COM(2023) 209 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2022/2023

Reçu à la Présidence de l'Assemblée nationale
le 26 mai 2023

Enregistré à la Présidence du Sénat
le 26 mai 2023

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

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

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

E 17790

COMMISSION
EUROPÉENNE

Strasbourg, le 18.4.2023
COM(2023) 209 final

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Le présent exposé des motifs accompagne la proposition de règlement sur la cybersolidarité. 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. Cette utilisation accrue des technologies numériques augmente l'exposition aux incidents de cybersécurité et à leurs conséquences potentielles. Dans le même temps, les États membres sont confrontés à des risques croissants en matière de cybersécurité et à un paysage global complexe de menaces, impliquant un risque évident de propagation rapide des cyberincidents d'un État membre à l'autre.

En outre, les cyberopérations sont de plus en plus intégrées dans les stratégies de guerre hybrides, avec des effets significatifs sur la cible. En particulier, l'agression militaire de la Russie contre l'Ukraine a été précédée et s'accompagne d'une stratégie de cyberopérations hostiles, ce qui change la donne en ce qui concerne la perception et l'évaluation de la préparation collective de l'Union à la gestion des crises de cybersécurité et nécessite une action urgente. La menace d'un éventuel incident de cybersécurité majeur provoquant de graves perturbations et dommages à des infrastructures critiques exige une préparation accrue à tous les niveaux de l'écosystème de cybersécurité de l'Union. Cette menace va au-delà de l'agression militaire de la Russie contre l'Ukraine et comprend des cybermenaces permanentes émanant d'acteurs étatiques et non étatiques, qui sont susceptibles de durer compte tenu de la multiplicité des acteurs criminels et hacktivistes proches de l'État qui sont impliqués dans les tensions géopolitiques actuelles. Ces dernières années, les cyberattaques ont vu leur nombre augmenter considérablement, notamment les attaques de la chaîne d'approvisionnement visant le cyberespionnage, les rançongiciels ou les perturbations. En 2020, l'attaque de la chaîne d'approvisionnement de SolarWinds a touché plus de 18 000 organisations dans le monde, dont des agences gouvernementales et de grandes entreprises. Les incidents de cybersécurité importants peuvent être trop perturbateurs pour permettre à un ou plusieurs États membres concernés d'y faire face seuls. C'est la raison pour laquelle une solidarité renforcée au niveau de l'Union est nécessaire afin de mieux détecter les menaces et incidents de cybersécurité, de mieux s'y préparer et de mieux y réagir.

En ce qui concerne la détection des menaces et incidents de cybersécurité, il est urgent d'intensifier l'échange d'informations et d'améliorer nos capacités collectives afin de réduire considérablement le temps nécessaire à la détection des cybermenaces, avant qu'elles n'occasionnent des dommages de grande ampleur et des coûts considérables[1]. Alors que de

[1] Selon un rapport du Ponemon Institute et d'IBM Security, le délai moyen pour détecter une violation en 2022 était de 207 jours, tandis que 70 jours supplémentaires étaient nécessaires pour l'endiguer. Dans le même temps, en 2022, les violations de données ayant un cycle de vie supérieur à 200 jours

nombreux incidents et menaces de cybersécurité peuvent avoir une dimension transfrontière en raison de l'interconnexion des infrastructures numériques, le partage d'informations pertinentes entre les États membres reste limité. La mise en place d'un réseau de centres d'opérations de sécurité (SOC, pour «Security Operations Centres») transfrontières afin d'améliorer les capacités de détection et de réaction devrait contribuer à résoudre ce problème.

En ce qui concerne la préparation et la réaction aux incidents de cybersécurité, le soutien au niveau de l'Union et la solidarité entre les États membres sont actuellement limités. Dans ses conclusions d'octobre 2021, 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 présent règlement met également en œuvre la stratégie de cybersécurité de l'UE adoptée en décembre 2020[3], 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 SOC nationaux et transfrontières.

Le présent règlement s'appuie sur les premières mesures déjà mises au point en étroite collaboration avec les principales parties intéressées et soutenues par le programme pour une Europe numérique. En particulier, en ce qui concerne les SOC, un appel à manifestation d'intérêt pour des acquisitions conjointes d'outils et d'infrastructures en vue de la création de SOC transfrontières et un appel à subventions pour permettre le renforcement des capacités des SOC desservant des organisations publiques et privées ont été organisés dans le cadre du programme de travail cybersécurité pour 2021-2022 du programme pour une Europe numérique. En ce qui concerne la préparation et la réaction aux incidents, la Commission a mis en place un programme à court terme pour soutenir les États membres, aux fins duquel un financement supplémentaire a été alloué à l'Agence de l'Union européenne pour la cybersécurité (ENISA), afin de renforcer immédiatement la préparation et les capacités de réaction à des cyberincidents majeurs. Ces deux actions ont été préparées en étroite collaboration avec les États membres. Le présent règlement remédie aux lacunes et intègre les enseignements tirés de ces actions.

Enfin, la présente proposition respecte l'engagement pris dans le cadre de la communication conjointe sur la cyberdéfense[4], adoptée le 10 novembre, de préparer une proposition d'initiative européenne de cybersolidarité ayant pour objectif de renforcer les capacités communes de détection, d'appréciation de la situation et de réponse de l'Union, pour constituer de manière progressive une réserve cyber au niveau de l'Union avec les services de

---

représentaient un coût moyen de 4,86 millions d'EUR, contre 3,74 millions d'EUR pour un cycle de vie inférieur à 200 jours («Cost of a data breach 2022», https://www.ibm.com/reports/data-breach).

[2] 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).

[3] Communication conjointe au Parlement européen et au Conseil intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique», JOIN(2020) 18 final.

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

fournisseurs privés de confiance et aider à soumettre les entités critiques à des tests de détection.

Dans ce contexte, la Commission propose le présent règlement sur la cybersolidarité en vue de renforcer la solidarité au niveau de l'Union afin de mieux détecter les menaces et incidents de cybersécurité, de mieux s'y préparer et de mieux y réagir, en poursuivant les objectifs spécifiques suivants:

- renforcer les capacités communes de l'Union en matière de détection et d'appréciation de la situation des menaces et incidents de cybersécurité, et contribuer ainsi à la souveraineté technologique européenne dans le domaine de la cybersécurité;
- améliorer la préparation des entités critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités communes de réaction aux incidents de cybersécurité importants ou majeurs, y compris en mettant à la disposition des pays tiers qui sont associés au programme pour une Europe numérique un soutien à la réaction aux incidents;
- augmenter la résilience de l'Union et contribuer à une réaction efficace en analysant et en évaluant les incidents importants ou majeurs, y compris en tirant les enseignements des expériences acquises et, au besoin, en formulant des recommandations.

Afin d'atteindre ces objectifs, les actions suivantes seront poursuivies:

- le déploiement d'une infrastructure paneuropéenne composée de SOC (le cyberbouclier européen) dans le but de mettre en place et d'améliorer les capacités communes de détection et d'appréciation de la situation;
- la création d'un mécanisme d'urgence dans le domaine de la cybersécurité afin d'aider les États membres à se préparer et à réagir aux incidents de cybersécurité importants et majeurs, et à s'en rétablir immédiatement. Le soutien à la réaction aux incidents est également mis à la disposition des institutions, organes et organismes de l'Union;
- la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents de cybersécurité importants ou majeurs.

Le cyberbouclier européen et le mécanisme d'urgence dans le domaine de la cybersécurité bénéficieront d'un financement au titre du programme pour une Europe numérique, que le présent instrument législatif modifiera afin de mettre en place les actions susmentionnées, de prévoir un soutien financier pour leur développement et de préciser les conditions à remplir pour bénéficier de ce soutien financier.

•Cohérence avec les dispositions existantes dans le domaine d'action

Le cadre de l'Union comprend plusieurs législations déjà en vigueur ou proposées au niveau de l'Union afin de réduire les vulnérabilités, de renforcer la résilience des entités critiques face aux risques de cybersécurité et de soutenir la gestion coordonnée des incidents et crises

de cybersécurité majeurs, notamment la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union (directive SRI 2)[5], le règlement sur la cybersécurité[6], la directive relative aux attaques contre les systèmes d'information[7] et la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs[8].

Les actions proposées dans le cadre du règlement sur la cybersolidarité portent sur l'appréciation de la situation, le partage d'informations, ainsi que le soutien à la préparation et à la réaction aux cyberincidents. Ces actions sont cohérentes avec les objectifs du cadre réglementaire en place au niveau de l'Union, notamment au titre de la directive (UE) 2022/2555 (la «directive SRI 2»), et les soutiennent. Le règlement sur la cybersolidarité s'appuiera en particulier sur les cadres existants de coopération opérationnelle et de gestion de crise en matière de cybersécurité, notamment le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) et le réseau des centres de réponse aux incidents de sécurité informatiques (réseau des CSIRT), et les soutiendra.

Les plateformes SOC transfrontières devraient constituer une nouvelle capacité venant compléter le réseau des CSIRT, en regroupant et en partageant des données sur les menaces de cybersécurité issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données à l'aide d'analyses d'experts et à des outils de pointe, et en contribuant au renforcement des capacités et de la souveraineté technologique de l'Union.

Enfin, la présente proposition est conforme à la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques[9], qui 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 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).

6 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).

7 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.

8 Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM(2022) 454 final.

9 Recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques (Texte présentant de l'intérêt pour l'EEE), 2023/C 20/01.

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

La proposition est cohérente avec d'autres mécanismes et protocoles d'urgence en cas de crise, tels que le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR). Le règlement sur la cybersolidarité complétera ces cadres et protocoles de gestion de crise en apportant un soutien spécifique à la préparation et à la réaction aux incidents de cybersécurité. La proposition sera également cohérente avec l'action extérieure de l'Union en réaction à des incidents majeurs dans le cadre de la politique étrangère et de sécurité commune (PESC), notamment dans le cadre de la boîte à outils cyberdiplomatique de l'Union. La proposition complètera les actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne ou dans les situations définies à l'article 222 du traité sur le fonctionnement de l'Union européenne.

Elle complète également le mécanisme de protection civile de l'Union (MPCU)[10] établi en décembre 2013 et complété par une nouvelle législation adoptée en mai 2021[11], qui renforce les piliers «prévention», «préparation» et «réaction» du MPCU et dote l'Union de capacités supplémentaires pour réagir à de nouveaux risques en Europe et dans le monde et renforcer la réserve rescEU.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La présente proposition a pour base juridique l'article 173, paragraphe 3, et l'article 322, paragraphe 1, point a), du traité sur le fonctionnement de l'Union européenne (TFUE). L'article 173 du TFUE prévoit que l'Union et les États membres sont tenus de veiller à ce que les conditions nécessaires à la compétitivité de l'industrie de l'Union soient assurées. Le présent règlement vise à consolider la position concurrentielle de l'industrie et des services en Europe dans tous les secteurs d'activité passés au numérique et à soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Il vise notamment à renforcer la résilience des citoyens, des entreprises et des entités actives dans des secteurs critiques et hautement critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie.

La proposition est également fondée sur l'article 322, paragraphe 1, point a), du TFUE, car elle contient des règles spécifiques en matière de report qui dérogent au principe d'annualité établi dans le règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil (ci-

[10] 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).

[11] Règlement (UE) 2021/836 du Parlement européen et du Conseil du 20 mai 2021 modifiant la décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union (Texte présentant de l'intérêt pour l'EEE).

après le «règlement financier»)[12]. Aux fins de la bonne gestion financière et compte tenu de la nature imprévisible, exceptionnelle et spécifique du paysage de la cybersécurité et des cybermenaces, le mécanisme d'urgence dans le domaine de la cybersécurité devrait se voir accorder un certain degré de flexibilité en matière de gestion budgétaire, notamment en autorisant le report automatique à l'exercice suivant des crédits d'engagement et de paiement non utilisés pour des actions poursuivant les objectifs fixés dans le règlement. Étant donné que cette nouvelle règle soulève des questions par rapport au règlement financier, ce point pourrait être traité dans le cadre des négociations actuelles sur la refonte du règlement financier.

- **Subsidiarité (en cas de compétence non exclusive)**

La nature fortement transfrontière des menaces de cybersécurité et le nombre croissant de risques et d'incidents ayant des répercussions transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs de la présente intervention ne peuvent pas être atteints efficacement par les seuls États membres et nécessitent une action commune et une solidarité au niveau de l'Union.

L'expérience acquise dans la lutte contre les cybermenaces découlant de la guerre menée par la Russie contre l'Ukraine ainsi que les enseignements tirés d'un exercice de cybersécurité mené sous la présidence française (EU CyCLES) ont montré qu'il convient de mettre en place des mécanismes concrets de soutien mutuel, notamment une coopération avec le secteur privé, afin de parvenir à une solidarité au niveau de l'Union. C'est dans ce contexte que, dans ses conclusions du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne, le Conseil a invité la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité.

Le soutien et les actions menées au niveau de l'Union en vue de mieux détecter les menaces de cybersécurité et de renforcer les capacités de préparation et de réaction apportent une valeur ajoutée car ils évitent les doubles emplois dans l'Union et les États membres. Cela permettrait de mieux exploiter les ressources existantes et d'améliorer la coordination et l'échange d'informations sur les enseignements tirés. Le mécanisme d'urgence dans le domaine de la cybersécurité prévoit également de fournir une aide aux pays tiers qui sont associés au programme pour une Europe numérique dans le cadre de la réserve de cybersécurité de l'Union.

Le soutien apporté par les différentes initiatives à mettre en place et à financer au niveau de l'Union complétera les capacités nationales de détection, d'appréciation de la situation, de préparation et de réaction aux menaces et incidents de cybersécurité sans faire double emploi.

- **Proportionnalité**

[12] 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 (JO L 193 du 30.7.2018, p. 1).

Les actions ne vont pas au-delà de ce qui est nécessaire pour atteindre les objectifs généraux et spécifiques du règlement. Les actions prévues par le présent règlement n'affectent pas les compétences des États membres en matière de sécurité nationale, de sécurité publique, de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Elles n'ont pas non plus d'incidence sur les obligations légales qu'ont les entités actives dans des secteurs critiques et hautement critiques d'adopter des mesures de cybersécurité, conformément à la directive SRI 2.

Les actions couvertes par le présent règlement complètent ces efforts et ces mesures, en soutenant la création d'infrastructures pour une meilleure détection et une meilleure analyse des menaces et en soutenant les actions de préparation et de réaction en cas d'incidents importants ou majeurs.

- **Choix de l'instrument**

La proposition prend la forme d'un règlement du Parlement européen et du Conseil. Il s'agit de l'instrument juridique le plus approprié étant donné que seul un règlement, dont les dispositions juridiques sont directement applicables, peut offrir le degré d'uniformité requis aux fins de la mise en place et du fonctionnement d'un cyberbouclier européen et d'un mécanisme d'urgence dans le domaine de la cybersécurité, en prévoyant le soutien du programme pour une Europe numérique pour leur mise en place ainsi que des conditions claires pour l'utilisation et l'attribution de ce soutien.

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

- **Consultation des parties intéressées**

Les actions prévues dans le présent règlement seront soutenues par le programme pour une Europe numérique, qui a fait l'objet d'une large consultation. De plus, elles s'appuieront sur les premières étapes qui ont été préparées en étroite collaboration avec les principales parties intéressées. En ce qui concerne les SOC, la Commission a élaboré un document de réflexion sur le développement de plateformes SOC transfrontières et un appel à manifestation d'intérêt en étroite collaboration avec les États membres dans le cadre du centre de compétences européen en matière de cybersécurité (ECCC). Dans ce contexte, une enquête sur les capacités nationales des SOC a été menée et des approches communes et des exigences techniques ont été examinées au sein du groupe de travail technique de l'ECCC qui réunit des représentants des États membres. En outre, des échanges ont eu lieu avec le secteur, notamment dans le cadre du groupe d'experts sur les SOC créé par l'ENISA et l'Organisation européenne pour la cybersécurité (ECSO).

Ensuite, en ce qui concerne la préparation et la réaction aux incidents, la Commission a mis en place un programme à court terme pour soutenir les États membres, aux fins duquel un financement supplémentaire a été alloué à l'ENISA au titre du programme pour une Europe

numérique, afin de renforcer immédiatement la préparation et les capacités de réaction à des cyberincidents majeurs. Les commentaires des États membres et du secteur recueillis au cours de la mise en œuvre de ce programme à court terme fournissent déjà des informations précieuses qui ont été prises en considération lors de la préparation de la proposition de règlement en vue de remédier aux lacunes constatées. Il s'agissait d'une première étape conforme aux conclusions du Conseil sur la posture cyber, qui invitaient la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité.

Enfin, un atelier réunissant des experts des États membres sur le mécanisme d'urgence dans le domaine de la cybersécurité a été organisé le 16 février 2023, sur la base d'un document de réflexion. Tous les États membres ont participé à cet atelier et onze d'entre eux ont fourni des contributions supplémentaires par écrit.

- **Analyse d'impact**

En raison du caractère urgent de la proposition, aucune analyse d'impact n'a été réalisée. Les actions prévues dans le présent règlement seront soutenues par le programme pour une Europe numérique et sont conformes à celles définies dans le règlement sur le programme pour une Europe numérique, qui a fait l'objet d'une analyse d'impact spécifique. Le présent règlement n'aura pas d'incidences administratives ou environnementales significatives autres que celles déjà évaluées dans l'analyse d'impact du règlement sur le programme pour une Europe numérique.

En outre, il s'appuie sur les premières mesures conçues en étroite collaboration avec les principales parties intéressées, comme indiqué ci-dessus, et fait suite aux conclusions du Conseil invitant la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité d'ici à la fin du troisième trimestre 2022.

Plus précisément, en ce qui concerne l'appréciation de la situation et la détection dans le cadre du cyberbouclier européen, un appel à manifestation d'intérêt pour des acquisitions conjointes d'outils et d'infrastructures en vue de la création de SOC transfrontières, et un appel à subventions pour permettre le renforcement des capacités des SOC desservant des organisations publiques et privées, ont été organisés dans le cadre du programme de travail cybersécurité pour 2021-2022 du programme pour une Europe numérique.

Dans le domaine de la préparation et de la réaction aux incidents, comme mentionné ci-dessus, la Commission a mis en place un programme à court terme pour soutenir les États membres dans le cadre du programme pour une Europe numérique, qui est mis en œuvre par l'ENISA. Les services fournis comprennent des mesures de préparation, telles que des tests de pénétration des entités critiques afin d'en déterminer les vulnérabilités. Les possibilités d'aide aux États membres en cas d'incident majeur touchant des entités critiques sont également renforcées. La mise en œuvre par l'ENISA de ce programme à court terme est en cours et a déjà fourni des informations précieuses qui ont été prises en considération lors de la préparation du présent règlement.

- **Droits fondamentaux**

En contribuant à la sécurité de l'information numérique, la présente proposition contribuera à protéger le droit à la liberté et à la sûreté, conformément à l'article 6 de la charte des droits fondamentaux de l'Union européenne, et le droit au respect de la vie privée et familiale, conformément à l'article 7 de la charte. En protégeant les entreprises contre des cyberattaques préjudiciables sur le plan économique, la proposition contribuera également à la liberté d'entreprise, conformément à l'article 16 de la charte des droits fondamentaux de l'Union européenne, et au droit de propriété, conformément à l'article 17 de la charte. Enfin, en protégeant l'intégrité des infrastructures critiques face aux cyberattaques, la proposition contribuera au droit à la protection de la santé, conformément à l'article 35 de la charte des droits fondamentaux de l'Union européenne, et au droit d'accès aux services d'intérêt économique général, conformément à l'article 36 de la charte.

4. INCIDENCE BUDGÉTAIRE

Les actions prévues par le présent règlement 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 présent règlement 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 l'ECCC 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.

Une vue d'ensemble des coûts engendrés est présentée dans la «fiche financière législative» qui accompagne la présente proposition.

5. AUTRES ÉLÉMENTS

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

La Commission suivra la mise en œuvre, l'application et le respect de ces nouvelles dispositions pour évaluer leur efficacité. La Commission présente au Parlement européen et

au Conseil un rapport sur l'évaluation et le réexamen du présent règlement dans un délai de quatre ans à compter de la date de son application.

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

Objectifs généraux, objet et définitions (chapitre I)

Le chapitre I définit les objectifs du règlement, à savoir renforcer la solidarité au niveau de l'Union afin de mieux détecter les menaces et incidents de cybersécurité, de mieux s'y préparer et de mieux y réagir, et en particulier renforcer les capacités communes de détection et d'appréciation de la situation des menaces et incidents de cybersécurité au niveau de l'Union, renforcer 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 communes de réaction aux incidents de cybersécurité importants ou majeurs, et renforcer la résilience de l'Union en analysant et en évaluant les incidents importants ou majeurs. Le chapitre présente également les actions qui permettront d'atteindre ces objectifs: le déploiement d'un cyberbouclier européen, la création d'un mécanisme d'urgence dans le domaine de la cybersécurité et l'établissement d'un mécanisme d'analyse des incidents de cybersécurité. Il contient également les définitions des termes utilisés dans l'ensemble de l'acte.

Le cyberbouclier européen (chapitre II)

Le chapitre II établit le cyberbouclier européen et présente ses différents éléments ainsi que les conditions de participation. Tout d'abord, il annonce l'objectif général du cyberbouclier européen, à savoir développer des capacités avancées pour l'Union afin de détecter, d'analyser et de traiter les données sur les menaces et incidents de cybersécurité dans l'Union, ainsi que les objectifs opérationnels spécifiques. Il précise que le financement de l'Union prévu pour le cyberbouclier européen est mis en œuvre conformément au règlement sur le programme pour une Europe numérique.

Le chapitre décrit ensuite la nature des entités qui constitueront le cyberbouclier européen. Le bouclier est composé de centres d'opérations de sécurité nationaux («SOC nationaux») et de centres d'opérations de sécurité transfrontières («SOC transfrontières»). Un SOC national est désigné par chaque État membre participant. Il sert de point de référence et d'accès à d'autres organisations publiques et privées au niveau national en vue de collecter et d'analyser des informations sur les menaces et incidents de cybersécurité et de contribuer aux travaux d'un SOC transfrontière. À la suite d'un appel à manifestation d'intérêt, un SOC national peut être sélectionné par l'ECCC pour participer à une acquisition conjointe d'outils et d'infrastructures avec l'ECCC et bénéficier d'une subvention pour l'exploitation des outils et des infrastructures. Si un SOC national bénéficie du soutien de l'Union, il s'engage à demander à participer à un SOC transfrontière dans un délai de deux ans.

Un SOC transfrontière est un consortium d'au moins trois États membres, représentés par des SOC nationaux, qui s'engagent à collaborer pour coordonner leurs activités de détection et de

surveillance des cybermenaces. À la suite d'un premier appel à manifestation d'intérêt, un consortium d'hébergement peut être sélectionné par l'ECCC pour participer à des acquisitions conjointes d'outils et d'infrastructures avec l'ECCC et bénéficier d'une subvention pour l'exploitation des outils et des infrastructures. Les membres du consortium d'hébergement concluent un accord de consortium écrit qui définit leurs modalités internes. Le chapitre détaille ensuite les exigences relatives à l'échange d'informations entre les participants à un SOC transfrontière, et à l'échange d'informations entre un SOC transfrontière et d'autres SOC transfrontières, ainsi qu'avec les entités concernées de l'Union. Les SOC nationaux participant à un SOC transfrontière partagent entre eux les informations pertinentes relatives aux cybermenaces, et les modalités, notamment l'engagement à partager des quantités importantes de données et les conditions y afférentes, doivent être définies dans un accord de consortium. Les SOC transfrontières garantissent un niveau élevé d'interopérabilité entre eux. Ils devraient également conclure des accords de coopération avec d'autres SOC transfrontières, qui précisent les principes relatifs au partage d'informations. Lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils communiquent les informations pertinentes à EU-CyCLONe, au réseau des CSIRT et à la Commission, compte tenu de leurs rôles respectifs en matière de gestion de crise conformément à la directive (UE) 2022/2555. Le chapitre II se termine en précisant les conditions de sécurité à remplir pour participer au cyberbouclier européen.

Le mécanisme d'urgence dans le domaine de la cybersécurité (chapitre III)

Le chapitre III établit le mécanisme d'urgence dans le domaine de la cybersécurité visant à améliorer la résilience de l'Union face à des menaces de cybersécurité majeures ainsi qu'à s'y préparer et à atténuer, dans un esprit de solidarité, les effets à court terme des incidents ou des crises de cybersécurité importants et majeurs. Les actions de mise en œuvre du mécanisme d'urgence dans le domaine de la cybersécurité seront soutenues par un financement au titre du programme pour une Europe numérique. Le mécanisme prévoit des actions visant à soutenir la préparation, notamment des tests coordonnés d'entités actives dans des secteurs hautement critiques, la réaction à des incidents de cybersécurité importants ou majeurs et le rétablissement immédiat, ou l'atténuation des cybermenaces importantes, ainsi que des mesures d'assistance mutuelle.

Les mesures de préparation du mécanisme d'urgence dans le domaine de la cybersécurité comprennent des tests de préparation coordonnés des entités actives dans des secteurs hautement critiques. La Commission, après avoir consulté l'ENISA et le groupe de coopération SRI, devrait régulièrement déterminer les secteurs ou sous-secteurs pertinents des secteurs hautement critiques énumérés à l'annexe I de la directive (UE) nº 2022/2555, dont les entités peuvent faire l'objet de tests de préparation coordonnés au niveau de l'Union.

Aux fins de la mise en œuvre des mesures de réaction aux incidents proposées, le présent règlement établit une réserve de cybersécurité de l'Union, composée de services de réaction aux incidents fournis par des fournisseurs de confiance, sélectionnés conformément aux critères établis dans le présent règlement. Les utilisateurs des services de la réserve de cybersécurité de l'Union comprennent les autorités des États membres chargées de la gestion

des crises de cybersécurité et les CSIRT ainsi que les institutions, organes et organismes de l'Union. La Commission assume la responsabilité globale de la mise en œuvre de la réserve de cybersécurité de l'Union et peut confier, en tout ou en partie, à l'ENISA le fonctionnement et l'administration de la réserve de cybersécurité de l'Union.

Pour bénéficier de l'aide de la réserve de cybersécurité de l'Union, les utilisateurs devraient prendre leurs propres mesures afin d'atténuer les effets de l'incident pour lequel ils demandent l'aide. Les demandes d'aide adressées à la réserve de cybersécurité de l'Union devraient inclure les informations pertinentes nécessaires sur l'incident et les mesures déjà prises par les utilisateurs. Le chapitre décrit également les modalités de mise en œuvre, notamment l'évaluation des demandes adressées à la réserve de cybersécurité de l'Union.

Le règlement définit également les principes d'adjudication et les critères de sélection des fournisseurs de confiance de la réserve de cybersécurité de l'Union.

Les pays tiers peuvent solliciter l'aide de la réserve de cybersécurité de l'Union lorsque les accords d'association conclus concernant leur participation au programme pour une Europe numérique le prévoient. Le chapitre décrit les conditions et les modalités de cette participation.

Le mécanisme d'analyse des incidents de cybersécurité (chapitre IV)

À la demande de la Commission, d'EU-CyCLONe ou du réseau des CSIRT, l'ENISA devrait analyser et évaluer les menaces, les vulnérabilités et les mesures d'atténuation relatives à un incident de cybersécurité important ou majeur. L'analyse et l'évaluation devraient être communiquées par l'ENISA sous la forme d'un rapport d'analyse au réseau des CSIRT, à EU-CyCLONe et à la Commission afin de les aider dans l'exercice de leurs fonctions. Lorsque l'incident concerne un pays tiers, la Commission devrait également transmettre le rapport au haut représentant. Il y a lieu que le rapport contienne les enseignements tirés et, au besoin, des recommandations destinées à améliorer la posture cyber de l'Union.

Dispositions finales (chapitre V)

Le chapitre V contient des modifications du règlement sur le programme pour une Europe numérique et prévoit l'obligation pour la Commission de préparer des rapports réguliers aux fins de l'évaluation et du réexamen du règlement au Parlement européen et au Conseil. La Commission est habilitée à adopter des actes d'exécution en conformité avec la procédure d'examen visée à l'article 21 pour les finalités suivantes: préciser les conditions de l'interopérabilité entre les SOC transfrontières; déterminer les modalités procédurales du partage d'informations relatives à un incident de cybersécurité majeur, potentiel ou actuel, entre les SOC transfrontières et les entités de l'Union; établir des exigences techniques pour garantir un niveau élevé de sécurité des données et de sécurité physique des infrastructures et protéger les intérêts de l'Union en matière de sécurité lors de l'échange d'informations avec des entités qui ne sont pas des organismes publics des États membres; préciser les types et le nombre de services de réaction aux incidents requis pour la réserve de cybersécurité de

l’Union; et préciser davantage les modalités d’attribution des services d’aide de la réserve de cybersécurité de l’Union.

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

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[1],

vu l'avis du Comité économique et social européen[2],

vu l'avis du Comité des régions[3],

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 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.

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

[1] JO C […] du […], p. […].
[2] JO C du , p. .
[3] JO C du , p. .

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.

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[4], 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.

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[5], de la recommandation (UE) 2017/1584 de la Commission[6], de la directive 2013/40/UE du Parlement européen et du Conseil[7] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[8]. 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'UE afin de mieux détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir. Dans

---

4 https://futureu.europa.eu/fr/

5 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).

6 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).

7 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).

8 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).

les conclusions du Conseil sur la posture cyber de l'Union[9], 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.

6) La communication conjointe relative à la politique de cyberdéfense de l'UE[10], 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.

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).

8) Pour atteindre ces objectifs, il est également nécessaire de modifier certains points du règlement (UE) 2021/694 du Parlement européen et du Conseil[11]. 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 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).

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

11 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).

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.

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 financier 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.

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.

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 directive (UE) 2022/2555 du Parlement européen et du Conseil[12].

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

[12] 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).

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.

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, 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.

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.

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.

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.

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 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.

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[13].

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

[13] 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).

partage d'informations au sein de la communauté de cyberdéfense, en étroite coopération avec le haut représentant.

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 de la réglementation nationale ou de l'Union devrait se limiter au minimum nécessaire et être proportionné à l'objectif de cet échange. L'échange de 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 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 en cas d'incident informatique de la CSP[14] 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.

[14] 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) 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[15], l'IPCR[16,] 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 et les États membres touchés. Lorsqu'un État membre sollicite une aide au titre du mécanisme d'urgence dans le domaine de la cybersécurité, il devrait fournir des informations pertinentes permettant de justifier sa demande aide.

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.

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

---

15 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).

16 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.

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[17]. 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. Les services en question devraient permettre d’aider les autorités nationales à apporter une

[17] 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.

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.

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.

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.

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.

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.

39) L'objectif poursuivi par le présent règlement peut être mieux atteint au niveau de l'Union que par les États membres. 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. 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'une infrastructure paneuropéenne 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 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;

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, y compris en tirant les enseignements de l'expérience acquise et, le cas échéant, en formulant des recommandations.

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) **«centre d'opérations de sécurité transfrontière» («SOC transfrontière»)**: une plateforme multinationale qui rassemble, au sein d'une structure de réseau coordonnée, les SOC nationaux d'au moins trois États membres qui forment un consortium d'hébergement, et qui est conçue pour prévenir les cybermenaces et les incidents et pour soutenir la production de renseignements de haute qualité, notamment par l'échange de données provenant de différentes sources, publiques et privées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance;

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[18];

3) **«consortium d'hébergement»**: un consortium formé par des États participants, représentés par les SOC nationaux, qui ont accepté de mettre en place un SOC transfrontière et de contribuer à l'acquisition des outils et de l'infrastructure nécessaires à ce centre, ainsi qu'au fonctionnement de celui-ci;

[18] 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).

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

5) **«entités actives dans des secteurs critiques ou hautement critiques»**: un type d'entités parmi ceux énumérés à l'annexe I et à l'annexe II de la directive (UE) 2022/2555;

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

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;

11) «**fournisseurs de confiance**»: les fournisseurs de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555 sélectionnés conformément à l'article 16 du présent règlement.

Chapitre II

LE CYBERBOUCLIER EUROPÉEN

Article 3

Création du cyberbouclier européen

1. Une infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité («cyberbouclier européen») est mise en place pour doter l'Union de capacités avancées lui permettant de détecter, d'analyser et de traiter des données sur les cybermenaces et les incidents sur son territoire. Elle est formée 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;

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;

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 de participer au cyberbouclier européen. Le SOC national est un organisme public.

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.

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.

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.

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.

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) vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;

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 une quantité importante de données 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, ces derniers garantissent un niveau élevé d'interopérabilité entre eux. Afin de faciliter l'interopérabilité entre les SOC transfrontières, la Commission peut, au moyen d'actes d'exécution, après consultation de l'ECCC, préciser les conditions de cette interopérabilité. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

4. Les SOC transfrontières concluent des accords de coopération entre eux, qui précisent les principes de partage d'informations en vigueur entre les plateformes transfrontières.

Article 7

Coopération et partage d'informations avec les entités de l'Union

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.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les dispositions procédurales du partage d'informations prévu au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement.

Article 8

Sécurité

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.

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. 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.

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 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.

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 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.

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.

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.

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.

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.

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.

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, 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 peut confier, 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, 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.

8. La Commission peut, au moyen d'actes d'exécution, préciser les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.

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 peut, au moyen d'actes d'exécution, préciser davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2.

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 dans les meilleurs délais aux utilisateurs visés à l'article 12, paragraphe 3.

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) 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.

4. Les accords visés au paragraphe 3 peuvent se baser sur des modèles élaborés par l'ENISA, après consultation des États membres.

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.

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 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.

7. La Commission fait régulièrement rapport au groupe de coopération SRI sur l'utilisation de cette aide et les résultats obtenus.

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[19], 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.

[19] 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).

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 sur l'Union européenne.

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 sur le fonctionnement de l'Union européenne.

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.

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:

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 nécessaire au service demandé;

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;

j) dès qu'un schéma de certification de l'UE pour les services de sécurité gérés conformément au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma.

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 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 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.

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.

4. Le cas échéant, le rapport formule des recommandations 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:

1) 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;»;

2) le point g) suivant est ajouté:

«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.»;

a) 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[20], à l'exception des actions mettant en œuvre la réserve de cybersécurité de l'UE, qui sont exécutées par la Commission et l'ENISA.».

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) 1 629 566 000 EUR pour l'objectif spécifique 3 – Cybersécurité et confiance;

d) 482 347 000 EUR pour l'objectif spécifique 4 - Compétences numériques avancées;»;

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 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.».

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

[20] 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).

«2. Le programme peut octroyer un financement sous l'une ou l'autre des formes prévues dans le règlement financier, 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/XX, 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) XXX/XXXX [FR Refonte], 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/XX, 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) XXX/XXXX [FR Refonte], 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:

«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/XX. En cas de conflit entre les dispositions du présent règlement et les articles 4 et 5 du règlement (UE) 2023/XX, 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 financier et peuvent couvrir jusqu'à 100 % des coûts éligibles, sans préjudice du principe de cofinancement prévu à l'article 190 du règlement financier. 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 XXXX et au consortium d'hébergement visé à l'article 5 du règlement XXXX, conformément à l'article 195, paragraphe 1, point d), du règlement financier.

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 XXXX 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 financier.

En ce qui concerne les mesures énoncées à l'article 10, paragraphe 1, point c), du règlement 202X/XXXX, 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 XXXX, et conformément à l'article 193, paragraphe 2, deuxième alinéa, point a), du règlement financier, 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 sont modifiées conformément à l'annexe du présent règlement.

Article 20

Évaluation

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.

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*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

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

1.3. La proposition/l'initiative porte sur:

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

1.4.2. Objectif(s) spécifique(s)

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

1.4.4. Indicateurs de performance

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

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union, qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

1.5.3. Leçons tirées d'expériences similaires

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) d'exécution budgétaire prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. Mesures de prévention des fraudes et irrégularités

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

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

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

3.2.3.1 Besoins estimés en ressources humaines

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

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

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

Une Europe adaptée à l'ère du numérique

Investissements stratégiques européens

Activité(s): façonner l'avenir numérique de l'Europe.

1.3. La proposition/l'initiative porte sur:

☒ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[33]

☐ **la prolongation d'une action existante**

☐ **une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

Le règlement sur la cybersolidarité renforcera la solidarité au niveau de l'Union afin de mieux détecter les menaces et incidents de cybersécurité, de mieux s'y préparer et de mieux y réagir. Il vise à:

a) renforcer les capacités communes de l'Union en matière de détection et d'appréciation de la situation de menaces et incidents de cybersécurité;

b) améliorer la préparation des entités critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités communes de réaction aux incidents de cybersécurité importants ou majeurs, y compris en mettant à la disposition des pays tiers qui sont associés au programme pour une Europe numérique un soutien à la réaction aux incidents;

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.

1.4.2. Objectif(s) spécifique(s)

Le règlement sur la cybersolidarité atteindra les objectifs fixés par les moyens suivants:

[33] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

a) le déploiement d'une infrastructure paneuropéenne composée de centres d'opérations de sécurité (le cyberbouclier européen) afin de créer et d'améliorer les capacités communes de détection et d'appréciation de la situation;

b) la création d'un mécanisme d'urgence dans le domaine de la cybersécurité afin d'aider les États membres à se préparer et à réagir aux incidents de cybersécurité importants et majeurs, et à s'en rétablir immédiatement. Le soutien à la réaction aux incidents est également mis à la disposition des institutions, organes et organismes de l'Union;

Ces actions seront soutenues par un financement au titre du programme pour une Europe numérique, que le présent instrument législatif modifiera afin de mettre en place les actions susmentionnées, de prévoir un soutien financier pour leur développement et de préciser les conditions à remplir pour bénéficier de ce soutien financier.

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

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

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

La proposition présenterait des avantages significatifs pour les différentes parties intéressées. 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/au rétablissement du fonctionnement des services essentiels.

Ces actions renforceront la position concurrentielle de l'industrie et des entreprises en Europe dans tous les secteurs d'activité passés au numérique et soutiendront leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Le présent règlement vise notamment à renforcer la résilience des citoyens, des entreprises et des entités actives dans des secteurs critiques ou hautement critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Pour ce faire, il prévoit un investissement dans des outils qui permettront de détecter plus rapidement les menaces et incidents de cybersécurité et d'y réagir, ainsi qu'une aide destinée aux États membres afin qu'ils puissent mieux se préparer et réagir aux incidents de cybersécurité importants et majeurs. Il devrait également permettre de doter l'Europe de capacités plus solides dans ces domaines, notamment en ce qui concerne la collecte et l'analyse de données sur les menaces et incidents de cybersécurité.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Afin de promouvoir la solidarité au niveau de l'Union, plusieurs indicateurs pourraient être pris en considération:

1) le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints;

2) le nombre d'actions soutenant la préparation et la réaction aux incidents de cybersécurité dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité.

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

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Le présent règlement devrait être intégralement applicable peu après son adoption, c'est-à-dire le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union, qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

La nature fortement transfrontière des menaces sur la cybersécurité en général et le nombre croissant de risques et d'incidents ayant des répercussions transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs de la présente intervention ne peuvent pas être atteints efficacement par les seuls États membres et nécessitent une action commune et une solidarité au niveau de l'Union. L'expérience acquise dans la lutte contre les cybermenaces découlant de la guerre menée par la Russie contre l'Ukraine ainsi que les enseignements tirés d'un exercice de cybersécurité mené sous la présidence française (EU CyCLES) ont montré qu'il convient de mettre en place des mécanismes concrets de soutien mutuel, notamment une coopération avec le secteur privé, afin de parvenir à une solidarité au niveau de l'Union. C'est dans ce contexte que, dans ses conclusions du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne, le Conseil a invité la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité. Le soutien et les actions menées au niveau de l'Union en vue de mieux détecter les menaces de cybersécurité et de renforcer les capacités de préparation et de réaction apportent une valeur ajoutée car ils évitent les doubles emplois dans l'Union et les États membres. Cela permettrait de mieux exploiter les ressources existantes et d'améliorer la coordination et l'échange d'informations sur les enseignements tirés.

1.5.3. Leçons tirées d'expériences similaires

En ce qui concerne l'appréciation de la situation et la détection dans le cadre du cyberbouclier européen, un appel à manifestation d'intérêt pour des acquisitions conjointes d'outils et d'infrastructures en vue de la création de SOC transfrontières et un appel à subventions pour permettre le renforcement des capacités des SOC desservant des organisations publiques et privées ont été organisés dans le cadre du programme de travail cybersécurité pour 2021-2022 du programme pour une Europe numérique.

En ce qui concerne la préparation et la réaction aux incidents, la Commission a mis en place un programme à court terme pour soutenir les États membres, aux fins duquel un financement supplémentaire a été alloué à l'ENISA afin de renforcer immédiatement la préparation et les capacités de réaction à des cyberincidents majeurs. Les services fournis comprennent des mesures de préparation, telles que des

tests de pénétration des entités critiques afin d'en déterminer les vulnérabilités. Les possibilités d'aide aux États membres en cas d'incident majeur touchant des entités critiques sont également renforcées. La mise en œuvre par l'ENISA de ce programme à court terme est en cours et a déjà fourni des informations précieuses qui ont été prises en considération dans la préparation du présent règlement.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Le règlement sur la cybersolidarité s'appuiera sur les actions actuellement soutenues par l'Union et les États membres en vue d'améliorer l'appréciation de la situation et la détection des cybermenaces ainsi que de réagir aux incidents de cybersécurité transfrontières et majeurs. En outre, l'instrument est cohérent avec d'autres cadres de gestion des crises, notamment l'IPCR, la politique de sécurité et de défense commune, prévoyant des équipes d'intervention rapide en cas d'incident informatique, et l'assistance fournie par un État membre à un autre État membre au titre de l'article 42, paragraphe 7, du traité sur l'Union européenne. La nouvelle proposition compléterait et soutiendrait également les structures développées dans le cadre d'autres instruments de cybersécurité tels que la directive (UE) 2022/2555 (directive SRI 2) ou le règlement (UE) 2019/881 (le règlement sur la cybersécurité).

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

La gestion des domaines d'action assignés à l'ENISA s'inscrit dans son mandat et ses tâches générales. Ces domaines d'action peuvent nécessiter des profils spécifiques ou de nouvelles affectations, mais ces besoins pourraient être couverts par les ressources existantes de l'ENISA et par la redistribution ou l'association de diverses missions. L'ENISA met actuellement en œuvre un programme à court terme mis en place en 2022 par la Commission afin de renforcer immédiatement la préparation et les capacités de réaction à des cyberincidents majeurs. Les services fournis comprennent des possibilités d'aide aux États membres en cas d'incident majeur touchant des entités critiques. La mise en œuvre par l'ENISA de ce programme à court terme est en cours et a déjà fourni des informations précieuses qui ont été prises en considération lors de la préparation du présent règlement. Les ressources allouées au programme à court terme pourraient également être utilisées dans le cadre du présent règlement.

1.6. Durée et incidence financière de la proposition/de l'initiative

☒ **durée limitée**

– ☒ en vigueur à compter de la date d'adoption de 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 (le «règlement sur la cybersolidarité»)

– ☒ Incidence financière de 2023 jusqu'en 2027 pour les crédits d'engagement et de 2023 jusqu'en 2031 pour les crédits de paiement[34].

☐ **durée illimitée**

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

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

1.7. Mode(s) d'exécution budgétaire prévu(s)[35]

☒ **Gestion directe** par la Commission

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

– ☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

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

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

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

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

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

– ☐ à des établissements de droit public;

– ☐ à des entités de droit privé investies d'une mission de service public, pour autant qu'elles soient dotées de garanties financières suffisantes;

– ☐ à des entités de droit privé d'un État membre qui sont chargées de la mise en œuvre d'un partenariat public-privé et dotées de garanties financières suffisantes;

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

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

Remarques

Les actions relatives au cyberbouclier européen seront mises en œuvre par l'ECCC. Jusqu'à ce que l'ECCC ait la capacité d'exécuter son propre budget, la Commission européenne

[34] Les actions prévues par le règlement devraient être soutenues par le prochain cadre financier pluriannuel.

[35] Les explications sur les modes d'exécution budgétaire ainsi que les références au règlement financier sont disponibles sur le site BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

mettra en œuvre les actions en gestion directe au nom de l'ECCC. L'ECCC peut sélectionner des entités sur la base d'appels à manifestation d'intérêt pour participer à des acquisitions conjointes d'outils. L'ECCC peut accorder des subventions pour le fonctionnement de ces outils.

En outre, l'ECCC peut accorder des subventions pour des actions de préparation dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité.

La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission peut confier, par voie de conventions de contribution, le fonctionnement et l'administration de la réserve de cybersécurité de l'Union, en tout ou en partie, à l'ENISA. Les actions assignées à l'ENISA par le présent règlement sont conformes à son mandat existant. Il s'agit notamment des actions suivantes: i) aider le groupe de coopération SRI à définir les mesures de préparation en fonction des évaluations des risques; ii) aider la Commission à établir et à superviser la mise en œuvre de la réserve de cybersécurité de l'Union, notamment à recevoir et à traiter les demandes d'aide; iii) élaborer des modèles pour faciliter la présentation des demandes d'aide et des accords spécifiques à conclure entre le prestataire de services et l'utilisateur auquel l'aide est fournie dans le cadre de la réserve de cybersécurité de l'Union; iv) examiner et évaluer les menaces, les vulnérabilités et les mesures d'atténuation relatives à un incident de cybersécurité important ou majeur et préparer des rapports à ce sujet.

Toutes ces missions sont estimées à environ 7 ETP sur les ressources existantes de l'ENISA, en s'appuyant déjà sur son expertise et sur les travaux préparatoires qu'elle effectue actuellement dans le cadre du projet pilote d'aide d'urgence pour la préparation et la réaction aux incidents.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

La Commission suivra la mise en œuvre, l'application et le respect de ces nouvelles dispositions pour évaluer leur efficacité. La Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement dans un délai de quatre ans à compter de la date de son application.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée

Le règlement prévoit un cadre de mise en œuvre du financement de l'Union en vue de renforcer la résilience en matière de cybersécurité par des actions améliorant les capacités de détection, de réaction et de rétablissement en cas d'incidents de cybersécurité importants et majeurs. Les unités au sein de la DG CNECT chargées de ce domaine politique assureront la mise en œuvre du règlement.

Afin qu'ils soient en mesure d'assumer les nouvelles tâches, il est nécessaire de doter les services de la Commission des ressources appropriées. On estime que l'application du nouveau règlement nécessite 6 ETP (dont trois AD et trois CA) pour couvrir les tâches suivantes:

- définir les mesures de préparation en fonction des évaluations des risques;
- garantir l'interopérabilité entre les plateformes SOC transfrontières;
- élaborer d'éventuels actes d'exécution (deux pour les SOC et deux pour le mécanisme d'urgence dans le domaine de la cybersécurité);
- gérer les accords d'hébergement et d'utilisation pour les SOC;
- établir et gérer la réserve de cybersécurité de l'Union, directement ou au moyen d'une convention de contribution à l'ENISA. En cas de convention de contribution à l'ENISA, élaborer et superviser la mise en œuvre de la convention de contribution pour les tâches assignées à l'ENISA;
- participer aux groupes de consultation réunis par l'ENISA afin d'analyser et d'évaluer les incidents de cybersécurité importants et majeurs et préparer les rapports.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

L'un des risques recensés pour le cyberbouclier européen est que les États membres ne partagent pas suffisamment d'informations pertinentes sur les cybermenaces, que ce soit au sein des plateformes SOC transfrontières ou entre les plateformes transfrontières et d'autres entités concernées au niveau de l'Union. Afin d'atténuer ces risques, l'attribution des fonds se fera à la suite d'un appel à manifestation d'intérêt dans le cadre duquel les États membres s'engageront à partager un certain nombre d'informations avec l'Union. Cet engagement sera ensuite formalisé dans un accord d'hébergement et d'utilisation, qui donnera à l'ECCC le pouvoir de mener des audits pour s'assurer que les outils et les infrastructures ayant fait l'objet

d'acquisitions conjointes sont utilisés conformément à l'accord. Les engagements en faveur d'un niveau élevé de partage d'informations au sein des SOC transfrontières seront formalisés dans un accord de consortium.

L'un des risques recensés pour le mécanisme d'urgence dans le domaine de la cybersécurité est que les utilisateurs participant au mécanisme ne prennent pas de mesures suffisantes pour se préparer à des cyberattaques. Ainsi, pour pouvoir bénéficier de l'aide de la réserve de cybersécurité de l'Union, les utilisateurs sont tenus de prendre de telles mesures de préparation. Lorsqu'ils adressent des demandes d'aide à la réserve de cybersécurité de l'Union, les utilisateurs doivent expliquer les mesures qui ont déjà été prises pour réagir à l'incident, lesquelles seront prises en considération lors de l'évaluation des demandes adressées à la réserve de cybersécurité de l'Union.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Étant donné que les règles de participation au programme pour une Europe numérique qui sont applicables au soutien fourni au titre du règlement sur la cybersolidarité sont semblables à celles que la Commission utilisera dans ses programmes de travail, et que la population de bénéficiaires présente un profil de risque semblable à celle des programmes faisant l'objet d'une gestion directe, on peut s'attendre à ce que le niveau d'erreur soit semblable à celui établi par la Commission pour le programme pour une Europe numérique, c'est-à-dire de nature à fournir une assurance raisonnable que le risque d'erreur au cours de la période de dépenses pluriannuelle se situe, sur une base annuelle, entre 2 % et 5 %, l'objectif final étant d'arriver à un taux d'erreur résiduel aussi proche que possible de 2 % à la clôture des programmes pluriannuels, après prise en compte des incidences financières de tous les audits et de toutes les mesures de correction et de recouvrement.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

Dans le cas du cyberbouclier européen, l'ECCC aura le pouvoir d'auditer, en accédant aux informations et en menant des contrôles sur place, les outils et infrastructures ayant fait l'objet d'acquisitions conjointes, conformément à l'accord d'hébergement et d'utilisation qui doit être signé entre le consortium d'hébergement et l'ECCC.

Les mesures de prévention des fraudes existantes applicables aux institutions, organes et organismes de l'Union couvriront les crédits supplémentaires nécessaires aux fins du présent règlement.

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

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

- Lignes budgétaires existantes

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

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND[36].	de pays AELE[37]	de pays candidats et pays candidats potentiels[38]	d'autres pays tiers	autres recettes affectées
1	02 04 01 10 – Programme pour une Europe numérique – Cybersécurité	CD	OUI	OUI	NON	NON
1	02 04 01 11– Programme pour une Europe numérique – Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité	CD	OUI	OUI	NON	NON
1	02 04 03 – Programme pour une Europe numérique – Intelligence artificielle	CD	OUI	OUI	NON	NON
1	02 04 04 – Programme pour une Europe numérique – Compétences	CD	OUI	OUI	NON	NON
1	02 01 30 – Dépenses d'appui pour le programme pour une Europe numérique	CND	OUI	OUI	NON	NON

[36] CD = crédits dissociés / CND = crédits non dissociés.
[37] AELE: Association européenne de libre-échange.
[38] Pays candidats et, le cas échéant, pays candidats potentiels

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

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

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

En Mio EUR (à la 3e décimale)

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

La proposition n'augmentera pas le niveau total des engagements au titre du programme pour une Europe numérique. En effet, la contribution à cette initiative est une redistribution des engagements provenant de l'OS2 et de l'OS4 pour renforcer le budget de l'OS3 et de l'ECCC. Toute augmentation des engagements au titre du programme pour une Europe numérique résultant d'une révision du CFP pourrait être utilisée aux fins de cette initiative.

DG CNECT			Année **2025**	Année **2026**	Année **2027**	Année **2028**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			**TOTAL**
○ Crédits opérationnels										
Ligne budgétaire[39] 02.040110 (redistribution de 02.0403 et 02.0404)	Engagements	1a)	15,000	15,000	6,000	p.m.				**36,000**
	Paiements	2a)	15,000	15,000	6,000					**36,000**
Ligne budgétaire 02.040111.02 (redistribution de 02.0403 et 02.0404)	Engagements	1b)	13,000	23,000	28,000	p.m.				**64,000**
	Paiements	2b)	8,450	18,200	25,250	12,100				**64,000**
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[40]										

39 Selon la nomenclature budgétaire officielle.

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

Ligne budgétaire 02.0130		3)	0,150	0,150	0,150	p.m.				0,450
TOTAL des crédits pour la DG CNECT	Engagements	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Paiements	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ TOTAL des crédits opérationnels	Engagements	4)	28,000	38,000	34,000	p.m.				**100,000**
	Paiements	5)	23,450	33,200	31,250	12,100				**100,000**
○ TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		6)	0,150	0,150	0,150	p.m.				**0,450**
Total des crédits pour la RUBRIQUE 1 du cadre financier pluriannuel	Engagements	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Paiements	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Si plusieurs rubriques opérationnelles sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

○ TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	4)	28,000	38,000	34,000	p.m.				**100,000**
	Paiements	5)	23,450	33,200	31,250	12,100				**100,000**
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		6)	0,150	0,150	0,150					**0,450**
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (Montant de référence)	Engagements	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Paiements	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Rubrique du cadre financier pluriannuel	**7**	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe 5 de la décision de la Commission relative aux règles internes sur l'exécution de la section «Commission» du budget général de l'Union européenne), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2025**	Année **2026**	Année **2027**	Année **2028**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			**TOTAL**
DG: CNECT									
○ Ressources humaines		0,786	0,786	0,786	p.m.				**2,358**
○ Autres dépenses administratives		0,035	0,035	0,035	p.m.				**0,105**
TOTAL DG CNECT	Crédits	**0,821**	**0,821**	**0,821**					**2,463**

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	**0,821**	**0,821**	**0,821**					**2,463**

En Mio EUR (à la 3e décimale)

		Année **2025**	Année **2026**	Année **2027**	Année **2028**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Engagements	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Paiements	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

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

Indiquer les objectifs et les réalisations ⇩			Année **N**		Année **N+1**		Année **N+2**		Année **N+3**		Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)						**TOTAL**	
	RÉALISATIONS (outputs)																	
	Type[41]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[42]…																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique nº 1																		
OBJECTIF SPÉCIFIQUE nº 2…																		
- Réalisation																		
Sous-total objectif spécifique nº 2																		
TOTAUX																		

41 Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites).

42 Tel que décrit au point 1.4.2. «Objectif(s) spécifique(s)…».

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

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

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

En Mio EUR (à la 3e décimale)

	Année 2025	Année 2026	Année 2027	Année N+3	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			**TOTAL**
RUBRIQUE 7 du cadre financier pluriannuel								
Ressources humaines	0,786	0,786	0,786					**2,358**
Autres dépenses administratives	0,035	0,035	0,035					**0,105**
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	**0,821**	**0,821**	**0,821**					**2,463**

Hors RUBRIQUE 7[43] du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses de nature administrative	0,150	0,150	0,150					**0,450**
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel	**0,150**	**0,150**	**0,150**					**0,450**

TOTAL	**0,971**	**0,971**	**0,971**					**2,913**

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

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

3.2.3.1 Besoins estimés en ressources humaines

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

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

Estimation à exprimer en équivalents temps plein

		Année **2025**	Année **2026**	Année 2027	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)		
O Emplois du tableau des effectifs (fonctionnaires et agents temporaires)								
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		3	3	3				
20 01 02 03 (Délégations)								
01 01 01 01 (Recherche indirecte)								
01 01 01 11 (Recherche directe)								
Autres lignes budgétaires (à préciser)								
O Personnel externe (en équivalents temps plein: ETP)[44]								
20 02 01 (AC, END, INT de l'enveloppe globale)		3	3	3				
20 02 03 (AC, AL, END, INT et JPD dans les délégations)								
XX 01 **xx yy zz** [45]	- au siège							
	- en délégation							
01 01 01 02 (AC, END, INT sur recherche indirecte)								
01 01 01 12 (AC, END, INT sur recherche directe)								
Autres lignes budgétaires (à préciser)								
TOTAL		**6**	**6**	**6**				

XX est le domaine politique ou le titre concerné.

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

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	- définir les mesures de préparation en fonction des évaluations des risques (article 11) - élaborer d'éventuels actes d'exécution (deux pour les SOC et deux pour le mécanisme d'urgence dans le domaine de la cybersécurité) - gérer les accords d'hébergement et d'utilisation pour les SOC - établir et gérer la réserve de cybersécurité de l'Union, directement ou au moyen d'une convention de contribution à l'ENISA
Personnel externe	sous la supervision d'un agent, - définir les mesures de préparation en fonction des évaluations des risques (article 11) - élaborer d'éventuels actes d'exécution (deux pour les SOC et deux pour le mécanisme d'urgence dans le domaine de la cybersécurité)

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

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

	- gérer les accords d'hébergement et d'utilisation pour les SOC - établir et gérer la réserve de cybersécurité de l'Union, directement ou au moyen d'une convention de contribution à l'ENISA

3.2.4. *Compatibilité avec le cadre financier pluriannuel actuel*

La proposition/l'initiative:

– ☒ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants. Veuillez fournir un tableau Excel en cas de reprogrammation de grande envergure.

	23	24	25	26	27	total
OS1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
OS2 initial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
A l'initiative			18.000.000	28.000.000	19.000.000	
CYBER						65.000.000
NOUVEAU OS2	**226.316.819**	**295.067.000**	**177.649.000**	**193.809.000**	**227.608.000**	**1.120.449.819**
OS3 DB 24	24.361.553	35.596.172	3.638.000	3.638.000	11.175.000	78.408.725
De OS2-OS4			15.000.000	15.000.000	6.000.000	36.000.000
Nouveau OS3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC initial	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
De OS2-OS4			13.000.000	23.000.000	28.000.000	64.000.000
Nouveau ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
OS4 initial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
A l'initiative			10.000.000	10.000.000	15.000.000	
CYBER						35.000.000
NOUVEAU OS4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

– ☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

Explicitez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont l'utilisation est proposée.

– ☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. *Participation de tiers au financement*

La proposition/l'initiative:

– ☒ ne prévoit pas de cofinancement par des tierces parties

– ☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[46]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL des crédits cofinancés								

[46] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

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

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

  – ☐ sur les ressources propres

  – ☐ sur les autres recettes

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

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[47]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)		
Article …….								

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

[…]

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

[…]

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