont constituées:

   (a) d'une contribution du budget de l'Union;

   (b) de recettes allouées à des postes de dépense spécifiques conformément à ses règles financières visées à l'article 29;

   (c) d'un financement de l'Union sous la forme de conventions de délégation ou de subventions ad hoc, conformément à ses règles financières visées à l'article 29 et aux dispositions des instruments pertinents appuyant les politiques de l'Union;

   (d) de contributions de pays tiers participant aux travaux de l'Agence en vertu de l'article 39;

   (e) de toute contribution volontaire des États membres en espèces ou en nature. Les États membres qui apportent une contribution volontaire ne peuvent prétendre à aucun droit ou service spécifique du fait de celle-ci.

2. Les dépenses de l'Agence comprennent la rémunération du personnel, l'assistance administrative et technique, les dépenses d'infrastructure et de fonctionnement et les dépenses résultant de contrats passés avec des tiers.

Article 28
Exécution du budget

1. Le directeur exécutif est responsable de l'exécution du budget de l'Agence.

2. L'auditeur interne de la Commission exerce à l'égard de l'Agence les mêmes compétences que celles qui lui sont attribuées à l'égard des services de la Commission.

3. Au plus tard le 1er mars suivant l'achèvement de l'exercice (1er mars de l'année N + 1), le comptable de l'Agence transmet les comptes provisoires au comptable de la Commission et à la Cour des comptes.

4. À la réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'Agence, le comptable de l'Agence établit les comptes définitifs de l'Agence sous sa propre responsabilité.

5. Le directeur exécutif transmet pour avis les comptes définitifs au conseil d'administration.

6. Au plus tard le 31 mars de l'année N + 1, le directeur exécutif transmet le rapport sur la gestion budgétaire et financière au Parlement européen, au Conseil, à la Commission et à la Cour des comptes.

7. Au plus tard le 1er juillet de l'année N + 1, le comptable transmet les comptes définitifs, accompagnés de l'avis du conseil d'administration, au Parlement européen, au Conseil, au comptable de la Commission et à la Cour des comptes.

8. À la même date que la transmission de ses comptes définitifs, le comptable transmet également à la Cour des comptes une lettre de déclaration portant sur ces comptes définitifs, avec copie au comptable de la Commission.

9. Le directeur exécutif publie les comptes définitifs avant le 15 novembre de l'année suivante.

10. Le directeur exécutif adresse à la Cour des comptes une réponse aux observations de celle-ci, le 30 septembre de l'année N + 1 au plus tard, et adresse également une copie de cette réponse au conseil d'administration et à la Commission.

11. Le directeur exécutif soumet au Parlement européen, à la demande de celui-ci, comme prévu à l'article 165, paragraphe 3, du règlement financier, toute information nécessaire au bon déroulement de la procédure de décharge pour l'exercice budgétaire en question.

12. Le Parlement européen, statuant sur recommandation du Conseil, donne avant le 15 mai de l'année N + 2, décharge au directeur exécutif sur l'exécution du budget de l'exercice N.

Article 29
Règles financières

Les règles financières applicables à l'Agence sont arrêtées par le conseil d'administration, après consultation de la Commission. Elles ne peuvent s'écarter du règlement (UE) n° 1271/2013 que si les exigences spécifiques du fonctionnement de l'Agence le nécessitent et moyennant l'accord préalable de la Commission.

*Article 30****Lutte contre la fraude***

1. Afin de faciliter la lutte contre la fraude, la corruption et d'autres activités illégales au titre du règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil[39], l'Agence, dans un délai de six mois à compter de son entrée en fonction, adhère à l'accord interinstitutionnel du 25 mai 1999 relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF) et adopte les dispositions

[39] Règlement (UE, Euratom) n° 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) n° 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) n° 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

appropriées applicables à tout le personnel de l'Agence, en utilisant le modèle figurant à l'annexe dudit accord.

2. 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 de l'Agence.

3. 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) n° 883/2013 du Parlement européen et du Conseil et le règlement (Euratom, CE) n° 2185/96 du Conseil[40] 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 l'Agence.

4. Sans préjudice des paragraphes 1, 2 et 3, les accords de coopération conclus avec des pays tiers et des organisations internationales, les contrats, les conventions de subvention et les décisions de subvention de l'Agence contiennent des dispositions habilitant expressément la Cour des comptes et l'OLAF à procéder à ces audits et ces enquêtes, conformément à leurs compétences respectives.

CHAPITRE IV
PERSONNEL DE L'AGENCE

Article 31
Dispositions générales

Le statut et le régime applicable aux autres agents, ainsi que les réglementations arrêtées d'un commun accord des institutions de l'Union visant à exécuter le statut, s'appliquent au personnel de l'Agence.

Article 32
Privilèges et immunités

Le protocole n° 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 à l'Agence ainsi qu'à son personnel.

Article 33
Directeur exécutif

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

40 Règlement (Euratom, CE) n° 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).

2. Le directeur exécutif est nommé par le conseil d'administration sur la base d'une liste de candidats proposés par la Commission, à la suite d'une procédure de sélection ouverte et transparente.

3. Aux fins de la conclusion du contrat du directeur exécutif, l'Agence est représentée par le président du conseil d'administration.

4. Avant d'être nommé, le candidat retenu par le conseil d'administration est invité à faire une déclaration devant la commission concernée du Parlement européen et à répondre aux questions des députés.

5. Le mandat du directeur exécutif est de cinq 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 missions et défis futurs de l'Agence.

6. Le conseil d'administration statue sur la nomination, la prolongation du mandat et la révocation du directeur exécutif à la majorité des deux tiers de ses membres disposant du droit de vote.

7. Le conseil d'administration, 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 cinq ans.

8. Le conseil d'administration informe le Parlement européen de son intention de prolonger le mandat du directeur exécutif. Dans les trois mois précédant cette prolongation, le directeur exécutif fait, s'il y est invité, une déclaration devant la commission concernée du Parlement européen et répond aux questions des députés.

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

10. Le directeur exécutif ne peut être démis de ses fonctions que sur décision du conseil d'administration, statuant sur proposition de la Commission.

Article 34
Experts nationaux détachés et autre personnel

1. L'Agence peut avoir recours à des experts nationaux détachés ou à d'autres personnes qu'elle n'emploie pas. Le statut et le régime applicable aux autres agents ne s'appliquent pas à ces personnes.

2. Le conseil d'administration adopte une décision établissant le régime applicable aux experts nationaux détachés auprès de l'Agence.

CHAPITRE V
DISPOSITIONS GÉNÉRALES

Article 35
Statut juridique de l'Agence

1. L'Agence est un organisme de l'Union et est dotée de la personnalité juridique.

2. Dans chaque État membre, l'Agence jouit de la capacité juridique la plus étendue accordée aux personnes morales en droit national. Elle peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et/ou ester en justice.

3. L'Agence est représentée par son directeur exécutif.

Article 36
Responsabilité de l'Agence

1. La responsabilité contractuelle de l'Agence est régie par la législation applicable au contrat en question.
2. La Cour de justice de l'Union européenne est compétente pour statuer en vertu de toute clause compromissoire contenue dans un contrat conclu par l'Agence.
3. En cas de responsabilité non contractuelle, l'Agence, conformément aux principes généraux communs aux droits des États membres, répare tout dommage causé par ses services ou par ses agents dans l'exercice de leurs fonctions.
4. La Cour de justice de l'Union européenne est compétente pour tout litige relatif à la réparation de tels dommages.
5. La responsabilité personnelle à l'égard de l'Agence de ses propres agents est régie par les dispositions pertinentes applicables au personnel de l'Agence.

Article 37
Régime linguistique

1. Les dispositions du règlement nº 1 du Conseil[41] s'appliquent à l'Agence. Les États membres et les autres organismes désignés par ceux-ci peuvent s'adresser à l'Agence et en recevoir une réponse dans la langue officielle des institutions de l'Union de leur choix.
2. Les services de traduction nécessaires au fonctionnement de l'Agence sont assurés par le Centre de traduction des organes de l'Union européenne.

Article 38
Protection des données à caractère personnel

1. Les opérations de traitement de données à caractère personnel effectuées par l'Agence sont soumises aux dispositions du règlement (CE) nº 45/2001 du Parlement européen et du Conseil[42].
2. Le conseil d'administration adopte les dispositions d'application visées à l'article 24, paragraphe 8, du règlement (CE) nº 45/2001. Le conseil d'administration peut adopter des mesures supplémentaires nécessaires pour l'application du règlement (CE) nº 45/2001 par l'Agence.

---

41 Règlement nº 1, portant fixation du régime linguistique de la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 401).

42 Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

Article 39

Coopération avec des pays tiers et des organisations internationales

1. Dans la mesure où cela est nécessaire pour atteindre les objectifs énoncés dans le présent règlement, l'Agence peut coopérer avec les autorités compétentes de pays tiers et/ou avec des organisations internationales. À cet effet, l'Agence peut, sous réserve de l'approbation préalable de la Commission, établir des arrangements de travail avec les autorités de pays tiers et des organisations internationales. Ces arrangements ne créent pas d'obligations juridiques à l'égard de l'Union ou de ses États membres.

2. L'Agence est ouverte à la participation des pays tiers qui ont conclu des accords en ce sens avec l'Union européenne. Conformément aux dispositions pertinentes de ces accords, des arrangements sont élaborés pour préciser notamment la nature, l'étendue et les modalités de la participation de ces pays aux travaux de l'Agence. Ces arrangements comprennent notamment des dispositions relatives à la participation aux initiatives prises par l'Agence, aux contributions financières et au personnel. En ce qui concerne les questions relatives au personnel, lesdits arrangements respectent, en tout état de cause, le statut.

3. Le conseil d'administration adopte une stratégie en ce qui concerne les relations avec les pays tiers ou les organisations internationales sur les questions relevant de la compétence de l'Agence. La Commission veille à ce que l'Agence fonctionne dans les limites de son mandat et du cadre institutionnel existant en concluant un arrangement de travail approprié avec le directeur exécutif de l'Agence.

Article 40

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

En consultation avec la Commission, l'Agence adopte ses propres règles de sécurité, en appliquant les principes de sécurité énoncés dans les règles de sécurité de la Commission visant à protéger les informations classifiées de l'Union européenne (ICUE) et les informations sensibles non classifiées, exposées dans les décisions (UE, Euratom) 2015/443 et 2015/444 de la Commission. Ces principes couvrent, entre autres, les dispositions relatives à l'échange, au traitement et au stockage de telles informations.

Article 41

Accord de siège et conditions de fonctionnement

1. Les dispositions relatives à l'implantation de l'Agence dans l'État membre du siège et aux prestations à fournir par cet État, ainsi que les règles particulières qui y sont applicables au directeur exécutif, aux membres du conseil d'administration, au personnel de l'Agence et aux membres de leurs familles sont arrêtées dans un accord de siège conclu entre l'Agence et l'État membre où son siège est situé, après approbation par le conseil d'administration et au plus tard [deux ans après l'entrée en vigueur du règlement].

2. L'État membre d'accueil de l'Agence offre les meilleures conditions possibles pour assurer le bon fonctionnement de l'Agence, notamment l'accessibilité de l'emplacement, l'existence de services d'éducation appropriés pour les enfants des membres du personnel et un accès adéquat au marché du travail, à la sécurité sociale et aux soins médicaux pour les enfants et les conjoints.

Article 42
Contrôle administratif

Les activités de l'Agence sont soumises au contrôle du Médiateur, conformément à l'article 228 du traité sur le fonctionnement de l'Union européenne.

TITRE III
CADRE DE CERTIFICATION DE CYBERSÉCURITÉ

Article 43

Systèmes européens de certification de cybersécurité

Un système européen de certification de cybersécurité atteste que les produits et services TIC qui ont été certifiés conformément à ce système satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces produits, processus, services et systèmes.

Article 44

Élaboration et adoption d'un système européen de certification de cybersécurité

1. À la suite d'une demande de la Commission, l'ENISA élabore un système européen de certification de cybersécurité candidat qui satisfait aux exigences énoncées aux articles 45, 46 et 47 du présent règlement. Les États membres ou le Groupe européen de certification de cybersécurité (le «Groupe») établi en vertu de l'article 53 peuvent proposer à la Commission l'élaboration d'un système européen de certification de cybersécurité candidat.
2. Lors de l'élaboration des systèmes candidats visés au paragraphe 1, l'ENISA consulte toutes les parties prenantes concernées et travaille en étroite collaboration avec le Groupe. Celui-ci fournit à l'ENISA l'aide et l'expertise dont elle a besoin dans le cadre de l'élaboration du système candidat, notamment en formulant des avis si nécessaire.
3. L'Agence transmet à la Commission le système européen de certification de cybersécurité candidat élaboré conformément au paragraphe 2.
4. La Commission, se fondant sur le système candidat proposé par l'ENISA, peut adopter des actes d'exécution, conformément à l'article 55, paragraphe 1, prévoyant des systèmes européens de certification de cybersécurité pour les produits et services TIC qui satisfont aux exigences des articles 45, 46 et 47 du présent règlement.
5. L'ENISA tient à jour un site Web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité et leur assurant une publicité.

Article 45

Objectifs de sécurité des systèmes européens de certification de cybersécurité

Un système européen de certification de cybersécurité est conçu de façon à prendre en compte, le cas échéant, les objectifs de sécurité suivants:

(a) protéger les données stockées, transmises ou traitées d'une autre façon contre le stockage, le traitement, l'accès ou la diffusion accidentels ou non autorisés;

(b) protéger les données stockées, transmises ou traitées d'une autre façon contre la destruction accidentelle ou non autorisée, la perte ou l'altération accidentelles;

(c) garantir que les personnes autorisées, les programmes ou les machines peuvent exclusivement accéder aux données, services ou fonctions concernés par leurs droits d'accès;

(d) garder une trace des données, fonctions ou services qui ont été communiqués, du moment où ils l'ont été et des personnes qui les ont communiqués;

(e) garantir la possibilité de vérifier quels sont les données, services ou fonctions qui ont été consultés ou utilisés, à quel moment et par quelles personnes;

(f) rétablir la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci dans les plus brefs délais en cas d'incident physique ou technique;

(g) veiller à ce que les produits et services TIC soient dotés de logiciels à jour et sans vulnérabilités connues, et de mécanismes permettant d'assurer les mises à jour des logiciels en toute sécurité.

Article 46

Niveaux d'assurance des systèmes européens de certification de cybersécurité

1. Un système européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants: élémentaire, substantiel et/ou élevé, pour les produits et services TIC certifiés dans le cadre de ce système.

2. Les niveaux d'assurance élémentaire, substantiel et élevé satisfont respectivement aux critères suivants:

(a) le niveau d'assurance élémentaire renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré limité de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou d'un service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'incidents de cybersécurité;

(b) le niveau d'assurance substantiel renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré substantiel de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou d'un service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'incidents de cybersécurité;

(c) le niveau d'assurance élevé renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou service TIC plus élevé que les certificats ayant le niveau d'assurance substantiel, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de prévenir les incidents de cybersécurité;

Article 47

Éléments des systèmes européens de certification de cybersécurité

1. Un système européen de certification de cybersécurité comprend les éléments suivants:

   (a) l'objet et le champ d'application de la certification, notamment le type ou les catégories de produits et services TIC;

   (b) une description détaillée des exigences de cybersécurité utilisées pour évaluer les produits et services TIC, par exemple par référence aux normes ou spécifications techniques européennes ou internationales;

   (c) le cas échéant, un ou plusieurs niveaux d'assurance;

   (d) les critères et méthodes d'évaluation spécifiques utilisés, notamment les types d'évaluation, afin de démontrer que les objectifs spécifiques visés à l'article 45 sont atteints;

   (e) les informations nécessaires à la certification qu'un demandeur doit fournir aux organismes d'évaluation de la conformité;

   (f) lorsque le système prévoit des marques ou des labels, les conditions dans lesquelles ces marques ou labels peuvent être utilisés;

   (g) lorsque le système comprend une surveillance, les modalités relatives au contrôle du respect des exigences associées aux certificats, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité;

   (h) les conditions permettant de délivrer, maintenir et poursuivre la certification et d'étendre ou de réduire son champ d'application;

   (i) les règles relatives aux conséquences de la non-conformité des produits et services TIC certifiés aux exigences en matière de certification;

   (j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des produits et services TIC;

   (k) les règles relatives à la conservation des archives par les organismes d'évaluation de la conformité;

   (l) l'identification des systèmes nationaux de certification de cybersécurité couvrant le même type ou les mêmes catégories de produits et services TIC;

   (m) le contenu du certificat délivré.

2. Les exigences spécifiées du système ne sont pas contraires aux exigences légales applicables, notamment les exigences découlant de la législation harmonisée de l'Union.

3. Lorsqu'un acte spécifique de l'Union le prévoit, la certification au titre d'un système européen de certification de cybersécurité peut être utilisée pour démontrer la présomption de conformité aux exigences de cet acte.

4. En l'absence de législation harmonisée de l'Union, le droit d'un État membre peut aussi prévoir qu'un système européen de certification de cybersécurité soit utilisé pour établir la présomption de conformité aux exigences légales.

Article 48

Certification de cybersécurité

1. Les produits et services TIC qui ont été certifiés dans le cadre d'un système européen de certification de cybersécurité adopté conformément à l'article 44 sont présumés conformes aux exigences de ce système.

2. La certification est volontaire, sauf indication contraire dans le droit de l'Union.

3. Les organismes d'évaluation de la conformité visés à l'article 51 délivrent un certificat européen de cybersécurité au titre du présent article sur la base des critères figurant dans le système européen de certification de cybersécurité adopté conformément à l'article 44.

4. Par dérogation au paragraphe 3, dans des cas dûment justifiés, un système européen de cybersécurité particulier peut prévoir que seul un organisme public puisse délivrer un certificat européen de cybersécurité dans le cadre dudit système. Cet organisme public est l'une des entités suivantes:

   (a) une autorité nationale de contrôle de la certification visée à l'article 50, paragraphe 1;

   (b) un organisme accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 51, paragraphe 1; ou

   (c) un organisme créé en vertu des lois, actes réglementaires ou autres procédures administratives officielles d'un État membre concerné et satisfaisant aux exigences applicables aux organismes certifiant les produits, les procédés et les services selon la norme ISO/IEC 17065: 2012.

5. La personne physique ou morale qui soumet ses produits ou services TIC au mécanisme de certification fournit à l'organisme d'évaluation de la conformité visé à l'article 51 toutes les informations nécessaires pour mener la procédure de certification.

6. Les certificats sont délivrés pour une durée maximale de trois ans et peuvent être renouvelés dans les mêmes conditions pourvu que les exigences applicables continuent d'être satisfaites.

7. Un certificat européen de cybersécurité délivré au titre du présent article est reconnu dans tous les États membres.

Article 49

Systèmes nationaux de certification de cybersécurité et certificats

1. Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les produits et services TIC couverts par un système européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution adopté en application de l'article 44, paragraphe 4. Les systèmes nationaux de certification de cybersécurité existants et les procédures connexes pour les produits et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.

2. Les États membres s'abstiennent d'instaurer de nouveaux systèmes nationaux de certification de cybersécurité des produits et services TIC couverts par un système européen de certification de cybersécurité en vigueur.

3. Les certificats existants, délivrés en vertu de systèmes nationaux de certification de cybersécurité, restent valables jusqu'à leur date d'expiration.

Article 50

Autorités nationales de contrôle de la certification

1. Chaque État membre désigne une autorité nationale de contrôle de la certification.

2. Chaque État membre informe la Commission de l'identité de l'autorité désignée.

3. Chaque autorité nationale de contrôle de la certification est indépendante, en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel, des entités qu'elle surveille.

4. Les États membres veillent à ce que les autorités nationales de contrôle de la certification disposent de ressources adéquates pour exercer leurs pouvoirs et exécuter, de manière efficace et efficiente, les missions qui leur sont dévolues.

5. Afin d'assurer la mise en œuvre efficace du présent règlement, il convient que ces autorités participent, d'une manière active, efficace, efficiente et sécurisée, au Groupe européen de certification de cybersécurité institué en vertu de l'article 53.

6. Les autorités nationales de contrôle de la certification:

   (a) contrôlent et assurent l'application des dispositions du présent titre au niveau national et supervisent la conformité des certificats qui ont été délivrés par les organismes d'évaluation de la conformité établis sur leur territoire aux exigences énoncées dans le présent titre et dans le système européen de certification de cybersécurité correspondant;

   (b) contrôlent et supervisent les activités des organismes d'évaluation de la conformité aux fins du présent règlement, notamment en ce qui concerne la notification des organismes d'évaluation de la conformité et des missions connexes énoncées à l'article 52 du présent règlement;

   (c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, examinent l'objet de la réclamation dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;

   (d) coopèrent avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques;

   (e) suivent les évolutions pertinentes dans le domaine de la certification de cybersécurité.

7. Chaque autorité nationale de contrôle de la certification dispose au moins des pouvoirs suivants:

(a) demander aux organismes d'évaluation de la conformité et aux titulaires d'un certificat européen de cybersécurité de lui communiquer toute information dont elle a besoin pour l'accomplissement de sa mission;

(b) effectuer des enquêtes, sous la forme d'audits, auprès des organismes d'évaluation de la conformité et des titulaires de certificats européens de cybersécurité afin de vérifier le respect des dispositions en vertu du titre III;

(c) prendre les mesures appropriées, conformément au droit national, afin de veiller à ce que les organismes d'évaluation de la conformité ou les titulaires d'un certificat respectent le présent règlement ou un système européen de certification de cybersécurité;

(d) obtenir l'accès à tous les locaux des organismes d'évaluation de la conformité et des titulaires de certificats européens de cybersécurité afin d'effectuer des enquêtes conformément au droit de l'Union ou au droit procédural des États membres;

(e) retirer, conformément au droit national, les certificats qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité;

(f) imposer des sanctions, comme prévu à l'article 54, conformément au droit national, et exiger la cessation immédiate des manquements aux obligations énoncées dans le présent règlement.

8. Les autorités nationales de contrôle de la certification coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits et services TIC.

Article 51
Organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité ne sont accrédités par l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil que lorsqu'ils satisfont aux exigences énoncées à l'annexe du présent règlement.

2. L'accréditation est accordée pour une durée maximale de cinq ans et peut être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences énoncées au présent article. Les organismes d'accréditation révoquent l'accréditation d'un organisme d'évaluation de la conformité accordée en vertu du paragraphe 1 lorsque les conditions de l'accréditation ne sont pas ou plus remplies ou que des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.

Article 52
Notification

1. Pour chaque système européen de certification de cybersécurité adopté en vertu de l'article 44, les autorités nationales de contrôle de la certification notifient à la Commission les organismes d'évaluation de la conformité accrédités pour délivrer

des certificats aux niveaux d'assurance spécifiés visés à l'article 46 et l'informent, sans délai indu, de toute modification ultérieure qui y est apportée.

2. Un an après la date d'entrée en vigueur d'un système européen de certification de cybersécurité, la Commission publie au Journal officiel une liste des organismes d'évaluation de la conformité notifiés.

3. Si la Commission reçoit une notification après expiration du délai visé au paragraphe 1, elle publie au Journal officiel de l'Union européenne les modifications apportées à la liste visée au paragraphe 2 dans un délai de deux mois à compter de la date de réception de cette notification.

4. Une autorité nationale de contrôle de la certification peut présenter à la Commission une demande visant à retirer de la liste visée au paragraphe 2 un organisme d'évaluation de la conformité notifié par l'autorité en cause. La Commission publie au Journal officiel de l'Union européenne les modifications correspondantes apportées à la liste dans un délai d'un mois à compter de la date de réception de la demande présentée par l'autorité nationale de contrôle de la certification.

5. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, formats et procédures des notifications visées au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 55, paragraphe 2.

Article 53

Systèmes européens de certification de cybersécurité

1. Le Groupe européen de certification de cybersécurité (ci-après le «Groupe») est institué.

2. Le Groupe est composé d'autorités nationales de contrôle de la certification. Les autorités sont représentées par leur dirigeant ou par d'autres représentants de haut niveau.

3. Le Groupe a pour mission:

   (a) de conseiller et d'assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes des dispositions du présent titre, notamment en ce qui concerne les questions de politique de certification de cybersécurité, la coordination des approches et l'élaboration de systèmes européens de certification de cybersécurité;

   (b) d'assister, de conseiller et de coopérer avec l'ENISA en ce qui concerne l'élaboration d'un système candidat conformément à l'article 44 du présent règlement;

   (c) de proposer à la Commission de demander à l'Agence d'élaborer un système européen de certification de cybersécurité candidat conformément à l'article 44 du présent règlement;

   (d) d'adopter des avis adressés à la Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants;

   (e) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et de l'échange de bonnes pratiques sur les systèmes de certification de cybersécurité;

(f) de faciliter la coopération entre les autorités nationales de contrôle de la certification en vertu du présent titre par l'échange d'informations, notamment en établissant des méthodes permettant un échange d'informations efficace sur toutes les questions relatives à la certification de cybersécurité.

4. La Commission préside le Groupe et en assure le secrétariat, avec l'aide de l'ENISA conformément à l'article 8, point a).

Article 54
Sanctions

Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions du présent titre et des systèmes européens de certification de cybersécurité et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres notifient ces règles et ces mesures à la Commission [au plus tard le ... /sans retard], et l'informent de toute modification ultérieure les concernant.

TITRE IV
DISPOSITIONS FINALES

Article 55
Procédure de comité

1. La Commission est assistée par un comité. Celui-ci est un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 s'applique.

Article 56
Évaluation et révision

1. Au plus tard cinq ans après la date visée à l'article 58, et ensuite tous les cinq ans, la Commission évalue l'incidence, l'efficacité et l'efficience de l'Agence et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'Agence et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'Agence en réaction à ses activités. Lorsque la Commission estime que le maintien de l'Agence n'est plus justifié au regard des objectifs, du mandat et des missions qui lui ont été assignés, elle peut proposer que les dispositions du présent règlement relatives à l'Agence soient modifiées.
2. L'évaluation porte également sur l'impact, l'efficacité et l'efficience des dispositions du titre III au regard des objectifs consistant à garantir un niveau suffisant de cybersécurité des produits et services TIC dans l'Union et à améliorer le fonctionnement du marché intérieur.
3. La Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions du rapport d'évaluation sont rendues publiques.

Article 57
Abrogation et succession

1. Le règlement (CE) n° 526/2013 est abrogé avec effet au [....].
2. Les références au règlement (CE) n° 526/2013 et à l'ENISA s'entendent comme faites au présent règlement et à l'Agence.
3. L'Agence succède à l'Agence qui a été instituée par le règlement (CE) n° 526/2013 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités. Toutes les décisions du conseil d'administration et du conseil exécutif restent valables, pour autant qu'elles ne soient pas en contradiction avec les dispositions du présent règlement.
4. L'Agence est instituée pour une durée indéterminée à compter du [….].

5. Le directeur exécutif nommé en vertu de l'article 24, paragraphe 4, du règlement (CE) n° 526/2013 est le directeur exécutif de l'Agence pour la durée restante de son mandat.

6. Les membres, et leurs suppléants, du conseil d'administration nommés en application de l'article 6 du règlement (CE) n° 526/2013 sont les membres, et leurs suppléants, du conseil d'administration de l'Agence pour la durée restante de leur mandat.

Article 58

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

2. 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

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)

1.2. Domaine(s) politique(s) concerné(s)

Domaine(s) politique(s): 09 - Réseaux de communication, contenu et technologies

Activité(s): 09.02 Marché unique numérique

1.3. Nature de la proposition/de l'initiative

☒ La proposition/l'initiative porte sur **une action nouvelle (Titre III — Certification)**

☐ La proposition/l'initiative porte sur **une action nouvelle suite à un projet pilote/une action préparatoire**[43]

☒La proposition/l'initiative est relative à **la prolongation d'une action existante** (**Titre II – Mandat de l'ENISA)**

☐ 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. Accroître la résilience des États membres, des entreprises et de l'UE dans son ensemble

2. Assurer le bon fonctionnement du marché intérieur de l'UE pour les produits et services TIC

3. Accroître la compétitivité mondiale des entreprises de l'UE opérant dans le domaine des TIC

4. Rapprocher les dispositions législatives, réglementaires et administratives des États membres qui fixent des exigences en matière de cybersécurité

1.4.2. Objectif(s) spécifique(s)

En gardant les objectifs généraux à l'esprit, dans le contexte plus large de la stratégie de cybersécurité, l'instrument vise, en délimitant le champ d'application et le mandat de l'ENISA et en instaurant un cadre européen de certification des produits et services TIC, à atteindre les objectifs spécifiques suivants:

1. développer **les moyens et la préparation** des États membres et des entreprises;
2. améliorer **la coopération et la coordination** entre les États membres et les institutions, organes et organismes de l'UE;
3. accroître **les moyens au niveau de l'UE pour compléter l'action des États membres**, notamment en cas de crises transfrontières dans le domaine de la

[43] Telle que visée à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

cybersécurité;

4. davantage **sensibiliser** les particuliers et les entreprises aux questions de cybersécurité;
5. susciter davantage la confiance dans le marché unique numérique et l'innovation numérique en accroissant globalement la **transparence de l'assurance de la cybersécurité**[44] des produits et services TIC.

L'ENISA contribuera à la réalisation des objectifs ci-dessus par les moyens suivants:

Soutien accru à l'élaboration des politiques – fournir des orientations et des conseils à la Commission et aux États membres en vue de développer et d'actualiser un cadre normatif global dans le domaine de la cybersécurité ainsi que des initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité; contribuer, par son expertise et son concours, aux travaux du groupe de coopération [article 11 de la directive (UE) 2016/1148]; contribuer à l'élaboration et à la mise en œuvre de la politique dans le domaine de l'identification électronique et des services de confiance; promouvoir l'échange de bonnes pratiques entre les autorités compétentes;

Soutien accru au renforcement des capacités – fournir un soutien aux États membres, aux institutions, organes et organismes de l'Union en vue de développer et d'améliorer la prévention, la détection et l'analyse des problèmes et incidents de cybersécurité, et la capacité d'y réagir; aider les États membres, à leur demande, dans l'élaboration de CSIRT nationaux, de stratégies nationales en matière de cybersécurité; aider les institutions de l'Union dans l'élaboration et le réexamen des stratégies de l'Union en matière de cybersécurité; offrir des formations dans le domaine de la cybersécurité; aider les États membres, grâce au groupe de coopération, dans l'échange de bonnes pratiques; faciliter la mise en place de centres d'échange et d'analyse d'informations (ISAC) sectoriels;

Soutien à la coopération opérationnelle et à la gestion des crises – soutenir la coopération entre les organismes publics compétents et entre les parties prenantes en établissant une coopération systématique avec les institutions, organes, et organismes de l'Union traitant de la cybersécurité, de la lutte contre la cybercriminalité et de la protection de la vie privée et des données à caractère personnel; assurer le secrétariat du réseau des CSIRT [article 12, paragraphe 2, de la directive (UE) 2016/1148] et contribuer à la coopération sur le plan opérationnel au sein du réseau en fournissant, en coopération avec la CERT-EU, un soutien aux États membres, à leur demande; organiser régulièrement des exercices de cybersécurité; contribuer à l'élaboration d'une réaction concertée en cas d'incidents ou de crises transfrontières de cybersécurité majeurs; mener, en coopération avec le réseau des CSIRT, des enquêtes techniques ex post sur des incidents importants et formuler des recommandations de suivi;

Missions relatives au marché (normalisation, certification) – exécuter un certain nombre de fonctions afin de soutenir spécifiquement le marché intérieur; constituer un «observatoire du marché» de la cybersécurité, en analysant les tendances pertinentes sur ledit marché pour mieux faire correspondre l'offre et la demande; soutenir et promouvoir le développement et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits et services TIC en élaborant des systèmes européens de certification de cybersécurité des produits et services TIC candidats, en assurant le secrétariat du Groupe de certification de cybersécurité de l'Union, en fournissant des lignes

[44] Par transparence de l'assurance de la cybersécurité on entend le fait de fournir aux utilisateurs suffisamment d'informations sur les caractéristiques de cybersécurité pour leur permettre de déterminer, de façon objective, le niveau de sécurité offert par un produit, service ou processus TIC donné.

directrices et des bonnes pratiques concernant les exigences de sécurité de certains produits et services TIC, en coopération avec les autorités nationales de contrôle de la certification et avec les entreprises; **Soutien accru à la connaissance, à l'information et à la sensibilisation** – prêter assistance et donner des conseils à la Commission et aux États membres pour qu'ils atteignent un niveau élevé de connaissances, dans toute l'Union, sur les questions relatives à la SRI et à son application aux entreprises concernées. Cela suppose également la mise en commun, l'organisation et la mise à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la sécurité des réseaux et des systèmes d'information [ou cybersécurité]. Les activités de sensibilisation et les campagnes d'information à l'intention du grand public sur les risques en matière de cybersécurité constituent un autre élément important;

Soutien accru à la recherche et à l'innovation – fournir des conseils sur les besoins en matière de recherche et sur la fixation des priorités dans le domaine de la cybersécurité;

Soutien à la coopération internationale — soutenir les efforts de l'Union visant à coopérer avec des pays tiers et des organisations internationales pour promouvoir la coopération internationale en matière de cybersécurité.

CERTIFICATION

Le cadre de certification contribuera à la réalisation des objectifs en accroissant globalement la transparence de l'assurance de la cybersécurité[45] des produits et services TIC et en suscitant ainsi davantage la confiance dans le marché unique numérique et l'innovation numérique. Cela éviterait également la multiplication des systèmes de certification dans l'UE, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres et secteurs d'activité.

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.

Un renforcement de l'ENISA (soutenant les capacités, la prévention, la coopération et la sensibilisation au niveau de l'UE et destiné par conséquent à renforcer la cyber-résilience globale de l'UE) et l'appui au cadre européen de certification des produits et services TIC devraient produire les effets suivants (liste non exhaustive):

Impact global

– Impact global positif sur le marché intérieur dû au moindre morcellement du marché et à la plus grande confiance dans les technologies numériques grâce à une meilleure coopération, à une harmonisation accrue des approches dans le domaine des politiques de cybersécurité de l'UE et à un renforcement des capacités à l'échelle de l'UE. Il devrait en résulter une incidence économique positive contribuant à réduire le coût des incidents de cybersécurité/cybercriminalité, dont l'impact économique dans l'Union est estimé à 0,41 % du PIB de l'UE (soit environ 55 milliards d'EUR).

Résultats spécifiques

Accroissement des capacités dans le domaine de la cybersécurité et de la préparation des États membres et des entreprises

[45] Par transparence de l'assurance de la cybersécurité, on entend le fait de fournir aux utilisateurs suffisamment d'informations sur les caractéristiques de cybersécurité pour leur permettre de déterminer, de façon objective, le niveau de sécurité offert par un produit, service ou processus TIC donné.

– accroissement des capacités dans le domaine de la cybersécurité et amélioration de la préparation des États membres (grâce aux éléments suivants: analyse stratégique à long terme des cybermenaces et cyberincidents, orientations et rapports, échange d'expertise et de bonnes pratiques, mise à disposition de formations et de matériel pédagogique, exercices «CyberEurope» renforcés);

– accroissement des capacités des acteurs privés grâce au soutien apporté à la mise en place de centres d'échange et d'analyse d'informations (ISAC) dans divers secteurs;

– amélioration de la préparation de l'UE et des États membres en matière de cybersécurité grâce à la disponibilité de plans convenus en cas de cyberincident transfrontière majeur, bien éprouvés et testés lors d'exercices «CyberEurope».

Amélioration de la coopération et de la coordination entre les États membres et les institutions, organes et organismes de l'UE

– meilleure coopération entre les secteurs public et privé et en leur sein;

– approche plus cohérente de l'application de la directive SRI à travers les frontières et dans tous les secteurs;

– meilleure coopération dans le domaine de la certification grâce à un cadre institutionnel permettant le développement de systèmes européens de certification de cybersécurité et au développement d'une politique commune dans ce domaine.

Accroissement des moyens au niveau de l'UE pour compléter l'action des États membres

– amélioration de la «capacité opérationnelle de l'UE» pour compléter l'action des États membres et les soutenir, sur demande, et en ce qui concerne des services limités et présélectionnés. Cela devrait avoir un impact positif sur la réussite de la prévention, la détection et la réaction à la fois au niveau des États membres et au niveau de l'Union.

Sensibilisation accrue des particuliers et des entreprises aux questions de cybersécurité

– amélioration de la sensibilisation générale des particuliers et des entreprises aux questions de cybersécurité;

– amélioration de la capacité à prendre des décisions en connaissance de cause grâce à la certification de cybersécurité, pour l'achat de produits et services TIC.

Confiance accrue dans le marché unique numérique et l'innovation numérique grâce à une meilleure transparence de l'assurance de la cybersécurité des produits et services TIC

– meilleure transparence de l'assurance de la cybersécurité[46] des produits et services TIC grâce à une simplification des procédures de certification de sécurité dans un cadre à l'échelle de l'UE;

– relèvement du niveau d'assurance concernant les caractéristiques de sécurité des produits et services TIC;

– utilisation accrue de la certification de sécurité encouragée par des procédures simplifiées, des coûts réduits, et la perspective de débouchés commerciaux à l'échelle de l'UE qui ne seront pas entravés par un morcellement du marché;

– amélioration de la compétitivité du marché européen de la cybersécurité grâce à la baisse des coûts et de la charge administrative pour les PME et à l'élimination des éventuels

[46] Par transparence de l'assurance de la cybersécurité, on entend le fait de fournir aux utilisateurs suffisamment d'informations sur les caractéristiques de cybersécurité pour leur permettre de déterminer, de façon objective, le niveau de sécurité offert par un produit, service ou processus TIC donné.

obstacles à l'entrée sur le marché dus au grand nombre de systèmes nationaux de certification.

Autres

– aucun des objectifs ne devrait entraîner d'incidence environnementale significative;

– en ce qui concerne le budget de l'UE, le renforcement de la coopération et de la coordination des activités entre les institutions, organes et organismes de l'UE devrait se traduire par des gains d'efficacité.

1.4.4. Indicateurs de résultats et d'incidences

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

(g)

Objectif: développer les moyens et la préparation des États membres et des entreprises

- nombre de formations organisées par l'ENISA;
- couverture géographique (nombre de pays et de zones) de l'aide directe accordée par l'ENISA
- niveau de préparation atteint par les États membres en termes de maturité CSIRT et surveillance des mesures réglementaires de cybersécurité;
- nombre de bonnes pratiques à l'échelle de l'UE pour les infrastructures critiques, fournies par l'ENISA;
- nombre de bonnes pratiques à l'échelle de l'UE pour les PME, fournies par l'ENISA;
- publication, par l'ENISA, d'une analyse stratégique annuelle des cybermenaces et cyberincidents en vue d'identifier les tendances émergentes;
- contribution régulière de l'ENISA aux travaux des groupes de travail sur la cybersécurité des organismes européens de normalisation (OEN).

Objectif: améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE

- nombre d'États membres ayant appliqué les recommandations et avis de l'ENISA dans leur processus d'élaboration de politiques;
- nombre d'institutions, organes et organismes de l'UE ayant appliqué les recommandations et avis de l'ENISA dans leur processus d'élaboration de politiques;
- application régulière du programme de travail du réseau des CSIRT et bon fonctionnement de l'infrastructure informatique et des moyens de communication dudit réseau;
- nombre de rapports techniques mis à la disposition du groupe de coopération et utilisés par ce dernier;
- approche cohérente de l'application de la directive SRI à travers les frontières et dans tous les secteurs;
- nombre d'évaluations de la conformité à la réglementation effectuées par

l'ENISA;

- nombre de centres d'échange et d'analyse d'informations (ISAC) mis en place dans différents secteurs, en particulier pour les infrastructures critiques;
- mise en place et bon fonctionnement d'une plateforme d'information diffusant des informations de cybersécurité provenant des institutions, organes et organismes de l'UE;
- contribution régulière à l'élaboration des programmes de travail de recherche et d'innovation de l'UE;
- accord de coopération mis en place entre l'ENISA, l'EC3 et la CERT-EU;
- nombre de systèmes de certification intégrés et développés au titre du Cadre.

Objectif: accroître les moyens au niveau de l'UE pour compléter l'action des États membres, notamment en cas de crises transfrontières dans le domaine de la cybersécurité

- publication, par l'ENISA, d'une analyse stratégique annuelle des cybermenaces et cyberincidents en vue d'identifier les tendances émergentes;
- publication d'informations agrégées sur les incidents signalés par l'ENISA au titre de la directive SRI;
- nombre d'exercices paneuropéens coordonnés par l'Agence et nombre d'États membres et d'organisations concernés;
- nombre de demandes d'un soutien à l'intervention en cas d'urgence présentées par les États membres à l'ENISA et prises en charge par l'Agence;
- nombre d'analyses des vulnérabilités, artefacts et incidents effectuées par l'ENISA en coopération avec la CERT-EU;
- disponibilité de rapports de situation à l'échelle de l'UE, sur la base des informations communiquées à l'ENISA par les États membres et par d'autres entités en cas de cyberincident transfrontière majeur.

Objectif: davantage sensibiliser les particuliers et les entreprises aux questions de cybersécurité

- organisation régulière de campagnes de sensibilisation nationales et à l'échelle de l'UE, et mise à jour régulière des thèmes en fonction des nouveaux besoins en matière de formation;
- sensibilisation accrue des citoyens de l'UE à la cybersécurité;
- organisation régulière de quiz de sensibilisation à la cybersécurité et accroissement au fil du temps du pourcentage de réponses correctes;
- publication régulière de bonnes pratiques en matière de cybersécurité et d'hygiène, à l'attention des employés et des organisations.

Objectif: Susciter davantage la confiance dans le marché unique numérique et l'innovation numérique en accroissant globalement la transparence de l'assurance de la cybersécurité[47] des produits et services TIC

[47] Par transparence de l'assurance de la cybersécurité, on entend le fait de fournir aux utilisateurs suffisamment d'informations sur les caractéristiques de cybersécurité pour leur permettre de déterminer, de façon objective, le niveau de sécurité offert par un produit, service ou processus TIC donné.

- nombre de systèmes qui adhèrent au cadre de l'UE;
- diminution du coût d'obtention d'un certificat de sécurité en matière de TIC;
- nombre d'organismes d'évaluation de la conformité spécialisés dans la certification des TIC, dans l'ensemble des États membres;
- mise en place du Groupe européen de certification de cybersécurité et organisation régulière de réunions;
- lignes directrices relatives à la certification, conformément au cadre de l'UE établi;
- publication régulière d'analyses des principales tendances du marché européen de la cybersécurité;
- nombre de produits et services TIC certifiés conformément aux règles du cadre européen de certification en matière de sécurité des TIC;
- augmentation du nombre d'utilisateurs finals conscients des caractéristiques de sécurité des produits et services TIC.

(h)

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

Compte tenu des exigences réglementaires et de l'évolution rapide de l'éventail des menaces en matière de cybersécurité, il est nécessaire de revoir le mandat de l'ENISA afin de définir un ensemble renouvelé de missions et de fonctions en vue de soutenir, de façon efficace et efficiente, les efforts déployés par les États membres, les institutions de l'UE et d'autres parties intéressées pour assurer la sécurité du cyberespace dans l'Union européenne. Le mandat suggéré prévoit des domaines d'action bien délimités. Sont renforcés les domaines où l'Agence apporte une valeur ajoutée avérée, et sont ajoutés les nouveaux domaines où un soutien s'impose vu les priorités et instruments politiques nouveaux, en particulier la directive SRI, le réexamen de la stratégie de cybersécurité de l'UE, le plan de l'UE en matière de cybersécurité pour la coopération en cas de crise et la certification de sécurité en matière de TIC. Le nouveau mandat proposé vise à donner un rôle plus important et plus central à l'Agence qui, en particulier, est appelée à aider aussi les États membres à faire face plus activement aux menaces particulières (capacité opérationnelle), et à devenir un centre d'expertise apportant un soutien aux États membres et à la Commission en matière de certification de cybersécurité.

Dans le même temps, la proposition vise à instaurer un Cadre européen de certification de cybersécurité des produits et services TIC, et précise les fonctions et missions essentielles de l'ENISA dans ce domaine. Le Cadre prévoit des dispositions et procédures communes permettant la création de systèmes de certification de cybersécurité à l'échelle de l'Europe pour des produits/services TIC spécifiques ou des risques de cybersécurité particuliers. La création de systèmes européens de certification de cybersécurité conformément au Cadre permettra de faire en sorte que les certificats délivrés en vertu de ces systèmes soient valables et reconnus dans tous les États membres et de remédier ainsi au morcellement actuel du marché.

1.4.6. Valeur ajoutée de l'intervention de l'Union

La cybersécurité est une question d'envergure véritablement mondiale, qui est transfrontalière par nature et devient de plus en plus transsectorielle en raison de l'interdépendance entre les réseaux et les systèmes d'information. Le nombre, la

complexité et l'ampleur des incidents de cybersécurité et de leurs conséquences sur l'économie et sur la société augmentent au fil du temps et devraient continuer à le faire parallèlement à l'évolution technologique, comme le développement de l'internet des objets. Il restera donc nécessaire à l'avenir d'intensifier l'effort commun des États membres, des institutions de l'UE et des acteurs privés pour réagir aux menaces qui pèsent sur la cybersécurité.

Depuis sa création en 2004, l'ENISA s'est employée à encourager la coopération entre les États membres et les parties prenantes en matière de SRI, notamment en soutenant la coopération entre les secteurs public et privé. Ce soutien à la coopération comprenait les travaux techniques nécessaires pour faire l'inventaire des menaces à l'échelle de l'UE, la mise en place de groupes d'experts et l'organisation d'exercices paneuropéens de gestion de cyberincidents et cybercrises pour les secteurs public et privé (en particulier les exercices «Cyber Europe»). La directive SRI a confié à l'ENISA des tâches supplémentaires, notamment le rôle de secrétariat du réseau des CSIRT en vue d'une coopération opérationnelle entre États membres.

Les conclusions du Conseil de 2016[48] ont reconnu la valeur ajoutée de l'action au niveau de l'UE, en particulier pour renforcer la coopération entre États membres mais aussi entre communautés SRI, et l'évaluation de 2017 de l'ENISA montre clairement aussi que la valeur ajoutée de l'Agence réside principalement dans sa capacité à renforcer la coopération entre ces parties prenantes. Il n'y a aucune autre entité au niveau de l'UE qui favorise la coopération d'autant de parties intéressées par la SRI.

La valeur ajoutée de l'ENISA pour ce qui est de rassembler les communautés et les parties prenantes dans le domaine de la cybersécurité est également constatée dans le domaine de la certification. L'augmentation de la cybercriminalité et des menaces pour la sécurité a suscité des initiatives nationales fixant des exigences élevées en matière de cybersécurité et de certification pour les composants TIC utilisés dans les infrastructures traditionnelles. Pour importantes qu'elles soient, ces initiatives risquent d'entraîner un morcellement du marché unique et de créer des obstacles à l'interopérabilité. Un fournisseur de TIC pourrait donc être obligé de se soumettre à plusieurs processus de certification pour pouvoir vendre dans plusieurs États membres. Il est peu probable que le manque d'efficacité/efficience des systèmes de certification actuels puisse être résolu en l'absence d'intervention de l'Union. Faute d'action, le morcellement du marché augmentera très probablement à court ou à moyen terme (dans les 5 à 10 prochaines années) avec l'émergence de nouveaux systèmes de certification. Le manque de coordination et d'interopérabilité entre ces systèmes entame le potentiel du marché unique numérique. Cela prouve la valeur ajoutée de la création d'un Cadre européen de certification de cybersécurité pour les produits et services TIC, qui instaure les conditions adéquates pour lutter efficacement contre le problème lié à la coexistence de procédures de certification multiples dans les différents États membres, réduit les coûts de la certification et renforce donc globalement l'attrait de cette dernière dans l'UE sur le plan commercial et du point de vue de la compétitivité.

1.4.7. Leçons tirées d'expériences similaires

Conformément à la base juridique de l'ENISA, la Commission a procédé à une évaluation de l'Agence, comprenant une étude indépendante ainsi qu'une consultation publique.

[48] Conclusions du Conseil intitulées «Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», 15 novembre 2016.

L'évaluation a permis de conclure que les objectifs de l'ENISA restent d'actualité aujourd'hui. Compte tenu de l'évolution des technologies et des menaces et du besoin pressant d'accroître la sécurité des réseaux et de l'information (SRI) dans l'UE, il est nécessaire de disposer d'une expertise technique sur l'évolution des questions de sécurité des réseaux et de l'information. Il faut se doter de moyens, dans les États membres, pour comprendre les menaces et y réagir, et les parties intéressées doivent coopérer dans tous les champs thématiques et toutes les institutions.

L'Agence a contribué avec succès à améliorer la SRI en Europe en aidant à se doter de moyens dans les 28 États membres, en intensifiant la coopération entre les États membres et les parties intéressées par la SRI, et en fournissant une expertise, la possibilité de nouer des relations et un soutien à l'élaboration de politiques.

L'ENISA est certes parvenue à avoir une influence, au moins relative, dans le vaste domaine de la SRI, mais elle n'a pas vraiment réussi à se forger une réputation solide et à acquérir assez de visibilité pour être reconnue comme «le» centre d'expertise en Europe. Cela s'explique par le fait que le mandat de l'ENISA est large mais n'a pas été assorti de ressources suffisantes en proportion. De plus, l'ENISA reste la seule agence de l'UE dont le mandat est à durée déterminée, ce qui limite sa capacité à élaborer une vision à long terme et à apporter un soutien durable aux parties intéressées. Cela est également en contradiction avec les dispositions de la directive SRI, en vertu de laquelle l'ENISA se voit confier des missions sans date de fin.

En ce qui concerne la certification de cybersécurité des produits et services TIC, il n'existe à l'heure actuelle aucun cadre européen. Or, la hausse de la cybercriminalité et des menaces pour la sécurité a fait apparaître des initiatives nationales, ce qui entraîne un risque de morcellement du marché unique.

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

L'initiative est tout à fait cohérente avec les politiques existantes, notamment dans le domaine du marché intérieur. Elle est en effet conçue selon l'approche globale en matière de cybersécurité, selon la définition donnée dans le réexamen de la stratégie pour un marché unique numérique, afin de compléter un ensemble global de mesures, telles que le réexamen de la stratégie de cybersécurité de l'UE, le plan pour la coopération en cas de crise dans le domaine de la cybersécurité et les initiatives visant à lutter contre la cybercriminalité. Elle permettrait de s'aligner et de s'appuyer sur les dispositions de l'actuelle législation en matière de cybersécurité, notamment la directive SRI, afin d'approfondir la cyberrésilience de l'UE grâce au renforcement des capacités, de la coopération, de la gestion des risques et de la sensibilisation à la cybersécurité.

Les mesures suggérées en matière de certification devraient porter sur le risque de morcellement dû aux systèmes de certification nationaux existants et émergents et contribuer ainsi au développement du marché unique numérique. L'initiative vient également en soutien et en complément de la mise en œuvre de la directive SRI en fournissant aux entreprises visées par celle-ci un moyen de prouver qu'elles satisfont aux exigences SRI dans l'ensemble de l'Union.

Le cadre européen de certification de cybersécurité dans le domaine des TIC, tel que proposé, est sans préjudice du règlement général sur la protection des données (RGPD)[49] et, en particulier, des dispositions pertinentes relatives à la certification[50] dans la mesure où elles s'appliquent à la sécurité du traitement de données à caractère personnel. Dernier point, mais non des moindres, les systèmes proposés dans le futur cadre européen devraient s'appuyer autant que possible sur des normes internationales, de manière à éviter de créer des entraves aux échanges et à garantir la cohérence avec les initiatives internationales.

[49] Règlement (UE) 2016/679 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).

[50] Notamment les articles 42 (Certification) et 43 (Organismes de certification), ainsi que les articles 57, 58 et 70 concernant, respectivement, les missions et les pouvoirs des autorités de contrôle indépendantes et les missions du comité européen de la protection des données.

1.5. Durée et incidence financière

☐ Proposition/initiative à **durée limitée**

– ☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

☒Proposition/initiative à **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de 2019 jusqu'en 2020,

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

1.6. Mode(s) de gestion prévu(s)[51]

☒ **Gestion directe** par la Commission (Titre III – Certification)

– ☐ Agences exécutives

☐ **Gestion partagée** avec les États membres

☒ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

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

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

☒ aux organismes visés aux articles 208 et 209 (Titre II – ENISA);

☐ 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.

Remarques

Le règlement porte sur les points suivants: – le titre II du règlement proposé examine le mandat de l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information (ENISA) en lui donnant un rôle important de certification, tandis que – le titre III établit un cadre pour la création de systèmes européens de certification de cybersécurité des produits et services TIC, dans lequel l'ENISA joue un rôle capital.

[51] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Le suivi débutera immédiatement après l'adoption de l'instrument juridique et mettra l'accent sur son application. La Commission organisera des réunions avec l'ENISA, des représentants des États membres (par exemple, le groupe d'experts) et les parties prenantes concernées, notamment en vue de faciliter la mise en œuvre des dispositions relatives à la certification telles que la mise en place du conseil.

La première évaluation devrait avoir lieu 5 ans après l'entrée en vigueur de l'instrument juridique, pour autant que l'on dispose de données suffisantes. L'instrument juridique comprend une clause explicite d'évaluation et de révision [article XXX] prévoyant que la Commission procédera à une évaluation indépendante. 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 du règlement et sa valeur ajoutée. De nouvelles évaluations devraient avoir lieu tous les cinq ans. La Commission appliquera ses méthodes d'évaluation figurant dans l'initiative «Mieux légiférer». Ces évaluations seront effectuées à l'aide d'études ciblées, de discussions d'experts, d'études et de vastes consultations des parties prenantes.

Le directeur exécutif de l'ENISA devrait présenter tous les deux ans au conseil d'administration une évaluation ex post des activités de l'ENISA. L'Agence devrait également élaborer un plan d'action de suivi relatif aux conclusions des évaluations rétrospectives et présenter des rapports à la Commission tous les deux ans sur les progrès accomplis. Le conseil d'administration devrait prêter une attention vigilante au suivi adéquat de ces conclusions.

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

Les principales sources de données pour le suivi prévu seraient l'ENISA, le Groupe européen de certification de cybersécurité, le groupe de coopération, le réseau des CSIRT et les autorités des États membres. Outre les données issues des rapports (y compris les rapports d'activité annuels) de l'ENISA, du Groupe européen de certification de cybersécurité, du groupe de coopération et du réseau des CSIRT, des outils de collecte de données spécifiques seront utilisés en cas de besoin (par exemple, des enquêtes auprès des autorités nationales, des sondages Eurobaromètre ainsi que les rapports découlant de la campagne du «mois de la cybersécurité» et des exercices paneuropéens).

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Les risques identifiés sont limités: une agence de l'Union existe déjà et son mandat prévoira des domaines d'action bien délimités. Sont renforcés les domaines où l'Agence apporte une valeur ajoutée avérée, et sont ajoutés les nouveaux domaines où un soutien s'impose vu les priorités et instruments politiques nouveaux, en particulier la directive SRI, le réexamen de la

stratégie de cybersécurité de l'UE, le prochain plan de l'UE en matière de cybersécurité pour la coopération en cas de crise et la certification de sécurité en matière de TIC.

Par conséquent, la proposition précise les fonctions de l'Agence et conduit à des gains d'efficacité. L'accroissement des compétences opérationnelles et des missions ne présente aucun risque réel, car il s'agirait de compléter l'action des États membres et de les soutenir, à leur demande et concernant des services limités et prédéterminés.

En outre, le modèle proposé de l'Agence, conformément à l'approche commune, garantit l'existence d'un contrôle suffisant pour s'assurer que l'ENISA s'emploie à la réalisation de ses objectifs. Les risques opérationnels et financiers des modifications proposées semblent être limités.

Dans le même temps, il est nécessaire d'assurer des ressources financières adéquates pour que l'ENISA remplisse les missions qui lui sont confiées par le nouveau mandat, y compris dans le domaine de la certification.

2.2.2. Moyen(s) de contrôle prévu(s)

Les comptes de l'Agence seront soumis à l'approbation de la Cour des Comptes et sujets à la procédure de décharge, et des audits sont envisagés.

Les activités de l'Agence sont également soumises au contrôle du médiateur, conformément aux dispositions de l'article 228 du traité.

Voir le point 2.1 et le point 2.2.1 ci-dessus.

2.3. Mesures de prévention des fraudes et irrégularités

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

Les mesures de prévention et de protection de l'ENISA s'appliqueraient, et notamment:

- Le contrôle du paiement de tout service ou étude nécessaire est effectué par le personnel de l'Agence avant le paiement, compte tenu de toute obligation contractuelle, des principes économiques et des bonnes pratiques financières ou de gestion. Des dispositions antifraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.

- Aux fins de la lutte contre la fraude, la corruption et les autres actes illégaux, les dispositions du règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil du 25 mai 1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) s'appliquent sans restriction.

- Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, l'Agence 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) et adopte immédiatement les dispositions appropriées applicables à l'ensemble de son personnel.

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)

- Lignes budgétaires existantes

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

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
		CD/CND[52].	de pays AELE[53]	de pays candidats[54]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
1a Compétitivité pour la croissance et l'emploi	09.0203 ENISA et certification des technologies de l'information et des communications en matière de cybersécurité	C.D.	OUI	NON	NON	NON
5 Dépenses administratives]	09.0101 Dépenses liées au personnel en activité dans le domaine des réseaux de communication, du contenu et des technologies 09.0102 Dépenses liées au personnel externe en activité dans le domaine des réseaux de	CND	NON	NON	NON	NON

52 CD = crédits dissociés / CND = crédits non dissociés.

53 AELE: Association européenne de libre-échange.

54 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

	communication, du contenu et des technologies 09.010211 Autres dépenses de gestion					

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	1a	Compétitivité pour la croissance et l'emploi

ENISA			**Base** **2017 (31/12/2016)**		**2019** ***(à partir du 1.7.2019)***	**2020**	**2021**	**2022**	**TOTAL**
Titre 1: Dépenses de personnel *(y compris les dépenses relatives au recrutement de personnel, à la formation, aux infrastructures socio-médicales et aux prestations externes)*	Engagements	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Paiements	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Titre 2: Dépenses d'infrastructure et de fonctionnement	Engagements	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Paiements	(2a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Titre 3: Dépenses opérationnelles	Engagements	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Paiements	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTAL des crédits pour l'ENISA	Engagements	=1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Paiements	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rubrique du cadre financier pluriannuel	**5**	«Dépenses administratives»

En Mio EUR (à la 3e décimale)

		2019 *(à partir du 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAL**
DG: CNECT						
• Ressources humaines		0,216	0,846	0,846	0,846	**2,754**
• Autres dépenses administratives		0,102	0,235	0,238	0,242	**0,817**
TOTAL DG CNECT	Crédits	0,318	1,081	1,084	1,088	**3,571**

Les frais de personnel ont été calculés en fonction de la date de recrutement prévue (début de l'emploi prévu le 1.7.2019).

Les perspectives en matière de ressources au-delà de 2020 sont indicatives et sans préjudice des propositions présentées par la Commission pour le cadre financier pluriannuel post-2020.

TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	(Total engagements = Total paiements)	0,318	1,081	1,084	1,088	**3,571**

En Mio EUR (à la 3e décimale)

	2019	**2020**	**2021**	**2022**	**TOTAL**

TOTAL des crédits pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements	16,868	21,727	23,332	24,11	**86,038**
	Paiements	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Incidence estimée sur les crédits de l'Agence

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

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

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAL**
Développer les moyens et la préparation des États membres et des entreprises	1,408	1,900	1,931	1,969	7,208
Améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE	0,939	1,266	1,288	1,313	4,806
Accroître les moyens au niveau de l'UE pour compléter l'action des États membres, notamment en cas de crise transfrontière dans le domaine de la cybersécurité	0,704	0,950	0,965	0,985	3,604
Davantage sensibiliser les particuliers et les entreprises aux questions de cybersécurité	0,704	0,950	0,965	0,985	3,604
Susciter davantage la confiance dans le marché unique numérique et l'innovation numérique en accroissant globalement la transparence de l'assurance de la cybersécurité des produits et services TIC.	0,939	1,266	1,288	1,313	4,806
COÛT TOTAL	4,694	6,332	6,437	6,565	24,028

[55] Le présent tableau n'expose que les dépenses opérationnelles prévues au titre 3.

3.2.3. Incidence estimée sur les ressources humaines de l'Agence

3.2.3.1. Synthèse

– ☐ 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)

	3e et 4e trimestres 2019	**2020**	**2021**	**2022**
Agents temporaires (grades AD)	4,242	5,695	6,381	6,709
Agents temporaires (grades AST)	1,601	1,998	2,217	2,217
Agents contractuels	2,041	2,041	2,041	2,041
Experts nationaux détachés	0,306	0,447	0,656	0,796
TOTAL	**8,190**	**10,181**	**11,295**	**11,763**

Les frais de personnel ont été calculés en fonction de la date de recrutement prévue (plein emploi supposé à partir du 1.1.2019 pour le personnel actuel de l'ENISA). Pour le nouveau personnel, emploi progressif débutant le 1.7.2019 et plein emploi atteint en 2022. Les perspectives en matière de ressources au-delà de 2020 sont indicatives et sans préjudice des propositions présentées par la Commission pour le cadre financier pluriannuel post-2020.

Incidence estimée sur le personnel (ETP supplémentaires) – Tableau des effectifs

Groupe de fonctions et grade	2017 **Actuel ENISA**	3e et 4e trimestres 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	

AD5					
Total AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Total AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Total AST/SC					
TOTAL GÉNÉRAL	48	12	10	7	3

Les missions du personnel supplémentaire AD/AST afin de réaliser les objectifs de l'instrument sont décrites au point 1.4.2:

Missions	AD	AST	END	Total
Politique et dotation de moyens	8	1		9
Coopération opérationnelle	8	1	7	16
Certification (missions relatives au marché)	9	3	2	14
Connaissances, information et sensibilisation	1	1		2
TOTAL	26	6	9	41

Description des tâches à effectuer:

Missions	**Ressources supplémentaires nécessaires**
Élaboration et mise en œuvre de la politique de l'UE & dotation de moyens	Les missions consisteraient notamment à assister le groupe de coopération, à soutenir une application cohérente de la directive SRI à travers les frontières, à rendre compte régulièrement de l'état d'avancement de la mise en œuvre du cadre juridique de l'UE, à conseiller et coordonner des

	initiatives sectorielles de cybersécurité, y compris dans les domaines de l'énergie, des transports (par exemple, transport aérien/routier/maritime/véhicules connectés), de la santé, de la finance, à faciliter la création de centres d'échange et d'analyse d'informations (ISAC) dans divers secteurs.
Coopération opérationnelle et gestion des crises	**Les missions comprendraient les éléments suivants:** Assurer le secrétariat du réseau des CSIRT en veillant, entre autres, au bon fonctionnement de l'infrastructure informatique du réseau des CSIRT et des canaux de communication. Assurer une coopération structurée avec la CERT-UE, la CE3 et d'autres instances de l'UE. Organiser des **exercices «Cyber Europe»**[56] – les missions consistent à augmenter la fréquence des exercices (chaque année au lieu de tous les deux ans) et à assurer que les incidents sont examinés du début à la fin. **Assistance technique** – les missions comprendraient une coopération structurée avec la CERT-UE afin d'apporter une assistance technique en cas d'incidents significatifs et à faciliter l'analyse des incidents. Il s'agirait notamment d'offrir aux États membres une assistance pour gérer les incidents et analyser les vulnérabilités, artefacts et incidents. Faciliter la coopération entre les différents États membres en matière d'intervention en cas d'urgence en analysant et en agrégeant les rapports de situation nationaux établis à partir des informations fournies à l'Agence par les États membres et d'autres entités. **Plan de coordination des réactions aux incidents transfrontières de cybersécurité majeurs** – l'Agence contribuera à élaborer une réaction concertée, au niveau de l'Union et des États membres, en cas d'incidents ou de crises transfrontières majeurs dans le domaine de la cybersécurité, par une série de missions allant de

[56] «Cyber Europe» est l'exercice de cybersécurité le plus vaste et le plus complet à ce jour dans l'UE, impliquant plus de 700 professionnels de la cybersécurité provenant de l'ensemble des 28 États membres. Il a lieu tous les deux ans. L'évaluation de l'ENISA et la stratégie de cybersécurité de 2013 de l'UE attirent l'attention sur le fait que de nombreuses parties prenantes préconisent de l'organiser dorénavant tous les ans vu la rapidité d'évolution des cybermenaces. Cette augmentation de fréquence n'est toutefois pas réalisable à l'heure actuelle, compte tenu des ressources limitées de l'Agence.

	la contribution en vue de former une appréciation de la situation à l'échelle de l'Union à la mise à l'essai de plans de coopération en cas d'incident. **Enquêtes techniques ex post sur les incidents** – procéder ou contribuer à des enquêtes techniques ex post sur les incidents en coopération avec le réseau des CSIRT dans le but de formuler des recommandations et de renforcer les capacités, sous la forme de rapports publics afin de mieux prévenir les incidents futurs.
Missions relatives au marché (normalisation, certification de cybersécurité)	Les missions consisteraient entre autres à soutenir activement les travaux entrepris dans le contexte du Cadre de certification, notamment en fournissant une expertise technique pour l'élaboration de systèmes européens de certification de cybersécurité candidats. Elles consisteront aussi à soutenir l'élaboration et la mise en œuvre de la politique de l'Union dans les domaines de la normalisation, la certification et l'«observatoire du marché», ce qui nécessitera de faciliter l'adoption de normes de gestion des risques pour les produits, réseaux et services électroniques, et à conseiller les opérateurs de services essentiels et les fournisseurs de service numérique sur les exigences techniques de sécurité. Les missions consisteront également à fournir une analyse des principales tendances dans le marché de la cybersécurité.
Connaissances, information et sensibilisation	Afin de faciliter l'accès à des informations mieux structurées sur les risques de cybersécurité et les solutions possibles, la proposition confère à l'Agence une nouvelle tâche consistant à mettre sur pied et à gérer le «pôle d'information» de l'Union. Les missions consisteraient notamment à regrouper, organiser et mettre à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la sécurité des réseaux et des systèmes d'information, en particulier sur la cybersécurité, fournies par les institutions, organes et organismes de l'UE. Les tâches consisteraient également à soutenir les activités de l'ENISA dans le domaine de la sensibilisation afin de permettre à l'Agence d'intensifier les efforts.

3.2.3.2. Besoins estimés en ressources humaines pour la DG de tutelle

– ☐ 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 valeur entière (ou au plus avec une décimale)

		Augmentation de personnel			
	Ligne de base 2017	3e/4e trimestre 2019	2020	2021	2020
• **Emplois du tableau des effectifs (fonctionnaires et agents temporaires)**					
09 01 01 01 (au siège et dans les bureaux de représentation de la Commission)	1	2	3		
• **Personnel externe (en équivalents temps plein: ETP)**[57]					
09 01 02 01 (AC, END, INT de l'enveloppe globale)	1	2			
TOTAL		**4**	**3**		

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Représenter la Commission au conseil d'administration de l'Agence. Rédiger l'avis de la Commission sur le document unique de programmation de l'ENISA et surveiller la mise en œuvre de ce dernier. Superviser la préparation du budget de l'Agence et assurer le suivi de son exécution. Aider l'Agence à développer ses activités conformément aux politiques de l'Union, y compris en participant aux réunions pertinentes. Superviser la mise en œuvre du cadre pour les systèmes européens de certification de cybersécurité des produits et services TIC. Maintenir des contacts avec les États membres et les autres parties prenantes concernées en ce qui concerne les travaux de certification. Coopérer avec l'ENISA en ce qui concerne les systèmes candidats. Élaborer des systèmes européens de cybersécurité candidats.

[57] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JED = jeune expert en délégation.

Personnel externe	Voir ci-dessus

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

– ☐ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

– ☒ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

La proposition nécessite une reprogrammation de l'article 09 02 03 en raison de la révision du mandat de l'ENISA, qui confère à l'Agence de nouvelles missions liées, entre autres, à l'application de la directive SRI et du Cadre européen de certification de cybersécurité. Les montants correspondants:

Année	Prévu	Demandé
2019	10,739	16,550
2020	10,954	20,646
2021	Sans objet	22,248*
2022	Sans objet	23,023*

* Il s'agit d'une estimation. Le financement de l'UE au-delà de 2020 sera examiné dans le contexte d'un débat au sein de la Commission sur toutes les propositions pour la période après 2020. Cela signifie que lorsqu'elle aura présenté sa proposition concernant le prochain cadre financier pluriannuel, la Commission présentera une fiche financière législative modifiée tenant compte des conclusions de l'analyse d'impact[58].

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[59].

3.2.5. Participation de tiers au financement

– ☐ La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

– ☒ La proposition/l'initiative prévoit un cofinancement estimé ci-après:

[58] Lien vers la page de l'évaluation d'impact

[59] Voir les articles 11 et 17 du règlement (UE, Euratom) nº 1311/2013 du Conseil fixant le cadre financier pluriannuel pour la période 2014-2020.

	Année **2019**	Année **2020**	Année **2021**	Année **2022**
AELE	p.m[60].	p.m.	p.m.	p.m.

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 recettes diverses

[60] Le montant exact pour les années suivantes sera connu lorsque le facteur de proportionnalité de l'AELE aura été fixé pour l'année en question.