Parlement européen
2019-2024

Document de séance

A9-0426/2023

8.12.2023

***I
RAPPORT

sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Commission de l'industrie, de la recherche et de l'énergie

Rapporteure: Lina Gálvez Muñoz

Légende des signes utilisés

*	Procédure de consultation
***	Procédure d'approbation
***I	Procédure législative ordinaire (première lecture)
***II	Procédure législative ordinaire (deuxième lecture)
***III	Procédure législative ordinaire (troisième lecture)

(La procédure indiquée est fondée sur la base juridique proposée par le projet d'acte.)

Amendements à un projet d'acte

Amendements du Parlement présentés en deux colonnes

Les suppressions sont signalées par des ***italiques gras*** dans la colonne de gauche. Les remplacements sont signalés par des ***italiques gras*** dans les deux colonnes. Le texte nouveau est signalé par des ***italiques gras*** dans la colonne de droite.

Les première et deuxième lignes de l'en-tête de chaque amendement identifient le passage concerné dans le projet d'acte à l'examen. Si un amendement porte sur un acte existant, que le projet d'acte entend modifier, l'en-tête comporte en outre une troisième et une quatrième lignes qui identifient respectivement l'acte existant et la disposition de celui-ci qui est concernée.

Amendements du Parlement prenant la forme d'un texte consolidé

Les parties de textes nouvelles sont indiquées en ***italiques gras***. Les parties de texte supprimées sont indiquées par le symbole ▌ ou barrées. Les remplacements sont signalés en indiquant en ***italiques gras*** le texte nouveau et en effaçant ou en barrant le texte remplacé.
Par exception, les modifications de nature strictement technique apportées par les services en vue de l'élaboration du texte final ne sont pas marquées.

SOMMAIRE

Page

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Procédure législative ordinaire: première lecture)

Le Parlement européen,

– vu la proposition de la Commission au Parlement européen et au Conseil (COM(2023)0209),

– vu l'article 294, paragraphe 2, et les articles 173, paragraphe 3, et 322, paragraphe 1, point a), du traité sur le fonctionnement de l'Union européenne, conformément auxquels la proposition lui a été présentée par la Commission (C9-0136/2023),

– vu l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne,

– vu l'avis du Comité économique et social européen du 13 juillet 2023[1],

– vu l'article 59 de son règlement intérieur,

– vu les avis de la commission des affaires internationales et de la commission des transports et du tourisme,

– vu le rapport de la commission de l'industrie, de la recherche et de l'énergie (A9-0426/2023),

1. arrête la position en première lecture figurant ci-après;

2. approuve sa déclaration annexée à la présente résolution;

3. demande à la Commission de le saisir à nouveau, si elle remplace, modifie de manière substantielle ou entend modifier de manière substantielle sa proposition;

4. charge sa Présidente de transmettre la position du Parlement au Conseil et à la Commission ainsi qu'aux parlements nationaux.

[1] JO C 349 du 29.9.2023, p. 167.

Amendement 1

AMENDEMENTS DU PARLEMENT EUROPÉEN*

à la proposition de la Commission

2023/0109 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, *et modifiant le règlement (UE) 2021/694*

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 173, paragraphe 3, et son article 322, paragraphe 1, point a),

vu la proposition de la Commission européenne,

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

vu l'avis de la Cour des comptes[2],

vu l'avis du Comité économique et social européen[3],

vu l'avis du Comité des régions[4],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux***, mais qui créent dans le même temps de possibles vulnérabilités,*** dans tous les secteurs d'activité économique ***et de la démocratie***, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos administrations publiques, de nos entreprises et de nos citoyens par-delà les secteurs et les frontières.

(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, ***tant du point de vue des méthodes utilisées que des effets produits, au niveau de***

---

* Amendements: le texte nouveau ou modifié est signalé par des italiques gras; les suppressions sont signalées par le symbole ▌.

2 JO C […], […], p. […].

3 JO C , , p. .

4 JO C , , p. .

l'Union comme au niveau mondial, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques ***pour les économies ou les démocraties dans l'ensemble de l'Union*** nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique ***et*** criminels ▌ qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays. ***Une coopération étroite et coordonnée entre le secteur public, le secteur privé, le monde universitaire, la société civile et les médias est donc nécessaire. L'Union doit en outre coordonner sa réaction avec les institutions internationales et les partenaires internationaux de confiance et qui partagent ses principes. Les partenaires internationaux de confiance et qui partagent ses principes sont les pays qui partagent les valeurs de l'Union que sont la démocratie, la défense des droits humains, un multilatéralisme efficace et un ordre fondé sur des règles, en cohérence avec les cadres et accords de coopération internationale. Pour garantir la coopération avec les partenaires internationaux de confiance et qui partagent ses principes, ainsi que la protection contre les adversaires systémiques, les entités établies dans des pays tiers qui ne sont pas parties à l'accord sur les marchés publics (AMP) ne devraient pas être autorisées à participer à des passations de marché au titre du présent règlement.***

(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[5], il convient d'accroître la résilience des citoyens, des entreprises***, en particulier des micro-entreprises et des petites et moyennes entreprises (PME), y compris les jeunes pousses,*** et des entités exploitant des infrastructures critiques***, y compris les autorités locales et régionales,*** face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services***, et renforcer les capacités de développer des compétences en matière de cybersécurité,*** qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement***; il faut également*** aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité.

[5] https://futureu.europa.eu/fr/

(3 bis) Les cyberattaques ciblent souvent des services et infrastructures publics locaux, régionaux et nationaux. Les collectivités locales sont parmi les cibles les plus vulnérables aux cyberattaques en raison de la faiblesse de leurs ressources financières et humaines. Il est donc particulièrement important que les décideurs locaux soient sensibilisés à la nécessité d'améliorer la résilience numérique, d'accroître leur capacité à réduire les effets des cyberattaques et de saisir les possibilités offertes par le présent règlement.

(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[6], de la recommandation (UE) 2017/1584 de la Commission[7], de la directive 2013/40/UE du Parlement européen et du Conseil[8] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[9]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.

(5) En raison de l'augmentation des risques liés à la cybersécurité et de la complexité globale du panorama des menaces, ainsi que du risque évident de propagation rapide des incidents de cybersécurité d'un État membre à un autre et d'un pays tiers à l'Union, il est nécessaire de renforcer la solidarité au niveau de l'Union afin de mieux détecter les menaces et incidents de cybersécurité, de s'y préparer**,** d'y réagir ***et de se rétablir après de tels incidents***. Dans les conclusions du Conseil sur la posture cyber de l'Union, les États membres ont également invité la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité[10].

(6) La communication conjointe relative à la politique de cyberdéfense de l'UE[11], adoptée le 10 novembre 2022, a annoncé une initiative de l'Union en matière de cybersolidarité dont les objectifs sont les suivants: renforcer les capacités communes de détection,

---

6 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

7 Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

8 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

9 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

10 Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, approuvées par le Conseil lors de sa session du 23 mai 2022 (9364/22).

11 Communication conjointe au Parlement européen et au Conseil intitulée «La politique de cyberdéfense de l'UE» (JOIN(2022) 49 final).

d'appréciation de la situation et de réaction de l'Union en promouvant le déploiement ***d'un réseau*** de centres d'opérations de sécurité (SOC) de l'Union, constituer progressivement une réserve de cybersécurité au niveau de l'Union comprenant des services de fournisseurs privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'Union.

(7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des menaces et incidents de cybersécurité dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités ***de prévention et*** de réaction des États membres et de l'Union en cas d'incidents de cybersécurité importants et majeurs. Par conséquent, il convient d'établir: ***un réseau paneuropéen*** de SOC (le cyberbouclier européen), afin de mettre en place et de renforcer les capacités communes en matière de détection et d'appréciation de la situation***, de sorte à renforcer les capacités de l'Union en matière de détection des menaces et de partage des informations***; un mécanisme d'urgence dans le domaine de la cybersécurité, afin d'aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs et à y réagir, ainsi qu'à se rétablir immédiatement après de tels incidents; et un mécanisme d'analyse des incidents de cybersécurité, afin d'examiner et d'évaluer des incidents importants ou majeurs particuliers. Ces actions doivent s'entendre sans préjudice des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne (TFUE).

(8) Pour atteindre ces objectifs, il est également nécessaire de modifier certains points du règlement (UE) 2021/694 du Parlement européen et du Conseil[12]. Plus particulièrement, le présent règlement devrait modifier le règlement (UE) 2021/694 en ajoutant de nouveaux objectifs opérationnels relatifs au cyberbouclier européen et au mécanisme d'urgence dans le domaine de la cybersécurité à l'objectif spécifique 3 du programme pour une Europe numérique, qui vise à garantir la résilience, l'intégrité et la fiabilité du marché unique numérique, à renforcer les capacités de surveillance des cyberattaques et des cybermenaces et de réaction à celles-ci, ainsi qu'à renforcer la coopération transfrontière en matière de cybersécurité. À cela devraient s'ajouter les conditions spécifiques dans lesquelles une aide financière peut être accordée pour ces actions, et la définition des mécanismes de gouvernance et de coordination nécessaires pour atteindre les objectifs poursuivis. Parmi les autres modifications à apporter au règlement (UE) 2021/694 devraient figurer des descriptions des actions proposées au titre des nouveaux objectifs opérationnels, ainsi que des indicateurs mesurables servant à suivre la mise en œuvre de ces nouveaux objectifs opérationnels.

(9) Le financement des actions entreprises au titre du présent règlement devrait être prévu par le règlement (UE) 2021/694, qui devrait rester l'acte de base régissant les actions entrant dans le cadre de l'objectif spécifique 3 du programme pour une Europe numérique. Les conditions spécifiques de participation à chaque action devraient être définies dans les programmes de travail correspondants, conformément aux dispositions applicables du règlement (UE) 2021/694.

(9 bis) À la lumière des évolutions géopolitiques et de l'intensification des cybermenaces, et afin d'assurer la poursuite et le renforcement après 2027 des mesures définies dans le présent règlement, en particulier en ce qui concerne le cyberbouclier européen et

[12] Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240 (JO L 166 du 11.5.2021, p. 1).

le mécanisme européen d'urgence dans le domaine de la cybersécurité, il est nécessaire de prévoir une ligne budgétaire qui leur soit consacrée dans le cadre financier pluriannuel pour la période 2028-2034. Il convient que les États membres fassent en sorte de s'engager à soutenir toutes les mesures nécessaires pour réduire les menaces et incidents de cybersécurité dans l'ensemble de l'Union, ainsi que pour renforcer leur solidarité.

(10) Les règles financières horizontales adoptées par le Parlement européen et le Conseil sur la base de l'article 322 du TFUE s'appliquent au présent règlement. Ces règles sont énoncées dans le règlement ***(UE, Euratom) 2018/1046 du Parlement européen et du Conseil***[13] et fixent notamment les modalités relatives à l'établissement et à l'exécution du budget de l'Union, et organisent le contrôle de la responsabilité des acteurs financiers. Les règles adoptées sur la base de l'article 322 du TFUE comprennent également un régime général de conditionnalité pour la protection du budget de l'Union, tel qu'établi par le règlement (UE, Euratom) 2020/2092 du Parlement européen et du Conseil[14].

(11) Aux fins de la bonne gestion financière, il convient d'établir des règles spécifiques portant sur le report des crédits d'engagement et de paiement non utilisés. Tout en respectant le principe en vertu duquel le budget de l'Union est établi sur une base annuelle, il convient que le présent règlement prévoie, compte tenu de la nature imprévisible, exceptionnelle et spécifique de la situation en matière de cybersécurité, des possibilités de reporter des fonds non utilisés qui aillent au-delà de celles établies dans le règlement ***(UE, Euratom) 2018/1046***, afin d'optimiser la capacité du mécanisme d'urgence dans le domaine de la cybersécurité à aider les États membres à contrer efficacement les cybermenaces.

(11 bis) Le mécanisme d'urgence dans le domaine de la cybersécurité et la réserve de cybersécurité de l'UE créés par le présent règlement sont des initiatives nouvelles qui n'avaient donc pas été prévues lors de la mise en place du cadre financier pluriannuel pour la période 2021-2027; il convient de limiter autant que possible la réduction des fonds à destination d'autres priorités du programme pour une Europe numérique due au financement desdites initiatives. Il convient donc de réduire le montant des ressources financières consacrées à la réserve de cybersécurité de l'UE et de prélever celui-ci en premier lieu sur les marges non allouées sous les plafonds du cadre financier pluriannuel ou de le mobiliser au moyen des instruments spéciaux non thématiques du cadre financier pluriannuel. Il convient de réduire au minimum absolu toute affectation ou réallocation de fonds depuis des programmes existants afin de préserver les programmes existants, notamment Erasmus+, de toute répercussion préjudiciable et de garantir que ces programmes puissent parvenir aux objectifs qui leur ont été fixés.

---

13 ***Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE) nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 (JO L 193 du 30.7.2018, p. 1), ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=fr).***

14 ***Règlement (UE, Euratom) 2020/2092 du Parlement européen et du Conseil du 16 décembre 2020 relatif à un régime général de conditionnalité pour la protection du budget de l'Union (JO L 433 I du 22.12.2020, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/oj?locale=fr).***

(12) Afin de prévenir, évaluer et contrer les menaces et incidents de cybersécurité***, et de se rétablir après leur survenue,*** de manière plus efficace, il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures. ***Une approche proactive en vue de l'identification, de l'atténuation et de la prévention des cybermenaces potentielles suppose des capacités accrues en matière de détection avancée, qui sont nécessaires pour mettre un terme aux menaces avancées persistantes. Le renseignement en matière de menaces recouvre la collecte, l'analyse et l'interprétation des informations afin de comprendre les menaces et risques potentiels. L'analyse et le croisement de grandes quantités de données permet de découvrir des schémas, des tendances et des indicateurs de compromission, et ainsi éventuellement de révéler des activités malveillantes ou des vulnérabilités.*** Il convient de mettre en place ***un réseau*** de SOC (le cyberbouclier européen), comprenant plusieurs plateformes transfrontières interopérables qui regroupent chacune plusieurs SOC nationaux. Une telle infrastructure devrait servir les intérêts et les besoins des États et de l'Union en matière de cybersécurité, en tirant parti de technologies de pointe pour la collecte et l'analyse avancées des données, en renforçant les capacités de détection et de gestion des incidents de cybersécurité et en permettant une appréciation de la situation en temps réel. ***Un SOC national est une capacité centralisée chargée de la collecte continue de renseignements en matière de menaces ainsi que de l'amélioration de la posture de cybersécurité des entités sous juridiction nationale par la prévention, la détection et l'analyse des menaces de cybersécurité.*** Le réseau de SOC devrait également permettre d'améliorer la détection des menaces et incidents de cybersécurité, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion de crise dans l'UE, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) tel que défini dans la directive (UE) 2022/2555 du Parlement européen et du Conseil[15].

(13) Chaque État membre devrait***, en vue de participer au cyberbouclier,*** désigner un organisme public au niveau national chargé de coordonner les activités de détection des cybermenaces sur son territoire. ***Les États membres sont encouragés à intégrer la capacité du SOC national à leur structure et à leur gouvernance de cybersécurité existantes afin d'éviter de créer des niveaux de gouvernance supplémentaires, ainsi qu'à harmoniser le présent règlement avec les actes législatifs en vigueur, notamment la directive (UE) 2022/2555.*** Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation ***d'entités publiques et privées, notamment les SOC nationaux,*** au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle. ***Il convient que les SOC nationaux renforcent la coopération et le partage d'informations entre les entités publiques et privées afin de décloisonner la communication. Ce faisant, les SOC nationaux pourront soutenir la création de modèles d'échange de données et devraient permettre et encourager le partage d'informations dans un environnement sûr et de confiance. Une coopération étroite***

[15] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

et coordonnée entre les entités publiques et privées est essentielle pour renforcer la résilience de l'Union dans le domaine de la cybersécurité.

(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres afin de tirer pleinement parti des avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, ***y compris par la collecte et le partage de données et d'informations sur de possibles piratages malveillants, des menaces et exploitations malveillantes nouvelles qui n'ont pas encore été activées lors de cyberincidents, ainsi que des travaux d'analyse,*** notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, à l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement ***sûr et*** de confiance***, avec l'aide de l'Agence de l'Union européenne pour la cybersécurité (ENISA), en matière de coopération opérationnelle entre les États membres***. Les SOC transfrontières devraient ***permettre et encourager le partage d'informations dans un environnement sûr et de confiance et*** apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les centres de réponse aux incidents de sécurité informatique (CSIRT) et sur d'autres acteurs pertinents, et en les complétant.

(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant ***s'intégrer à l'infrastructure de cybersécurité existante, en particulier au*** réseau des CSIRT***,*** en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, ***et notamment de leurs SOC,*** en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant ***à la souveraineté technologique de l'Union, à son autonomie stratégique ouverte, à sa compétitivité et à sa résilience, ainsi qu'au développement d'un important écosystème de cybersécurité, y compris par la coopération avec les partenaires internationaux de confiance et qui partagent ses principes***.

(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs (par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures critiques)***, afin de favoriser le décloisonnement de la communication***. ***Ce faisant, les SOC transfrontières pourraient également soutenir la création de modèles d'échange de données dans l'ensemble de l'Union.*** Les informations échangées entre les participants à un SOC transfrontière pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités***, y compris par la***

collecte et le partage de données et d'informations sur de possibles piratages malveillants, des menaces et exploitations malveillantes nouvelles qui n'ont pas encore été activées lors de cyberincidents, ainsi que des travaux d'analyse. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.

(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil[16], ainsi que sa responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'Union pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993 ***du Conseil***[17]. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT et à la Commission***, conformément à la directive (UE) 2022/2555***. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations transmises.

(18) Les entités participant au cyberbouclier européen devraient assurer un haut niveau d'interopérabilité entre elles, notamment, s'il y a lieu, en matière de formats des données, de taxonomie, d'outils de gestion et d'analyse des données et de sécurité des canaux de communication, ainsi qu'un niveau minimal de sécurité de la couche application, un tableau d'appréciation de la situation et des indicateurs. L'adoption d'une taxonomie commune et l'élaboration d'un modèle pour les rapports de situation visant à décrire les causes techniques et les conséquences des incidents de cybersécurité devraient tenir compte des travaux en cours sur la notification des incidents dans le contexte de la mise en œuvre de la directive (UE) 2022/2555.

(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement ***sûr et*** de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et

---

16 ***Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (Texte présentant de l'intérêt pour l'EEE) (***JO L 347 du 20.12.2013, p. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

17 ***Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (*****JO L 320 du 17.12.2018, p. 28,*** ***ELI: https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj?locale=fr).***

d'infrastructures de pointe hautement sécurisés***, ainsi que d'un personnel qualifié***. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.

(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer la souveraineté technologique de l'Union***, son autonomie stratégique ouverte, sa compétitivité et sa résilience, ainsi que le développement d'un important écosystème de cybersécurité de l'Union***. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. ***L'intelligence artificielle produit son efficacité maximale lorsqu'elle est couplée à l'analyse humaine. Une main-d'œuvre qualifiée reste donc essentielle à la mise en commun des données de haute qualité.*** Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[18].

(21) Bien que le cyberbouclier européen soit un projet civil, le renforcement des capacités civiles de détection et d'appréciation de la situation pour la protection des infrastructures critiques pourrait aussi profiter à la communauté de cyberdéfense. Les SOC transfrontières, avec le soutien de la Commission et du Centre de compétences européen en matière de cybersécurité (ECCC) et en coopération avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant»), devraient progressivement élaborer des protocoles et des normes spécifiques ***en matière de conditions d'accès et de garanties*** afin de permettre une coopération avec la communauté de la cyberdéfense, y compris en ce qui concerne les conditions de vérification et de sécurité***, tout en respectant le caractère civil des institutions et la destination des financements, de sorte que les fonds mis à disposition de la communauté de défense soient utilisés***. La mise en place du cyberbouclier européen devrait s'accompagner d'une réflexion qui permette une collaboration future avec les réseaux et plateformes de partage d'informations au sein de la communauté de cyberdéfense, en étroite coopération avec le haut représentant ***et dans le plein respect des droits et des libertés***.

(22) Le partage d'informations entre les participants au cyberbouclier européen devrait respecter les exigences juridiques en vigueur, et en particulier le droit de l'Union et le droit national en matière de protection des données, ainsi que les règles de concurrence de l'Union régissant l'échange d'informations. Le destinataire des informations devrait mettre en œuvre, dans la mesure où le traitement des données à caractère personnel est nécessaire, des mesures techniques et organisationnelles garantissant les droits et libertés des personnes concernées, détruire les données dès qu'elles ne sont plus nécessaires à la finalité indiquée et informer l'organisme mettant les données à disposition que ces données ont été détruites.

(23) Sans préjudice de l'article 346 du TFUE, l'échange d'informations considérées comme confidentielles en application ***du droit de l'Union ou du droit national*** devrait se limiter au minimum nécessaire et être proportionné à l'objectif de cet échange. L'échange de

[18] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3, ***ELI: https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=fr***).

telles informations devrait préserver la confidentialité des informations et protéger la sécurité et les intérêts commerciaux des entités concernées, dans le plein respect des secrets commerciaux et d'affaires.

(24) Compte tenu de l'augmentation des risques et du nombre d'incidents touchant les États membres, il est nécessaire de mettre en place un instrument de soutien en cas de crise visant à améliorer la résilience de l'Union face aux incidents de cybersécurité importants et majeurs et à compléter les mesures prises par les États membres au moyen d'une aide financière d'urgence destinée à la préparation, à la réaction et au rétablissement immédiat des services essentiels. Cet instrument devrait permettre de déployer rapidement ***et efficacement*** de l'aide, dans des circonstances définies et des conditions claires, et permettre une surveillance et une évaluation minutieuses de l'utilisation des ressources. Si la responsabilité première en matière de prévention, de préparation et de réaction face aux incidents et aux crises de cybersécurité incombe aux États membres, le mécanisme d'urgence dans le domaine de la cybersécurité promeut la solidarité entre les États membres, conformément à l'article 3, paragraphe 3, du traité sur l'Union européenne (TUE).

(25) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement immédiat en cas d'incidents de cybersécurité importants et majeurs, tels que les services fournis par l'Agence de l'Union européenne pour la cybersécurité (ENISA) conformément à son mandat, la réaction et l'assistance coordonnée du réseau des CSIRT, les mesures d'atténuation apportées par EU-CyCLONe, et l'assistance mutuelle que se prêtent les États membres notamment au titre de l'article 42, paragraphe 7, du TUE, ainsi que dans le contexte des équipes d'intervention rapide[19] en cas d'incident informatique de la CSP et des équipes de réaction rapide en cas de menaces hybrides. Ce mécanisme devrait faire en sorte que des moyens spécialisés soient mis à disposition pour soutenir la préparation et la réaction aux incidents de cybersécurité dans toute l'Union et dans les pays tiers.

(26) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination de la réaction aux crises au niveau de l'Union, en particulier le MPCU[20], l'IPCR[21], et la directive (UE) 2022/2555. Il pourrait contribuer aux actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du TUE ou dans les situations définies à l'article 222 du TFUE, ou les compléter. Le recours à cet instrument devrait également être coordonné, s'il y a lieu, avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatique.

(27) L'aide apportée dans le cadre du présent règlement devrait appuyer et compléter les mesures prises par les États membres au niveau national. À cette fin, il est nécessaire d'assurer une coopération et une consultation étroites entre la Commission***, l'ENISA*** et les États membres touchés. Lorsqu'un État membre sollicite une aide au titre du

[19] Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants.

[20] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

[21] Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR); conformément à la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

mécanisme d'urgence dans le domaine de la cybersécurité, il devrait fournir des informations pertinentes permettant de justifier sa demande ***d'***aide.

(28) La directive (UE) 2022/2555 impose aux États membres de désigner ou d'établir une ou plusieurs autorités de gestion des crises ***de cybersécurité*** et de veiller à ce qu'elles disposent de ressources suffisantes pour s'acquitter de leurs tâches de manière effective et efficace. Elle exige aussi que les États membres recensent les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise et qu'ils adoptent un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Les États membres sont également tenus de mettre en place un ou plusieurs CSIRT, qui sont chargés de la gestion des incidents selon un processus bien défini et qui couvrent au moins les secteurs, les sous-secteurs et les types d'entités relevant du champ d'application de ladite directive, ainsi que de veiller à ce que les CSIRT disposent de ressources suffisantes pour s'acquitter efficacement de leurs tâches. Le présent règlement est sans préjudice du rôle de la Commission, chargée de garantir que les États membres respectent les obligations qui leur incombent en vertu de la directive (UE) 2022/2555. Le mécanisme d'urgence dans le domaine de la cybersécurité devrait fournir une assistance dans le cadre des mesures destinées à renforcer la préparation ainsi que des mesures de réaction visant à atténuer les effets des incidents de cybersécurité importants et majeurs, à soutenir un rétablissement immédiat ou à rétablir le fonctionnement des services essentiels.

(29) Dans le cadre des mesures de préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE); l'évaluation coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du

Parlement européen et du Conseil[22]. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

(30) En outre, le mécanisme d'urgence dans le domaine de la cybersécurité devrait proposer une aide dans le cadre d'autres mesures de préparation et soutenir la préparation dans d'autres secteurs, qui ne sont pas pris en compte par les tests coordonnés auxquels sont soumises les entités actives dans des secteurs hautement critiques. Ces mesures pourraient inclure divers types d'activités nationales de préparation.

(31) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait également apporter une assistance dans le cadre de mesures de réaction aux incidents visant à atténuer les effets des incidents de cybersécurité importants et majeurs, à soutenir un rétablissement immédiat ou à rétablir le fonctionnement des services essentiels. Il devrait, s'il y a lieu, compléter le MPCU afin d'assurer une approche globale en matière de réaction aux effets des incidents de cybersécurité sur les citoyens.

(32) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir les États membres lorsqu'ils apportent une assistance à un État membre touché par un incident de cybersécurité important ou majeur, y compris l'assistance fournie par le réseau des CSIRT en vertu de l'article 15 de la directive (UE) 2022/2555. Les États membres apportant une assistance devraient être en mesure de demander que les coûts liés à l'envoi d'équipes d'experts dans le cadre de l'assistance mutuelle soient couverts. Les coûts éligibles pourraient inclure les frais de déplacement et de logement ainsi que les indemnités journalières des experts en cybersécurité.

(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services, ***tout en renforçant la résilience de l'Union, notamment la participation de fournisseurs européens de services de sécurité gérés qui sont des PME, en veillant à la création d'un écosystème de la cybersécurité, y compris des micro-entreprises, des PME, notamment des jeunes pousses, grâce à des investissements dans la recherche et l'innovation qui permettront d'élaborer des technologies de pointe, par exemple relatives à l'informatique en nuage et à l'intelligence artificielle***. ***Les fournisseurs de confiance, dont les PME, devraient pouvoir coopérer les uns avec les autres afin de satisfaire aux critères susmentionnés.*** Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. ***Il convient donc que la réserve de cybersécurité incite à investir dans la recherche et l'innovation afin d'encourager le développement de ces technologies. Le cas échéant, des exercices communs réunissant les fournisseurs de confiance et les utilisateurs potentiels de la réserve de cybersécurité pourraient être menés afin de garantir le bon fonctionnement de la réserve.*** Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser

[22] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires. ***La Commission devrait garantir la participation et des échanges approfondis avec les États membres afin d'éviter les doubles emplois avec des initiatives similaires, y compris au sein de l'Organisation du traité de l'Atlantique Nord (OTAN).***

(34) La sélection des fournisseurs de services privés qui proposeront des services dans le cadre de la réserve de cybersécurité de l'UE nécessite de définir un ensemble de critères minimaux à inclure dans l'appel d'offres visant à sélectionner ces fournisseurs, afin de garantir que les besoins des autorités des États membres et des entités actives dans des secteurs critiques ou hautement critiques sont satisfaits. ***La participation de petits prestataires, actifs aux niveaux régional et local, devrait être encouragée.***

(35) Aux fins de la mise en place de la réserve de cybersécurité de l'UE, la Commission pourrait envisager de demander à l'ENISA de préparer un schéma de certification candidat, conformément au règlement (UE) 2019/881, pour les services de sécurité gérés dans les domaines couverts par le mécanisme d'urgence dans le domaine de la cybersécurité. ***Il convient que l'ENISA soit dotée de financements supplémentaires suffisants pour pouvoir remplir les missions supplémentaires qui découlent de la présente disposition.***

(36) Dans le droit fil des objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents importants et majeurs poursuivis par le présent règlement, EU-CyCLONe, le réseau des CSIRT ou la Commission devraient être en mesure de demander à l'ENISA d'analyser et d'évaluer les menaces, vulnérabilités et mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA devrait établir un rapport d'analyse, en collaboration avec les parties prenantes concernées, notamment les représentants du secteur privé, les États membres, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En ce qui concerne le secteur privé, l'ENISA met en place des canaux d'échange d'informations avec des fournisseurs spécialisés, notamment des fournisseurs de solutions de sécurité gérées et des vendeurs, afin de contribuer à sa mission, qui consiste à atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. En s'appuyant sur la collaboration avec les parties prenantes, y compris avec le secteur privé, les rapports d'analyse portant sur des incidents spécifiques devraient servir à évaluer les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits. Il convient d'accorder une attention particulière aux informations et aux enseignements transmis par les fournisseurs de services de sécurité gérés qui font preuve du plus haut niveau d'intégrité professionnelle, d'impartialité et d'expertise technique requise, comme l'exige le présent règlement. Le rapport devrait être communiqué à EU-CyCLONe, au réseau des CSIRT et à la Commission, et devrait être intégré à leurs travaux. Lorsque l'incident en question touche un pays tiers, la Commission devrait également transmettre le rapport au haut représentant.

(37) Compte tenu de la nature imprévisible des cyberattaques, du fait qu'elles ne se limitent souvent pas à une zone géographique déterminée et qu'elles présentent un risque élevé de propagation, le renforcement de la résilience des pays voisins et leur capacité à réagir

efficacement à des incidents de cybersécurité importants et majeurs contribuent à la protection de l'Union dans son ensemble. Par conséquent, les pays tiers associés au programme pour une Europe numérique peuvent recevoir l'aide de la réserve de cybersécurité de l'UE lorsque leur accord d'association à ce programme le prévoit. Le soutien apporté à ces pays tiers associés devrait être financé par l'Union dans le cadre des partenariats et des instruments de financement concernés pour ces pays. Il devrait couvrir les services correspondant à la réaction et au rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. Les conditions relatives à la réserve de cybersécurité de l'UE et aux fournisseurs de confiance fixées dans le présent règlement devraient s'appliquer au soutien apporté aux pays tiers associés au programme pour une Europe numérique.

(37 bis) Les pays tiers pourraient avoir accès à des ressources et à un soutien en vertu du présent règlement, en utilisant le soutien de la réserve de cybersécurité de l'UE en réaction aux incidents. En outre, les fournisseurs de services de réaction aux incidents de pays tiers, notamment de pays tiers associés au programme pour une Europe numérique, ou d'autres pays partenaires internationaux, et de pays membres de l'OTAN, peuvent jouer un rôle utile pour ce qui est de fournir des services spécifiques au sein de la réserve de cybersécurité de l'Union. Par dérogation au règlement (UE, Euratom) 2018/1046, afin de renforcer la souveraineté technologique de l'Union, son autonomie stratégique ouverte, sa compétitivité et sa résilience, et de préserver les actifs stratégiques, les intérêts ou la sécurité de l'Union, les entités établies dans des pays tiers qui ne sont pas parties à l'AMP et qui n'ont pas fait l'objet d'un filtrage au sens du règlement (UE) 2019/452 du Parlement européen et du Conseil[23] et, le cas échéant, de mesures d'atténuation, compte tenu des objectifs énoncés dans le présent règlement, ne devraient pas être autorisées à participer. Il convient que la dimension extérieure du présent règlement soit conforme aux dispositions de l'accord d'association adopté au titre du programme pour une Europe numérique. Il convient également que la participation de pays tiers soit soumise à un contrôle public auquel contribue le pouvoir législatif afin de garantir la participation des citoyens au processus.

(38) Afin de garantir que les conditions de mise en œuvre du présent règlement soient uniformes, il convient de conférer des compétences d'exécution à la Commission pour qu'elle puisse préciser les conditions d'interopérabilité entre les SOC transfrontières; définir les modalités applicables à l'échange d'informations relatives aux incidents de cybersécurité majeurs potentiels ou en cours entre les SOC transfrontières et les entités de l'Union; établir les exigences techniques nécessaires pour garantir la sécurité du cyberbouclier européen; déterminer les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE; et détailler davantage les modalités d'attribution des services d'aide de la réserve de cybersécurité de l'UE. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil*.

---

[23] Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79I du 21.3.2019, p. 1), ELI: https://eur-lex.europa.eu/eli/reg/2019/452/oj?locale=fr.

* ***Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13), ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj).***

***(38 bis) Il est impératif de disposer de personnel qualifié, capable de fournir les services de cybersécurité pertinents de manière fiable et dans le respect des normes les plus rigoureuses, afin de garantir le déploiement efficace du cyberbouclier européen et du mécanisme d'urgence dans le domaine de la cybersécurité. Il y a donc lieu de se préoccuper de la pénurie de talents dont souffre l'Union, qui se caractérise par le manque de professionnels qualifiés, alors qu'elle doit faire face à un panorama de menaces en constante évolution, comme le reconnaît la Commission dans sa communication du 18 avril 2023 sur l'Académie des compétences en matière de cybersécurité. Il importe de remédier à cette pénurie de talents en renforçant la coopération et la coordination entre les différentes parties prenantes, notamment le secteur privé, les milieux universitaires, les États membres, la Commission et l'ENISA, afin d'intensifier et de créer des synergies, dans tous les territoires, en faveur des investissements dans l'éducation et la formation, du développement de partenariats public-privé, du soutien aux initiatives de recherche et d'innovation, de l'élaboration et de la reconnaissance mutuelle de normes communes et de la certification des compétences dans le domaine de la cybersécurité, y compris au moyen du cadre européen pour les compétences en matière de cybersécurité. Cette mesure devrait également faciliter la mobilité des professionnels de la cybersécurité au sein de l'Union. Le présent règlement devrait viser à promouvoir une main-d'œuvre plus diversifiée dans le domaine de la cybersécurité. Toutes les mesures visant à accroître les compétences en matière de cybersécurité nécessitent des garanties pour éviter une «fuite des cerveaux» et un risque pour la mobilité de la main-d'œuvre.**

(38 ter) Il est nécessaire de renforcer les compétences et les aptitudes spécialisées, interdisciplinaires et générales dans l'ensemble de l'Union, en accordant une attention particulière aux femmes. En effet, un écart entre les genres persiste en matière de cybersécurité puisque la présence moyenne des femmes dans ce secteur à l'échelle mondiale est de 20 %. Les femmes doivent être présentes dans la conception de l'avenir et de la gouvernance du numérique et en être actrices.

(38 quater) Renforcer la recherche et l'innovation (R&I) en matière de cybersécurité améliorera la résilience et l'autonomie stratégique ouverte de l'Union. De même, il importe de créer des synergies avec les programmes de R&I ainsi qu'avec les instruments et institutions existants et de renforcer la coopération et la coordination entre les différentes parties prenantes, y compris le secteur privé, la société civile, le monde universitaire, les États membres, la Commission et l'ENISA;

(38 quinquies)Le présent règlement devrait contribuer à remplir l'engagement, énoncé dans la déclaration européenne sur les droits et principes numériques pour la décennie numérique, de protéger les intérêts de nos démocraties, citoyens, entreprises et institutions publiques contre les risques liés à la cybersécurité et la cybercriminalité, y compris les violations de données et l'usurpation ou la manipulation d'identité. L'application du présent règlement devrait également contribuer à améliorer la mise en œuvre d'autres actes législatifs, par exemple sur l'intelligence artificielle, la

protection des données et la réglementation sur les données en matière de cybersécurité et de cyberrésilience.

(38 sexies) Renforcer la culture de la cybersécurité, en vertu de laquelle la sécurité, y compris celle de l'environnement numérique, est un bien public, sera essentiel à la bonne application du présent règlement. Par conséquent, l'élaboration de mesures pour associer et sensibiliser davantage les citoyens devrait être un moyen supplémentaire de garantir la protection de nos démocraties et de nos valeurs fondamentales.

(38 septies) En vue de compléter certains éléments non essentiels du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité FUE afin de préciser les conditions d'interopérabilité entre les SOC transfrontières, d'établir les modalités procédurales applicables à l'échange d'informations entre les SOC transfrontières, d'une part, et EU-CyCLONe, le réseau des CSIRT et la Commission, d'autre part, de préciser les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE et de préciser davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»*. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

****JO L 123 du 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

(39) ***Étant donné que les objectifs du*** présent règlement***, à savoir renforcer les capacités de l'Union en matière de prévention des cybermenaces, de détection, de réaction et de rétablissement et mettre en place un cadre général pour décloisonner la communication, ne peuvent pas être atteints de manière suffisante*** par les États membres ***mais peuvent l'être mieux au niveau de l'Union***. En conséquence, l'Union peut adopter des mesures conformément aux principes de subsidiarité et de proportionnalité énoncés à l'article 5 du traité sur l'Union européenne. ***Conformément au principe de proportionnalité énoncé audit article,*** le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I

OBJECTIFS GÉNÉRAUX, OBJET ET DÉFINITIONS

Article premier

Objet et objectifs

1. Le présent règlement établit des mesures destinées à renforcer les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, notamment par les actions suivantes:

a) le déploiement ***d'un réseau paneuropéen*** de centres d'opérations de sécurité («cyberbouclier européen») dans le but de mettre en place et de développer des capacités communes de détection et d'appréciation de la situation;

b) la création d'un mécanisme d'urgence dans le domaine de la cybersécurité pour aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs, à y réagir et à s'en rétablir immédiatement;

c) la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents importants ou majeurs.

2. Le présent règlement a pour but de renforcer la solidarité au niveau de l'Union en poursuivant les objectifs spécifiques suivants:

a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de ***soutenir la capacité industrielle de l'Union et des États membres dans le secteur de la cybersécurité, et de*** consolider la position concurrentielle des secteurs de l'industrie***, en particulier des microentreprises, des PME, y compris des jeunes pousses,*** et des services de l'Union dans l'ensemble de l'économie numérique***,*** et de contribuer à la souveraineté technologique de l'Union***, à son autonomie stratégique ouverte, sa compétitivité et sa résilience dans ce secteur, en renforçant l'écosystème de cybersécurité en vue de garantir des capacités solides de l'Union, y compris en coopération avec des partenaires internationaux***;

b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;

c) augmenter la résilience de l'Union et contribuer à une réaction efficace en analysant et en évaluant les incidents importants ou majeurs, notamment en tirant les

enseignements de l'expérience acquise et, au besoin, en formulant des recommandations.

c bis) développer, de manière coordonnée, les aptitudes, le savoir-faire et les compétences de la main-d'œuvre, en vue d'assurer la cybersécurité et de créer des synergies avec l'Académie des compétences en matière de cybersécurité.

3. Le présent règlement est sans préjudice de la responsabilité première des États membres dans le domaine de la sécurité nationale, de la sécurité publique, de la prévention et de la détection des infractions pénales et d'enquêtes et de poursuites en la matière.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

-1 bis) «centre d'opérations de sécurité national» ou «SOC national»: une capacité nationale centralisée rassemblant et analysant en permanence des informations et des renseignements sur les cybermenaces et améliorant la posture de cybersécurité conformément à l'article 4;

1) **«centre d'opérations de sécurité transfrontière» ou «SOC transfrontière»:** une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, ***des*** SOC nationaux ***conformément à l'article 5;***

2) **«organisme public»**: un organisme de droit public au sens de l'article 2, paragraphe 1, point 4), de la directive 2014/24/UE du Parlement européen et du Conseil[24];

3) **«consortium d'hébergement»**: un consortium formé par des États participants, représentés par ***des*** SOC nationaux, ***conformément à l'article 5***;

4) **«entité»**: une entité au sens de l'article 6, point 38), de la directive (UE) 2022/2555;

4 bis) «entité critique»: une entité critique au sens de l'article 2, point 1), de la directive (UE) 2022/2557 du Parlement européen et du Conseil[25].

5) **«entités actives dans des secteurs critiques ou hautement critiques»**: entités ***dans les secteurs*** énumérés ***aux annexes*** I et II de la directive (UE) 2022/2555;

5 bis) «traitement des incidents»: le traitement des incidents au sens de l'article 6, point 8), de la directive (UE) 2022/2555;

5 ter) «risque»: un risque au sens de l'article 6, point 9), de la directive (UE) 2022/2555;

---

[24] Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

[25] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

6) **«cybermenace»**: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

6 bis) «cybermenace importante»: une cybermenace au sens de l'article 6, point 11), de la directive (UE) 2022/2555;

7) **«incident de cybersécurité important»**: un incident de cybersécurité répondant aux critères énoncés à l'article 23, paragraphe 3, de la directive (UE) 2022/2555;

8) **«incident de cybersécurité majeur»**: un incident au sens de l'article 6, point 7), de la directive (UE) 2022/2555;

9) **«préparation»**: un état de préparation et une capacité d'assurer une réaction rapide et efficace à un incident de cybersécurité important ou majeur, résultant d'une évaluation des risques et de mesures de surveillance prises à l'avance;

10) **«réaction»**: une action en cas d'incident de cybersécurité important ou majeur, ou pendant ou après un tel incident, menée afin de faire face à ses conséquences négatives immédiates et à court terme;

10 bis) «fournisseur de services de sécurité gérés»: un fournisseur de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555;

11) **«fournisseurs de services de sécurité gérés de confiance»**: les fournisseurs de services de sécurité gérés sélectionnés ***en vue d'être inclus dans la réserve de cybersécurité de l'Union*** conformément à l'article 16 du présent règlement.

Chapitre II

LE CYBERBOUCLIER EUROPÉEN

Article 3

Création du cyberbouclier européen

1. ***Un réseau*** de centres d'opérations de sécurité («cyberbouclier européen») est ***mis*** en place pour doter l'Union de capacités avancées lui permettant de détecter, d'analyser et de traiter des données sur les cybermenaces ***ainsi que de prévenir*** les incidents sur son territoire. ***Il*** est ***formé*** par l'ensemble des centres d'opérations de sécurité nationaux («SOC nationaux») et des centres d'opérations de sécurité transfrontières («SOC transfrontières»).

Les actions mettant en œuvre le cyberbouclier européen sont soutenues par un financement au titre du programme pour une Europe numérique et réalisées conformément au règlement (UE) 2021/694, et notamment à son objectif spécifique 3.

2. Le cyberbouclier européen:

a) met en commun et partage, par l'intermédiaire des SOC transfrontières, des données sur les cybermenaces et les incidents provenant de différentes sources***, ainsi que, le cas échéant, les échanges d'informations avec le réseau des CSIRT***;

b) produit des informations de haute qualité et exploitables et des renseignements sur les cybermenaces, en utilisant des outils de pointe, notamment l'intelligence artificielle et les technologies d'analyse des données;

c) contribue à améliorer la protection contre les cybermenaces et la réaction face à celles-ci***, notamment en formulant des recommandations concrètes à l'intention des entités***;

d) participe à une détection plus rapide des cybermenaces et à l'appréciation de la situation dans l'ensemble de l'Union;

e) fournit des services et des activités à la communauté de la cybersécurité dans l'Union, y compris en contribuant au développement d'outils avancés d'intelligence artificielle et d'analyse de données.

Il est mis au point en coopération avec l'infrastructure paneuropéenne de calcul à haute performance établie conformément au règlement (UE) 2021/1173.

Article 4

Centres d'opérations de sécurité nationaux

1. Chaque État membre désigne au moins un SOC national en vue ***d'être en mesure*** de participer au cyberbouclier européen. Le SOC national est ***une capacité centralisée au sein d'un*** organisme public. ***Dans la mesure du possible, les SOC nationaux sont intégrés dans les CSIRT ou dans d'autres infrastructures de cybersécurité ou structures de gouvernance existantes.***

Le SOC national peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national***, en particulier leurs SOC nationaux,*** pour collecter et analyser des informations sur les menaces et incidents de cybersécurité***, et, le cas échéant, partager ces informations avec les membres du réseau des CSIRT de cet États membre,*** et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant ***de prévenir,*** de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.

Un SOC national ou un CSIRT peut demander des données de télémétrie, de capteurs ou d'enregistrement de leurs entités critiques nationales aux fournisseurs de services de sécurité gérés qui fournissent un service à l'entité critique. Ces données sont partagées conformément au droit de l'Union en matière de protection des données et dans le seul but d'aider le SOC national ou le CSIRT à détecter et à prévenir les menaces et incidents de cybersécurité.

2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux ***peuvent être*** sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

3. Un SOC national sélectionné conformément au paragraphe 2 s'engage à demander à participer à un SOC transfrontière dans un délai de deux ans à compter de la date d'acquisition des outils et infrastructures ou de la date à laquelle il reçoit une subvention, selon ce qui se produit plus tôt. Si, à l'expiration de ce délai, le SOC national n'est pas devenu un participant à un SOC transfrontière, il ne pourra pas bénéficier d'un soutien supplémentaire de l'Union au titre du présent règlement.

Article 5

Centres d'opérations de sécurité transfrontières

1. Un consortium d'hébergement composé d'au moins trois États membres, représentés par des SOC nationaux, résolus à collaborer pour coordonner leurs activités de détection des incidents de cybersécurité et de surveillance des cybermenaces, peut participer à des actions visant à mettre en place un SOC transfrontière. ***Un SOC transfrontière est conçu pour détecter et analyser les cybermenaces, prévenir les incidents et contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, à l'aide du partage d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention des cybermenaces et de protection contre ces dernières dans un environnement de confiance et sécurisé.***

2. À la suite d'un appel à manifestation d'intérêt, un consortium d'hébergement ***peut être*** sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le consortium d'hébergement. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le consortium d'hébergement concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

2 bis. Par dérogation à l'article 176 du règlement (UE, Euratom) 2018/1046, les entités établies dans des pays tiers qui ne sont pas parties à l'AMP ne participent pas à la passation conjointe de marchés d'outils et d'infrastructures.

3. Les membres du consortium d'hébergement concluent un accord de consortium écrit qui définit les modalités internes de mise en œuvre de la convention d'hébergement et d'utilisation.

4. Un SOC transfrontière est représenté à des fins juridiques par un SOC national agissant en tant que SOC coordinateur, ou par le consortium d'hébergement s'il est doté de la personnalité juridique. Le SOC coordinateur est responsable du respect des exigences prévues dans la convention d'hébergement et d'utilisation et dans le présent règlement.

Article 6

Coopération et partage d'informations au sein des SOC transfrontières et entre ceux-ci

1. Les membres d'un consortium d'hébergement s'échangent des informations pertinentes au sein du SOC transfrontière, y compris des informations sur les cybermenaces, les incidents évités, les vulnérabilités, les techniques et les procédures, les indicateurs de compromission, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

a) ***améliore l'échange de renseignements sur les cybermenaces entre les SOC nationaux et transfrontières et les ISAC sectoriels dans le but de prévenir, de détecter et d'atténuer les menaces;***

b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de menaces entre les entités publiques et privées.

2. L'accord de consortium écrit visé à l'article 5, paragraphe 3, établit:

a) un engagement de partager ***les*** données ***importantes*** visées au paragraphe 1 et les conditions dans lesquelles ces informations doivent être échangées;

b) un cadre de gouvernance favorisant le partage d'informations par tous les participants;

c) des objectifs pour la contribution au développement d'outils avancés d'intelligence artificielle et d'analyse de données.

3. Afin d'encourager l'échange d'informations entre les SOC transfrontières ***et les ISAC sectoriels***, ***les SOC transfrontières*** garantissent un niveau élevé d'interopérabilité entre eux ***et, dans la mesure du possible, avec les ISAC sectoriels***. Afin de faciliter l'interopérabilité entre les SOC transfrontières ***et avec les ISAC sectoriels***, ***les normes et les protocoles de partage d'informations peuvent être harmonisés avec les normes internationales et les meilleures pratiques du secteur. La passation conjointe de marchés portant sur des***

infrastructures, services et outils de cybersécurité est également encouragée. En outre, après consultation de l'ECCC ***et de l'ENISA, la Commission est habilitée, au plus tard le... [six mois après la date d'entrée en vigueur du présent règlement], à adopter des actes délégués conformément à l'article 20 bis afin de compléter le présent règlement en précisant*** les conditions de cette interopérabilité***, en étroite coordination avec les SOC transfrontières et sur la base des normes internationales et des meilleures pratiques du secteur***.

4. Les SOC transfrontières concluent des accords de coopération entre eux ***et, le cas échéant, avec les ISAC sectoriels***, qui précisent les principes de partage d'informations ***et d'interopérabilité*** en vigueur entre les plateformes transfrontières***, en tenant compte des mécanismes de partage d'informations pertinents qui existent déjà en vertu de la directive (UE) 2022/2555***. ***Le cas échéant, les SOC transfrontières nouent des accords de coopération avec les ISAC sectoriels. Les mécanismes de partage d'informations relatives à un incident de cybersécurité majeur potentiel ou en cours sont conformes aux dispositions applicables au titre de la directive (UE) 2022/2555.***

Article 7

Coopération et partage d'informations avec *le réseau des CSIRT*

1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours ***aux fins d'une appréciation commune de la situation***, ***le SOC coordinateur fournit*** sans retard injustifié les informations pertinentes ***à son CSIRT ou à une autorité compétente, qui, à son tour, les communiquera*** à EU-CyCLONe, au réseau des CSIRT et à la Commission ***ainsi qu'à l'ENISA***, compte tenu de leurs rôles ***et procédures*** respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555. ***Le présent paragraphe n'impose pas aux entités publiques ou privées d'autres obligations de communiquer un incident de cybersécurité majeur potentiel ou en cours aux fins du respect des obligations énoncées dans la directive (UE) 2022/2555.***

2. La Commission ***est habilitée à adopter des actes délégués conformément à l'article 20 bis après consultation du réseau des CSIRT pour compléter le présent règlement en déterminant*** les dispositions procédurales du partage d'informations prévu au paragraphe 1 ***du présent article et conformément à la directive (UE) 2022/2555***.

Article 8

Sécurité

1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé ***de confidentialité et*** de sécurité des données et de sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris celle des données échangées par l'intermédiaire de l'infrastructure.

2. Les États membres participant au cyberbouclier européen veillent à ce que le partage d'informations au sein du cyberbouclier européen avec des entités qui ne sont pas des organismes publics des États membres ne nuise pas aux intérêts de l'Union en matière de sécurité.

3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. ***Ils sont conformes aux directives (UE) 2022/2555 et (UE) 2022/2557. Dans ses actes d'exécution***, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.

Chapitre III

MÉCANISME D'URGENCE DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Article 9

Mise en place du mécanisme d'urgence dans le domaine de la cybersécurité

1. Un mécanisme d'urgence dans le domaine de la cybersécurité est mis en place afin d'améliorer la résilience de l'Union face aux cybermenaces majeures et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme des incidents de cybersécurité importants et majeurs (ci-après le «mécanisme»).

2. Les actions mettant en œuvre le mécanisme ▌ sont soutenues par un financement au titre du programme pour une Europe numérique et réalisées conformément au règlement (UE) 2021/694, et notamment à son objectif spécifique 3.

Article 10

Types de mesures

1. Le mécanisme soutient les types de mesures suivantes:

a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union;

b) les mesures de réaction, qui soutiennent la réaction aux incidents de cybersécurité importants et majeurs ainsi que le rétablissement immédiat, prévues par les fournisseurs ***de services de sécurité gérés*** de confiance participant à la réserve de cybersécurité de l'UE établie en vertu de l'article 12;

c) les mesures d'assistance mutuelle consistant en la fourniture d'une assistance par les autorités nationales d'un État membre à un autre État membre, notamment conformément à l'article 11, paragraphe 3, point f), de la directive (UE) 2022/2555.

1 bis. Après le déclenchement du mécanisme, la Commission procède à une évaluation et dresse un rapport chaque année sur les points forts et les points faibles du fonctionnement du mécanisme, en indiquant notamment si des exigences supplémentaires en matière de coopération ou de formation sont nécessaires.

Article 11

Tests de préparation coordonnés des entités

1. Aux fins de contribuer aux tests de préparation coordonnés des entités visés à l'article 10, paragraphe 1, point a), dans l'ensemble de l'Union, la Commission, après consultation du groupe de coopération SRI et de l'ENISA, recense les secteurs ou sous-secteurs concernés, dans les secteurs hautement critiques énumérés à l'annexe I de la directive (UE) 2022/2555, dont les entités peuvent être soumises à des tests de préparation coordonnés, en tenant compte des évaluations coordonnées des risques et des tests de résilience existants et prévus au niveau de l'Union***, conformément aux modalités fixées pour les entités dans les secteurs hautement critiques énumérés à l'annexe I de la directive (UE) 2022/2555***.

2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA, ▌le haut représentant ***et les entités susceptibles d'être soumises à des tests de préparation coordonnés conformément au paragraphe 1***, élabore des scénarios de risque et des méthodologies communs pour les exercices de tests ***de préparation*** coordonnés, ***qui donnent lieu à l'élaboration d'un plan de travail concerté***. ***Les entités soumises à des tests de préparation coordonnés conçoivent et mettent en œuvre un plan de mesures correctives qui met en application les recommandations formulées à l'issue des tests de préparation.***

Le groupe de coopération SRI peut contribuer à la hiérarchisation des secteurs ou sous-secteurs pour les exercices de tests de préparation coordonnés.

Article 12

Création de la réserve de cybersécurité de l'UE

1. Une réserve de cybersécurité de l'Union est créée afin d'aider les utilisateurs visés au paragraphe 3 à réagir aux incidents de cybersécurité importants ou majeurs, ou à fournir une assistance à cet effet, et à favoriser le rétablissement immédiat après de tels incidents.

Lorsqu'il apparaît que les services acquis ne peuvent pas être pleinement utilisés pour réagir à des incidents importants ou majeurs, ces services peuvent, à titre exceptionnel, être convertis en exercices ou formations pour la gestion des incidents, et être fournis aux utilisateurs sur demande par le pouvoir adjudicateur.

2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs ***de services de sécurité gérés*** de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve ***de cybersécurité de l'Union*** comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres***, renforcent la souveraineté technologique de l'Union, son autonomie stratégique ouverte, sa compétitivité et sa résilience dans le secteur de la cybersécurité, notamment en stimulant l'innovation dans le marché unique numérique dans l'ensemble de l'Union***.

3. Les utilisateurs des services de la réserve de cybersécurité de l'Union sont:

a) les autorités des États membres chargées de la gestion des crises de cybersécurité et les CSIRT visés respectivement à l'article 9, paragraphes 1 et 2, et à l'article 10 de la directive (UE) 2022/2555;

b) les institutions, organes et organismes de l'Union ***au sens de l'article 3, point 1), du règlement (UE) .../2023 du Parlement européen et du Conseil[26] et la CERT-UE.***

4. Les utilisateurs visés au paragraphe 3, point a), ont recours aux services de la réserve de cybersécurité de l'Union afin de réagir aux incidents importants ou majeurs touchant des entités actives dans des secteurs critiques ou hautement critiques, ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.

5. La Commission assume la responsabilité globale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, ***en coordination avec le groupe de coopération SRI 2 et***, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.

6. La Commission ***confie***, par voie de conventions de contribution, le fonctionnement et l'administration de la réserve de cybersécurité de l'UE, en tout ou en partie, à l'ENISA.

7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, ***notamment des compétences et des capacités recherchées auprès de la main-d'œuvre dans le domaine de la cybersécurité,*** après consultation des États membres et de la Commission ***et, le cas échéant, des fournisseurs de services de sécurité gérés ainsi que d'autres représentants du secteur de la cybersécurité***. L'ENISA établit une autre carte similaire, après consultation de la Commission, ***des fournisseurs de services de sécurité gérés et, le cas échéant, d'autres représentants du secteur de la cybersécurité,*** afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant ***et informe le Conseil des besoins des pays tiers***.

8. La Commission ***est habilitée à adopter des actes délégués conformément à l'article 20 bis pour compléter le présent règlement en précisant*** les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE. ▌

---

[26] ***Règlement (UE) .../2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO C , , p, , ELI: ...).***

Article 13

Demandes d'aide adressées à la réserve de cybersécurité de l'UE

1. Les utilisateurs visés à l'article 12, paragraphe 3, peuvent adresser à la réserve de cybersécurité de l'Union des demandes d'aide en ce qui concerne la réaction aux incidents de cybersécurité importants ou majeurs ainsi que le rétablissement immédiat.

2. Pour bénéficier de l'aide de la réserve de cybersécurité de l'Union, les utilisateurs visés à l'article 12, paragraphe 3, prennent des mesures pour atténuer les effets de l'incident pour lequel ils demandent de l'aide, y compris la fourniture d'une assistance technique directe et d'autres ressources pour contribuer à la réaction à l'incident ainsi qu'aux efforts de rétablissement immédiat.

3. Les demandes d'aide formulées par les utilisateurs visés à l'article 12, paragraphe 3, point a), du présent règlement sont transmises à la Commission et à l'ENISA par l'intermédiaire du point de contact unique désigné ou établi par l'État membre conformément à l'article 8, paragraphe 3, de la directive (UE) 2022/2555.

4. Les États membres informent le réseau des CSIRT et, le cas échéant, EU-CyCLONe des demandes d'aide en ce qui concerne la réaction à un incident et le rétablissement immédiat reçues en vertu du présent article.

5. Les demandes d'aide en ce qui concerne la réaction à un incident et le rétablissement immédiat contiennent:

a) des informations appropriées concernant l'entité touchée et les répercussions potentielles de l'incident, ainsi que l'utilisation prévue de l'aide demandée, y compris une indication des besoins estimés;

b) des informations sur les mesures prises pour atténuer l'incident pour lequel l'aide a été demandée, visées au paragraphe 2;

c) des informations sur les autres formes d'aide dont dispose l'entité touchée, y compris les dispositions contractuelles en vigueur relatives aux services de réaction aux incidents et de rétablissement immédiat, ainsi que les contrats d'assurance couvrant potentiellement ce type d'incident.

6. L'ENISA, en collaboration avec la Commission et le groupe de coopération SRI, élabore un modèle pour faciliter la présentation des demandes d'aide adressées à la réserve de cybersécurité de l'UE.

7. La Commission ***est habilitée à adopter des actes délégués en conformité avec l'article 20 bis pour compléter le présent règlement en précisant*** davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. ▌

Article 14

Mise en œuvre de l'aide de la réserve de cybersécurité de l'UE

1. Les demandes d'aide adressées à la réserve de cybersécurité de l'Union sont évaluées par la Commission, assistée par l'ENISA ou selon les modalités définies dans les conventions de contribution visées à l'article 12, paragraphe 6, et une réponse est transmise ▌ aux utilisateurs visés à l'article 12, paragraphe 3***, dans les meilleurs délais, et en tout état de cause dans les 24 heures***.

2. En cas de demandes simultanées multiples, les critères suivants sont pris en compte pour classer les demandes, si nécessaire:

a) la gravité de l'incident de cybersécurité;

b) le type d'entité touchée, la priorité étant accordée aux incidents touchant des entités essentielles au sens de l'article 3, paragraphe 1, de la directive (UE) 2022/2555;

c) l'incidence potentielle sur les États membres ou les utilisateurs concernés;

d) ***l'ampleur et*** la nature transfrontière potentielle de l'incident et le risque de propagation à d'autres États membres ou utilisateurs;

e) les mesures prises par l'utilisateur pour contribuer à la réaction et aux efforts de rétablissement immédiat, visées à l'article 13, paragraphe 2, et à l'article 13, paragraphe 5, point b).

3. Les services de la réserve de cybersécurité de l'UE sont fournis conformément à des accords spécifiques conclus entre le fournisseur de services et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'UE. Ces accords contiennent des conditions de responsabilité ***et toute autre disposition que les parties à l'accord jugent nécessaire à la fourniture du service concerné***.

4. Les accords visés au paragraphe 3 ***se fondent*** sur des modèles élaborés par l'ENISA, après consultation des États membres ***et, le cas échéant, d'autres utilisateurs de la réserve de cybersécurité de l'Union***.

5. La Commission et l'ENISA ne sont pas contractuellement responsables des dommages causés à des tiers par les services fournis dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE***, sauf en cas de négligence grave lors de l'évaluation de la demande du fournisseur de services, ou dans les cas où la Commission ou l'ENISA sont elles-mêmes utilisatrices de la réserve de cybersécurité de l'UE conformément à l'article 14, paragraphe 3***.

6. Au plus tard un mois après avoir bénéficié de l'aide de la réserve, l'utilisateur présente à la Commission et à l'ENISA***, au réseau des CSIRT et, le cas échéant, à EU-CyCLONe,*** un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés. Lorsque l'utilisateur est originaire d'un pays tiers conformément aux dispositions de l'article 17, ce rapport est également communiqué au haut représentant.
Le rapport respecte le droit de l'Union et le droit national relatif à la protection des informations sensibles ou classifiées.

7. La Commission fait ▌ rapport ***régulièrement, et au moins deux fois par an,*** au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus. ***Les informations confidentielles sont protégées, conformément au droit de l'Union et au droit national relatif à la protection des informations sensibles ou classifiées.***

Article 15

Coordination avec les mécanismes de gestion des crises

1. Dans les cas où des incidents de cybersécurité importants ou majeurs sont la conséquence ou la cause de catastrophes telles que définies dans la décision nº 1313/2013/UE[27], le soutien apporté au titre du présent règlement pour réagir à de tels incidents est le complément des actions entreprises conformément à la décision nº 1313/2013/UE, sans préjudice de celle-ci.

2. Dans le cas d'un incident de cybersécurité majeur et transfrontière pour lequel le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) est activé, le soutien apporté au titre du présent règlement pour réagir à cet incident suit les protocoles et procédures applicables de l'IPCR.

3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique. Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre dans le cadre de l'article 42, paragraphe 7, du traité ***UE***.

4. Le soutien au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut faire partie de la réponse conjointe donnée par l'Union et les États membres dans les situations visées à l'article 222 du traité ***FUE***.

Article 16

Fournisseurs de confiance

1. Dans les procédures de passation de marchés menées pour la création de la réserve de cybersécurité de l'UE, le pouvoir adjudicateur agit conformément aux principes énoncés dans le règlement (UE, Euratom) 2018/1046 et aux principes suivants:

a) la réserve de cybersécurité de l'UE comprend des services qui peuvent être déployés dans tous les États membres, compte tenu en particulier des exigences nationales relatives à la fourniture de ces services, y compris la certification ou l'accréditation;

b) la protection des intérêts essentiels de l'Union et de ses États membres en matière de sécurité;

c) la réserve de cybersécurité de l'UE apporte une valeur ajoutée européenne, en contribuant à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris la promotion du développement des compétences en matière de cybersécurité dans l'UE ***et de la réalisation d'un équilibre hommes-femmes dans le secteur, et au renforcement de la souveraineté technologique, de l'autonomie stratégique ouverte, de la compétitivité et de la résilience de l'Union***.

2. Lors de la passation de marchés de services pour la réserve de cybersécurité de l'UE, le pouvoir adjudicateur inclut les critères de sélection suivants dans les documents de marché:

[27] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

a) le fournisseur démontre que son personnel possède le plus haut niveau d'intégrité professionnelle, d'indépendance, de responsabilité et de compétence technique requise pour mener à bien les activités dans son domaine spécifique, et il garantit la permanence/la continuité de l'expertise ainsi que les ressources techniques requises;

b) le fournisseur, ses filiales et ses sous-traitants disposent d'un cadre pour protéger les informations sensibles relatives au service, et notamment les éléments de preuve, les conclusions et les rapports, qui est conforme aux règles de sécurité de l'Union relatives à la protection des informations classifiées de l'UE;

c) le fournisseur apporte la preuve suffisante que sa structure de gouvernance est transparente, qu'elle n'est pas susceptible de compromettre son impartialité ni la qualité de ses services ou de provoquer des conflits d'intérêts;

d) le fournisseur dispose d'une habilitation de sécurité appropriée, au moins pour le personnel qu'il compte déployer pour ce service;

e) le fournisseur dispose du niveau de sécurité approprié pour ses systèmes informatiques;

f) le fournisseur possède l'équipement technique matériel et logiciel ***à jour*** nécessaire au service demandé ***et se conforme, s'il y a lieu, au règlement (UE) .../... du Parlement européen et du Conseil[28] (2022/0272(COD));***

g) le fournisseur est en mesure de démontrer qu'il possède une expérience dans la fourniture de services similaires à des autorités nationales ou à des entités pertinentes actives dans des secteurs critiques ou hautement critiques;

h) le fournisseur est en mesure de fournir le service dans un bref délai dans le ou les États membres où il peut le faire;

i) le fournisseur est en mesure de fournir le service dans la langue locale du ou des États membres où il peut le faire***, ou dans l'une des langues de travail des institutions de l'Union***;

j) dès qu'un schéma ***européen*** de certification ***de cybersécurité*** pour les services de sécurité ▌conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma ***dans un délai de deux ans à compter de l'adoption du schéma;***

j bis) le fournisseur est en mesure de fournir le service de manière indépendante et non dans le cadre d'une offre groupée, préservant ainsi la possibilité pour l'utilisateur de passer à un autre fournisseur de services;

j ter) aux fins de l'article 12, paragraphe 1, le fournisseur inclut dans la proposition pour l'appel d'offres la possibilité de convertir les services inutilisés de réaction aux incidents en exercices ou en formations;

j quater) le fournisseur est établi et a ses structures exécutives de gestion dans l'Union, dans un pays associé ou dans un pays tiers qui fait partie de l'accord sur les marchés publics (AMP) dans le cadre de l'Organisation mondiale du commerce;

---

28 Règlement (UE) .../... du Parlement européen et du Conseil du ... sur ... (JO L du …, ELI: …).

j quinquies) le destinataire n'est pas soumis au contrôle d'un pays tiers non associé ou d'une entité de pays tiers non associé qui n'est pas partie à l'AMP, ou bien cette entité a fait l'objet d'un filtrage au sens du règlement (UE) 2019/452 et, lorsque cela est nécessaire, de mesures d'atténuation, compte tenu des objectifs énoncés dans le présent règlement.

Article 17

Aide aux pays tiers

1. Les pays tiers peuvent demander une aide à la réserve de cybersécurité de l'UE lorsque les accords d'association conclus en ce qui concerne leur participation au programme pour une Europe numérique le prévoient.

2. L'aide apportée par la réserve de cybersécurité de l'Union est conforme au présent règlement et respecte toutes les conditions spécifiques énoncées dans les accords d'association visés au paragraphe 1.

3. Les utilisateurs de pays tiers associés pouvant bénéficier de services au titre de la réserve de cybersécurité de l'UE sont des autorités compétentes telles que les CSIRT et les autorités chargées de la gestion des crises de cybersécurité.

4. Chaque pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE désigne une autorité qui joue le rôle de point de contact unique aux fins du présent règlement.

5. Avant de recevoir une aide de la réserve de cybersécurité de l'UE, les pays tiers fournissent à la Commission et au haut représentant des informations sur leurs capacités en matière de cyberrésilience et de gestion des risques, y compris au moins des informations sur les mesures nationales prises pour anticiper les incidents de cybersécurité importants ou majeurs, ainsi que des informations sur les entités nationales responsables, notamment les CSIRT ou entités équivalentes, leurs capacités et les ressources qui leur sont allouées. Lorsque les dispositions des articles 13 et 14 du présent règlement font référence aux États membres, elles s'appliquent aux pays tiers visés au paragraphe 1.

6. La Commission et le haut représentant ***informent le Conseil sans retard injustifié et*** se coordonnent en ce qui concerne les demandes reçues et la mise en œuvre de l'aide accordée aux pays tiers au titre de la réserve de cybersécurité de l'UE.

Chapitre IV

MÉCANISME D'ANALYSE DES INCIDENTS DE CYBERSÉCURITÉ

Article 18

Mécanisme d'analyse des incidents de cybersécurité

1. À la demande de la Commission, d'EU-CyCLONe ou du réseau des CSIRT, l'ENISA analyse et évalue les menaces, les vulnérabilités et les mesures d'atténuation d'un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident,

l'ENISA remet un rapport d'analyse au réseau des CSIRT, à EU-CyCLONe et à la Commission afin de les aider à s'acquitter de leurs tâches, compte tenu notamment de celles énoncées aux articles 15 et 16 de la directive (UE) 2022/2555. Le cas échéant, la Commission transmet le rapport au haut représentant.

2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés ***par les SOC nationaux et transfrontières*** et les utilisateurs de services de cybersécurité***, et recueille leurs retours d'information, étant précisés les garanties et le suivi nécessaires pour que les acteurs du secteur des services de cybersécurité reprennent à leur compte les enseignements tirés et les bonnes pratiques identifiées***. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.

3. Le rapport comprend une analyse et un examen de l'incident de cybersécurité important ou majeur, y compris des principales causes, vulnérabilités et enseignements tirés. Il protège les informations confidentielles, conformément au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées. ***Il ne comporte pas de précisions relatives aux vulnérabilités activement exploitées qui n'ont pas encore été corrigées.***

3 bis. Le rapport visé au paragraphe 1 du présent article comprend les enseignements tirés des évaluations par les pairs réalisées en application de l'article 19 de la directive (UE) 2022/2555.

4. Le cas échéant, le rapport formule des recommandations***, y compris à l'intention de toutes les parties prenantes,*** afin d'améliorer la posture cyber de l'Union.

5. Si possible, une version du rapport est rendue publique. Cette version contient uniquement des informations publiques.

Chapitre V

DISPOSITIONS FINALES

Article 19

Modifications du règlement (UE) 2021/694

Le règlement (UE) 2021/694 est modifié comme suit:

1) L'article 6 est modifié comme suit:

a) le paragraphe 1 est modifié comme suit:

i) le point a bis) suivant est inséré:

«a bis) soutenir le développement d'un cyberbouclier européen, y compris la mise au point, le déploiement et l'exploitation de plateformes SOC nationales et transfrontières qui contribuent à l'appréciation de la situation dans l'Union et au renforcement des capacités en matière de renseignement sur les cybermenaces de l'Union;»;

ii) le point g) suivant est ajouté:

«g) mettre en place et exploiter un mécanisme d'urgence dans le domaine de la cybersécurité pour aider les États membres à se préparer aux incidents de cybersécurité importants et à y réagir, en complément des ressources et capacités nationales et des autres formes de soutien disponibles au niveau de l'Union, notamment la création d'une réserve de cybersécurité de l'UE.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Les actions entreprises au titre de l'objectif spécifique 3 sont mises en œuvre principalement via le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, conformément au règlement (UE) 2021/887 du Parlement européen et du Conseil*, à l'exception des actions mettant en œuvre la réserve de cybersécurité de l'UE, qui sont exécutées par la Commission et l'ENISA.».

---

* Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1, ***ELI: https://eur-lex.europa.eu/eli/reg/2021/887/oj?locale=fr).».***

2) L'article 9 est modifié comme suit:

a) au paragraphe 2, les points b), c) et d) sont remplacés par le texte suivant:

«b) 1 776 956 000 EUR pour l'objectif spécifique 2 – Intelligence artificielle;

c) ***1 620 566 000*** EUR pour l'objectif spécifique 3 – Cybersécurité et confiance;

d) ***500 347 000 EUR*** pour l'objectif spécifique 4 - Compétences numériques avancées;»;

a bis) le nouveau paragraphe 2 bis suivant est inséré:

« 2 bis. Le montant visé au paragraphe 2, point c), est principalement utilisé pour atteindre les objectifs opérationnels visés à l'article 6, paragraphe 1, points a) à f), du programme.»;

a ter) le nouveau paragraphe 2 ter suivant est inséré:

« 2 ter. Le montant pour l'établissement et la mise en œuvre de la réserve de cybersécurité de l'UE ne dépasse pas 27 000 000 EUR pour la durée prévue du règlement établissant des mesures destinées à renforcer la solidarité et les capacités

dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir.»;

b) le paragraphe 8 suivant est ajouté:

«8. Par dérogation à l'article 12, paragraphe 4, du règlement (UE, Euratom) 2018/1046, les crédits d'engagement et de paiement non utilisés pour les actions ***menées dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'UE*** poursuivant les objectifs énoncés à l'article 6, paragraphe 1, point g), du présent règlement sont reportés de droit et peuvent être engagés et payés jusqu'au 31 décembre de l'exercice suivant.

La Commission informe le Parlement et le Conseil des crédits reportés conformément à l'article 12, paragraphe 6, du règlement (UE, Euratom) 2018/1046.».

3) À l'article 14, le paragraphe 2 est remplacé par le texte suivant:

«2. Le programme peut octroyer un financement sous l'une ou l'autre des formes prévues dans le règlement ***(UE, Euratom) 2018/1046***, y compris en particulier par la passation de marchés en premier lieu, ou des subventions et des prix.

Lorsque la réalisation de l'objectif d'une action nécessite l'achat de biens et services innovants, des subventions ne peuvent être octroyées qu'à des bénéficiaires qui sont des pouvoirs adjudicateurs ou des entités adjudicatrices au sens des directives 2014/24/UE[27] et 2014/25/UE[28] du Parlement européen et du Conseil.

Lorsque la fourniture de biens ou services innovants qui ne sont pas encore disponibles commercialement à grande échelle est nécessaire à la réalisation des objectifs d'une action, le pouvoir adjudicateur ou l'entité adjudicatrice peut autoriser l'attribution de plusieurs marchés dans le cadre d'une même procédure de passation de marchés.

Pour des raisons de sécurité publique dûment justifiées, le pouvoir adjudicateur ou l'entité adjudicatrice peut exiger que le lieu d'exécution du marché soit situé à l'intérieur du territoire de l'Union.

Lors de la mise en œuvre des procédures de passation de marchés pour la réserve de cybersécurité de l'UE établie par l'article 12 du règlement (UE) 2023***/...***, la Commission et l'ENISA peuvent agir en tant que centrale d'achat pour passer des marchés pour le compte ou au nom des pays tiers associés au programme, conformément à l'article 10. La Commission et l'ENISA peuvent également agir en qualité de grossiste, en achetant, en stockant et en revendant ou en donnant des fournitures et des services, y compris des locations, à ces pays tiers. Par dérogation à l'article 169, paragraphe 3, du règlement (UE) ***.../...***, la demande d'un seul pays tiers suffit pour charger la Commission ou l'ENISA d'agir.

Lors de la mise en œuvre des procédures de passation de marchés pour la réserve de cybersécurité de l'UE établie par l'article 12 du règlement (UE) 2023***/...***, la Commission et l'ENISA peuvent agir en tant que centrale d'achat pour passer des marchés pour le compte ou au nom des institutions, organes et organismes de l'Union. La Commission

et l'ENISA peuvent également agir en qualité de grossiste, en achetant, en stockant et en revendant ou en donnant des fournitures et des services, y compris des locations, aux institutions, organes et organismes de l'Union. Par dérogation à l'article 169, paragraphe 3, du règlement (UE) ***.../...***, la demande d'une seule institution, d'un seul organe ou organisme de l'Union suffit pour charger la Commission ou l'ENISA d'agir.

Le programme peut aussi octroyer un financement sous la forme d'instruments financiers dans le cadre d'opérations de mixage. ».

4) L'article 16 bis suivant est ajouté:

«***Article 16 bis***

Dans le cas d'actions mettant en œuvre le cyberbouclier européen établi par l'article 3 du règlement (UE) 2023/XX, les règles applicables sont celles énoncées aux articles 4 et 5 du règlement (UE) 2023***/...***. En cas de conflit entre les dispositions du présent règlement et les articles 4 et 5 du règlement (UE) 2023***/...***, ces derniers prévalent et s'appliquent à ces actions spécifiques.».

5) L'article 19 est remplacé par le texte suivant:

«Les subventions au titre du programme sont octroyées et gérées conformément au titre VIII du règlement ***(UE, Euratom) 2018/1046*** et peuvent couvrir jusqu'à 100 % des coûts éligibles, sans préjudice du principe de cofinancement prévu à l'article 190 du règlement ***(UE, Euratom) 2018/1046***. Ces subventions sont octroyées et gérées comme il est précisé pour chaque objectif spécifique.

L'aide sous forme de subventions peut être octroyée directement par l'ECCC sans appel à propositions aux SOC nationaux visés à l'article 4 du règlement ***(UE) .../...*** et au consortium d'hébergement visé à l'article 5 du règlement ***(UE) .../...***, conformément à l'article 195, paragraphe 1, point d), du règlement ***(UE, Euratom) 2018/1046***.

L'aide sous forme de subventions pour le mécanisme d'urgence dans le domaine de la cybersécurité tel que défini à l'article 10 du règlement ***(UE) .../...*** peut être octroyée directement par l'ECCC aux États membres sans appel à propositions, conformément à l'article 195, paragraphe 1, point d), du règlement ***(UE, Euratom) 2018/1046***.

En ce qui concerne les mesures énoncées à l'article 10, paragraphe 1, point c), du règlement ***(UE) .../...***, l'ECCC informe la Commission et l'ENISA des demandes de subventions directes sans appel à propositions présentées par les États membres.

Pour soutenir une mesure d'assistance mutuelle déclenchée en réaction à un incident de cybersécurité important ou majeur au sens de l'article 10, point c), du règlement ***(UE) .../...***, et conformément à l'article 193, paragraphe 2, deuxième alinéa, point a), du règlement ***(UE, Euratom) 2018/1046***, dans des cas dûment justifiés, les coûts peuvent être considérés comme éligibles même s'ils ont été exposés avant le dépôt de la demande de subvention.».

6) Les annexes I et II du règlement (UE) 2021/694 sont modifiées conformément à l'annexe du présent règlement.

Article 19 bis
Ressources supplémentaires pour l'ENISA

L'ENISA reçoit des ressources supplémentaires pour mener à bien les tâches supplémentaires qui lui ont été confiées par le présent règlement. Ces ressources supplémentaires, y compris les financements, ne compromettent pas la réalisation des objectifs d'autres programmes de l'Union, en particulier le programme pour une Europe numérique.

Article 20

Évaluation *et réexamen*

1. Au plus tard le [***deux*** ans après la date d'application du présent règlement] ***et tous les deux ans par la suite***, la Commission ***procède à une évaluation du fonctionnement des mesures définies dans le présent règlement et*** présente un rapport ▌au Parlement européen et au Conseil.

2. Cette évaluation porte, en particulier, sur les aspects suivants:

a) l'utilisation et la valeur ajoutée des SOC transfrontières et la mesure dans laquelle ils contribuent à accélérer la détection des cybermenaces et la réaction à celles-ci ainsi que l'appréciation de la situation; la participation active des SOC nationaux au cyberbouclier européen, y compris le nombre de SOC nationaux et de SOC transfrontières établis et la mesure dans laquelle ils ont contribué à la production et à l'échange d'informations exploitables de haute qualité et de renseignements sur les cybermenaces; le nombre et le coût des infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints; le nombre d'accords de coopération conclus entre les SOC transfrontières et avec les ISAC sectoriels; le nombre d'incidents signalés au réseau des CSIRT et leur incidence sur les travaux du réseau des CSIRT;

b) tant les points forts que les points faibles du fonctionnement du mécanisme d'urgence dans le domaine de la cybersécurité, en indiquant si des exigences supplémentaires en matière de coopération ou de formation sont nécessaires;

c) la contribution du présent règlement au renforcement de la résilience et de l'autonomie stratégique ouverte de l'Union, à l'amélioration de la compétitivité des secteurs industriels, des microentreprises, des PME, y compris les start-up, concernés ainsi qu'au développement des compétences en matière de cybersécurité dans l'Union;

d) l'utilisation et la valeur ajoutée de la réserve de cybersécurité de l'UE, y compris le nombre de fournisseurs de sécurité de confiance faisant partie de la réserve de cybersécurité de l'UE; le nombre, le type, les coûts et l'incidence des actions menées à l'appui de la réaction aux incidents de cybersécurité, ainsi que ses utilisateurs et fournisseurs; le délai moyen pour que la Commission reconnaisse des incidents, pour que la réserve de cybersécurité de l'UE soit déployée et réagisse aux incidents, et pour que l'utilisateur se remette de ces incidents; s'il y a lieu d'élargir la portée de la réserve de cybersécurité de l'UE aux services de préparation aux incidents ou aux exercices communs qui réunissent les fournisseurs de services de sécurité gérés de confiance et les utilisateurs potentiels de la réserve de cybersécurité de l'UE afin de garantir, si nécessaire, le bon fonctionnement de la réserve de cybersécurité de l'UE;

e) la contribution du présent règlement au développement et à l'amélioration des aptitudes et des compétences de la main-d'œuvre dans le secteur de la cybersécurité, qui sont indispensables pour renforcer la capacité de l'Union à détecter et à prévenir les menaces et les incidents de cybersécurité, à y réagir et à s'en rétablir;

f) la contribution du présent règlement au déploiement et au développement de technologies de pointe dans l'Union.

3. Sur la base des rapports visés au paragraphe 1, la Commission présente au Parlement et au Conseil, s'il y a lieu, une proposition législative de modification du présent règlement.

Article 20 bis

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 6, paragraphe 3, à l'article 7, paragraphe 2, à l'article 12, paragraphe 8, et à l'article 13, paragraphe 7, est conféré à la Commission pour une période de ... ans à compter du ... [date d'entrée en vigueur de l'acte législatif de base ou toute autre date fixée par les colégislateurs]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de

... ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 6, paragraphe 3, à l'article 7, paragraphe 2, à l'article 12, paragraphe 8, et à l'article 13, paragraphe 7, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu de l'article 6, paragraphe 3, de l'article 7, paragraphe 2, de l'article 12, paragraphe 8, ou de l'article 13, paragraphe 7, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil, ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de [deux mois] à l'initiative du Parlement européen ou du Conseil.

Article 21

Comité

1. La Commission est assistée par le comité de coordination du programme pour une Europe numérique établi par le règlement (UE) 2021/694. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Article 22

Entrée en vigueur

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

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

Fait à Strasbourg, le

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

ANNEXE

Le règlement (UE) 2021/694 est modifié comme suit:

(1) À l'annexe I, la section «Objectif spécifique nº 3 — Cybersécurité et confiance» est remplacée par le texte suivant:

«Objectif spécifique 3 – Cybersécurité et confiance

Le programme stimule le renforcement, la création et l'acquisition des capacités essentielles pour sécuriser l'économie numérique, la société et la démocratie dans l'Union en renforçant le potentiel industriel et la compétitivité de l'Union en matière de cybersécurité, et en améliorant la capacité des secteurs privé et public à protéger les citoyens et les entreprises des cybermenaces, y compris en soutenant la mise en œuvre de la directive (UE) 2016/1148.

Les actions initiales et, le cas échéant, les actions ultérieures relevant du présent objectif comprennent:

1. Un co-investissement avec les États membres dans des équipements, des infrastructures et des savoir-faire avancés en matière de cybersécurité qui sont essentiels pour protéger les infrastructures critiques et le marché unique numérique dans son ensemble. Un tel co-investissement pourrait comprendre des investissements dans des installations quantiques et des ressources de données pour la cybersécurité, l'appréciation de la situation dans le cyberespace, ***notamment des SOC nationaux et des SOC transfrontières constituant le cyberbouclier européen***, ainsi que d'autres outils à mettre à la disposition des secteurs public et privé dans toute l'Europe.

2. L'extension des capacités technologiques existantes et la mise en réseau des centres de compétence des États membres, en veillant à ce que ces capacités répondent aux besoins du secteur public et de l'industrie, notamment par le biais de produits et services qui renforcent la cybersécurité et la confiance au sein du marché unique numérique.

3. Un large déploiement de solutions de pointe efficaces en matière de cybersécurité et de confiance dans tous les États membres. Ce déploiement comprend notamment le renforcement de la sécurité et de la sûreté des produits, depuis leur conception jusqu'à leur commercialisation.

4. Un soutien comblant le déficit de compétences en matière de cybersécurité, ***en veillant notamment à parvenir à l'équilibre entre les femmes et les hommes dans ce secteur,*** par exemple en alignant les programmes de compétences en matière de cybersécurité, en les adaptant aux besoins sectoriels spécifiques, ***l'accent étant mis sur les besoins interdisciplinaires et généraux,*** et en facilitant l'accès à des formations spécialisées ciblées ***de sorte à permettre à toutes les personnes dans tous les territoires, sans exclusion, de tirer***

parti des possibilités offertes par le présent règlement.

5. La promotion de la solidarité entre les États membres en ce qui concerne la préparation et la réaction aux incidents majeurs de cybersécurité par le déploiement de services de cybersécurité par-delà les frontières, y compris un soutien à l'assistance mutuelle entre les autorités publiques et la création d'une réserve de fournisseurs ***de services de sécurité gérés*** de confiance au niveau de l'Union.»;

(2) À l'annexe II, la section «Objectif spécifique nº 3 — Cybersécurité et confiance» est remplacée par le texte suivant:

«Objectif spécifique 3 – Cybersécurité et confiance

3.1. Le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints ***dans le cadre du bouclier de cybersécurité***.

3.2. Le nombre d'utilisateurs et de communautés d'utilisateurs ayant accès à des installations européennes de cybersécurité.

3.3. Le nombre***, le type, le coût et l'incidence des actions menées en soutien*** à la préparation et à la réaction aux incidents de cybersécurité dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité. ***La mesure dans laquelle les recommandations des tests de préparation ont été mises en œuvre et appliquées par l'utilisateur, ainsi que le délai moyen pour que la Commission reconnaisse les incidents, pour que la réserve de cybersécurité de l'UE réagisse aux incidents et pour que l'utilisateur se remette de ces incidents.»***

EXPOSÉ DES MOTIFS

CONTEXTE

La cybersécurité est, comme il se doit, centrale dans nos démocraties. Aux cybermenaces sont liés la montée de l'insécurité pour les personnes et pour les entreprises, ainsi que l'essor de la désinformation, qui met à mal les principes démocratiques fondamentaux pour le respect des droits de l'homme. Pour contrer ces menaces, un environnement numérique sûr et soumis à un contrôle public est donc indispensable à nos démocraties.

Au sein de l'Union, les cyberattaques sont en plein essor, tant du point de vue des méthodes utilisées que des effets qu'elles produisent. En outre, l'agression de l'Ukraine par la Russie a profondément changé la donne, et ce en amont même de l'invasion, et a ouvert une ère nouvelle de la **cyberguerre**, selon le panorama des menaces 2022 de l'ENISA[1]. La priorité identifiée au cours de ce cyberconflit est la nécessité de **renforcer les capacités** en matière de projets et **programmes multilatéraux**, ainsi que de **développer des compétences** rapidement. Une réaction européenne commune, fondée sur une coopération renforcée au niveau européen, en sus du niveau national, est une nécessité absolue pour améliorer notre résilience.

Renforcer la culture de la cybersécurité, en vertu de laquelle la sécurité, y compris celle de l'environnement numérique, est un bien public, sera essentiel à la bonne application du présent règlement.

En outre, les cyberattaques ciblent souvent des **services et infrastructures publics locaux, régionaux et nationaux** (ainsi, le secteur de la santé demeure une cible privilégiée des cyberattaques[2]). Tout indique aussi que les **collectivités locales** sont parmi les cibles les plus vulnérables en raison de la faiblesse de leurs ressources financières et humaines, et il est donc particulièrement important de sensibiliser les décideurs locaux à la nécessité d'améliorer la résilience numérique[3]. Les attaques frappent en premier lieu et directement les citoyens et mettent donc nos démocraties en péril, y compris par des campagnes de désinformation. Le sentiment d'insécurité que ces situations peuvent faire naître au sein de la population est susceptible de se traduire par des choix politiques en faveur d'une préférence radicale pour la sécurité au mépris du respect des droits fondamentaux. Cela étant, la sécurité fait partie intégrante de nos démocraties et est compatible avec tous les autres droits, dont elle est une nécessaire condition.

Les entreprises, et notamment les PME, de l'Union sont elles aussi confrontées à la cybercriminalité; alors que la sphère numérique est de plus en plus utilisée pour les activités commerciales, la cybersécurité constitue une préoccupation croissante. Les PME sont les moins bien préparées car elles disposent de moins de ressources pour se protéger et sont aussi

[1] ENISA, «Threat Landscape 2022» (Panorama des menaces 2022), octobre 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport.
[2] Panorama des menaces établi par l'ENISA: secteur de la santé, juillet 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport
[3] Comité européen des régions, «Digital Resilience» (Résilience numérique), 2023, https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf.

moins informées qu'elles peuvent être victimes de cyberattaques.

Les cyberattaques, selon toute probabilité, devraient se poursuivre et prendre de l'ampleur à l'avenir, notamment en cas d'instabilité politique et plus particulièrement de guerre. Alors que nous avançons chaque jour sur la voie de la transition numérique, la résilience numérique devient donc de plus en plus essentielle pour notre vie quotidienne et pour garantir l'**autonomie stratégique ouverte de l'Union**.

PROPOSITION DE LA RAPPORTEURE

La rapporteure estime que l'Union doit être mieux préparée à l'avenir et elle se félicite de ce texte législatif qu'il est urgent d'adopter pour mettre en commun les ressources, les informations et les connaissances afin de garantir la solidarité entre les États membres, d'accroître la capacité industrielle de l'Union, de développer **de manière coordonnée les compétences et les capacités** qui conditionnent la cybersécurité, d'être plus résilients face aux futures attaques et de protéger nos démocraties contre toute exploitation individuelle des impératifs de sécurité. Il est aussi important de protéger l'intégrité de nos processus électoraux. Ce texte constitue donc un engagement essentiel pour remplir l'objectif de l'**autonomie stratégique ouverte**.

Pour toutes ces raisons, l'Union a donc besoin d'une **gouvernance coordonnée** et solide en son sein, ainsi que d'une coopération structurée avec le secteur privé afin de favoriser l'essor d'une cyberindustrie européenne. La collaboration avec des partenaires internationaux partageant nos principes, mais également avec d'autres pays qui ne disposent pas des mêmes capacités et peuvent avoir besoin d'aide en cas de cyberattaques, est aussi souhaitable. Le règlement de l'Union sur la cybersolidarité doit prévoir une gouvernance soigneusement définie, qui évite tout doublon avec les initiatives et les actes législatifs déjà en vigueur, tels que la directive SRI2.

La proposition à l'examen est tout particulièrement fondée sur l'échange d'informations à titre volontaire entre les États membres. C'est pourquoi la rapporteure propose de renforcer les garanties qui fondent la confiance entre les États membres, afin d'accroître la participation et la coopération de ceux-ci, par exemple en matière de passations conjointes de marchés pour des infrastructures, ainsi que la participation du pouvoir législatif, afin d'obtenir la confiance des citoyens et des **garanties démocratiques**.

En deuxième lieu, la rapporteure propose de **sécuriser le budget** consacré à cette initiative dans les prochains CFP, y compris par l'engagement des États membres, afin de garantir la continuité après 2027 des activités mises en place au titre du règlement de l'Union sur la cybersolidarité.

En troisième lieu, la rapporteure propose d'améliorer la **structure de gouvernance**, de sorte à disposer d'une gouvernance clairement définie et articulée avec la législation en vigueur.

La rapporteure propose également d'améliorer la **coordination** entre les différentes entités des États membres chargées de la cybersécurité de sorte à ce qu'elles proposent un cyberbouclier commun. Elle suggère également de renforcer la contribution de l'ENISA à la coordination et aux interactions entre les différents acteurs opérant au niveau national.

En ce qui concerne la **nouvelle réserve de cybersécurité**, la rapporteure considère qu'elle pourrait permettre le développement des capacités industrielles au sein de l'Union, y compris à destination des PME, grâce à des investissements dans la recherche et l'innovation qui permettront d'élaborer des technologies de pointe, par exemple relatives à l'informatique en nuage et à l'intelligence artificielle. La rapporteure propose en outre de conserver la participation des entreprises, de renforcer les critères et les garanties de fiabilité conditionnant leur participation (par exemple, une participation en association avec une entreprise nationale ou locale) en précisant les **critères** et la définition de la **souveraineté technologique**, ainsi que de s'assurer de l'équilibre entre acteurs de l'Union et de pays tiers. La rapporteure propose en outre qu'un **schéma de certification** soit appliqué aux fournisseurs privés dans le cadre du **mécanisme d'urgence dans le domaine de la cybersécurité** pour bâtir des partenariats fiables et de long terme.

En ce qui concerne le **mécanisme d'analyse des incidents**, la rapporteure souhaite renforcer le rôle de l'ENISA et du secteur privé dans les SOC, assorti des garanties et du suivi qui permettront de vérifier que les acteurs du secteur reprennent à leur compte les enseignements tirés. Elle propose par ailleurs de tenir compte des enseignements tirés des évaluations par les pairs conformément à la directive SRI2 et d'accroître le financement de l'ENISA destiné à garantir la bonne application de la législation et une protection adaptée contre les cybermenaces.

La proposition à l'examen présente, par définition, une **dimension extérieure** très marquée, que ce soit parce que des pays tiers pourront avoir accès aux ressources et au soutien prévu par le règlement sur la cybersolidarité via le soutien à la réaction aux incidents de la réserve de cybersécurité de l'Union ou parce que la participation d'acteurs du secteur privé de pays tiers à la cyberréserve reste nécessaire. La dimension extérieure devrait donc elle aussi être soumise à un contrôle public auquel contribuera le pouvoir législatif afin de garantir la participation des citoyens au processus. Il convient de considérer la cybersécurité comme un bien public.

Le développement d'aptitudes et de compétences, qui ne se limite pas à l'investissement dans l'acquisition de connaissances, mais passe par des investissements dans l'accès de tous les citoyens à des possibilités de formation à ces compétences, est une autre clef de voûte de la proposition à l'examen. La rapporteure propose de renforcer le lien avec l'**académie des compétences en matière de cybersécurité de l'Union**, qui cherche à remédier au déficit de talents en matière de cybersécurité par le rapprochement d'initiatives publiques et privées et la mise à disposition de formations et de qualifications pour les citoyens. Ce renforcement du lien exigera des garanties afin d'éviter une «fuite des cerveaux»; il ne devrait pas nuire non plus à la mobilité professionnelle.

La rapporteure propose également la réalisation d'investissements et l'adoption de mesures volontaristes pour développer les compétences dans ce secteur, compte tenu du fait que 2023 est l'Année européenne des compétences, ainsi que pour mieux sensibiliser les citoyens. Les mesures devront être conçues de telle sorte qu'elles ne créent pas de déséquilibres entre les États membres, étant donné que la forte demande de main-d'œuvre et le niveau élevé des salaires dans le secteur peuvent produire une forme de fuite des cerveaux vers les situations les mieux rémunérées.

C’est pourquoi la rapporteure propose de renforcer les compétences et les aptitudes spécialisées, interdisciplinaires et générales dans l’ensemble de l’Union, en accordant une attention particulière aux femmes. En effet, un écart entre les genres persiste en matière de cybersécurité puisque la présence moyenne des femmes dans ce secteur à l’échelle mondiale est de 20 %[4]. Les femmes doivent être présentes dans la conception de l’avenir et de la gouvernance du numérique et en être actrices.

La rapporteure propose également de renforcer le triangle réunissant les centres de compétences nationaux, le Centre de compétences européen en matière de cybersécurité (ECCC) et l’ENISA en matière de développement des aptitudes et des compétences. Il convient en outre de renforcer le rôle des **entreprises** dans le **développement des compétences** et de nouer des partenariats avec le **monde universitaire** et des acteurs de la société civile, compte étant tenu des expériences, connaissances et spécialisations régionales, ainsi que des alliances avec des pays tiers et des partenaires partageant nos principes afin d’intensifier les échanges et de faire émerger une approche mondiale au service des citoyens, des entreprises et des institutions.

La rapporteure propose aussi une coopération partagée en matière de talents, ainsi que d’évaluation du préjudice des cyberattaques pour les personnes (par exemple, l’incidence d’une attaque par rançongiciel dans le secteur de la santé).

La rapporteure propose l’élaboration de mesures pour, sans alarmisme, associer et sensibiliser davantage les citoyens, ce qui peut être un moyen supplémentaire de garantir la protection de nos démocraties et de nos valeurs fondamentales. Il convient aussi de renforcer la **culture de la cybersécurité**, en vertu de laquelle la sécurité, y compris celle de l’environnement numérique, est un bien public. C’est ainsi que nous parviendrons à défendre un modèle de démocratie numérique, par opposition à l’autoritarisme numérique, fondé sur la transparence, la démocratie et la sécurité juridique qu’apporte une législation élaborée ex ante.

La rapporteure estime par ailleurs que renforcer **la recherche et l’innovation** en matière de cybersécurité améliorera la résilience et l’autonomie stratégique ouverte de l’Union. De même, il convient de veiller aux synergies avec les programmes de recherche et d’innovation et avec les instruments et institutions existants, ainsi que de renforcer le triangle de la connaissance afin de remédier au déficit de compétences dans l’ensemble de l’Union.

Par ailleurs, la législation à l’examen améliorera la résilience de l’Union et de ses États membres, non seulement de manière directe par les dispositions législatives sur la cybersécurité et la cyberrésilience, mais aussi par ses effets possibles sur l’accélération du développement de l’intelligence artificielle, ainsi que par les effets possibles de la réglementation relative aux données et à la protection des données sur la cybersécurité.

En outre, la législation à l’examen nous aidera à remplir l’engagement, énoncé dans la **déclaration européenne sur les droits et principes numériques pour la décennie numérique**, de protéger les intérêts des citoyens, des entreprises et des institutions publiques

[4] Résolution du Parlement européen du 10 juin 2021 sur la promotion de l’égalité des genres en matière de formation et d’emploi dans le domaine des sciences, des technologies, de l’ingénierie et des mathématiques (STIM) (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_FR.html.

contre les risques liés à la cybersécurité et la cybercriminalité, y compris les violations de données et l'usurpation ou la manipulation d'identité.

Au regard de ce qui précède, la rapporteure estime souhaitable que la proposition à l'examen prenne effet le plus rapidement possible, y compris le bouclier de cybersécurité européen et le mécanisme d'urgence dans le domaine de la cybersécurité, afin de disposer d'un cadre général et d'éviter les cloisonnements, puisque le cyberespace est sans frontières.

ANNEXE: ENTITÉS OU PERSONNES DONT LA RAPPORTEURE A REÇU DES CONTRIBUTIONS

Conformément à l'article 8 de l'annexe I du règlement intérieur, la rapporteure déclare avoir reçu des contributions des entités ou personnes suivantes pour l'élaboration du rapport, préalablement à son adoption en commission:

Entité et/ou personne
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

La liste ci-dessus est établie sous la responsabilité exclusive de la rapporteure.

27.10.2023

AVIS DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Rapporteur pour avis: Dragoş Tudorache

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux dans tous les secteurs d'activité économique, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos administrations publiques, de nos entreprises et de nos citoyens par-delà les secteurs et les frontières.	(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux dans tous les secteurs d'activité économique ***et militaire***, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos administrations publiques, de nos entreprises et de nos citoyens***, ainsi que des acteurs de l'armée et de la défense*** par-delà les secteurs et les frontières.

Amendement 2

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent	(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent

de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. ***Ce risque va*** au-delà de l'agression militaire de la Russie contre l'Ukraine et ***il est susceptible*** de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.

de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. ***Ces menaces s'avèrent d'autant plus graves depuis le retour de la guerre sur notre continent. Ces risques vont*** au-delà de l'agression militaire de la Russie contre l'Ukraine et ***ils sont susceptibles*** de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie ***et à la sécurité*** de l'Union, voire mettre en danger la santé ou la vie des personnes ***en compromettant éventuellement des installations liées à la sécurité locale ou nationale***. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays. ***La cybersécurité est importante pour protéger nos valeurs européennes et garantit le fonctionnement de nos démocraties en protégeant nos infrastructures électorales et nos procédures démocratiques de toute***

ingérence étrangère.

Amendement 3

Proposition de règlement
Considérant 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 bis) La cybersécurité est essentielle pour assurer la sécurité de l'Union et éviter que des acteurs malveillants, étatiques ou non, ne portent atteinte à notre démocratie, à notre économie et à notre sécurité. Il est nécessaire d'éviter un paysage fragmenté, car une telle situation ne serait pas une démarche pertinente, en particulier face au défi d'une éventuelle cyberattaque à grande échelle visant simultanément plusieurs États membres ou infrastructures critiques transnationales. Par conséquent, il est nécessaire d'établir un organe de l'Union qui ferait office de plateforme de coordination pour tous les instruments, fonds et mécanismes présents et à venir en matière de cybersécurité.

Amendement 4

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités	(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités

exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité.

[16] https://futureu.europa.eu/fr/

exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité***, ainsi que renforcer sa capacité à agir de manière proactive et à réagir de manière décisive face aux menaces et incidents de cybersécurité***.

[16] https://futureu.europa.eu/fr/

Amendement 5

Proposition de règlement
Considérant 4

Texte proposé par la Commission

(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États

Amendement

(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États

membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.

membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, ***proactive,*** solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur. ***L'Union a par ailleurs approuvé et lancé en mars 2022 sa boussole stratégique pour la sécurité et la défense, qui met notamment l'accent sur le renforcement de la cybersécurité et l'intensification de la coopération internationale avec les alliés et partenaires démocratiques partageant les mêmes valeurs, en particulier dans ce domaine. En outre, la cybersécurité constitue un point central dans la troisième déclaration conjointe sur la coopération UE-OTAN adoptée en janvier 2023. En particulier, le rapport d'évaluation final de l'équipe spéciale UE-OTAN recommandait de tirer pleinement parti des synergies entre l'Union et l'OTAN[1], en favorisant notamment l'échange de bonnes pratiques entre les acteurs civils et militaires en ce qui concerne la mise en œuvre des politiques et de la législation pertinentes en matière de cybersécurité.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

[18] Recommandation (UE) 2017/1584 de la

[17] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

[18] Recommandation (UE) 2017/1584 de la

Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

[19] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

[20] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

[19] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

[20] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Amendement 6

Proposition de règlement
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) La communication conjointe relative à la politique de cyberdéfense de l'UE[22], adoptée le 10 novembre 2022, a annoncé une initiative de l'UE en matière de cybersolidarité dont les objectifs sont les suivants: renforcer les capacités communes de détection, d'appréciation de la situation et de réaction de l'UE en promouvant le déploiement d'une infrastructure de centres d'opérations de sécurité (SOC) de l'UE, constituer progressivement une réserve de cybersécurité au niveau de l'Union comprenant des services de fournisseurs privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'UE.	(6) La communication conjointe relative à la politique de cyberdéfense de l'UE[22], adoptée le 10 novembre 2022, a annoncé une initiative de l'UE en matière de cybersolidarité dont les objectifs sont les suivants: renforcer les capacités communes de détection, d'appréciation de la situation et de réaction de l'UE en promouvant le déploiement d'une infrastructure de centres d'opérations de sécurité (SOC) de l'UE, constituer progressivement une réserve de cybersécurité au niveau de l'Union comprenant des services de fournisseurs privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'UE. ***En outre, l'évolution rapide du panorama des***

cybermenaces et la rapidité du progrès technologique démontrent également la nécessité d'une coordination et d'une coopération civilo-militaires renforcées, comme l'a souligné le Conseil dans ses conclusions sur la politique de cyberdéfense de l'UE[1].

[1] Conclusions du Conseil sur la politique de cyberdéfense de l'UE, approuvées par le Conseil lors de sa session du 22 mai 2023 (9618/23).

---

[22] Communication conjointe au Parlement européen et au Conseil intitulée «La politique de cyberdéfense de l'UE» [JOIN(2022) 49 final].

---

[22] Communication conjointe au Parlement européen et au Conseil intitulée «La politique de cyberdéfense de l'UE» [JOIN(2022) 49 final].

Amendement 7

Proposition de règlement
Considérant 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(6 bis) Compte tenu du brouillage des frontières entre affaires civiles et militaires ainsi que du double usage qui peut être fait des cybertechnologies et des outils y afférents, il convient de définir une démarche globale dans le domaine du numérique. En cas d'incident ou de crise de cybersécurité majeur qui implique plus d'un État membre, des structures appropriées de gestion de crise et de gouvernance devraient être mises en place. Ces structures devraient organiser l'échange d'informations, la coordination et la coopération avec les structures de gestion des crises d'ordre militaire ou touchant à la sécurité extérieure, ainsi qu'avec les organes des États membres chargés de la sécurité et de la défense (la communauté de cyberdéfense). Il devrait en aller de même pour les opérations et missions menées par l'Union dans le cadre de la politique de sécurité et de

défense commune afin d'assurer la paix et la stabilité dans son voisinage et au-delà.

Amendement 8

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des menaces et incidents de cybersécurité dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités de réaction des États membres et de l'UE en cas d'incidents de cybersécurité importants et majeurs. Par conséquent, il convient d'établir: une infrastructure paneuropéenne composée de SOC (le cyberbouclier européen), afin de mettre en place et de renforcer les capacités communes en matière de détection et d'appréciation de la situation; un mécanisme d'urgence dans le domaine de la cybersécurité, afin d'aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs et à y réagir, ainsi qu'à se rétablir immédiatement après de tels incidents; et un mécanisme d'analyse des incidents de cybersécurité, afin d'examiner et d'évaluer des incidents importants ou majeurs particuliers. Ces actions doivent s'entendre sans préjudice des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne (TFUE).	(7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des menaces et incidents de cybersécurité dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités de réaction des États membres et de l'UE en cas d'incidents de cybersécurité importants et majeurs. Par conséquent, il convient d'établir: une infrastructure paneuropéenne composée de SOC (le cyberbouclier européen), afin de mettre en place et de renforcer les capacités communes en matière de détection et d'appréciation de la situation; un mécanisme d'urgence dans le domaine de la cybersécurité, afin d'aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs et à y réagir, ainsi qu'à se rétablir immédiatement après de tels incidents***, notamment lorsque ceux-ci touchent plusieurs États membres. Lorsque c'est possible et nécessaire, un mécanisme d'urgence en matière de cybersécurité devrait organiser le partage d'informations et la coopération avec les autorités de défense des États membres et le soutien des institutions, organes et agences de l'Union (la communauté de cyberdéfense de l'UE)***; et un mécanisme d'analyse des incidents de cybersécurité, afin d'examiner et d'évaluer des incidents importants ou majeurs particuliers***. Ces nouvelles structures devraient également soutenir les opérations et missions de la PSDC de l'Union***. Ces actions doivent s'entendre sans préjudice des articles 107

et 108 du traité sur le fonctionnement de l'Union européenne (TFUE).

Amendement 9

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Aux fins de la bonne gestion financière, il convient d'établir des règles spécifiques portant sur le report des crédits d'engagement et de paiement non utilisés. Tout en respectant le principe en vertu duquel le budget de l'Union est établi sur une base annuelle, il convient que le présent règlement prévoie, compte tenu de la nature imprévisible, exceptionnelle et spécifique de la situation en matière de cybersécurité, des possibilités de reporter des fonds non utilisés qui aillent au-delà de celles établies dans le règlement financier, afin d'optimiser la capacité du mécanisme d'urgence dans le domaine de la cybersécurité à aider les États membres à contrer efficacement les cybermenaces.	(11) Aux fins de la bonne gestion financière, il convient d'établir des règles spécifiques portant sur le report des crédits d'engagement et de paiement non utilisés. Tout en respectant le principe en vertu duquel le budget de l'Union est établi sur une base annuelle, il convient que le présent règlement prévoie, compte tenu de la nature imprévisible, exceptionnelle et spécifique de la situation en matière de cybersécurité, des possibilités de reporter des fonds non utilisés qui aillent au-delà de celles établies dans le règlement financier, afin d'optimiser la capacité du mécanisme d'urgence dans le domaine de la cybersécurité à aider les États membres à contrer efficacement les cybermenaces. ***Ces règles spécifiques permettraient également de fournir un soutien financier à plus long terme aux fins d'une acquisition conjointe d'outils et d'infrastructures ultrasécurisés de nouvelle génération, afin d'améliorer les capacités collectives de détection en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.***

Amendement 10

Proposition de règlement
Considérant 13

Texte proposé par la Commission	*Amendement*
(13) Chaque État membre devrait désigner un organisme public au niveau	(13) Chaque État membre devrait désigner un organisme public au niveau

national chargé de coordonner les activités de détection des cybermenaces sur son territoire. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle.

national chargé de coordonner les activités de détection des cybermenaces sur son territoire. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle. ***Lorsque cela est possible et nécessaire, les SOC devraient également permettre la participation d'entités de défense, en mettant sur pied un «pilier de défense» en matière de gouvernance et en ce qui concerne le type d'informations transmises, tel que prévu dans la communication conjointe relative à la politique de cyberdéfense de l'UE[1], et avec le soutien du haut-représentant.***

[1] Communication conjointe au Parlement européen et au Conseil intitulée «La politique de cyberdéfense de l'UE» (JOIN(2022) 49 final).

Amendement 11

Proposition de règlement
Considérant 14

Texte proposé par la Commission	*Amendement*
(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres afin de tirer pleinement parti des avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements	(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres***, notamment un «pilier en matière de défense»,*** afin de tirer pleinement parti des avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de

de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, ***à*** l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. Ils devraient également apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les centres de réponse aux incidents de sécurité informatique (CSIRT) et sur d'autres acteurs pertinents, et en les complétant.	contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées ***et***, ***lorsque cela est nécessaire et possible, militaires avec des orientations suffisantes pour le partage d'informations, ainsi qu'à*** l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. Ils devraient également apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les centres de réponse aux incidents de sécurité informatique (CSIRT) et sur d'autres acteurs pertinents, et en les complétant.

Amendement 12

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la ***souveraineté technologique*** de l'Union.	(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la ***résilience*** de l'Union.

Amendement 13

Proposition de règlement
Considérant 16

Texte proposé par la Commission	*Amendement*
(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures ***critiques]***. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.	(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures ***critiques, ainsi que la communauté de cyberdéfense]***. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle ***et participer, lorsqu'il sera mis en place, au réseau opérationnel pour les CERT militaires (réseau MICNET)***.

Amendement 14

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*
(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La	(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La

directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT et à la Commission. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations transmises.

directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT***, à la communauté de cyberdéfense*** et à la Commission. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations transmises.

Amendement 15

Proposition de règlement
Considérant 19

Texte proposé par la Commission	*Amendement*
(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.	(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés***, à l'exclusion des fournisseurs à haut risque de produits critiques comportant des éléments numériques***. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données. ***L'IA devrait faire l'objet d'un contrôle humain, et il convient de s'assurer que les personnes qui exercent cette fonction disposent du niveau de connaissance de l'outil, du soutien et de l'autorité nécessaires.***

Amendement 16

Proposition de règlement
Considérant 19 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(19 bis) Conformément au règlement [XX/XXXX (loi sur la cyberrésilience)], les entités qui participent au cyberbouclier européen devraient également satisfaire aux exigences énoncées dans le présent règlement en ce qui concerne tous les produits comportant des éléments numériques. Compte tenu des risques croissants liés aux dépendances économiques, il est nécessaire de réduire

	au minimum l'exposition aux fournisseurs à haut risque de produits critiques, au moyen d'un cadre stratégique commun pour assurer la sécurité économique de l'Union. La dépendance à l'égard des fournisseurs à haut risque de produits critiques comportant des éléments numériques pose un risque stratégique qui devrait être traité à l'échelle de l'Union, en particulier si un pays se livre à des activités d'espionnage économique ou exerce des pressions économiques et si sa législation impose un accès arbitraire aux opérations ou aux données de l'entreprise de quelque nature qu'elles soient, notamment lorsque les produits critiques sont destinés à être utilisés par les entités essentielles visées dans la directive (UE) nº 2022/2555.

Amendement 17

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer la souveraineté technologique de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].	(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer la souveraineté technologique de l'Union***, son autonomie stratégique, sa compétitivité et sa résilience***. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].
[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le	[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le

règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

Amendement 18

Proposition de règlement
Considérant 25

Texte proposé par la Commission	*Amendement*
(25) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement immédiat en cas d'incidents de cybersécurité importants et majeurs, tels que les services fournis par l'Agence de l'Union européenne pour la cybersécurité (ENISA) conformément à son mandat, la réaction et l'assistance coordonnée du réseau des CSIRT, les mesures d'atténuation apportées par EU-CyCLONe, et l'assistance mutuelle que se prêtent les États membres notamment au titre de l'article 42, paragraphe 7, du TUE, ainsi que dans le contexte des équipes d'intervention rapide en cas d'incident informatique de la CSP***26*** et des équipes de réaction rapide en cas de menaces hybrides. Ce mécanisme devrait ***faire en sorte*** que des moyens ***spécialisés*** soient mis à disposition pour soutenir la préparation et la réaction aux incidents de cybersécurité dans toute l'Union et dans les pays tiers.	(25) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement immédiat en cas d'incidents de cybersécurité importants et majeurs, tels que les services fournis par l'Agence de l'Union européenne pour la cybersécurité (ENISA) conformément à son mandat, la réaction et l'assistance coordonnée du réseau des CSIRT, les mesures d'atténuation apportées par EU-CyCLONe, et l'assistance mutuelle que se prêtent les États membres notamment au titre de l'article 42, paragraphe 7, du TUE, ainsi que dans le contexte des équipes d'intervention rapide en cas d'incident informatique de la CSP ***[1], du nouveau projet CSP relatif au Centre de coordination dans le domaine du cyber*** et ***de l'information (CIDCC) et du Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC) envisagé pour lui succéder, ainsi que*** des équipes de réaction rapide en cas de menaces hybrides. Ce mécanisme devrait ***permettre*** que des moyens ***spécifiques*** soient mis à disposition pour soutenir la préparation et la réaction aux incidents de cybersécurité dans toute l'Union et dans les pays tiers***, en particulier les pays candidats à l'adhésion à la politique étrangère et de sécurité commune et à la politique de sécurité et de défense commune de l'Union, en les aidant à renforcer leurs capacités cybernétiques et à améliorer la***

coopération transfrontière et régionale entre ces pays dans le domaine de la cybernétique.

[1] Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants.

---

[26] Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants.

[26] Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants.

Amendement 19

Proposition de règlement
Considérant 26

Texte proposé par la Commission	*Amendement*
(26) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination de la réaction aux crises au niveau de l'Union, en particulier le MPCU[27], l'IPCR[28], et la directive (UE) 2022/2555. Il pourrait contribuer aux actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du TUE ou dans les situations définies à l'article 222 du TFUE, ou les compléter. Le recours à cet instrument devrait également être coordonné***, s'il y a lieu,*** avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatique.	(26) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination de la réaction aux crises au niveau de l'Union, en particulier le MPCU[27], l'IPCR[28], et la directive (UE) 2022/2555. Il pourrait contribuer aux actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du TUE ou dans les situations définies à l'article 222 du TFUE, ou les compléter. Le recours à cet instrument devrait également être coordonné avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatique***, en consolidant la coopération aux niveaux stratégique, opérationnel et technique entre la communauté de cyberdéfense et les autres cybercommunautés, en particulier afin de renforcer les capacités de lutte contre les menaces de cybersécurité provenant de pays tiers, y compris par des mesures restrictives pouvant être utilisées pour prévenir les actes de cybermalveillance et y répondre***.

[27] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

[28] Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) et conformément à la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

[27] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

[28] Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) et conformément à la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

Amendement 20

Proposition de règlement
Considérant 28

Texte proposé par la Commission	*Amendement*
(28) La directive (UE) 2022/2555 impose aux États membres de désigner ou d'établir une ou plusieurs autorités de gestion des crises cyber et de veiller à ce qu'elles disposent de ressources suffisantes pour s'acquitter de leurs tâches de manière effective et efficace. Elle exige aussi que les États membres recensent les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise et qu'ils adoptent un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Les États membres sont également tenus de mettre en place un ou plusieurs CSIRT, qui sont chargés de la gestion des incidents selon un processus bien défini et qui couvrent au moins les secteurs, les sous-secteurs et les types d'entités relevant du champ d'application de ladite directive, ainsi que de veiller à ce que les CSIRT disposent de ressources suffisantes pour s'acquitter efficacement de leurs tâches. Le présent règlement est sans préjudice du	(28) La directive (UE) 2022/2555 impose aux États membres de désigner ou d'établir une ou plusieurs autorités de gestion des crises cyber et de veiller à ce qu'elles disposent de ressources suffisantes pour s'acquitter de leurs tâches de manière effective et efficace. Elle exige aussi que les États membres recensent les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise et qu'ils adoptent un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Les États membres sont également tenus de mettre en place un ou plusieurs CSIRT, qui sont chargés de la gestion des incidents selon un processus bien défini et qui couvrent au moins les secteurs, les sous-secteurs et les types d'entités relevant du champ d'application de ladite directive, ainsi que de veiller à ce que les CSIRT disposent de ressources suffisantes pour s'acquitter efficacement de leurs tâches. Le présent règlement est sans préjudice du

rôle de la Commission, chargée de garantir que les États membres respectent les obligations qui leur incombent en vertu de la directive (UE) 2022/2555. Le mécanisme d'urgence dans le domaine de la cybersécurité devrait fournir une assistance dans le cadre des mesures destinées à renforcer la préparation ainsi que des mesures de réaction visant à atténuer les effets des incidents de cybersécurité importants et majeurs, à soutenir un rétablissement immédiat ou à rétablir le fonctionnement des services essentiels.

rôle de la Commission, chargée de garantir que les États membres respectent les obligations qui leur incombent en vertu de la directive (UE) 2022/2555. Le mécanisme d'urgence dans le domaine de la cybersécurité devrait fournir une assistance dans le cadre des mesures destinées à renforcer la préparation ainsi que des mesures de réaction visant à atténuer les effets des incidents de cybersécurité importants et majeurs, à soutenir un rétablissement immédiat ou à rétablir le fonctionnement des services essentiels***, en recourant de façon appropriée à l'ensemble des options de défense à la disposition des communautés civiles et militaires***.

Amendement 21

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Dans le cadre des mesures de préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur	(29) Dans le cadre des mesures de préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. ***Il convient de faire intervenir, s'il y a lieu, le Service européen pour l'action extérieure (SEAE), notamment par l'intermédiaire du Centre de situation et du renseignement de l'UE (IntCen) et de sa***

des méthodes et des scénarios de risque communs. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE); l'évaluation coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du Parlement européen et du Conseil***29***. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

cellule de fusion contre les ***menaces hybrides, avec le soutien de la direction «Renseignement» de l'état-major de l'Union européenne (EMUE) dans le cadre de la capacité unique d'analyse du renseignement (SIAC), afin de fournir des évaluations à jour et ainsi contribuer au recensement des*** secteurs ou sous-secteurs ***qui*** devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs***. Ces exercices devraient également jouer un rôle important dans l'amélioration de la coopération entre les entités civiles et militaires. Lorsqu'ils organisent des exercices, la Commission, le SEAE et l'ENISA devraient donc systématiquement envisager la participation de représentants d'autres cybercommunautés, telles que l'Agence européenne de défense (AED) et d'autres entités concernées.*** La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications

électroniques (ORECE); l'évaluation coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du Parlement européen et du Conseil ***[1]***. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

[1] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

---

[29] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

---

[29] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

Amendement 22

Proposition de règlement
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir les États membres lorsqu'ils apportent une assistance à un État membre touché par un incident de cybersécurité important ou majeur, y compris l'assistance fournie par le réseau des CSIRT en vertu de l'article 15 de la	(32) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir les États membres lorsqu'ils apportent une assistance à un État membre touché par un incident de cybersécurité important ou majeur, y compris l'assistance fournie par le réseau des CSIRT en vertu de l'article 15 de la

directive (UE) 2022/2555. Les États membres apportant une assistance devraient être en mesure de demander que les coûts liés à l'envoi d'équipes d'experts dans le cadre de l'assistance mutuelle soient couverts. Les coûts éligibles pourraient inclure les frais de déplacement et de logement ainsi que les indemnités journalières des experts en cybersécurité.

directive (UE) 2022/2555. Les États membres apportant une assistance devraient être en mesure de demander que les coûts liés à l'envoi d'équipes d'experts dans le cadre de l'assistance mutuelle soient couverts***, en assurant une coordination efficace entre les programmes et instruments pertinents de l'Union, notamment la facilité européenne pour la paix (FEP), la politique étrangère et de sécurité commune (PESC) et l'instrument de voisinage, de coopération au développement et de coopération internationale, dans le cadre de l'assistance aux pays tiers, en particulier l'Ukraine et la Moldavie***. Les coûts éligibles pourraient inclure les frais de déplacement et de logement ainsi que les indemnités journalières des experts en cybersécurité.

Amendement 23

Proposition de règlement
Considérant 33

Texte proposé par la Commission	*Amendement*
(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il	(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il

devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires.

devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, ***y compris les missions PSDC,*** dans des conditions similaires.

Amendement 24

Proposition de règlement
Considérant 34

Texte proposé par la Commission	*Amendement*
(34) La sélection des fournisseurs de services privés qui proposeront des services dans le cadre de la réserve de cybersécurité de l'UE nécessite de définir un ensemble de critères minimaux à inclure dans l'appel d'offres visant à sélectionner ces fournisseurs, afin de garantir que les besoins des autorités des États membres et des entités actives dans des secteurs critiques ou hautement critiques sont satisfaits.	(34) La sélection des fournisseurs de services privés qui proposeront des services dans le cadre de la réserve de cybersécurité de l'UE nécessite de définir un ensemble de critères minimaux à inclure dans l'appel d'offres visant à sélectionner ces fournisseurs, afin de garantir que les besoins des autorités des États membres et des entités actives dans des secteurs critiques ou hautement critiques sont satisfaits***, en tenant également compte des risques liés à la participation de fournisseurs provenant de pays concurrents stratégiques, qui peuvent donner lieu à des risques pour la sécurité économique, ainsi que des implications pour la sécurité stratégique de l'Union***.

Amendement 25

Proposition de règlement
Considérant 36

Texte proposé par la Commission	*Amendement*
(36) Dans le droit fil des objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents importants et majeurs	(36) Dans le droit fil des objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents importants et majeurs

poursuivis par le présent règlement, EU-CyCLONe, le réseau des CSIRT ou la Commission devraient être en mesure de demander à l'ENISA d'analyser et d'évaluer les menaces, vulnérabilités et mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA devrait établir un rapport d'analyse, en collaboration avec les parties prenantes concernées, notamment les représentants du secteur privé, les États membres, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En ce qui concerne le secteur privé, l'ENISA met en place des canaux d'échange d'informations avec des fournisseurs spécialisés, notamment des fournisseurs de solutions de sécurité gérées et des vendeurs, afin de contribuer à sa mission, qui consiste à atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. En s'appuyant sur la collaboration avec les parties prenantes, y compris avec le secteur privé, les rapports d'analyse portant sur des incidents spécifiques devraient servir à évaluer les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits. Il convient d'accorder une attention particulière aux informations et aux enseignements transmis par les fournisseurs de services de sécurité gérés qui font preuve du plus haut niveau d'intégrité professionnelle, d'impartialité et d'expertise technique requise, comme l'exige le présent règlement. Le rapport devrait être communiqué à EU-CyCLONe, au réseau des CSIRT et à la Commission, et devrait être intégré à leurs travaux. Lorsque l'incident en question touche un pays tiers, la Commission devrait également transmettre le rapport au haut représentant.

poursuivis par le présent règlement, EU-CyCLONe, le réseau des CSIRT ou la Commission devraient être en mesure de demander à l'ENISA d'analyser et d'évaluer les menaces, vulnérabilités et mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique. ***En vue du développement d'un système de connectivité sécurisé s'appuyant sur l'infrastructure européenne de communication quantique (EuroQCI) et le programme de communication gouvernementale par satellite de l'Union européenne (Govsatcom), et notamment sur le déploiement du GALILEO GNSS pour les utilisateurs dans le domaine de la défense, tout développement futur devrait tenir compte de l'avènement de «l'hyperguerre», qui combine la vitesse et la complexité de l'informatique quantique avec des systèmes militaires hautement autonomes.*** Après l'analyse et l'évaluation d'un incident, l'ENISA devrait établir un rapport d'analyse, en collaboration avec les parties prenantes concernées, notamment les représentants du secteur privé, les États membres, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En ce qui concerne le secteur privé, l'ENISA met en place des canaux d'échange d'informations avec des fournisseurs spécialisés, notamment des fournisseurs de solutions de sécurité gérées et des vendeurs, afin de contribuer à sa mission, qui consiste à atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. En s'appuyant sur la collaboration avec les parties prenantes, y compris avec le secteur privé, les rapports d'analyse portant sur des incidents spécifiques devraient servir à évaluer les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits. Il convient d'accorder une attention particulière aux informations et aux enseignements transmis par les fournisseurs de services de sécurité gérés qui font preuve du plus haut niveau

d'intégrité professionnelle, d'impartialité et d'expertise technique requise, comme l'exige le présent règlement. Le rapport devrait être communiqué à EU-CyCLONe, au réseau des CSIRT et à la Commission, et devrait être intégré à leurs travaux. Lorsque l'incident en question touche un pays tiers, la Commission devrait également transmettre le rapport au haut représentant***, au SEAE et aux missions PSDC dans le pays touché par l'incident, par l'intermédiaire de leur siège***.

Amendement 26

Proposition de règlement
Considérant 37

Texte proposé par la Commission	*Amendement*
(37) Compte tenu de la nature imprévisible des cyberattaques, du fait qu'elles ne se limitent souvent pas à une zone géographique déterminée et qu'elles présentent un risque élevé de propagation, le renforcement de la résilience des pays voisins et leur capacité à réagir efficacement à des incidents de cybersécurité importants et majeurs contribuent à la protection de l'Union dans son ensemble. Par conséquent, les pays tiers associés au programme pour une Europe numérique ***peuvent*** recevoir l'aide de la réserve de cybersécurité de l'UE ***lorsque leur accord d'association à ce programme le prévoit***. Le soutien apporté à ces pays tiers associés devrait être financé par l'Union dans le cadre des partenariats et des instruments de financement concernés pour ces pays. Il devrait couvrir les services correspondant à la réaction et au rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. Les conditions relatives à la réserve de cybersécurité de l'UE et aux fournisseurs de confiance fixées dans le présent règlement devraient s'appliquer au soutien apporté aux pays tiers associés au	(37) Compte tenu de la nature imprévisible des cyberattaques, du fait qu'elles ne se limitent souvent pas à une zone géographique déterminée et qu'elles présentent un risque élevé de propagation, le renforcement de la résilience des pays voisins***, en particulier l'Ukraine et la Moldavie,*** et leur capacité à réagir efficacement à des incidents de cybersécurité importants et majeurs contribuent à la protection de l'Union dans son ensemble. Par conséquent, les pays tiers associés au programme pour une Europe numérique ***devraient*** recevoir l'aide de la réserve de cybersécurité de l'UE***. Il convient que cette aide soit également accordée aux pays tiers qui accueillent sur leur territoire une mission PSDC dotée d'un mandat précis consistant à renforcer la résilience face aux menaces hybrides, notamment face aux cybermenaces, ou qui bénéficient d'une mesure d'assistance au titre de la FEP aux fins du renforcement de la cyberrésilience du pays***. Le soutien apporté à ces pays tiers associés devrait être financé par l'Union dans le cadre des partenariats et des instruments de

programme pour une Europe numérique.	financement concernés pour ces pays. Il devrait couvrir les services correspondant à la réaction et au rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. Les conditions relatives à la réserve de cybersécurité de l'UE et aux fournisseurs de confiance fixées dans le présent règlement devraient s'appliquer au soutien apporté aux pays tiers associés au programme pour une Europe numérique.

Amendement 27

Proposition de règlement
Article 1 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents importants ou majeurs.	c) la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents ***ou menaces*** importants ou majeurs.

Amendement 28

Proposition de règlement
Article 1 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la ***souveraineté*** technologique de l'Union dans le domaine de la cybersécurité;	a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la ***résilience*** technologique de l'Union dans le domaine de la cybersécurité;

Amendement 29

Proposition de règlement
Article 1 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;	b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité***, ou aux pays tiers qui sont candidats à l'adhésion à l'Union et ne portent pas atteinte aux intérêts de sécurité et de défense de l'Union et de ses États membres, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE; Les États membres devraient envisager d'intégrer à leur stratégie nationale de cybersécurité un programme de cyberdéfense active assorti d'exercices d'entraînement communs entre les États membres et les organisations internationales. Un tel programme devrait permettre de détecter, d'analyser et d'atténuer les menaces de manière synchronisée et en temps réel.***

Amendement 30

Proposition de règlement
Article 1 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. réduire les risques systémiques en matière de cybersécurité liés à la dépendance à l'égard des équipements critiques provenant de pays qui porteraient atteinte aux intérêts de l'Union et de ses États membres en

matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE;

Amendement 31

Proposition de règlement
Article 2 – point 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	«communauté de cyberdéfense»: les autorités de défense des États membres, soutenues par les institutions, organes et organismes de l'Union, telle que définie dans la communication conjointe sur la politique de cyberdéfense de l'UE[1].
	[1] Communication conjointe au Parlement européen et au Conseil intitulée «La politique de cyberdéfense de l'UE» [JOIN(2022) 49 final].

Amendement 32

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) contribue à moderniser l'ensemble des systèmes de cyberdéfense, en améliorant les capacités de cyberdéfense par le déploiement de systèmes d'IA, et à accélérer l'échange d'informations entre les SOC nationaux et les SOC transfrontières;

Amendement 33

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	d bis) analyse et évalue les technologies

	et les équipements de cybersécurité critiques déployés par les SOC pour réagir face aux incidents de cybersécurité, afin de détecter les risques systémiques liés à l'influence sur des fournisseurs à haut risque par des pays qui porteraient atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE;

Amendement 34

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées au niveau national pour collecter et analyser des informations sur les menaces et incidents de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.	Il peut servir de point de référence et d'accès à d'autres organisations publiques et privées***, voire si nécessaire militaires,*** au niveau national pour collecter et analyser des informations sur les menaces et incidents de cybersécurité et contribuer aux travaux d'un SOC transfrontière. Il est équipé de technologies de pointe permettant de détecter, d'agréger et d'analyser les données pertinentes pour les menaces et incidents de cybersécurité.

Amendement 35

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux sont sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et	2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux sont sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et

infrastructures. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	infrastructures***, à la stricte condition que ces outils et infrastructures soient fournis par des fournisseurs de confiance, conformément à l'article 16***. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

Amendement 36

Proposition de règlement
Article 5 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, un consortium d'hébergement est sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement des outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le consortium d'hébergement. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le consortium d'hébergement concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	2. À la suite d'un appel à manifestation d'intérêt, un consortium d'hébergement est sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement de ces outils et infrastructures***, à la stricte condition que ces outils et infrastructures soient fournis par des fournisseurs de confiance, conformément à l'article 16***. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par le consortium d'hébergement. Avant de lancer la procédure d'acquisition des outils et infrastructures, l'ECCC et le consortium d'hébergement concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

Amendement 37

Proposition de règlement
Article 5 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Toute infrastructure ou tout fournisseur originaire d'un pays tiers à haut risque est automatiquement exclu.

Amendement 38

Proposition de règlement
Article 6 – paragraphe 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) contribue directement au renforcement des capacités militaires et de défense des membres participants ou permet de prévenir une menace directe et imminente à leur sécurité. Compte tenu des graves perturbations et dommages qui peuvent découler de l'exploitation des vulnérabilités dans le secteur de la défense, la cybersécurité de l'industrie de la défense doit reposer sur des mesures spéciales pour garantir la sécurité de la chaîne d'approvisionnement, au regard notamment des entités qui sont en bas de cette chaîne et qui n'ont pas besoin d'accéder à des informations classifiées, mais qui pourraient exposer l'ensemble du secteur à des risques importants. Il convient d'accorder une attention particulière aux répercussions d'un éventuel incident et de la menace émanant de toute manipulation des données de réseau qui pourrait paralyser des moyens de défense essentiels, voire neutraliser les systèmes d'exploitation et les rendre ainsi vulnérables au piratage.

Amendement 39

Proposition de règlement
Article 6 – paragraphe 1 – point b ter (nouveau)

Texte proposé par la Commission	*Amendement*
	b ter) contribue au renforcement des capacités de défense des membres participants ou permet de prévenir une menace directe et imminente à leur sécurité, en garantissant la sécurité des chaînes d'approvisionnement, au regard notamment des entités qui sont en bas de cette chaîne et qui n'ont pas besoin d'accéder à des informations classifiées, mais qui pourraient exposer l'ensemble du secteur à des risques importants.

Amendement 40

Proposition de règlement
Article 7 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe, au réseau des CSIRT et à la Commission, compte tenu de leurs rôles respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.	1. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils fournissent sans retard injustifié les informations pertinentes à EU-CyCLONe, au réseau des CSIRT et à la Commission, ***de même qu'au haut représentant et au SEAE lorsqu'il est question d'un pays tiers,*** compte tenu de leurs rôles respectifs en matière de gestion des crises conformément à la directive (UE) 2022/2555.

Amendement 41

Proposition de règlement
Article 8 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé de sécurité des données et de	1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé de sécurité des données et de

sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris ***celle*** des données échangées par l'intermédiaire de l'infrastructure.	sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, ***de réduire les risques et de promouvoir l'avantage technologique de l'Union dans les secteurs critiques,*** y compris ***des mesures visant à limiter ou à interdire les fournisseurs à haut risque, ainsi qu'à protéger la sécurité*** des données échangées par l'intermédiaire de l'infrastructure.

Amendement 42

Proposition de règlement
Article 8 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres participant au cyberbouclier européen veillent à ce que le partage d'informations au sein du cyberbouclier européen avec des entités qui ne sont pas des organismes publics des États membres ne nuise pas aux intérêts de l'Union en matière de sécurité.	2. Les États membres participant au cyberbouclier européen veillent à ce que le partage d'informations au sein du cyberbouclier européen avec des entités qui ne sont pas des organismes publics des États membres ne nuise pas aux intérêts de l'Union en matière de sécurité ***et à ce que le partage de toute information avec des fournisseurs à haut risque ait une portée limitée et ne nuise pas aux intérêts de l'Union en matière de sécurité et de stratégie***.

Amendement 43

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des	3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des

paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.	paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires***, en recourant de façon appropriée à l'ensemble des options de défense à la disposition des communautés civiles et militaires à des fins plus larges de sécurité et de défense de l'Union, et elle en informe le Parlement***.

Amendement 44

Proposition de règlement
Article 9 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les actions mettant en œuvre le mécanisme d'urgence dans le domaine de la cybersécurité sont soutenues par un financement au titre du programme pour une Europe numérique et réalisées conformément au règlement (UE) 2021/694, et notamment à son objectif spécifique 3.	2. Les actions mettant en œuvre le mécanisme d'urgence dans le domaine de la cybersécurité sont soutenues par un financement au titre du programme pour une Europe numérique et réalisées conformément au règlement (UE) 2021/694, et notamment à son objectif spécifique 3***, ainsi qu'au titre de la facilité européenne pour la paix (FEP) dans le cadre de l'octroi de mesures d'assistance à des pays tiers, en particulier l'Ukraine et la Moldavie***.

Amendement 45

Proposition de règlement
Article 10 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de	a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques, ***tels que les***

l'Union;	***infrastructures publiques, les infrastructures électorales, les transports, les soins de santé, les services financiers, les télécommunications, l'approvisionnement alimentaire et la sécurité*** dans l'ensemble de l'Union;

Amendement 46

Proposition de règlement
Article 10 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
c) les mesures d'assistance mutuelle consistant en la fourniture d'une assistance par les autorités nationales d'un État membre à un autre État membre, notamment conformément à l'article 11, paragraphe 3, point f), de la directive (UE) 2022/2555**.**	c) les mesures d'assistance mutuelle consistant en la fourniture d'une assistance par les autorités nationales d'un État membre à un autre État membre, notamment conformément à l'article 11, paragraphe 3, point f), de la directive (UE) 2022/2555 ***et dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne et de l'article 222 du traité sur le fonctionnement de l'Union européenne;***

Amendement 47

Proposition de règlement
Article 10 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) le remplacement et la suppression progressive des équipements critiques fournis par des fournisseurs à haut risque, qui porteraient atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE.

Amendement 48

Proposition de règlement
Article 11 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA ***et*** le haut représentant, élabore des scénarios de risque et des méthodologies communs pour les exercices de tests coordonnés.	2. Le groupe de coopération SRI, en collaboration avec la Commission, l'ENISA***,*** le haut représentant, ***le SEAE et, le cas échéant, l'Agence européenne de défense (AED),*** élabore des scénarios de risque et des méthodologies communs pour les exercices de tests coordonnés.

Amendement 49

Proposition de règlement
Article 12 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres.	2. La réserve de cybersécurité de l'Union se compose de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés conformément aux critères énoncés à l'article 16. La réserve comprend des services affectés au préalable. Les services peuvent être déployés dans tous les États membres ***et pays tiers qui satisfont aux exigences applicables au titre du présent règlement***.

Amendement 50

Proposition de règlement
Article 12 – paragraphe 3– point b

Texte proposé par la Commission	*Amendement*
b) les institutions, organes et organismes de l'Union.	b) les institutions, organes et organismes de l'Union***, y compris les missions PSDC***.

Amendement 51

Proposition de règlement
Article 12 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les utilisateurs visés au paragraphe 3, point a), ont recours aux services de la réserve de cybersécurité de l'Union afin de réagir aux incidents importants ou majeurs touchant des entités actives dans des secteurs critiques ou hautement critiques, ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.	4. Les utilisateurs visés au paragraphe 3, point a), ont recours aux services de la réserve de cybersécurité de l'Union afin de réagir aux incidents importants ou majeurs touchant des entités actives dans des secteurs critiques ou hautement critiques, ***tels que les infrastructures publiques, les infrastructures électorales, les transports, les soins de santé, les services financiers, les télécommunications, l'approvisionnement alimentaire et la sécurité,*** ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.

Amendement 52

Proposition de règlement
Article 12 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission assume la responsabilité globale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union.	5. La Commission assume la responsabilité globale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres ***objectifs,*** actions et programmes de l'Union***, en particulier l'objectif stratégique visant à réduire la dépendance à l'égard des fournisseurs à haut risque, qui porteraient atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en***

vertu du titre V du traité UE.

Amendement 53

Proposition de règlement
Article 12 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.	7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA***, soutenue par le SEAE,*** établit une autre carte similaire, après consultation de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.

Amendement 54

Proposition de règlement
Article 14 – paragraphe 2 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) les conséquences de l'incident sur la sécurité et la défense de l'Union;

Amendement 55

Proposition de règlement
Article 15 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la	3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la

politique de sécurité et de défense commune, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique. Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne.	politique de sécurité et de défense commune, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique ***(CRRT), afin de mieux soutenir les États membres de l'Union, les missions et les opérations au titre de la PSDC ainsi que les pays tiers qui se sont alignés sur la politique étrangère et de sécurité commune et la politique de sécurité et de défense commune de l'Union dans le cadre de leurs efforts de renforcement des capacités de cyberdéfense, en particulier l'Ukraine et la Moldavie***. Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne.

Amendement 56

Proposition de règlement
Article 16 – paragraphe 2 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) le fournisseur démontre que ses structures de décision et de gestion sont libres de toute influence injustifiée de gouvernements d'États qui porterait atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE;

Amendement 57

Proposition de règlement
Article 16 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) le fournisseur possède l'équipement technique matériel et logiciel nécessaire au service demandé;	f) le fournisseur possède l'équipement technique matériel et logiciel nécessaire au service demandé ***et satisfait aux exigences énoncées à l'article X du***

règlement XX/XXXX (loi sur la cyberrésilience);

Amendement 58

Proposition de règlement
Article 16 – paragraphe 2 – point j bis (nouveau)

Texte proposé par la Commission	*Amendement*
	j bis) aucun fournisseur originaire d'un pays tiers à haut risque n'est admissible.

Amendement 59

Proposition de règlement
Article 16 – paragraphe 2 – point j ter (nouveau)

Texte proposé par la Commission	*Amendement*
	j ter) le fournisseur coopère étroitement avec les PME concernées, dans la mesure du possible;

Amendement 60

Proposition de règlement
Article 17 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les pays tiers peuvent demander une aide à la réserve de cybersécurité de l'UE lorsque les accords d'association conclus en ce qui concerne leur participation au programme pour une Europe numérique le prévoient.	1. Les pays tiers peuvent demander une aide à la réserve de cybersécurité de l'UE lorsque***:***
	a) les accords d'association conclus en ce qui concerne leur participation au programme pour une Europe numérique le prévoient***;***
	b) ces mêmes pays tiers accueillent sur leur territoire une mission PSDC dotée d'un mandat précis consistant à renforcer la résilience face aux menaces hybrides,

notamment face aux cybermenaces, ou bénéficient d'une mesure d'assistance au titre de la FEP aux fins du renforcement de la cyberrésilience du pays.

Amendement 61

Proposition de règlement
Article 17 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'aide apportée par la réserve de cybersécurité de l'Union est conforme au présent règlement et respecte toutes les conditions spécifiques énoncées dans les accords d'association visés au paragraphe 1.	2. L'aide apportée par la réserve de cybersécurité de l'Union est conforme au présent règlement et respecte toutes les conditions spécifiques énoncées dans les accords d'association visés au paragraphe 1***, excepté pour les pays tiers couverts par les dispositions énoncées au paragraphe 1, point b)***.

Amendement 62

Proposition de règlement
Article 18 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. À la demande de la Commission, d'EU-CyCLONe ou du réseau des CSIRT, l'ENISA analyse et évalue les menaces, les vulnérabilités et les mesures d'atténuation d'un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA remet un rapport d'analyse au réseau des CSIRT, à EU-CyCLONe et à la Commission afin de les aider à s'acquitter de leurs tâches, compte tenu notamment de celles énoncées aux articles 15 et 16 de la directive (UE) 2022/2555. Le cas échéant, la Commission transmet le rapport au haut représentant.	1. À la demande de la Commission, d'EU-CyCLONe ou du réseau des CSIRT, l'ENISA analyse et évalue les menaces, les vulnérabilités et les mesures d'atténuation d'un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA remet un rapport d'analyse au réseau des CSIRT, à EU-CyCLONe et à la Commission afin de les aider à s'acquitter de leurs tâches, compte tenu notamment de celles énoncées aux articles 15 et 16 de la directive (UE) 2022/2555. Le cas échéant, ***en particulier lorsque l'incident en question touche un pays tiers,*** la Commission transmet le rapport au haut représentant ***et au SEAE***.

Amendement 63

Proposition de règlement
Article 18 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. Le rapport est communiqué au Parlement européen conformément au droit de l'Union ou au droit national en matière de protection des informations classifiées sensibles.

Amendement 64

Proposition de règlement
Article 19 – alinéa 1 – point 1) a) 1)
Règlement (UE) 2021/694
Article 6 – paragraphe 1 – point a bis)

Texte proposé par la Commission	*Amendement*
«a *bis*) soutenir le développement d'un cyberbouclier européen, y compris la mise au point, le déploiement et l'exploitation de plateformes SOC nationales et transfrontières qui contribuent à l'appréciation de la situation dans l'Union et au renforcement des capacités en matière de renseignement sur les cybermenaces de l'Union;»;	«a *bis*) soutenir le développement d'un cyberbouclier européen, y compris la mise au point, le déploiement et l'exploitation de plateformes SOC nationales et transfrontières qui contribuent à l'appréciation de la situation dans l'Union et au renforcement des capacités en matière de renseignement sur les cybermenaces de l'Union***, ainsi qu'à la réduction de la dépendance de l'Union à l'égard des fournisseurs à haut risque d'équipements ou de composants critiques en matière de cybersécurité qui porteraient atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE***;

Amendement 65

Proposition de règlement
Article 20

Texte proposé par la Commission	*Amendement*
Au plus tard le [***quatre*** ans après la date d'application du présent règlement], la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement.	Au plus tard le [***trois*** ans après la date d'application du présent règlement ***et tous les deux ans par la suite***], la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement.

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Établissement des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir
Références	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 1.6.2023
Avis émis par Date de l'annonce en séance	AFET 1.6.2023
Rapporteur pour avis Date de la nomination	Dragoş Tudorache 16.6.2023
Examen en commission	18.9.2023
Date de l'adoption	24.10.2023
Résultat du vote final	+: 39 –: 4 0: 0
Membres présents au moment du vote final	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Suppléants présents au moment du vote final	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION SAISIE POUR AVIS

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	–
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Légende des signes utilisés:
+ : pour
– : contre
0 : abstention

25.10.2023

AVIS DE LA COMMISSION DES TRANSPORTS ET DU TOURISME

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Rapporteur pour avis: Gheorghe Falcă

JUSTIFICATION SUCCINCTE

Les organisations touchées par les cyberattaques, y compris dans le secteur des transports, les signalent rarement, en particulier les entreprises du secteur privé, car elles ont tendance à les considérer comme de la «mauvaise publicité». La plupart des organisations préfèrent les traiter en interne et ce sont souvent les auteurs de ces attaques qui les rendent publiques. La bonne nouvelle, c'est que l'entrée en vigueur de la directive 2022/2555 sur la sécurité des réseaux (dite «directive SRI 2»), que les États membres ont jusqu'au mois d'octobre 2024 pour transposer, harmonise les obligations en matière de notification des incidents dans l'ensemble des États membres de l'Union européenne. Il devrait en découler une meilleure compréhension de la nature et de l'ampleur du problème dans les années à venir.

L'Agence de l'Union européenne pour la cybersécurité (ENISA) a récemment publié un rapport[1] qui fournit des informations sur les menaces pour la cybersécurité dans le secteur des transports. Dans ce rapport, elle souligne que les cybercriminels étaient responsables de plus de la moitié des incidents observés au cours de la période de référence de 2022 (55 %) et que la principale motivation de ces attaques était l'appât du gain. Elle relève également que la plupart des cyberattaques dans le secteur des transports ciblent les systèmes informatiques, ce qui provoque des perturbations opérationnelles.

En ce qui concerne la préparation et la réaction aux incidents de cybersécurité, le soutien au niveau de l'Union européenne et la solidarité entre les États membres sont actuellement limités. Dans ses conclusions de mai 2022, le Conseil a souligné la nécessité de combler ces lacunes, en invitant la Commission à présenter une proposition relative à un nouveau **fonds d'intervention d'urgence en matière de cybersécurité**[2].

Le règlement concerné met en œuvre la **stratégie de cybersécurité de l'Union** adoptée en

[1] «Understanding Cyber Threats in Transport», ENISA, publié le 21 mars 2023.
[2] Conclusions du Conseil du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne (9364/22).

décembre 2020, par laquelle la Commission a annoncé la création d'un **cyberbouclier européen** renforçant les capacités de détection des cybermenaces et de partage d'informations dans l'Union européenne grâce à une fédération de centres d'opérations de sécurité (SOC, pour «Security Operations Centres») nationaux et transfrontières. Les actions prévues par le règlement en question seront soutenues par un **financement au titre de l'objectif stratégique «Cybersécurité» du programme pour une Europe numérique**.

Le budget total comprend une augmentation de 100 millions d'EUR que le règlement concerné propose de prélever sur des fonds prévus pour d'autres objectifs stratégiques du programme pour une Europe numérique, ce qui portera le nouveau montant total disponible pour les actions de cybersécurité dans le cadre du programme pour une Europe numérique à 842,8 millions d'EUR.

Une partie des 100 millions d'EUR supplémentaires renforcera le budget géré par le Centre de compétences européen en matière de cybersécurité afin de mettre en œuvre des actions relatives aux SOC et à la préparation dans le cadre de leur(s) programme(s) de travail. En outre, le financement supplémentaire contribuera à soutenir la mise en place de la réserve de cybersécurité de l'Union. Ce financement complète le budget déjà prévu pour des actions similaires dans le cadre du principal programme de travail et du programme de travail «cybersécurité» pour 2023-2027 du programme pour une Europe numérique, ce qui pourrait porter le montant total à 551 millions d'EUR pour 2023-2027, tandis que 115 millions d'EUR ont déjà été alloués sous forme de projets pilotes pour 2021-2022. En incluant les contributions des États membres, le budget global pourrait s'élever à 1,109 milliard d'EUR.

Position du rapporteur

Votre rapporteur accueille favorablement la nouvelle proposition et estime qu'elle apportera des avantages importants aux différentes parties prenantes. Votre rapporteur souligne qu'il est nécessaire de mieux comprendre les besoins en matière de cybersécurité et les exigences relatives au transport, ainsi que de permettre aux entités critiques dans le secteur des transports d'avoir accès à un financement adéquat pour la préparation et la réaction aux incidents ainsi que pour leur résolution.

Votre rapporteur approuve la «boîte à outils pour la cybersécurité dans le domaine des transports», qui vise à contribuer à une plus grande sensibilisation à la cybersécurité et à une meilleure hygiène informatique, en mettant particulièrement l'accent sur le secteur des transports. Cette boîte à outils s'adresse aux organisations de transport, indépendamment de leur taille et de leur domaine d'activité, et couvre les infrastructures critiques de transport et la mobilité militaire, notamment dans le cadre de la guerre en Ukraine, en particulier mais pas uniquement:

- les transporteurs aériens, les entités gestionnaires d'aéroports, les aéroports du réseau central, les centres de gestion du trafic aérien et les centres de contrôle du trafic aérien, l'Agence de l'Union européenne pour la sécurité aérienne et Eurocontrol;
- les gestionnaires de l'infrastructure, les entreprises ferroviaires et le système européen de gestion du trafic ferroviaire (ERTMS);
- les sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, les entités gestionnaires des ports, y compris leurs installations portuaires, les entités exploitant des ateliers et des équipements à l'intérieur des ports, les exploitants de services de trafic maritime;
- les autorités routières chargées du contrôle de la gestion de la circulation, les exploitants de systèmes de transport intelligents;
- les services de poste et de courrier.

Votre rapporteur estime que le succès du **fonds d'intervention d'urgence en matière de cybersécurité** dépendra de l'ampleur du budget consacré à son fonctionnement; c'est pourquoi il devrait être suffisamment important pour aider les États membres à se **préparer aux incidents de cybersécurité importants et majeurs et à y réagir, ainsi qu'à se rétablir** après de tels incidents. Le soutien à la réaction aux incidents est également mis à la disposition des institutions, organes et organismes de l'Union.

Le **cyberbouclier européen** améliorera les capacités de détection des cybermenaces des États membres. Le **mécanisme d'urgence dans le domaine de la cybersécurité** complétera les actions des États membres par un soutien d'urgence à la préparation, à la réaction et au rétablissement immédiat du fonctionnement des services essentiels.

AMENDEMENTS

La commission des transports et du tourisme invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération ce qui suit:

Amendement 1

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique	(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information***, ainsi que pour les infrastructures informatiques et physiques critiques***. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics ***ainsi que les transports publics et privés*** et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union ***ainsi qu'à la mobilité au sein de l'Union***, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant

déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.

donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.

Amendement 2

Proposition de règlement
Considérant 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 bis) Le secteur des transports est confronté à une menace de plus en plus grave de cybersécurité du fait d'acteurs soutenus par l'État, de cybercriminels et de pirates informatiques qui ciblent les autorités, les opérateurs, les constructeurs, les fournisseurs et les prestataires de services dans les transports aériens, maritimes, ferroviaires et routiers. L'Agence de l'Union européenne pour la cybersécurité (ENISA) a observé une augmentation de 25 % du nombre mensuel moyen d'incidents signalés dans le secteur des transports en 2022, par rapport aux niveaux de 2021. La majorité des attaques contre le secteur des transports ciblent les systèmes informatiques, ce qui peut entraîner des perturbations opérationnelles[14 bis].
	[14 bis] ENISA (2023), «ENISA threat landscape» (Panorama des menaces établi par l'ENISA): secteur des transports, pages 7 et 17.

Amendement 3

Proposition de règlement
Considérant 2 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 ter) L'invasion non provoquée de l'Ukraine par la Russie a entraîné une augmentation significative des incidents de cybersécurité, y compris les cyberattaques par déni de service distribué (DDoS), ciblant le secteur des transports dans l'Union et des zones proches de l'Union, principalement les aéroports, les chemins de fer et les autorités chargées des transports[14 ter]. Il est fort probable que cette augmentation des attaques se poursuive.
	[14 ter] ENISA (2023), «ENISA threat landscape» (Panorama des menaces établi par l'ENISA): secteur des transports, page 9.

Amendement 4

Proposition de règlement
Considérant 2 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 quater) Les cyberattaques ciblent les autorités et les organismes de tous les sous-secteurs des transports et touchent notamment les entreprises ferroviaires et les gestionnaires de l'infrastructure ainsi que les opérateurs portuaires. En ce qui concerne le secteur routier, les fabricants d'équipements d'origine, les fournisseurs et les prestataires de services sont ciblés, de même que les opérateurs de transport public. Dans le secteur de l'aviation, les principales cibles sont les compagnies aériennes et les exploitants aéroportuaires, suivis par les prestataires de services, les transporteurs au sol et la chaîne d'approvisionnement[14 quater].
	[14 quater] ENISA (2023), «ENISA threat landscape» (Panorama des menaces établi

par l'ENISA): secteur des transports, page 17.

Amendement 5

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité.	(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises***, des opérateurs de transport*** et des entités exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité ***ainsi qu'à l'état et l'évolution du marché du travail dans le domaine de la cybersécurité, étant donné que ces données jouent un rôle déterminant dans la fourniture des services de détection et de réaction nécessaires***.
[16] https://futureu.europa.eu/en/	[16] https://futureu.europa.eu/en/

Amendement 6

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.	(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]***, ainsi que de la proposition de règlement sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et de la proposition concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (règlement sur la cyberrésilience).*** En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.
[17] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de	[17] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de

cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

[18] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

[19] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

[20] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

[18] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

[19] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

[20] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Amendement 7

Proposition de règlement
Considérant 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(4 bis) Si nous nous félicitons de la boîte à outils de la Commission européenne pour la cybersécurité dans le domaine des transports[2 bis], qui contient des informations de base sur les menaces susceptibles d'affecter les organisations de transport (diffusion de logiciels malveillants, déni de service, accès non autorisé et vol, manipulation de logiciels) et répertorie les bonnes pratiques d'atténuation, il convient néanmoins de fournir aux opérateurs de transport une

formation adéquate sur la cybersécurité et des outils appropriés pour prévenir les cybermenaces. Le budget de l'Union devrait également couvrir le soutien, tel que la formation, fourni par l'ENISA pour permettre la mise en œuvre effective, par les opérateurs de transport, des bonnes pratiques d'atténuation figurant dans la boîte à outils.

[1 bis] «ENISA threat landscape» (Panorama des menaces établi par l'ENISA): secteur des transports/ENISA, mars 2023.

[2 bis] Commission européenne (2021). Boîte à outils pour la cybersécurité dans le secteur des transports, disponible à l'adresse https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_fr

Amendement 8

Proposition de règlement
Considérant 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(4 bis) L'approche coordonnée à l'échelle de l'Union pour renforcer la préparation et la résilience des infrastructures critiques, comme les infrastructures de transport, repose sur le renforcement des capacités des États membres. Comme l'a reconnu la Commission dans sa communication récente au Parlement européen et au Conseil intitulée «Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE»[19 bis], la sécurité de l'Union ne saurait être garantie sans l'atout le plus précieux de l'Union: sa population.

[19 bis] Communication de la Commission au

Parlement européen et au Conseil – Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE («L'académie des compétences en matière de cybersécurité») (COM(2023)207 final).

Amendement 9

Proposition de règlement
Considérant 12

Texte proposé par la Commission	*Amendement*
(12) Afin de prévenir, évaluer et contrer les menaces et incidents de cybersécurité de manière plus efficace, il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures. Il convient de mettre en place une grande infrastructure de SOC à l'échelle de l'Union (le cyberbouclier européen), comprenant plusieurs plateformes transfrontières interopérables qui regroupent chacune plusieurs SOC nationaux. Une telle infrastructure devrait servir les intérêts et les besoins des États et de l'Union en matière de cybersécurité, en tirant parti de technologies de pointe pour la collecte et l'analyse avancées des données, en renforçant les capacités de détection et de gestion des incidents de cybersécurité et en permettant une appréciation de la situation en temps réel. Elle devrait également permettre d'améliorer la détection des menaces et incidents de cybersécurité, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion de crise dans l'UE, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) tel que défini dans la	(12) Afin de prévenir, évaluer et contrer les menaces et incidents de cybersécurité de manière plus efficace, il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures. ***Ces actifs et infrastructures critiques comprennent les systèmes de transport intelligents, qui, tout en étant essentiels à la mobilité automatisée et multimodale, fonctionnent sur la base d'échanges cruciaux de données sensibles.*** Il convient de mettre en place une grande infrastructure de SOC à l'échelle de l'Union (le cyberbouclier européen), comprenant plusieurs plateformes transfrontières interopérables qui regroupent chacune plusieurs SOC nationaux. Une telle infrastructure devrait servir les intérêts et les besoins des États et de l'Union en matière de cybersécurité, en tirant parti de technologies de pointe pour la collecte et l'analyse avancées des données, en renforçant les capacités de détection et de gestion des incidents de cybersécurité et en permettant une appréciation de la situation en temps réel. Elle devrait également permettre d'améliorer la détection des menaces et

directive (UE) 2022/2555 du Parlement européen et du Conseil[24].

incidents de cybersécurité, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion de crise dans l'UE, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) tel que défini dans la directive (UE) 2022/2555 du Parlement européen et du Conseil[24].

[24] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

[24] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

Amendement 10

Proposition de règlement
Considérant 14 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(14 bis) Le secteur des transports est en train de devenir l'un des secteurs les plus lucratifs pour les cybercriminels, les données clients étant considérées comme un produit très précieux et la chaîne d'approvisionnement des transports étant de plus en plus souvent ciblée. C'est pourquoi les infrastructures de transport caractérisées par un caractère transfrontalier ou par l'échange de données au moyen de technologies sans fil devraient être considérées comme un sujet essentiel d'analyse et de surveillance pour les SOC nationaux mais surtout transfrontières. Par exemple, la récente proposition de révision du règlement RTE-T exige une solidarité et une coopération accrues dans le partage d'informations sur les cybermenaces transfrontières auxquelles ce réseau transnational pourrait être confronté. De

même, les systèmes de transport intelligents (STI) sont essentiels pour rendre les transports plus sûrs, plus efficaces et plus durables, mais ils rendent les systèmes de transport plus vulnérables aux cyberattaques susceptibles de causer des accidents, des embouteillages ou des pertes économiques aux opérateurs privés et publics. Afin de préserver la sécurité des passagers et la protection des données des utilisateurs et des fournisseurs et d'éviter des dommages financiers, il est essentiel que le programme de mise en œuvre de la directive révisée sur les systèmes de transport intelligents comprenne des dispositions et des outils visant à renforcer la collaboration entre les États membres en vue de détecter les menaces et les incidents de cybersécurité, de s'y préparer et d'y réagir.

Amendement 11

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la souveraineté technologique de l'Union.	(15) Au niveau national, la surveillance, la détection et l'analyse des cybermenaces sont généralement assurées par les SOC relevant d'entités publiques et privées, alliés aux CSIRT. En outre, les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Les SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT en regroupant et en partageant des données sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant au développement des capacités et de la souveraineté technologique de l'Union. ***À cet égard, afin de renforcer l'autonomie***

de l'Union dans le domaine du cyberespace et en référence à l'article 47, paragraphe 4, de la proposition de règlement sur les orientations de l'Union pour le développement du réseau transeuropéen de transport (COM(2021)0812), il est également nécessaire d'empêcher l'accès aux données conduisant à des cybermenaces en appliquant un cadre réglementaire solide régissant la propriété étrangère et les investissements étrangers dans des infrastructures critiques, comme les transports.

Amendement 12

Proposition de règlement
Considérant 21

Texte proposé par la Commission	*Amendement*
(21) Bien que le cyberbouclier européen soit un projet civil, le renforcement des capacités civiles de détection et d'appréciation de la situation pour la protection des infrastructures critiques pourrait aussi profiter à la communauté de cyberdéfense. Les SOC transfrontières, avec le soutien de la Commission et du Centre de compétences européen en matière de cybersécurité (ECCC) et en coopération avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant»), devraient progressivement élaborer des protocoles et des normes spécifiques afin de permettre une coopération avec la communauté de la cyberdéfense, y compris en ce qui concerne les conditions de vérification et de sécurité. La mise en place du cyberbouclier européen devrait s'accompagner d'une réflexion qui permette une collaboration future avec les réseaux et plateformes de partage d'informations au sein de la communauté de cyberdéfense, en étroite	(21) Bien que le cyberbouclier européen soit un projet civil, le renforcement des capacités civiles de détection et d'appréciation de la situation pour la protection des infrastructures critiques pourrait aussi profiter à la communauté de cyberdéfense. Les SOC transfrontières, avec le soutien de la Commission et du Centre de compétences européen en matière de cybersécurité (ECCC) et en coopération avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant»), devraient progressivement élaborer des protocoles et des normes spécifiques afin de permettre une coopération avec la communauté de la cyberdéfense, y compris en ce qui concerne les conditions de vérification et de sécurité. La mise en place du cyberbouclier européen devrait s'accompagner d'une réflexion qui permette une collaboration future avec les réseaux et plateformes de partage d'informations au sein de la communauté de cyberdéfense, en étroite coopération avec le haut représentant. ***Il***

coopération avec le haut représentant.	***devrait également permettre des synergies avec le plan d'action sur la mobilité militaire 2.0. Un réseau de mobilité militaire performant doit être résilient, y compris dans le contexte des cybermenaces et autres menaces hybrides susceptibles de toucher des nœuds critiques du système de transport qui sont à double usage. Par exemple, une cyberattaque contre des systèmes utilisés dans les aéroports, les ports ou les voies ferrées ou une cyberattaque contre des ressources militaires pourrait avoir des conséquences majeures. Ainsi, la numérisation des processus et des procédures, y compris pour la nécessaire coopération civile et militaire, nécessitera de rendre les systèmes informatiques plus résistants aux cybermenaces.***

Amendement 13

Proposition de règlement
Considérant 21 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(21 bis) En cas de crise de cybersécurité, un échange efficace d'informations est essentiel pour garantir la connaissance de la situation dans les secteurs des transports militaires et civils. Cet échange d'informations devrait également stimuler la coopération entre les autorités sectorielles compétentes chargées des transports, les autorités compétentes en matière de cybersécurité, les SOC et les CSIRT.

Amendement 14

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Dans le cadre des mesures de	(29) Dans le cadre des mesures de

préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE); l'évaluation

préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. ***Il convient d'accorder une attention particulière au secteur des transports et à ses sous-secteurs (aérien, ferroviaire, maritime, routier), car ils intègrent des infrastructures critiques dans lesquelles les cyberincidents et les cyberattaques pourraient compromettre gravement la sécurité des passagers et des opérateurs.*** Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et

coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du Parlement européen et du Conseil[29]. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE); l'évaluation coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du Parlement européen et du Conseil[29]. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

[29] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

[29] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011.

Amendement 15

Proposition de règlement
Considérant 30 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(30 bis) Compte tenu du caractère critique du secteur et des conséquences des cybermenaces sur la mobilité et, par conséquent, sur la vie humaine des passagers et des piétons, il convient d'accorder la priorité au secteur des transports en ce qui concerne les tests coordonnés de préparation des entités.

Amendement 16

Proposition de règlement
Considérant 35 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(35 bis) Compte tenu de l'augmentation des tâches et des responsabilités confiées à l'ENISA par la présente proposition ainsi que par la proposition de règlement sur la cyberrésilience, l'adoption du budget rectificatif nº 1/2022 de l'ENISA pour la mise en œuvre pilote d'une action de soutien à la cybersécurité est nécessaire. En outre, compte tenu des intérêts de l'Union en jeu, des ressources financières et humaines supplémentaires devraient être allouées à l'ENISA.

Amendement 17

Proposition de règlement
Considérant 38 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(38 bis) Le développement des aptitudes et des compétences devrait donc occuper une place centrale dans tous les secteurs, en particulier pour les personnes qui sont vulnérables aux menaces en matière de cybersécurité, comme le personnel travaillant sur les infrastructures de transport à grande capacité ou les infrastructures critiques, y compris les systèmes de contrôle des trains et les outils numériques de planification des transports pour tous les modes de transport. L'introduction et le développement de la culture de la cybersécurité sont donc essentiels au succès de la mise en œuvre du présent règlement, tant pour la sensibilisation des citoyens que pour les connaissances des spécialistes dans tous les secteurs des infrastructures critiques.

Amendement 18

Proposition de règlement
Article 1 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;	a) renforcer la détection et l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ce qui permettra de consolider la position concurrentielle des secteurs de l'industrie***, des infrastructures de transport*** et des services de l'Union dans l'ensemble de l'économie numérique et de contribuer à la souveraineté technologique de l'Union dans le domaine de la cybersécurité;

Amendement 19

Proposition de règlement
Article 1 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;	b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, ***en accordant une attention particulière aux infrastructures informatiques et physiques critiques,*** y compris en permettant aux pays tiers associés au programme pour une Europe numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;

Amendement 20

Proposition de règlement
Article 1 – paragraphe 2 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) renforcer la préparation, la coopération et l'efficacité de l'Union en matière de protection des infrastructures et des services de transport dans les États membres contre les incidents de cybersécurité, afin de garantir le fonctionnement continu du secteur des transports, l'intégrité des chaînes d'approvisionnement et la mobilité à l'échelle de l'Union.

Amendement 21

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 1 – point c

Texte proposé par la Commission	*Amendement*
c) contribue à améliorer la protection contre les cybermenaces et la réaction face à celles-ci***;***	c) contribue à améliorer la protection contre les cybermenaces et la réaction face à celles-ci***, y compris pour les infrastructures de transport caractérisées par un caractère transfrontière, telles que le RTE-T, ou par l'échange de données au moyen de technologies sans fil, telles que les systèmes de transport intelligents.***

Amendement 22

Proposition de règlement
Article 3 – paragraphe 2 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il est mis au point en coopération avec l'infrastructure paneuropéenne de calcul à haute performance établie conformément au règlement (UE) 2021/1173.	Il est mis au point en coopération avec l'infrastructure paneuropéenne de calcul à haute performance établie conformément au règlement (UE) 2021/1173. ***Il permet une collaboration, au moyen de protocoles et de normes spécifiques, avec la communauté de cyberdéfense, afin d'assurer le développement de capacités civiles de détection et d'appréciation de la situation renforcées pour la protection des***

infrastructures critiques. À cet égard, des synergies sont également développées avec le plan d'action sur la mobilité militaire 2.0 et un échange d'informations efficace est assuré afin de permettre une appréciation de la situation dans les secteurs des transports militaires et civils.

Amendement 23

Proposition de règlement
Article 8 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. La Commission associe le cyberbouclier européen, en particulier les SOC transfrontières, à son avis aux États membres dans le cadre de la proposition de règlement sur le réseau transeuropéen de transport (COM(2021)0812) chaque fois que tout type de participation ou de contribution d'une personne physique d'un pays tiers ou d'une entreprise d'un pays tiers est susceptible d'affecter la cybersécurité d'infrastructures critiques transfrontières, telles que le RTE-T.

Amendement 24

Proposition de règlement
Article 10 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union;	a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union***, en accordant une attention particulière aux infrastructures de transport et à ses sous-secteurs figurant à l'annexe I de la directive (UE) 2022/2555***;

Amendement 25

Proposition de règlement
Article 18 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés et les utilisateurs de services de cybersécurité. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.	2. Pour préparer le rapport d'analyse visé au paragraphe 1, l'ENISA collabore avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'UE, les fournisseurs de services de sécurité gérés et les utilisateurs de services de cybersécurité. Le cas échéant, l'ENISA collabore également avec les entités touchées par des incidents de cybersécurité importants ou majeurs***, y compris les opérateurs de transport***. Pour étayer l'analyse, l'ENISA peut également consulter d'autres types de parties prenantes. Les représentants consultés déclarent tout conflit d'intérêts potentiel.

Amendement 26

Proposition de règlement
Article 19 – alinéa 1 – point 1 – sous-point b
Règlement (UE) 2021/694
Article 6 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Compte tenu des intérêts de l'Union en jeu, en rapport avec ses responsabilités en ce qui concerne la préparation de schémas de certification candidats en vertu du règlement (UE) 2019/881, avec ses responsabilités en matière d'examen et d'évaluation des cybermenaces, des vulnérabilités et de l'atténuation des cybermenaces, d'élaboration d'un rapport d'analyse dans le cadre du mécanisme d'analyse des incidents de cybersécurité, ainsi qu'en matière de formation sur les cyberattaques et les cyberincidents à dispenser aux opérateurs d'infrastructures critiques, et à la lumière

	des nouvelles responsabilités qui lui incombent dans le cadre de la proposition de règlement sur la cyberrésilience, l'ENISA est dotée des ressources nécessaires au titre du budget de l'Union conformément à la législation applicable.

Amendement 27

Proposition de règlement
Article 19 – alinéa 1 – point 1 bis (nouveau)
Règlement (UE) 2021/694
Article 7 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis) L'article 7 est modifié comme suit:
	a) le paragraphe 1 est modifié comme suit:
	(1) le point c bis) suivant est inséré:
	c bis) «c bis) soutenir une formation de haute qualité pour les opérateurs de transport ainsi que les gestionnaires et le personnel des infrastructures de transport critiques, notamment dans le but de partager et de mettre en œuvre efficacement des pratiques d'atténuation face aux cyberattaques ou aux cyberincidents touchant les infrastructures critiques, telles que celles prévues dans la boîte à outils pour la cybersécurité dans le secteur des transports.».

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Adoption de mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité
Références	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 1.6.2023
Avis émis par Date de l'annonce en séance	TRAN 1.6.2023
Rapporteur(e) pour avis Date de la nomination	Gheorghe Falcă 7.7.2023
Date de l'adoption	25.10.2023
Résultat du vote final	+: 38 –: 0 0: 0
Membres présents au moment du vote final	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Suppléants présents au moment du vote final	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention

PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND

Titre	Adoption de mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité			
Références	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Date de la présentation au PE	19.4.2023			
Commission compétente au fond Date de l'annonce en séance	ITRE 1.6.2023			
Commissions saisies pour avis Date de l'annonce en séance	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Avis non émis Date de la décision	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Rapporteurs Date de la nomination	Lina Gálvez Muñoz 2.5.2023			
Examen en commission	19.9.2023			
Date de l'adoption	7.12.2023			
Résultat du vote final	+: –: 0:	43 10 1		
Membres présents au moment du vote final	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Suppléants présents au moment du vote final	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Suppléants (art. 209, par. 7) présents au moment du vote final	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Date du dépôt	8.12.2023			

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION COMPÉTENTE AU FOND

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention