



UNION EUROPÉENNE

LE PARLEMENT EUROPÉEN

LE CONSEIL

**Bruxelles, le 19 décembre 2024
(OR. en)**

**2023/0109(COD)
LEX 2422**

**PE-CONS 94/1/24
REV 1**

**CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588**

**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 CYBERMENACES ET INCIDENTS, DE S'Y PRÉPARER
ET D'Y RÉAGIR ET MODIFIANT LE RÈGLEMENT (UE) 2021/694
(RÈGLEMENT SUR LA CYBERSOLIDARITÉ)**

RÈGLEMENT (UE) 2024/...
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 19 décembre 2024

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

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 comptes¹,

vu l'avis du Comité économique et social européen²,

vu l'avis du Comité des régions³,

statuant conformément à la procédure législative ordinaire⁴,

¹ Avis du 18 avril 2003 (non encore paru au Journal officiel).

² JO C 349 du 29.9.2023, p. 167.

³ JO C, C/2024/1049, 9.2.2024, ELI: <http://data.europa.eu/eli/C/2024/1049/oj>.

⁴ Position du Parlement européen du 24 avril 2024 (non encore parue au Journal officiel) et décision du Conseil du 2 décembre 2024.

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 et de la société, compte tenu de l'interconnexion et de l'interdépendance sans cesse croissantes des administrations publiques, des entreprises et des citoyens des États membres par-delà les secteurs et les frontières, créant dans le même temps de possibles vulnérabilités.

- (2) L'ampleur, la fréquence et les effets des incidents de cybersécurité y compris les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation ne cessent de croître au niveau de l'Union et au niveau mondial. 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 de cybersécurité provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite une préparation renforcée du cadre de cybersécurité de l'Union. Ce risque va au-delà de la guerre d'agression menée par la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics, étant donné que les cyberattaques ciblent souvent des services et infrastructures publics locaux, régionaux et nationaux, les collectivités locales étant particulièrement vulnérables, notamment en raison de leurs ressources limitées. Ils peuvent également nuire à la poursuite des activités économiques, notamment dans les secteurs hautement critiques ou d'autres secteurs critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie et aux systèmes démocratiques 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 rapidement, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays. Il est important d'avoir une coopération étroite entre le secteur public, le secteur privé, le monde universitaire, la société civile et les médias.

- (3) Il est nécessaire de renforcer la position concurrentielle de l'industrie et des services dans l'ensemble de l'économie numérique de 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. Il est nécessaire d'accroître la résilience des citoyens, des entreprises, y compris des microentreprises, des petites et moyennes entreprises et des jeunes pousses, et des entités exploitant des infrastructures critiques, face aux cybermenaces croissantes, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il est donc nécessaire d'investir dans les infrastructures et les services, et de renforcer les capacités pour développer les compétences en matière de cybersécurité qui permettront de détecter les cybermenaces et incidents et d'y réagir plus rapidement. En outre, les États membres ont besoin d'aide pour mieux se préparer aux incidents de cybersécurité importants et aux incidents de cybersécurité majeurs et pour y réagir, ainsi que pour assurer le rétablissement initial après ces incidents. En s'appuyant sur les structures existantes et en coopération étroite avec elles, l'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux cybermenaces et incidents.

- (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, en particulier dans le cadre du règlement (UE) 2019/881 du Parlement européen et du Conseil⁵, des directives 2013/40/UE⁶ et (UE) 2022/2555⁷ du Parlement européen et du Conseil et de la recommandation (UE) 2017/1584⁸ de la Commission. En outre, la 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 invite les États membres à prendre des mesures et à coopérer 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 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) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

⁶ 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).

⁷ 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) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022, p. 80).

⁸ 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).

- (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 d'un État membre à un autre et d'un pays tiers à l'Union, il est nécessaire de renforcer la solidarité au niveau de l'Union afin de mieux détecter les cybermenaces et incidents, de s'y préparer, d'y réagir et de s'en rétablir, notamment en renforçant les capacités des structures existantes. De plus, 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.
- (6) La communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 10 novembre 2022 au Parlement européen et au Conseil relative à la politique de cyberdéfense de l'UE a annoncé une initiative de l'Union en matière de cybersolidarité dont les objectifs sont de renforcer les capacités communes de détection, d'appréciation de la situation et de réaction de l'Union en promouvant le déploiement d'une infrastructure de centres d'opérations de sécurité (SOC) de l'UE, constituer progressivement une réserve cyber de l'UE comprenant des services de prestataires privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'Union.

- (7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des cybermenaces et incidents dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités de prévention et de réaction des États membres et de l'Union en cas d'incidents de cybersécurité importants et d'incidents de cybersécurité majeurs. Par conséquent, il convient d'établir un réseau paneuropéen de cyberpôles (ci-après dénommé "système européen d'alerte en matière de cybersécurité"), afin de mettre en place des capacités coordonnées en matière de détection et d'appréciation de la situation, de manière à renforcer les capacités de l'Union en matière de détection des menaces et de partage des informations; un mécanisme d'urgence dans le domaine de la cybersécurité, devrait être mis en place afin d'aider les États membres, à leur demande, à se préparer aux incidents de cybersécurité importants et aux incidents de cybersécurité majeurs, à y réagir, à en atténuer les effets et à amorcer le rétablissement à la suite d'incidents de cybersécurité importants et d'incidents de cybersécurité majeurs, et pour aider les autres utilisateurs à réagir aux incidents de cybersécurité importants et aux incidents de cybersécurité assimilés à des incidents majeurs; et un mécanisme européen d'analyse des incidents de cybersécurité, afin d'examiner et d'évaluer des incidents de cybersécurité importants ou les incidents de cybersécurité majeurs particuliers. Les actions prises au titre du présent règlement devraient être menées dans le respect des compétences des États membres et devraient compléter et ne pas faire double emploi avec les activités menées par le réseau des CSIRT, le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) ou le groupe de coopération (groupe de coopération SRI), tous institués en vertu de la directive (UE) 2022/2555. Lesdites actions s'entendent sans préjudice des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne.

- (8) Pour atteindre ces objectifs, il est nécessaire de modifier certains points du règlement (UE) 2021/694 du Parlement européen et du Conseil⁹. Plus particulièrement, le présent règlement devrait modifier le règlement (UE) 2021/694 en ce qui concerne l'ajout de nouveaux objectifs opérationnels relatifs au système européen d'alerte en matière de cybersécurité 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 et la coordination transfrontières en matière de cybersécurité. Le système européen d'alerte en matière de cybersécurité pourrait jouer un rôle important en aidant les États membres à anticiper les cybermenaces et à se protéger contre elles, et la réserve de cybersécurité de l'Union pourrait jouer un rôle important en aidant les États membres, les institutions, organes et organismes de l'Union et les pays tiers associés au programme pour une Europe numérique à réagir aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs et aux incidents de cybersécurité assimilés à des incidents majeurs, et à en atténuer les effets. Lesdits effets pourraient inclure des dommages matériels ou immatériels considérables et des risques graves pour la sécurité et la sûreté publiques. Compte tenu des rôles spécifiques que le système européen d'alerte en matière de cybersécurité et la réserve de cybersécurité de l'Union pourraient jouer, le présent règlement devrait modifier le règlement (UE) 2021/694 en ce qui concerne la participation d'entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers, lorsqu'il existe un risque réel que les outils, infrastructures et services nécessaires et suffisants, ou les technologies, l'expertise et les capacités, ne soient pas disponibles dans l'Union et que les avantages de l'inclusion de ces entités l'emportent sur le risque en matière de sécurité. Il convient d'établir les conditions spécifiques dans lesquelles une aide financière peut être accordée pour des actions mettant en œuvre le système européen d'alerte en matière de cybersécurité et la réserve de cybersécurité de l'Union et de définir les 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 desdits nouveaux objectifs opérationnels.

⁹ 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) Pour renforcer la réaction de l'Union aux cybermenaces et incidents de cybersécurité, une coopération avec les organisations internationales ainsi qu'avec les partenaires internationaux de confiance et partageant la même optique est essentielle. Dans ce contexte, par partenaires internationaux de confiance et partageant la même optique, il convient d'entendre des pays qui partagent avec l'Union les principes qui ont présidé à sa création, à savoir la démocratie, l'état de droit, l'universalité et l'indivisibilité des droits de l'homme et des libertés fondamentales, le respect de la dignité humaine, les principes d'égalité et de solidarité et le respect des principes de la charte des Nations unies et du droit international, et qui ne portent pas atteinte aux intérêts essentiels de sécurité de l'Union ou de ses États membres. Une telle coopération pourrait également être bénéfique en ce qui concerne les actions prises en vertu du présent règlement, en particulier le système européen d'alerte en matière de cybersécurité et la réserve de cybersécurité de l'Union. Le règlement (UE) 2021/694 devrait prévoir, sous réserve de certaines conditions de disponibilité et de sécurité que les appels d'offres pour le système européen d'alerte en matière de cybersécurité et la réserve de cybersécurité de l'Union soient ouverts aux entités juridiques contrôlées par des pays tiers, sous réserve des exigences de sécurité. Lors de l'évaluation du risque pour la sécurité lié à l'ouverture des marchés de cette manière, il importe de tenir compte des principes et des valeurs que l'Union partage avec des partenaires internationaux partageant la même optique, lorsque ces principes et valeurs sont liés aux intérêts essentiels de l'Union en matière de sécurité. En outre, lorsque de telles exigences de sécurité sont examinées au titre du règlement (UE) 2021/694, plusieurs éléments pourraient être pris en compte, tels que la structure institutionnelle et le processus décisionnel d'une entité, la sécurité des données et des informations classifiées ou sensibles, et en veillant à ce que les résultats de l'action ne fassent pas l'objet d'un contrôle ou de restrictions de la part de pays tiers non éligibles.

- (10) 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 sont à définir dans les programmes de travail correspondants, conformément au règlement (UE) 2021/694.
- (11) Les règles financières horizontales adoptées par le Parlement européen et le Conseil sur la base de l'article 322 du traité sur le fonctionnement de l'Union européenne s'appliquent au présent règlement. Ces règles sont énoncées dans le règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil¹⁰ 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 traité sur le fonctionnement de l'Union européenne 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 Conseil¹¹.

¹⁰ Règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil du 23 septembre 2024 relatif aux règles financières applicables au budget général de l'Union (JO L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

¹¹ Règlement (UE, Euratom) 2020/2092 du Parlement européen et du Conseil du 16 décembre 2020 relatif à un régime général de conditionnalité pour la protection du budget de l'Union (JO L 433 I du 22.12.2020, p. 1, ELI: <http://data.europa.eu/eli/reg/2020/2092/oj>).

- (12) Si les mesures de prévention et de préparation sont essentielles pour renforcer la résilience de l'Union face aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs et aux incidents de cybersécurité assimilés à des incidents majeurs, la survenance, le calendrier et l'ampleur de ces incidents sont, par nature, imprévisibles. Les ressources financières nécessaires pour assurer une réponse adéquate peuvent varier considérablement d'une année à l'autre et devraient pouvoir être mises à disposition immédiatement. Pour concilier le principe budgétaire de prévisibilité et la nécessité de réagir rapidement à de nouveaux besoins, il est par conséquent nécessaire d'adapter l'exécution financière des programmes de travail. Dès lors, il y a lieu d'autoriser le report des crédits non utilisés, mais uniquement à l'année suivante et uniquement pour la réserve de cybersécurité de l'Union et les mesures de soutien à l'assistance mutuelle, en sus du report des crédits autorisés en vertu de l'article 12, paragraphe 4, du règlement (UE, Euratom) 2024/2509.

- (13) Afin de prévenir, évaluer, contrer les cybermenaces et incidents et s'en rétablir de manière plus efficace, il est nécessaire d'acquérir des connaissances plus complètes sur les menaces qui pèsent sur les actifs et infrastructures critiques dans le territoire de l'Union, notamment leur répartition géographique, leur interconnexion et les effets potentiels de cyberattaques touchant ces infrastructures. Une approche proactive en vue de l'identification, de l'atténuation et de la prévention des cybermenaces suppose des capacités accrues en matière de détection avancée. Le système européen d'alerte en matière de cybersécurité devrait se composer de plusieurs cyberpôles transfrontières interopérables qui regroupent chacun trois cyberpôles nationaux ou plus. 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 avancée de données et d'informations pertinentes, anonymisées le cas échéant, et d'outils d'analyse, en renforçant les capacités de détection et de gestion coordonnées des incidents de cybersécurité et en permettant une appréciation de la situation en temps réel. Elle devrait également permettre d'améliorer la posture cyber, en augmentant la détection, l'agrégation et l'analyse des données et des informations dans le but de prévenir les cybermenaces et incidents de cybersécurité et, partant, complétant et soutenant ainsi les entités et réseaux de l'Union chargés de la gestion des crises cyber dans l'Union, en particulier EU-CyCLONe.

- (14) La participation au système européen d'alerte en matière de cybersécurité est volontaire pour les États membres. Chaque État membre devrait désigner une entité unique au niveau national chargée de coordonner les activités de détection des cybermenaces sur son territoire. Ces cyberpôles nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au système européen d'alerte en matière de cybersécurité 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. Les cyberpôles nationaux pourraient renforcer la coopération et le partage d'informations entre les entités publiques et privées et pourraient également soutenir l'échange de données et d'informations pertinentes avec les communautés sectorielles et transsectorielles concernées, y compris les centres d'échange et d'analyse d'informations (ISAC) pertinents pour l'industrie. Une coopération étroite et coordonnée entre les entités publiques et privées est essentielle pour renforcer la cyberrésilience de l'Union. Cette coopération est particulièrement utile dans le contexte du partage de renseignements sur les cybermenaces afin d'améliorer la cyberprotection active. Dans le cadre d'une telle coopération et de ce partage d'informations, les cyberpôles nationaux pourraient demander et recevoir des informations spécifiques. Ces cyberpôles nationaux ne sont ni obligés ni habilités par le présent règlement à exécuter ces demandes. Le cas échéant, et conformément au droit de l'Union et au droit national, les informations demandées ou reçues pourraient comprendre des données de télémétrie, de capteurs et d'enregistrement provenant d'entités, telles que des fournisseurs de services de sécurité gérés, qui opèrent dans des secteurs hautement critiques ou d'autres secteurs critiques au sein de cet État membre, afin de renforcer la détection rapide des cybermenaces et incidents potentiels à un stade plus précoce, améliorant ainsi l'appréciation de la situation. Si le cyberpôle national n'est pas l'autorité compétente désignée ou établie par l'État membre concerné en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, il est essentiel qu'il se coordonne avec cette autorité compétente en ce qui concerne les demandes et réceptions de telles données.

- (15) Dans le cadre du système européen d'alerte en matière de cybersécurité, il convient de créer un certain nombre de cyberpôles transfrontières. Lesdits cyberpôles transfrontières devraient regrouper les cyberpôles nationaux d'au moins trois États membres afin de garantir que les avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations peuvent être pleinement réalisés. L'objectif général des cyberpôles 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 d'informations pertinentes, le cas échéant anonymisées, dans un environnement sûr et de confiance, issues de diverses sources, publiques ou privées, à l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement sûr et de confiance. Les cyberpôles transfrontières devraient également apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les CSIRT et sur d'autres acteurs pertinents, y compris le réseau des CSIRT, et en les complétant.

- (16) Un État membre sélectionné par le centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (ECCC) institué par le règlement (UE) 2021/887 du Parlement européen et du Conseil¹² à la suite d'un appel à manifestations d'intérêt pour mettre en place ou renforcer les capacités d'un cyberpôle national devrait, conjointement avec l'ECCC, acquérir des outils, des infrastructures ou des services pertinents. Un tel État membre devrait pouvoir bénéficier d'une subvention pour l'exploitation des outils, infrastructures et services. Un consortium d'hébergement composé d'au moins trois États membres, qui a été sélectionné par l'ECCC à la suite d'un appel à manifestation d'intérêt pour mettre en place ou renforcer les capacités d'un cyberpôle transfrontière devrait acquérir des outils, des infrastructures ou des services pertinents conjointement avec l'ECCC. Le consortium d'hébergement devrait pouvoir bénéficier d'une subvention pour l'exploitation des outils, des infrastructures ou des services. La procédure de passation de marché pour l'achat des outils, infrastructures et services concernés devrait être menée conjointement par l'ECCC et les pouvoirs adjudicateurs compétents des États membres sélectionnés à la suite de de tels appels à manifestation d'intérêt. Une telle passation de marchés devrait se conformer à l'article 168, paragraphe 2, du règlement (UE, Euratom) 2024/2509 et à la réglementation financière de l'ECCC. Les entités privées ne devraient donc pas être autorisées à participer aux appels à manifestation d'intérêt pour l'achat conjoint d'outils, d'infrastructures ou de services avec l'ECCC, ni pour recevoir des subventions pour l'exploitation de ces outils, infrastructures ou services. Toutefois, les États membres devraient pouvoir associer des entités privées à la mise en place, au renforcement et au fonctionnement de leurs cyberpôles nationaux et de leurs cyberpôles transfrontières d'une manière qu'ils jugent appropriée, conformément au droit de l'Union et au droit national. Les entités privées pourraient également bénéficier d'un financement de l'Union en vertu du règlement (UE) 2021/887 aux fins d'apporter un soutien aux cyberpôles nationaux.

¹² Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1, ELI: <http://data.europa.eu/eli/reg/2021/887/oj>).

- (17) Afin d'améliorer la détection des cybermenaces et l'appréciation de la situation dans l'Union, un État membre qui, à la suite d'un appel à manifestation d'intérêt sélectionné pour mettre en place ou renforcer les capacités d'un cyberpôle national devrait s'engager à demander à participer à un cyberpôle transfrontière. Si un État membre n'est pas un participant à un cyberpôle transfrontière dans un délai de deux ans à compter de la date d'acquisition des outils, infrastructures et services, ou à laquelle il reçoit une subvention, selon l'événement qui se produit plus tôt, il ne devrait pas être éligible à d'autres actions de soutien de l'Union dans le cadre du système européen d'alerte en matière de cybersécurité visant à renforcer les capacités de son cyberpôle national. Dans de tels cas, les entités des États membres pourraient encore participer à des appels à propositions sur d'autres sujets dans le cadre du programme pour une Europe numérique ou d'autres programmes de financement de l'Union, y compris des appels relatifs à des capacités en matière de détection des cybermenaces et de partage d'informations, pour autant que ces entités satisfassent aux critères d'éligibilité établis dans lesdits programmes.
- (18) Les CSIRT échangent des informations dans le cadre du réseau des CSIRT, conformément à la directive (UE) 2022/2555. Le système européen d'alerte en matière de cybersécurité devrait constituer une nouvelle capacité venant compléter le réseau des CSIRT en contribuant à la mise en place d'une appréciation de la situation au niveau de l'Union permettant le renforcement des capacités du réseau CSIRT. Les cyberpôles transfrontières devraient coordonner leurs activités et coopérer étroitement avec le réseau des CSIRT. Ils devraient agir en mettant en commun des données et en partageant des informations pertinentes, le cas échéant anonymisées sur les cybermenaces issues d'entités publiques et privées, en apportant une valeur ajoutée à ces données et ces informations à l'aide d'analyses d'experts, d'infrastructures et d'outils de pointe acquis en commun, et en contribuant à la souveraineté technologique de l'Union, à son autonomie stratégique ouverte, à sa compétitivité et à sa résilience, ainsi qu'au développement des capacités de l'Union.

- (19) Les cyberpôles transfrontières devraient servir de points centraux 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 de parties prenantes telles que les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les SAC et les opérateurs d'infrastructures critiques. Les membres du consortium d'hébergement devraient préciser dans l'accord de consortium les informations pertinentes à partager entre les participants du cyberpôle transfrontière. Les informations échangées entre les participants à un cyberpôle transfrontière pourraient comprendre, par exemple, 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 cybermenaces, les incidents évités de justesse, les vulnérabilités, les techniques et procédures, les tactiques adverses, les informations spécifiques sur les acteurs de la menace, les alertes en matière de cybersécurité et les recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques. En outre, les cyberpôles transfrontières devraient également conclure des accords de coopération entre eux. De tels accords de coopération devraient, en particulier, préciser les principes de partage d'informations et l'interopérabilité. Leurs clauses relatives à l'interopérabilité, en particulier les formats et protocoles de partage d'informations, devraient être guidées par les lignes directrices en matière d'interopérabilité publiées par l'Agence de l'Union européenne pour la cybersécurité instituée par le règlement (UE) 2019/881 (ENISA) et donc les prendre comme point de départ. Ces lignes directrices devraient être publiées rapidement afin de garantir qu'elles puissent être prises en compte par les cyberpôles transfrontières à un stade précoce. Elles devraient tenir compte des normes internationales et des meilleures pratiques, ainsi que du fonctionnement de tout cyberpôle transfrontière existant.

- (20) Les cyberpôles transfrontières et le réseau des CSIRT devraient coopérer étroitement afin de garantir les synergies et la complémentarité des activités. À cette fin, ils devraient convenir de modalités procédurales relatives à la coopération et au partage des informations pertinentes. Il pourrait s'agir notamment de partager des informations pertinentes sur les cybermenaces et les incidents de cybersécurité importants et de veiller à ce que les expériences relatives aux outils de pointe utilisés dans le cadre des cyberpôles transfrontières, en particulier l'intelligence artificielle et la technologie d'analyse des données, soient partagées avec le réseau des CSIRT.

- (21) 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 directive (UE) 2022/2555 a également établi un réseau des CSIRT pour promouvoir une coopération opérationnelle rapide et efficace entre les États membres. Pour garantir une appréciation de la situation et renforcer la solidarité, dans des situations où les cyberpôles transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur, potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos au réseau des CSIRT et envoyer une alerte précoce à EU-CyCLONe. 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 principe du besoin d'en connaître et du caractère potentiellement sensible des informations transmises. La directive (UE) 2022/2555 réaffirme également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision n° 1313/2013/UE du Parlement européen et du Conseil¹³, ainsi que sa responsabilité de fournir les rapports analytiques pour le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise en vertu de la décision d'exécution (UE) 2018/1993¹⁴.

¹³ Décision n° 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, 20.12.2013, p. 924, ELI: <http://data.europa.eu/eli/dec/2013/1313/oj>).

¹⁴ Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (JO L 320, 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Lorsque les cyberpôles transfrontières partagent des informations pertinentes et des alertes précoces relatives à un incident de cybersécurité majeur, potentiel ou en cours, avec EU-CyCLONe et le réseau des CSIRT, il est impératif que ces informations soient partagées par l'intermédiaire de ces réseaux avec les autorités des États membres ainsi qu'avec la Commission. À cet égard, la directive (UE) 2022/2555 prévoit que l'objectif d'EU-CyCLONe est 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. Les tâches d'EU-CyCLONe consistent notamment à développer une appréciation de la situation commune en ce qui concerne ces crises et incidents. Il est de la plus haute importance qu'EU-CyCLONe veille, conformément à cet objectif et à ses missions, à ce que de telles informations soient immédiatement fournies aux représentants des États membres concernés et la Commission. À cette fin, il est essentiel que le règlement intérieur d'EU-CyCLONe comporte des dispositions appropriées.

- (22) Les entités participant au système européen d'alerte en matière de cybersécurité 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. Elles assurent également la 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 des cybermenaces détectées et les risques en matière de cybersécurité devraient tenir compte des travaux réalisés dans le contexte de la mise en œuvre de la directive (UE) 2022/2555.

- (23) Aux fins de l'échange des données et des informations pertinentes sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement sûr et de confiance, les entités participant au système européen d'alerte en matière de cybersécurité devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés, ainsi que d'un personnel qualifié. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.
- (24) En collectant, analysant, partageant et échangeant des données et des informations pertinentes, le système européen d'alerte en matière de cybersécurité devrait renforcer la souveraineté technologique de l'Union, son autonomie stratégique ouverte dans le domaine de la cybersécurité, sa compétitivité et sa résilience. La mise en commun de données de haute qualité faisant l'objet d'une curation pourrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Le contrôle humain et à cette fin, une main-d'œuvre qualifiée restent essentiels à la mise en commun effective des données de haute qualité.

- (25) Bien que le système européen d'alerte en matière de cybersécurité 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.
- (26) Le partage d'informations entre les participants au système européen d'alerte en matière de cybersécurité 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'entité mettant les données à disposition que ces données ont été détruites.

- (27) La préservation de la confidentialité et de la sécurité des informations revêt une importance capitale pour les trois piliers du présent règlement, qu'il s'agisse d'encourager le partage ou l'échange d'informations dans le cadre du système européen d'alerte en matière de cybersécurité, de préserver les intérêts des entités demandant un soutien au titre du mécanisme d'urgence en matière de cybersécurité ou de veiller à ce que les rapports au titre du mécanisme européen d'analyse des incidents de cybersécurité puissent tirer des enseignements utiles sans avoir d'effets négatifs sur les entités touchées par les incidents. La participation des États membres et des entités à ces mécanismes dépend des relations de confiance entre leurs composantes. Lorsque des informations sont confidentielles en vertu des règles de l'Union ou des règles nationales, leur partage ou leur échange au titre du présent règlement devrait être limité à ce qui est pertinent et proportionné à la finalité du partage ou de l'échange. Ce partage ou cet échange devrait également préserver la confidentialité de ces informations et notamment protéger la sécurité et les intérêts commerciaux de toutes les entités concernées. Le partage ou l'échange d'informations en vertu du présent règlement pourrait avoir lieu au moyen d'accords de non-divulgence ou d'orientations sur la distribution d'informations telles que le protocole d'échange d'informations sécurisé "Traffic Light Protocol" (TLP). Le TLP s'entend d'un moyen de communiquer des renseignements sur toute limitation applicable à la diffusion plus large des informations. Ce protocole est utilisé par la quasi-totalité des CSIRT et par certains centres d'échange et d'analyse d'informations (ISAC). Outre ces exigences générales, en ce qui concerne le système européen d'alerte en matière de cybersécurité, les accords de consortiums d'hébergement devraient établir des règles spécifiques concernant les conditions du partage d'informations au sein du cyberpôle transfrontière concerné. Ces accords pourraient notamment exiger que les informations ne soient échangées que conformément au droit de l'Union et au droit national.

- (28) En ce qui concerne le déploiement de la réserve de cybersécurité de l'Union, des règles de confidentialité spécifiques sont nécessaires. Un soutien sera demandé, évalué et fourni dans un contexte de crise et en ce qui concerne les entités actives dans des secteurs sensibles. Pour que la réserve de cybersécurité de l'Union fonctionne efficacement, il est essentiel que les utilisateurs et les entités soient en mesure de partager et de donner accès, sans retard, à toutes les informations nécessaires pour que chaque entité puisse jouer son rôle dans l'évaluation des demandes et le déploiement de l'aide. En conséquence, le présent règlement devrait prévoir que toutes ces informations ne sont utilisées ou partagées que lorsque cela est nécessaire au fonctionnement de la réserve de cybersécurité de l'Union, et que les informations confidentielles ou classifiées en vertu du droit de l'Union et du droit national ne sont utilisées et partagées que conformément à ce droit. En outre, les utilisateurs devraient être en mesure, le cas échéant, d'utiliser des protocoles de partage d'informations tels que le TLP pour préciser davantage les limitations. Si les utilisateurs disposent d'une marge d'appréciation à cet égard, il importe que, lorsqu'ils appliquent de telles limitations, ils tiennent compte des conséquences possibles, notamment en ce qui concerne les retards dans l'évaluation ou la fourniture des services demandés. Afin de disposer d'une réserve de cybersécurité de l'Union efficace, il est important que le pouvoir adjudicateur précise ces conséquences à l'utilisateur avant qu'il ne présente une demande. Ces garanties se limitent à la demande et à la fourniture de services de réserve de cybersécurité de l'Union et n'affectent pas l'échange d'informations dans d'autres contextes, tels que la passation de marchés relatifs à la réserve de cybersécurité de l'Union.

- (29) 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, à savoir le mécanisme d'urgence en matière de cybersécurité, visant à améliorer la résilience de l'Union face aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs et aux incidents de cybersécurité assimilés à des incidents 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 initial des services essentiels. Étant donné que le rétablissement intégral d'un incident est un processus complet visant à rétablir le fonctionnement de l'entité touchée par l'incident dans l'état antérieur à l'incident et qu'il pourrait s'agir d'un long processus entraînant des coûts importants, le soutien de la réserve de cybersécurité de l'Union devrait être limité à la phase initiale du processus de rétablissement, conduisant à la restauration des fonctionnalités de base des systèmes. Le mécanisme d'urgence en matière de cybersécurité devrait permettre de déployer rapidement et efficacement de l'aide, dans des circonstances définies et des conditions claires, et permettre une surveillance et une évaluation minutieuses de l'utilisation des ressources. Si la responsabilité première en matière de prévention, de préparation et de réaction face aux incidents et aux crises 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.

- (30) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et de leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement initial en cas d'incidents de cybersécurité importants et d'incidents de cybersécurité majeurs, tels que les services fournis par l'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 y compris, dans le contexte de l'article 42, paragraphe 7, du traité sur l'Union européenne, les équipes d'intervention rapide en cas d'incident informatique de la coopération structurée permanente (CSP) instituées en vertu de la décision (PESC) 2017/2315 du Conseil¹⁵. 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 et le rétablissement à la suite de ceux-ci dans toute l'Union et dans les pays tiers associés au programme pour une Europe numérique.

¹⁵ Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants ((JO L 331 du 14.12.2017, p. 57, ELI: <http://data.europa.eu/eli/dec/2017/2315/2023-05-23>).

- (31) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination des réactions aux crises au niveau de l'Union, en particulier la directive (UE) 2022/2555, le mécanisme de protection civile de l'Union établi par la décision n° 1313/2013/UE du Parlement européen et du Conseil¹⁶, le dispositif IPCR, la recommandation (UE) 2017/1584 de la Commission¹⁷. 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, compte tenu du caractère civil du mécanisme d'urgence en matière de cybersécurité. Le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter les actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne, y compris l'assistance fournie par un État membre à un autre État membre, ou 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. La mise en œuvre du présent règlement devrait également être coordonnée, s'il y a lieu, avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatie.

¹⁶ Décision n° 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).

¹⁷ 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).

- (32) L'aide apportée dans le cadre du présent règlement devrait appuyer et compléter les mesures prises par les États membres au niveau national. À cette fin, il est nécessaire d'assurer une coopération et une consultation étroites entre la Commission, l'ENISA, les États membres et, le cas échéant, l'ECCC. Lorsque les États membres sollicitent une aide au titre du mécanisme d'urgence dans le domaine de la cybersécurité, ils devraient fournir des informations pertinentes permettant de justifier sa demande d'aide.
- (33) 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 des incidents de cybersécurité majeurs, à soutenir un rétablissement initial ou à rétablir les fonctionnalités de base des services fournis par les entités actives dans des secteurs hautement critiques ou les entités actives dans d'autres secteurs critiques.

- (34) 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, y compris par des exercices et des formations. À cette fin, la Commission, après consultation de l'ENISA, du groupe de coopération SRI et EU-CyCLONe, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests de préparation coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir des secteurs hautement critiques énumérés à l'annexe I de la directive (UE) 2022/2555. Les tests de préparation coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs.

La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'Union, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque menés par la Commission, le haut représentant de l'Union pour les affaires étrangères et la et la politique de sécurité (ci-après dénommé "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 institué par le règlement (UE) 2018/1971 du Parlement européen et du Conseil¹⁸, les évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques qui doit être effectuée en vertu 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 Conseil¹⁹. 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.

¹⁸ Règlement (UE) 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018 établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office de l'ORECE), modifiant le règlement (UE) 2015/2120 et abrogeant le règlement (CE) n° 1211/2009 (JO L 321 du 17.12.2018, p. 1).

¹⁹ 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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).

- (35) En outre, le mécanisme d'urgence dans le domaine de la cybersécurité devrait prévoir 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 de préparation coordonnés auxquels sont soumises les entités actives dans des secteurs hautement critiques ou les entités actives d'autres secteurs critiques. Ces mesures pourraient inclure divers types d'activités nationales de préparation.
- (36) Lorsque les États membres reçoivent des subventions pour soutenir des mesures de préparation, les entités actives dans des secteurs hautement critiques peuvent participer à ces mesures sur une base volontaire. Il est de bonne pratique que, à la suite de ces mesures, les entités participantes élaborent un plan de mesures correctives afin de mettre en œuvre toute recommandation de mesures spécifiques qui en résulte afin de tirer pleinement profit des mesures de préparation. S'il est important que les États membres demandent, dans le cadre des mesures, que les entités participantes élaborent et mettent en œuvre de tels plans de mesures correctives, les États membres ne sont ni tenus de faire appliquer ces demandes ni habilités à le faire en vertu du présent règlement. Ces demandes sont sans préjudice des exigences relatives aux entités et des pouvoirs de supervision des autorités compétentes conformément à la directive (UE) 2022/2555.
- (37) 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, des incidents de cybersécurité majeurs et des incidents de cybersécurité assimilés à des incidents majeurs, à soutenir un rétablissement initial 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 les citoyens.

- (38) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir l'assistance technique fournie par un État membre à un autre État membre qui est touché par un incident de cybersécurité important ou un incident de cybersécurité majeur ou un incident de cybersécurité assimilé à un incident majeur, y compris par les CSIRT en vertu de l'article 11, paragraphe 3, point f), de la directive (UE) 2022/2555. Les États membres apportant une telle 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.
- (39) Compte tenu du rôle essentiel que jouent les entreprises privées dans la détection des incidents de cybersécurité majeurs et des incidents de cybersécurité assimilés à des incidents majeurs et dans la préparation et la réaction à ces incidents, il est important de reconnaître la valeur d'une coopération volontaire à titre gracieux avec ces entreprises, dans le cadre de laquelle elles proposent des services sans rémunération en cas de crises et d'incidents de cybersécurité majeurs et de crises et d'incidents de cybersécurité assimilés à des incidents majeurs. L'ENISA, en coopération avec EU-CyCLONe, pourrait suivre l'évolution de ces initiatives à titre gracieux et contribuer à leur conformité avec les critères applicables aux fournisseurs de services de sécurité gérés de confiance en vertu du présent règlement, y compris en ce qui concerne la fiabilité des entreprises privées, leur expérience ainsi que leur capacité à traiter les informations sensibles de manière sécurisée.

- (40) Dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité, une réserve de cybersécurité de l'Union devrait être mise en place progressivement et comprendre des services de fournisseurs de services de sécurité gérés de confiance visant à soutenir les mesures de réaction et à amorcer le rétablissement en cas d'incidents de cybersécurité importants, d'incidents de cybersécurité majeurs ou d'incidents de cybersécurité assimilés à des incidents majeurs touchant des États membres, des institutions, organes ou organismes de l'Union ou des pays tiers associés au programme pour une Europe numérique. La réserve de cybersécurité de l'Union devrait veiller à la disponibilité et à l'état de préparation de ces services. Elle devrait donc englober les services affectés au préalable, dont, par exemple, les capacités en attente déployables à brève échéance. Les services de la réserve de cybersécurité de l'Union devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs hautement critiques ou aux entités touchées actives dans d'autres secteurs critiques, en complément des mesures prises par ces autorités au niveau national. Les services de la réserve de cybersécurité de l'Union devraient également pouvoir servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires. La réserve de cybersécurité de l'Union pourrait également contribuer à renforcer la position concurrentielle de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique, y compris les microentreprises et les petites et moyennes entreprises ainsi que les jeunes pousses, y compris en encourageant les investissements dans la recherche et l'innovation. Il est important de tenir compte du cadre européen des compétences en matière de cybersécurité de l'ENISA lors de l'acquisition de services pour la réserve de cybersécurité de l'Union. Lorsqu'ils demandent l'aide de la réserve de cybersécurité de l'Union, les utilisateurs devraient inclure dans leur demande des informations appropriées concernant l'entité touchée et les effets potentiels, le service demandé au titre de la réserve de cybersécurité de l'Union et le soutien dont bénéficie l'entité touchée au niveau national, informations qu'il convient de prendre en compte lors de l'examen de la demande. Afin d'assurer la complémentarité avec les autres formes d'aide dont dispose l'entité touchée, la demande devrait aussi comprendre, le cas échéant, des informations sur les dispositions contractuelles en vigueur relatives aux services de réaction aux incidents et de rétablissement initial, ainsi que les contrats d'assurance couvrant potentiellement ce type d'incident.

- (41) Aux fins d'une utilisation efficace des fonds de l'Union, les services affectés au préalable relevant de la réserve de cybersécurité de l'Union devraient être convertibles, conformément au contrat correspondant, en services de préparation liés à la prévention des incidents et à la réaction à ceux-ci, dans le cas où ces services affectés au préalable ne sont pas utilisés pour la réaction aux incidents pendant la période pour laquelle ils sont affectés au préalable. Ces services devraient être complémentaires et ne devraient pas faire double emploi avec les mesures de préparation gérées par l'ECCC.
- (42) Les demandes d'aide au titre de la réserve de cybersécurité de l'Union émanant des autorités des États membres chargées de la gestion des crises cyber et des CSIRT, ou du CERT-UE, au nom des institutions, organes et organismes de l'Union, devraient être évaluées par le pouvoir adjudicateur. Lorsque l'ENISA est chargée de l'administration et le fonctionnement de la réserve de cybersécurité de l'Union, ledit pouvoir adjudicateur est l'ENISA. Les demandes d'aide émanant de pays tiers associés au programme pour une Europe numérique devraient être évaluées par la Commission. Afin de faciliter la soumission et l'évaluation des demandes d'aide, l'ENISA pourrait mettre en place une plateforme sécurisée.

- (43) Lorsque plusieurs demandes simultanées sont reçues, il y a lieu de hiérarchiser ces demandes selon les critères fixés par le présent règlement. Compte tenu des objectifs généraux du présent règlement, ces critères devraient comprendre l'ampleur et la gravité de l'incident, le type d'entité touchée, les effets potentiels de l'incident sur les États membres et les utilisateurs touchés, la nature transfrontière potentielle de l'incident et le risque de propagation, ainsi que les mesures déjà prises par l'utilisateur aux fins de la réaction et du rétablissement initial. À la lumière de ces mêmes objectifs et étant donné que les demandes des utilisateurs des États membres sont exclusivement destinées à aider, dans l'ensemble de l'Union, des entités actives dans des secteurs hautement critiques ou des entités actives dans d'autres secteurs critiques, il convient d'accorder une plus grande priorité aux demandes des utilisateurs des États membres lorsque deux demandes ou plus sont évaluées comme étant égales selon les critères d'évaluation. Cette disposition est sans préjudice de toute obligation incombant aux États membres, en vertu des conventions d'hébergement pertinentes, de prendre des mesures pour protéger et aider les institutions, organes et organismes de l'Union.

- (44) La responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union devrait revenir à la Commission. Compte tenu de la vaste expérience acquise par l'ENISA dans l'action de soutien à la cybersécurité, l'ENISA est l'agence la plus appropriée pour mettre en œuvre la réserve de cybersécurité de l'Union. Par conséquent, la Commission devrait confier à l'ENISA, en partie ou intégralement, lorsque la Commission le juge approprié, le fonctionnement et l'administration de la réserve de cybersécurité de l'Union. Cette responsabilité devrait être accomplie dans le respect des règles applicables en vertu du règlement (UE, Euratom) 2024/2509 et, en particulier, être subordonnée au respect des conditions pertinentes pour la signature d'une convention de contribution. Tous les aspects du fonctionnement et de l'administration de la réserve de cybersécurité de l'Union qui ne sont pas confiés à l'ENISA devraient faire l'objet d'une gestion directe par la Commission, notamment avant la signature de la convention de contribution.
- (45) Les États membres devraient jouer un rôle essentiel dans la constitution et le déploiement de la réserve de cybersécurité de l'Union ainsi que dans la période qui suit le déploiement de la réserve. Étant donné que le règlement (UE) 2021/694 est l'acte de base pertinent pour les mesures mettant en œuvre la réserve de cybersécurité de l'Union, les mesures relevant de la réserve de cybersécurité de l'Union devraient être prévues dans les programmes de travail visés à l'article 24 du règlement (UE) 2021/694. En vertu du paragraphe 6 dudit article, lesdits programmes de travail doivent être adoptés par la Commission au moyen d'actes d'exécution conformément à la procédure d'examen. En outre, la Commission, en coordination avec le groupe de coopération SRI, devrait déterminer les priorités et l'évolution de la réserve de cybersécurité de l'Union.

- (46) Les contrats établis dans le cadre de la réserve de cybersécurité de l'Union ne devraient pas avoir d'incidence sur les relations d'entreprise à entreprise ni sur les obligations existantes entre l'entité touchée ou les utilisateurs et le fournisseur de services.
- (47) La sélection des fournisseurs de services privés qui proposeront des services dans le cadre de la réserve de cybersécurité de l'Union nécessite de définir un ensemble de critères et d'exigences minimaux à inclure dans l'appel d'offres visant à sélectionner ces fournisseurs, afin de garantir que les besoins des autorités des États membres, des entités actives dans des secteurs hautement critiques ou des entités actives dans d'autres secteurs critiques sont satisfaits. Afin de répondre aux besoins spécifiques des États membres, lorsque le pouvoir adjudicateur achète des services pour la réserve de cybersécurité de l'Union, il devrait, le cas échéant, élaborer des critères et exigences de sélection supplémentaires par rapport à ceux énoncés dans le présent règlement. Il importe de soutenir la participation de petits fournisseurs, actifs aux niveaux régional et local.

- (48) Lors de la sélection des fournisseurs en vue de leur inclusion dans la réserve de cybersécurité de l'Union, le pouvoir adjudicateur devrait veiller à ce que la réserve de cybersécurité de l'Union, considérée dans son ensemble, contienne des fournisseurs capables de répondre aux besoins linguistiques des utilisateurs. À cette fin, avant de préparer le cahier des charges, le pouvoir adjudicateur devrait vérifier si les utilisateurs potentiels de la réserve de cybersécurité de l'Union ont des besoins linguistiques spécifiques, de sorte que les services d'aide de la réserve de cybersécurité de l'Union puissent être fournis dans une langue figurant parmi les langues officielles des institutions de l'Union ou des États membres susceptibles d'être comprise par l'utilisateur ou l'entité touchée. Lorsque plusieurs langues sont requises par un utilisateur aux fins de la fourniture de services d'aide de la réserve de cybersécurité de l'Union et que ces services ont été achetés dans ces langues pour cet utilisateur, l'utilisateur devrait pouvoir préciser, dans la demande d'aide adressée à la réserve de cybersécurité de l'Union, dans laquelle de ces langues les services devraient être fournis en lien avec l'incident spécifique ayant donné lieu à la demande.
- (49) Aux fins de la mise en place de la réserve de cybersécurité de l'Union, il importe que la Commission demande à l'ENISA de préparer un schéma de certification de cybersécurité candidat pour les services de sécurité gérés, conformément au règlement (UE) 2019/881, dans les domaines couverts par le mécanisme d'urgence dans le domaine de la cybersécurité.

- (50) Afin de soutenir les objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents de cybersécurité importants et incidents de cybersécurité majeurs poursuivis par le présent règlement, la Commission ou EU-CyCLONe, devrait être en mesure de demander à l'ENISA, avec le soutien du réseau des CSIRT et avec l'approbation des États membres concernés, d'analyser et d'évaluer les cybermenaces, les vulnérabilités exploitables constatées et les 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 l'État membre concerné, les parties prenantes concernées, notamment les représentants du secteur privé, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En s'appuyant sur la collaboration avec les parties prenantes, y compris celles du 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 utilisé pour éclairer leurs travaux ainsi qu'à ceux de l'ENISA. Lorsque l'incident en question touche un pays tiers associé au programme pour une Europe numérique, la Commission devrait également remettre le rapport au haut représentant.

- (51) 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 des incidents de cybersécurité assimilés à des incidents majeurs contribuent à la protection de l'Union dans son ensemble, et de son marché intérieur et de ses entreprises en particulier. De telles activités pourraient par ailleurs contribuer à la cyberdiplomatie de l'Union. Par conséquent, les pays tiers associés au programme pour une Europe numérique devraient pouvoir demander de l'aide de la réserve de cybersécurité de l'Union, sur tout ou partie de leur territoire, lorsque cela est prévu dans l'accord par lequel le pays tiers concerné est associé au programme pour une Europe numérique. Le soutien apporté aux pays tiers associés au programme pour une Europe numérique 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 aux incidents de cybersécurité importants ou incidents de cybersécurité assimilés à des incidents majeurs et au lancement du rétablissement après ces incidents.

- (52) Les conditions relatives à la réserve de cybersécurité de l'Union et aux fournisseurs de services de sécurité gérés de confiance fixées dans le présent règlement devraient s'appliquer au soutien apporté aux pays tiers associés au programme pour une Europe numérique. Les pays tiers associés au programme pour une Europe numérique devraient pouvoir solliciter l'aide de la réserve de cybersécurité de l'Union lorsque les entités ciblées et pour lesquelles ils demandent l'aide de la réserve de cybersécurité de l'Union sont des entités actives dans des secteurs hautement critiques ou des entités actives dans d'autres secteurs critiques et lorsque les incidents détectés entraînent des perturbations opérationnelles importantes ou sont susceptibles d'avoir des retombées dans l'Union. Les pays tiers associés au programme pour une Europe numérique ne devraient pouvoir bénéficier d'une aide que si l'accord par lequel ils sont associés au programme pour une Europe numérique prévoit expressément une telle aide. En outre, ces pays tiers ne devraient pouvoir bénéficier de l'aide que tant que trois critères sont remplis. Premièrement, le pays tiers doit se conformer pleinement aux dispositions pertinentes de cet accord. Deuxièmement, compte tenu du caractère complémentaire de la réserve de cybersécurité de l'Union, le pays tiers doit avoir pris des mesures adéquates pour se préparer aux incidents de cybersécurité importants ou aux incidents de cybersécurité assimilés à des incidents majeurs. Troisièmement, l'octroi d'une aide de la réserve de cybersécurité de l'Union devrait être compatible avec la politique de l'Union à l'égard de ce pays et ses relations globales avec ce pays, ainsi qu'avec les autres actions de l'Union dans le domaine de la sécurité. Dans le cadre de son évaluation du respect de ce troisième critère, la Commission devrait consulter le haut représentant afin de s'assurer que l'octroi de cette aide cadre avec la politique étrangère et de sécurité commune.

(53) La fourniture d'une aide aux pays tiers associés au programme pour une Europe numérique peut avoir une incidence sur les relations avec les pays tiers et la politique de sécurité de l'Union, notamment dans le contexte de la politique étrangère et de sécurité commune et de la politique de défense et de sécurité commune. En conséquence, il convient que le Conseil se voie conférer des compétences d'exécution pour autoriser et préciser la période pendant laquelle cette aide peut être fournie. Le Conseil devrait agir sur la base d'une proposition de la Commission, en tenant dûment compte de l'évaluation des trois critères par la Commission. Il devrait en aller de même pour les renouvellements et pour les propositions de modification ou d'abrogation de tels actes. Lorsque, dans des circonstances exceptionnelles, le Conseil estime qu'il y a eu un changement majeur de circonstances eu égard au troisième critère, il devrait être en mesure d'agir de sa propre initiative pour modifier ou abroger un acte d'exécution, sans attendre une proposition de la Commission. De tels changements majeurs sont susceptibles de nécessiter une action urgente, d'avoir des implications particulièrement importantes pour les relations avec les pays tiers et de ne pas exiger une évaluation détaillée à l'avance de la part de la Commission. En outre, la Commission devrait coopérer avec le haut représentant en ce qui concerne les demandes d'aide des pays tiers associés au programme pour une Europe numérique et la mise en œuvre de l'aide accordée aux pays tiers. La Commission devrait également tenir compte de tout avis fourni par l'ENISA concernant de telles demandes et une telle aide. La Commission devrait informer le Conseil des résultats de l'évaluation des demandes, et notamment des considérations pertinentes formulées à cet égard, et des services qui sont déployés.

- (54) Dans sa communication du 18 avril 2023 sur l'académie des compétences en matière de cybersécurité, la Commission a mis en avant la pénurie de professionnels qualifiés. Or, de telles qualifications sont indispensables pour la réalisation des objectifs du présent règlement. L'Union a besoin de toute urgence de professionnels possédant les aptitudes et les compétences nécessaires pour prévenir, détecter et décourager les cyberattaques et pour défendre l'Union, y compris ses infrastructures les plus critiques, contre ces attaques et assurer sa résilience. À cette fin, il importe d'encourager la coopération entre les parties prenantes, y compris celles du secteur privé, le monde universitaire et le secteur public. Il est tout aussi crucial de créer des synergies, sur tous les territoires de l'Union, pour que les investissements dans l'éducation et la formation servent à la mise en place de garanties afin d'éviter la fuite des cerveaux ou l'aggravation du déficit de compétences dans certaines régions plus que dans d'autres. Il est urgent de combler le déficit de compétences en matière de cybersécurité, en mettant particulièrement l'accent sur la réduction de l'écart entre les hommes et les femmes au sein de la main-d'œuvre dans le domaine de la cybersécurité afin de promouvoir la présence et la participation des femmes à la conception de la gouvernance numérique.
- (55) Afin de stimuler l'innovation dans le marché unique numérique, il importe de renforcer la recherche et l'innovation dans le domaine de la cybersécurité, en vue de contribuer à accroître la résilience des États membres et l'autonomie stratégique ouverte de l'Union, qui sont tous deux des objectifs du présent règlement. Des synergies sont essentielles pour renforcer la coopération et la coordination entre les différentes parties prenantes, y compris celles du secteur privé, la société civile et le monde universitaire.

- (56) Le présent règlement devrait tenir compte de l'engagement, énoncé dans la déclaration commune du 26 janvier 2022 du Parlement européen, du Conseil et de la Commission européenne intitulée "Déclaration européenne sur les droits et principes numériques pour la décennie numérique", de protéger les intérêts des démocraties, citoyens, entreprises et institutions publiques de l'Union contre les risques liés à la cybersécurité et à la cybercriminalité, y compris les violations de données et l'usurpation ou la manipulation d'identité.
- (57) Afin de compléter certains éléments non essentiels du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne afin de préciser les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'Union. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"²⁰. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

²⁰ JO L 123 du 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstitut/2016/512/oj.

- (58) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour qu'elle puisse préciser davantage les modalités détaillées d'attribution des services d'aide de la réserve de cybersécurité de l'Union. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil²¹.
- (59) Sans préjudice des règles relatives au budget annuel de l'Union prévues par les traités, la Commission devrait tenir compte des obligations découlant du présent règlement lorsqu'elle évalue le budget et les besoins en personnel de l'ENISA.
- (60) Il convient que la Commission procède régulièrement à une évaluation des mesures prévues par le présent règlement. La première évaluation de ce type devrait avoir lieu au cours des deux premières années à compter de la date d'entrée en vigueur du présent règlement, et au moins tous les quatre ans par la suite, en tenant compte du calendrier de révision du cadre financier pluriannuel institué en vertu de l'article 312 du traité sur le fonctionnement de l'Union européenne. La Commission devrait transmettre un rapport d'état des lieux au Parlement européen et au Conseil. Afin d'évaluer les différents éléments requis, y compris l'étendue des informations partagées au sein du système européen d'alerte en matière de cybersécurité, la Commission devrait se fonder exclusivement sur des informations aisément disponibles ou fournies volontairement. Compte tenu des évolutions géopolitiques et afin d'assurer la poursuite et le renforcement après 2027 des mesures définies dans le présent règlement, il importe que la Commission évalue la nécessité de mobiliser un budget approprié dans le cadre financier pluriannuel pour les années 2028 à 2034.

²¹ Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13, ELI: <https://eur-lex.europa.eu/eli/reg/2011/182/oj>).

- (61) Étant donné que les objectifs du présent règlement, à savoir renforcer la position concurrentielle de l'industrie et des services dans l'ensemble de l'économie numérique et contribuer à la souveraineté technologique et à l'autonomie stratégique ouverte de l'Union dans le domaine de la cybersécurité, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent en raison des dimensions ou des effets de l'action l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I

Dispositions générales

Article premier

Objet et objectifs

1. Le présent règlement établit des mesures destinées à renforcer les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir, en mettant en place:
 - a) un réseau paneuropéen de cyberpôles (ci-après dénommé "système européen d'alerte en matière de cybersécurité") dans le but de mettre en place et de développer des capacités de détection coordonnée et d'appréciation commune de la situation;
 - b) un mécanisme d'urgence dans le domaine de la cybersécurité pour aider les États membres à se préparer aux incidents de cybersécurité importants et aux incidents de cybersécurité majeurs, à y réagir, à en atténuer les effets et à amorcer le rétablissement à la suite de tels incidents, et pour aider d'autres utilisateurs à réagir aux incidents de cybersécurité importants et aux incidents de cybersécurité assimilés à des incidents majeurs;
 - c) un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents de cybersécurité importants ou incidents de cybersécurité majeurs.

2. Le présent règlement poursuit les objectifs généraux consistant à renforcer la position concurrentielle de l'industrie et des services dans l'ensemble de l'économie numérique de l'Union, y compris les microentreprises et les petites et moyennes entreprises ainsi que les jeunes pousses, et à contribuer à la souveraineté technologique et à l'autonomie stratégique ouverte de l'Union dans le domaine de la cybersécurité, notamment en stimulant l'innovation dans le marché unique numérique. Il poursuit ces objectifs en renforçant la solidarité au niveau de l'Union, en consolidant l'écosystème de cybersécurité, en accroissant la cyberrésilience des États membres et en développant les aptitudes, le savoir-faire, les capacités et les compétences de la main-d'œuvre dans le domaine de la cybersécurité.
3. La réalisation des objectifs généraux visés au paragraphe 2 passe par celle des objectifs spécifiques suivants:
 - a) renforcer les capacités communes de détection coordonnée au niveau de l'Union ainsi que l'appréciation commune de la situation concernant les cybermenaces et les incidents;
 - b) améliorer la préparation des entités actives dans des secteurs hautement critiques ou des entités actives dans d'autres secteurs critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des tests de préparation coordonnés et en accroissant les capacités de réaction et de rétablissement pour faire face aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs ou aux incidents de cybersécurité assimilés à des incidents 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 aux incidents efficace en analysant et en évaluant les incidents de cybersécurité importants ou les incidents de cybersécurité majeurs, y compris en tirant les enseignements de l'expérience acquise et, au besoin, en formulant des recommandations.
- 4. Les actions au titre du présent règlement sont menées dans le respect des compétences des États membres et complètent les activités réalisées par le réseau des CSIRT, EU-CyCLONe et le groupe de coopération SRI.
- 5. Le présent règlement est sans préjudice des fonctions essentielles des États membres, notamment celles d'assurer l'intégrité territoriale de l'État, de maintenir l'ordre public et de préserver la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.
- 6. Le partage ou l'échange d'informations au titre du présent règlement considérées comme confidentielles en application de la réglementation nationale ou de l'Union se limite au minimum nécessaire et est proportionné à l'objectif de ce partage ou de cet échange. Un tel partage ou échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités concernées. Il n'implique pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

- 1) "cyberpôle transfrontière": une plateforme multinationale, établie par un accord de consortium écrit, qui rassemble, au sein d'une structure de réseau coordonnée, les cyberpôles nationaux d'au moins trois États membres, et qui est conçue pour améliorer le suivi, la détection et l'analyse des cybermenaces pour prévenir les incidents et pour soutenir la production de renseignements sur les cybermenaces, notamment par l'échange de données et d'informations pertinentes, le cas échéant anonymisées, 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) "consortium d'hébergement": un consortium formé par des États membres participants, qui ont accepté de mettre en place un cyberpôle transfrontière et de contribuer à l'acquisition des outils, des infrastructures ou des services nécessaires à ce cyberpôle, ainsi qu'au fonctionnement de celui-ci;
- 3) "CSIRT": un CSIRT désigné ou établi conformément à l'article 10 de la directive (UE) 2022/2555;
- 4) "entité": une entité au sens de l'article 6, point 38), de la directive (UE) 2022/2555;

- 5) "entités actives dans des secteurs hautement critiques": les types d'entité énumérés à l'annexe I de la directive (UE) 2022/2555;
- 6) "entités actives dans d'autres secteurs critiques": les types d'entité énumérés à l'annexe II de la directive (UE) 2022/2555;
- 7) "risque": un risque au sens de l'article 6, point 9), de la directive (UE) 2022/2555;
- 8) "cybermenace": une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;
- 9) "incident": un incident au sens de l'article 6, point 6), de la directive (UE) 2022/2555;
- 10) "incident de cybersécurité important": un incident de cybersécurité répondant aux critères énoncés à l'article 23, paragraphe 3, de la directive (UE) 2022/2555;
- 11) "incident majeur": un incident majeur tel qu'il est défini à l'article 3, point 8), du règlement (UE, Euratom) 2023/2841 du Parlement européen et du Conseil²²;
- 12) "incident de cybersécurité majeur": un incident de cybersécurité majeur au sens de l'article 6, point 7), de la directive (UE) 2022/2555;

²² Règlement (UE, Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>).

- 13) "incident de cybersécurité assimilé à un incident majeur": dans le cas des institutions, organes et organismes de l'Union, un incident majeur, dans le cas des pays tiers associés au programme pour une Europe numérique, un incident qui provoque un niveau de perturbation supérieur à la capacité d'un pays tiers associé au programme pour une Europe numérique à y répondre;
- 14) "pays tiers associé au programme pour une Europe numérique": un pays tiers qui est partie à un accord avec l'Union permettant sa participation au programme pour une Europe numérique conformément à l'article 10 du règlement (UE) 2021/694;
- 15) "pouvoir adjudicateur": la Commission ou, si le fonctionnement et l'administration de la réserve de cybersécurité de l'Union ont été confiés à l'ENISA en vertu de l'article 14, paragraphe 5, l'ENISA;
- 16) "fournisseur de services de sécurité gérés": un fournisseur de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555;
- 17) "fournisseurs de services de sécurité gérés de confiance": les fournisseurs de services de sécurité gérés sélectionnés en vue d'être inclus dans la réserve de cybersécurité de l'Union conformément à l'article 17.

Chapitre II

Système européen d'alerte en matière de cybersécurité

Article 3

Création du système européen d'alerte en matière de cybersécurité

1. Réseau paneuropéen d'infrastructures composé de cyberpôles nationaux et de cyberpôles transfrontières y adhérant sur une base volontaire, le système européen d'alerte en matière de cybersécurité est mis en place pour soutenir le développement de capacités avancées permettant à l'Union de renforcer les capacités de détection, d'analyse et de traitement des données en rapport avec les cybermenaces et la prévention des incidents dans l'Union.
2. Le système européen d'alerte en matière de cybersécurité:
 - a) contribue à améliorer la protection et les réactions aux cybermenaces en soutenant les entités concernées, en particulier les CSIRT, le réseau des CSIRT, EU-CyCLONe et les autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, en coopérant avec elles et en renforçant leurs capacités;
 - b) met en commun les données et informations pertinentes sur les cybermenaces et incidents provenant de différentes sources au sein des cyberpôles transfrontières et partage les informations analysées ou agrégées par l'intermédiaire des cyberpôles transfrontières, le cas échéant avec le réseau des CSIRT;

- c) collecte et soutient la production d'informations exploitables de haute qualité et de renseignements sur les cybermenaces, en utilisant des outils de pointe et des technologies avancées, et partage ces informations et renseignements sur les cybermenaces;
 - d) contribue à améliorer la détection coordonnée des cybermenaces et l'appréciation commune de la situation dans l'ensemble de l'Union, et participe à l'émission d'alertes, y compris, le cas échéant, en formulant des recommandations concrètes à l'intention des entités;
 - e) fournit des services et des activités à la communauté de la cybersécurité dans l'Union, y compris en contribuant au développement d'outils et de technologies de pointe dans les domaines de l'intelligence artificielle et de l'analyse de données.
3. Les actions mettant en œuvre le système européen d'alerte en matière de 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 4

Cyberpôles nationaux

1. Lorsqu'un État membre décide de participer au système européen d'alerte en matière de cybersécurité, il désigne ou, le cas échéant, met en place un cyberpôle national aux fins du présent règlement.

2. Un cyberpôle national est une entité unique agissant sous l'autorité d'un État membre. Il peut s'agir d'un CSIRT ou, le cas échéant, d'une autorité nationale de gestion des crises cyber ou autre autorité compétente désignée ou établie en vertu de l'article 8, paragraphe 1 de la directive (UE) 2022/2555, ou d'une autre entité. Le cyberpôle national:
- a) 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 cybermenaces et incidents et contribuer aux travaux d'un cyberpôle transfrontière, tel que visé à l'article 5; et
 - b) peut détecter, agréger et analyser des données et des informations liées aux cybermenaces et incidents, tel que le renseignement sur les cybermenaces, en utilisant notamment des technologies de pointe, dans le but de prévenir les incidents.
3. Dans le cadre des fonctions visées au paragraphe 2 du présent article, les cyberpôles nationaux peuvent coopérer avec des entités du secteur privé pour échanger des données et des informations pertinentes aux fins de la détection et de la prévention des cybermenaces et incidents, y compris avec les communautés sectorielles et transsectorielles d'entités essentielles et importantes visées à l'article 3 de la directive 2022/2555. Le cas échéant et conformément au droit de l'Union et au droit national, les informations demandées ou reçues par les cyberpôles nationaux peuvent comprendre des données de télémétrie, de capteurs et de connexion.
4. Un État membre sélectionné en vertu de l'article 9, paragraphe 1, s'engage à demander que son cyberpôle participe à un cyberpôle transfrontière.

Article 5
Cyberpôles transfrontières.

1. Lorsqu'au moins trois États membres s'engagent à veiller à ce que leurs cyberpôles nationaux collaborent pour coordonner leurs activités de détection des incidents de cybersécurité et de surveillance des cybermenaces, ces États membres peuvent créer un consortium d'hébergement aux fins du présent règlement.
2. Un consortium d'hébergement est composé d'au moins trois États membres qui ont accepté de mettre en place un cyberpôle transfrontière et de contribuer à l'acquisition des outils, infrastructures ou services nécessaires à celui-ci ainsi qu'à son fonctionnement, conformément au paragraphe 4.
3. Lorsqu'un consortium d'hébergement est sélectionné conformément à l'article 9, paragraphe 3, ses membres concluent un accord de consortium écrit qui:
 - a) définit les modalités internes de mise en œuvre de la convention d'hébergement et d'utilisation conformément à l'article 9, paragraphe 3;
 - b) met en place le cyberpôle transfrontière du consortium d'hébergement; et
 - c) comprend les clauses spécifiques requises en vertu de l'article 6, paragraphes 1 et 2.

4. Un cyberpôle transfrontière est une plateforme multinationale établie par un accord de consortium écrit, tel que visé au paragraphe 3. Il réunit au sein d'une structure de réseau coordonnée les cyberpôles nationaux des États membres du consortium d'accueil. Il est conçu pour améliorer la surveillance, la détection et l'analyse des cybermenaces, pour prévenir les incidents et pour contribuer à l'obtention de renseignements sur les cybermenaces, notamment par l'échange de données et d'informations pertinentes, le cas échéant anonymisées, 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.
5. Un cyberpôle transfrontière est représenté à des fins juridiques par un membre du consortium d'hébergement correspondant agissant en tant que coordinateur, ou par le consortium d'hébergement s'il est doté de la personnalité juridique. La responsabilité de la conformité du cyberpôle transfrontière au présent règlement et à la convention d'hébergement et d'utilisation est attribuée dans l'accord de consortium écrit visé au paragraphe 3.
6. Un État membre peut rejoindre un consortium d'hébergement existant avec l'accord de ses membres. L'accord de consortium écrit visé au paragraphe 3 et la convention d'hébergement et d'utilisation sont modifiés en conséquence. Cela n'affecte pas les droits de propriété du Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (ECCC) sur les outils, infrastructures ou services déjà acquis conjointement avec ce consortium d'hébergement.

Article 6

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

1. Les membres d'un consortium d'hébergement veillent à ce que leurs cyberpôles nationaux partagent, conformément à l'accord de consortium écrit visé à l'article 5, paragraphe 3, des informations pertinentes, le cas échéant anonymisées, telles que des informations relatives aux cybermenaces, aux incidents évités de justesse, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, aux informations spécifiques aux acteurs de la menace, aux alertes de cybersécurité et aux recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, au sein du cyberpôle transfrontière où ce partage d'informations:
 - a) favorise et améliore la détection des cybermenaces et renforce les capacités du réseau des CSIRT à prévenir les incidents et à y réagir ou à en atténuer les effets;
 - b) renforce le niveau de cybersécurité, par exemple 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, 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, entre les membres du consortium d'hébergement, les informations visées au paragraphe 1, et les conditions dans lesquelles ces informations doivent être partagées;
 - b) un cadre de gouvernance précisant et encourageant le partage par tous les participants des informations pertinentes, le cas échéant anonymisées, visées au paragraphe 1;
 - c) des objectifs pour la contribution au développement d'outils et de technologies de pointe, notamment dans les domaines de l'intelligence artificielle et de l'analyse de données.

L'accord de consortium écrit peut préciser que les informations visées au paragraphe 1 sont à partager conformément au droit de l'Union et au droit national.

3. Les cyberpôles transfrontières concluent entre eux des accords de coopération précisant les principes d'interopérabilité et de partage des informations entre les cyberpôles transfrontières. Ils informent la Commission des accords de coopération conclus.

4. Le partage d'informations visé au paragraphe 1 entre les cyberpôles transfrontières est assuré par un niveau élevé d'interopérabilité. Afin de soutenir cette interopérabilité, l'ENISA, en étroite consultation avec la Commission, publie, sans retard injustifié et, en tout état de cause, au plus tard le ... *[12 mois après la date d'entrée en vigueur du présent règlement]*, des lignes directrices en matière d'interopérabilité précisant notamment les formats et protocoles d'échange d'informations, en tenant compte des normes et bonnes pratiques internationales, ainsi que le fonctionnement de tout cyberpôle transfrontière établi. Les exigences d'interopérabilité prévues dans les accords de coopération des cyberpôles transfrontières sont fondées sur les lignes directrices publiées par l'ENISA.

Article 7

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

1. Les cyberpôles transfrontières et le réseau des CSIRT coopèrent étroitement, notamment à des fins de partage des informations. À cette fin, ils conviennent des modalités procédurales relatives à la coopération et au partage des informations pertinentes et, sans préjudice du paragraphe 2, aux types d'informations à partager.
2. Lorsque les cyberpôles transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils veillent à ce que des informations pertinentes ainsi que des alertes rapides soient fournies sans retard injustifié aux autorités des États membres et à la Commission par l'intermédiaire du réseau EU-CyCLONe et du réseau des CSIRT aux fins d'une connaissance commune de la situation.

Article 8

Sécurité

1. Les États membres participant au système européen d'alerte en matière de cybersécurité garantissent un niveau élevé de cybersécurité, y compris en matière de confidentialité et de sécurité des données, ainsi que la sécurité physique du système européen d'alerte en matière de cybersécurité, et veillent également à ce que le réseau soit géré et contrôlé de manière adéquate de sorte qu'il soit possible de le protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris celle des données et des informations partagées par l'intermédiaire du réseau.
2. Les États membres participant au système européen d'alerte en matière de cybersécurité veillent à ce que le partage d'informations visé à l'article 6, paragraphe 1, au sein du système européen d'alerte en matière de cybersécurité avec toute entité autre qu'une autorité ou un organisme public d'un État membre ne porte pas atteinte aux intérêts de l'Union ou des États membres en matière de sécurité.

Article 9

Financement du système européen d'alerte en matière de cybersécurité

1. À la suite d'un appel à manifestation d'intérêt pour les États membres qui ont l'intention de participer au système européen d'alerte en matière de cybersécurité, l'ECCC sélectionne les États membres pour participer avec l'ECCC à une acquisition conjointe d'outils, d'infrastructures ou de services en vue de mettre en place ou de renforcer les capacités des pôles nationaux de cybersécurité désignés ou établis en vertu de l'article 4, paragraphe 1. L'ECCC peut octroyer aux États membres sélectionnés des subventions destinées à financer le fonctionnement de tels outils, infrastructures ou services. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils, infrastructures ou services et jusqu'à 50 % des coûts opérationnels. Les États membres couvrent les coûts restants. Avant de lancer la procédure d'acquisition des outils, infrastructures ou services, l'ECCC et les États membres sélectionnés concluent un accord d'hébergement et d'utilisation qui régit l'utilisation des outils, infrastructures ou services.
2. Lorsque le cyberpôle d'un État membre ne participe pas à un cyberpôle transfrontière dans un délai de deux ans à compter de la date à laquelle les outils, infrastructures et services ont été acquis ou de la date à laquelle il a reçu une subvention, la date la plus proche étant retenue, l'État membre ne peut prétendre à un soutien supplémentaire de l'Union au titre du présent chapitre tant qu'il n'a pas adhéré à un cyberpôle transfrontière.

3. 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, d'infrastructures ou de services avec ce Centre. L'ECCC peut octroyer au consortium d'hébergement une subvention destinée à financer le fonctionnement des outils, infrastructures et services. La contribution financière de l'Union couvre jusqu'à 75 % des coûts d'acquisition des outils, infrastructures et services, et jusqu'à 50 % des coûts opérationnels. Le consortium d'hébergement couvre les coûts restants. Avant de lancer la procédure d'acquisition des outils, infrastructures ou services, l'ECCC et l'État membre concluent un accord d'hébergement et d'utilisation qui régit l'utilisation des outils, infrastructures ou services.
4. L'ECCC élabore, au moins tous les deux ans, une cartographie des outils, infrastructures ou services nécessaires et de qualité suffisante pour mettre en place ou renforcer les capacités des cyberpôles nationaux et les cyberpôles transfrontières, ainsi que leur disponibilité, y compris auprès d'entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants des États membres. Lors de l'élaboration de la cartographie, l'ECCC consulte le réseau des CSIRT, tout cyberpôle transfrontière existant, l'ENISA et la Commission.

Chapitre III

Mécanisme d'urgence dans le domaine de la cybersécurité

Article 10

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 de favoriser l'amélioration de la résilience de l'Union face aux cybermenaces et d'anticiper et d'atténuer, dans un esprit de solidarité, les effets à court terme d'incidents de cybersécurité importants, d'incidents de cybersécurité majeurs ou d'incidents de cybersécurité assimilés à des incidents majeurs.
2. Dans le cas des États membres, les actions au titre du mécanisme d'urgence dans le domaine de la cybersécurité sont menées sur demande et complètent les efforts et actions des États membres pour se préparer aux incidents, y réagir et s'en remettre.
3. 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 sont mises en œuvre conformément au règlement (UE) 2021/694, et notamment à son objectif spécifique 3.
4. Les actions relevant du mécanisme d'urgence dans le domaine de la cybersécurité sont mises en œuvre principalement via l'ECCC, conformément au règlement (UE) 2021/887. Toutefois, les actions mettant en œuvre la réserve de cybersécurité de l'Union visées à l'article 11, point b), du présent règlement sont mises en œuvre par la Commission et l'ENISA.

Article 11
Types de mesures

Le mécanisme d'urgence dans le domaine de la cybersécurité soutient les types de mesures suivantes:

- a) actions de préparation, à savoir:
 - i) les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union, comme indiqué à l'article 12;
 - ii) d'autres actions de préparation pour les entités actives dans des secteurs critiques ou pour les entités actives dans des secteurs hautement critiques, comme précisé à l'article 13;
- b) les mesures prévues par les fournisseurs de services de sécurité gérés de confiance participant à la réserve de cybersécurité de l'Union établie en vertu de l'article 14 qui soutiennent la réaction aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs ou aux incidents de cybersécurité assimilés à des incidents majeurs et permettent d'amorcer le rétablissement suite à ces incidents.
- c) les mesures de soutien à l'assistance mutuelle visées à l'article 18.

Article 12

Tests de préparation coordonnés des entités

1. Le mécanisme d'urgence dans le domaine de la cybersécurité soutient les tests volontaires de préparation coordonnés des entités actives dans des secteurs hautement critiques.
2. Les tests de préparation coordonnés peuvent consister en des actions de préparation, telles que des tests de pénétration, et une évaluation des menaces.
3. Le soutien aux actions de préparation au titre du présent article est fourni aux États membres principalement sous la forme de subventions et sous réserve des conditions prévues dans les programmes de travail pertinents visés à l'article 24 du règlement (UE) 2021/694.
4. Aux fins de contribuer aux tests de préparation coordonnés des entités visés à l'article 11, point a) i), du présent règlement dans l'ensemble de l'Union, la Commission, après consultation du groupe de coopération SRI et de l'ENISA, du réseau EU-CyCLONe 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, pour lesquels un appel à propositions en vue de l'octroi de subventions peut être lancé. Les États membres choisissent de participer ou non à ces appels à propositions.
5. Lorsqu'elle détermine les secteurs ou sous-secteurs visés au paragraphe 4, la Commission tient compte de l'évaluation des risques et des tests de résilience coordonnés au niveau de l'Union et de leurs résultats.

6. Le groupe de coopération SRI, en coopération avec la Commission, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après dénommé "haut représentant") et l'ENISA, et, dans le cadre de son mandat, EU-CyCLONe, élaborent des scénarios de risque et des méthodes de risque communs pour les tests de préparation coordonnés visés à l'article 11, point a) i), et, le cas échéant, pour d'autres actions de préparation visées au point a) ii) dudit article.
7. Lorsqu'une entité évoluant dans un secteur hautement critique participe volontairement à des tests de préparation coordonnés et que ces tests donnent lieu à des recommandations de mesures spécifiques que l'entité participante pourrait intégrer dans un plan de mesures correctives, l'autorité de l'État membre responsable des tests de préparation coordonnés examine, le cas échéant, le suivi de ces mesures par les entités participantes en vue de renforcer la préparation.

Article 13

Autres actions de préparation

1. Le mécanisme d'urgence en matière de cybersécurité soutient les actions de préparation qui ne sont pas couvertes par l'article 12. Ces actions comprennent des actions de préparation pour les entités évoluant dans des secteurs non recensés pour des tests de préparation coordonnés conformément à l'article 12. Ces actions peuvent avoir pour finalité de promouvoir la surveillance de la vulnérabilité, le suivi des risques, les exercices et les formations.

2. Le soutien aux actions de préparation au titre du présent article est fourni aux États membres sur demande, principalement sous la forme de subventions et dans les conditions définies dans les programmes de travail pertinents visés à l'article 24 du règlement (UE) 2021/694.

Article 14

Création de la réserve de cybersécurité de l'Union

1. Une réserve de cybersécurité de l'Union est créée afin d'aider, à leur demande, les utilisateurs visés au paragraphe 3 à réagir aux incidents de cybersécurité importants, aux incidents de cybersécurité majeurs ou aux incidents de cybersécurité assimilés à des incidents majeurs, ou à fournir une assistance à cet effet, et à amorcer le rétablissement après de tels incidents.
2. La réserve de cybersécurité de l'Union se compose de services de réaction fournis par des fournisseurs de services de sécurité gérés de confiance sélectionnés conformément aux critères énoncés à l'article 17, paragraphe 2. La réserve de cybersécurité de l'Union peut comprendre des services affectés au préalable. Les services affectés au préalable d'un fournisseur de services de sécurité gérés de confiance sont convertibles en services de préparation liés à la prévention et à la réaction aux incidents, dans les cas où ces services affectés au préalable ne sont pas utilisés pour répondre à des incidents pendant la période pendant laquelle ces services sont affectés au préalable. La réserve de cybersécurité de l'Union peut être déployée sur demande dans tous les États membres, institutions, organes et organismes de l'Union et dans les pays tiers associés au régime de droits à l'importation visés à l'article 19, paragraphe 1.

3. Les utilisateurs des services fournis par la réserve de cybersécurité de l'Union sont les suivants:
- a) les autorités des États membres chargées de la gestion des crises cyber 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 services de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE) conformément à l'article 13 du règlement (UE, Euratom) 2023/2841;
 - c) les autorités compétentes, telles que les CSIRT, et les autorités chargées de la gestion des crises cyber des pays tiers associés au programme pour une Europe numérique, conformément à l'article 19, paragraphe 8.
4. La Commission a la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. La Commission définit les priorités et l'évolution de la réserve de cybersécurité de l'Union, en coordination avec le groupe de coopération SRI et, conformément aux exigences des utilisateurs visés au paragraphe 3, elle supervise sa mise en œuvre et elle garantit la complémentarité, la cohérence, les synergies et les liens avec d'autres mesures de soutien prises au titre du présent règlement ainsi qu'avec d'autres actions et programmes de l'Union. Ces priorités sont revues et, le cas échéant, révisées tous les deux ans. La Commission tient le Parlement européen et le Conseil au courant de ces priorités et de révision de celles-ci.

5. Sans préjudice de la responsabilité globale de la Commission pour la mise en œuvre de la réserve de cybersécurité de l'Union visée au paragraphe 4 du présent article et sous réserve d'un accord de contribution telle que définie à l'article 2, point 19), du règlement (UE, Euratom) 2024/2509, la Commission confie le fonctionnement et l'administration de la réserve de cybersécurité de l'Union en tout ou en partie, à l'ENISA. Les aspects qui ne sont pas confiés à l'ENISA continuent de faire l'objet d'une gestion directe par la Commission.
6. L'ENISA prépare, au moins tous les deux ans, une cartographie des services nécessaires aux utilisateurs visés au paragraphe 3, points a) et b), du présent article. La cartographie comprend également la disponibilité de ces services, y compris de la part d'entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres. Lorsqu'elle cartographie cette disponibilité, l'ENISA évalue les compétences et les capacités de la main-d'œuvre de l'Union en matière de cybersécurité en rapport avec les objectifs de la réserve de cybersécurité de l'Union. Lors de l'élaboration de la cartographie, l'ENISA consulte le groupe de coopération SRI, EU-CyCLONe, la Commission et, le cas échéant, le conseil interinstitutionnel de cybersécurité établi en vertu de l'article 10 du règlement (UE, Euratom) 2023/2841 (IICB). Pour cartographier la disponibilité des services, l'ENISA consulte également les parties prenantes concernées du secteur de la cybersécurité, y compris les fournisseurs de services de sécurité gérés. L'ENISA prépare une cartographie similaire, après avoir informé le Conseil et après avoir consulté EU-CyCLONe, la Commission et, le cas échéant, le haut représentant, afin de recenser les besoins des utilisateurs visés au paragraphe 3, point c), du présent article.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 23 pour compléter le présent règlement en précisant les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'Union. Lors de l'élaboration de ces actes délégués, la Commission tient compte de la cartographie visée au paragraphe 6 du présent article, et peut échanger des conseils et coopérer avec le groupe de coopération SRI et l'ENISA.

Article 15

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

1. Les utilisateurs visés à l'article 14, 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, aux incidents de cybersécurité majeurs ou aux incidents de cybersécurité assimilés à des incidents majeurs et à amorcer le rétablissement à la suite de tels incidents.
2. Pour bénéficier de l'aide de la réserve de cybersécurité de l'Union, les utilisateurs visés à l'article 14, paragraphe 3, prennent toutes les mesures appropriées pour atténuer les effets de l'incident pour lequel ils demandent de l'aide, y compris, le cas échéant, 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.
3. Les demandes de soutien sont transmises au pouvoir adjudicateur comme suit:
 - a) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point a), du présent règlement, par l'intermédiaire du point de contact unique désigné ou établi en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555;

- b) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point b), par lesdits utilisateurs;
 - c) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point c), par l'intermédiaire du point de contact unique visé à l'article 19, paragraphe 9;
4. dans le cas des demandes des utilisateurs visés à l'article 14, paragraphe 3, point a), les États membres informent le réseau des CSIRT et, le cas échéant, EU-CyCLONe des demandes d'intervention en cas d'incident et de soutien au rétablissement initial formulées par leurs utilisateurs conformément au présent article.
5. Les demandes d'aide en ce qui concerne la réaction à un incident et le rétablissement initial contiennent:
- a) des informations appropriées concernant l'entité touchée et les effets potentiels de l'incident sur:
 - i) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point a), les États membres et utilisateurs touchés, y compris le risque de propagation vers un autre État membre;
 - ii) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point b), les institutions, organes ou organismes de l'Union touchés;
 - iii) dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point c), les pays tiers associés au programme pour une Europe numérique touchés;

- b) des informations concernant le service requis, accompagnées d'une indication de l'utilisation prévue de l'aide demandée, y compris une indication des besoins estimés;
 - c) des informations appropriées sur les mesures prises pour atténuer l'incident pour lequel l'aide a été demandée, visées au paragraphe 2;
 - d) le cas échéant, si elles sont disponibles, des informations sur les autres formes d'aide dont dispose l'entité touchée.
6. L'ENISA, en collaboration avec la Commission et EU-CyCLONe, élabore un modèle pour faciliter la présentation des demandes d'aide adressées à la réserve de cybersécurité de l'Union.
7. La Commission peut, au moyen d'actes d'exécution, préciser de façon détaillée les modalités procédurales relatives à la manière dont les services d'appui de la réserve de cybersécurité de l'Union sont demandés et la manière dont ces demandes doivent être traitées en vertu du présent article, de l'article 16, paragraphe 1, et de l'article 19, paragraphe 10, y compris les modalités de présentation de ces demandes et de fourniture des réponses et des modèles pour les rapports visés à l'article 16, paragraphe 9. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2.

Article 16

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

1. Dans le cas des demandes des utilisateurs visées à l'article 14, paragraphe 3, points a) et b), les demandes d'aide au titre de la réserve de cybersécurité de l'Union sont évaluées par le pouvoir adjudicateur. Une réponse est transmise aux utilisateurs visés à l'article 14, paragraphe 3, points a) et b), sans retard et, en tout état de cause, au plus tard 48 heures après la présentation de la demande afin de garantir l'efficacité du soutien. Le pouvoir adjudicateur informe le Conseil et la Commission des résultats du processus.
2. En ce qui concerne les informations partagées dans le cadre de la demande et de la fourniture des services de la réserve de cybersécurité de l'Union, toutes les parties participant à l'application du présent règlement:
 - a) limitent l'utilisation et le partage de ces informations à ce qui est nécessaire pour s'acquitter de leurs obligations ou fonctions au titre du présent règlement;
 - b) utilisent et partagent toute information confidentielle ou classifiée en vertu du droit de l'Union et du droit national uniquement conformément à ce droit; et
 - c) assurent un échange d'informations efficace, efficient et sécurisé, le cas échéant en utilisant et en respectant les protocoles d'échange d'informations pertinents, y compris le TLP.

3. Lors de l'évaluation des demandes individuelles au titre de l'article 16, paragraphe 1, et de l'article 19, paragraphe 10, le pouvoir adjudicateur ou la Commission, selon le cas, évalue d'abord si les critères visés à l'article 15, paragraphes 1 et 2, sont remplis. Si tel est le cas, le pouvoir adjudicateur ou la Commission évaluent la durée et la nature de l'aide appropriée, compte tenu de l'objectif visé à l'article 1, paragraphe 3, point b), et des critères suivants, le cas échéant:
- a) l'ampleur et la gravité de l'incident;
 - b) le type d'entité touchée, la priorité étant accordée aux incidents touchant des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555;
 - c) les effets potentiels de l'incident sur l'État membre ou les États membres, les institutions, organes ou organismes de l'Union ou les pays tiers associés au programme pour une Europe numérique touchés;
 - d) l'éventuelle nature transfrontière de l'incident et le risque de propagation à d'autres États membres ou institutions, organes ou organismes de l'Union ou les pays tiers associés au programme pour une Europe numérique;
 - e) les mesures prises par l'utilisateur pour contribuer à la réaction et aux efforts de rétablissement initial, visées à l'article 15, paragraphe 2.

4. Pour classer les demandes par ordre de priorité, dans le cas de demandes concurrentes émanant d'utilisateurs visés à l'article 14, paragraphe 3, les critères visés au paragraphe 3 du présent article sont pris en compte, le cas échéant, sans préjudice du principe de coopération sincère entre les États membres et les institutions, organes et organismes de l'Union. Lorsque deux ou plusieurs demandes sont jugées égales au regard des critères, une priorité plus élevée est accordée aux demandes émanant d'utilisateurs des États membres. Lorsque le fonctionnement et l'administration de la réserve de cybersécurité de l'Union ont été confiés, en tout ou en partie, à l'ENISA en vertu de l'article 14, paragraphe 5, l'ENISA et la Commission coopèrent étroitement pour hiérarchiser les demandes conformément au présent paragraphe.
5. Les services de la réserve de cybersécurité de l'Union sont fournis conformément à des accords spécifiques conclus entre le fournisseur de services de sécurité gérés de confiance et l'utilisateur bénéficiant de l'aide de la réserve de cybersécurité de l'Union. Ces services peuvent être fournis conformément à des accords spécifiques conclus entre le fournisseur de services de sécurité gérés de confiance, l'utilisateur et l'entité touchée. Tous les accords visés au présent paragraphe comportent, entre autres, des conditions de responsabilité.
6. Les accords visés au paragraphe 5 se fondent sur des modèles élaborés par l'ENISA, après consultation des États membres et, le cas échéant, d'autres utilisateurs de la réserve de cybersécurité de l'Union.

7. La Commission, l'ENISA et les utilisateurs de la réserve de cybersécurité de l'Union 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'Union.
8. Les utilisateurs ne peuvent utiliser les services de la réserve de cybersécurité de l'Union fournis en réponse à une demande au titre de l'article 15, paragraphe 1, que pour soutenir la réaction à des incidents de cybersécurité importants, des incidents de cybersécurité majeurs ou des incidents de cybersécurité assimilés à des incidents majeurs à grande échelle et pour engager le rétablissement à la suite de tels incidents. Ils ne peuvent utiliser ces services que pour:
 - a) les entités actives dans des secteurs hautement critiques ou les entités actives dans d'autres secteurs critiques, dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point a), et des entités équivalentes dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point c); et
 - b) Les institutions, organes et organismes de l'Union, dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point b).
9. Dans les deux mois suivant la fin d'une aide, les utilisateurs qui ont bénéficié d'une aide fournissent un rapport de synthèse sur le service fourni, les résultats obtenus et les enseignements tirés:
 - a) à la Commission, à l'ENISA, au réseau des CSIRT et à EU-CyCLONe dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point a);
 - b) à la Commission, à l'ENISA et à l'IICB dans le cas de l'utilisateur visé à l'article 14, paragraphe 3, point b);

- c) à la Commission dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point c).

La Commission transmet tout rapport de synthèse reçu des utilisateurs visés à l'article 14, paragraphe 3, conformément au premier alinéa, point c), du présent paragraphe, au Conseil et au haut représentant.

- 10. Lorsque le fonctionnement et l'administration de la réserve de cybersécurité de l'Union ont été confiés, en tout ou en partie, à l'ENISA en vertu de l'article 14, paragraphe 5, du présent règlement, l'ENISA fait régulièrement rapport à la Commission et la consulte à cet égard. Dans ce contexte, l'ENISA transmet immédiatement à la Commission toute demande qu'elle reçoit des utilisateurs visés à l'article 14, paragraphe 3, point c), du présent règlement et, lorsque cela est nécessaire aux fins de la hiérarchisation des priorités en vertu du présent article, toute demande qu'elle a reçue des utilisateurs visés à l'article 14, paragraphe 3, point a) ou b), du présent règlement. Les obligations prévues au présent paragraphe sont sans préjudice de l'article 14 du règlement (UE) 2019/881.
- 11. Dans le cas des utilisateurs visés à l'article 14, paragraphe 3, points a) et b), le pouvoir adjudicateur fait rapport régulièrement et au moins deux fois par an au groupe de coopération SRI, sur l'utilisation de cette aide et les résultats obtenus.
- 12. Dans le cas des utilisateurs visés à l'article 14, paragraphe 3, point c), la Commission, régulièrement et au moins deux fois par an, fait rapport au Conseil et informe le haut représentant sur l'utilisation de cette aide et les résultats obtenus.

Article 17

Fournisseurs de services de sécurité gérés de confiance

1. Dans les procédures de passation de marchés menées pour la création de la réserve de cybersécurité de l'Union, le pouvoir adjudicateur agit conformément aux principes énoncés dans le règlement (UE, Euratom) 2024/2509 et aux principes suivants:
 - a) il veille à ce que les services inclus dans la réserve de cybersécurité de l'Union, pris dans leur ensemble, soient tels que la réserve de cybersécurité de l'Union comprenne des services pouvant être déployés dans tous les États membres, compte tenu notamment des exigences nationales relatives à la fourniture de ces services, y compris en ce qui concerne les langues, la certification ou l'accréditation;
 - b) il veille à protéger les intérêts essentiels de l'Union et de ses États membres en matière de sécurité;
 - c) il s'assure que la réserve de cybersécurité de l'Union apporte une valeur ajoutée européenne, en contribuant à la réalisation des objectifs énoncés à l'article 3 du règlement (UE) 2021/694, y compris en favorisant le développement des compétences en matière de cybersécurité dans l'Union.

2. Lors de la passation de marchés de services pour la réserve de cybersécurité de l'Union, le pouvoir adjudicateur inclut les critères et les exigences 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 et la continuité de l'expertise ainsi que les ressources techniques requises;
 - b) le fournisseur, ainsi que toute filiale et tout sous-traitant concernés, se conforment aux règles applicables en matière de protection des informations classifiées et mettent en place des mesures appropriées, y compris, le cas échéant, des accords entre eux, pour protéger les informations confidentielles relatives au service, et en particulier les éléments de preuve, les conclusions et les rapports;
 - 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, lorsqu'un État membre l'exige;
 - e) le fournisseur dispose du niveau de sécurité approprié pour ses systèmes informatiques;

- f) le fournisseur possède le matériel et les logiciels nécessaires au service demandé, qui ne contiennent pas de vulnérabilités exploitables constatées, comprennent les dernières mises à jour de sécurité et sont conformes en tout point avec toute disposition applicable du règlement (UE) 2024/... du Parlement européen et du Conseil²³⁺;
- g) le fournisseur est en mesure de démontrer qu'il possède une expérience dans la fourniture de services similaires à des autorités nationales, à des entités actives dans des secteurs hautement critiques ou à des entités actives dans d'autres secteurs critiques pertinentes;
- h) le fournisseur est en mesure de fournir le service dans un bref délai dans les États membres où il peut le faire;
- i) le fournisseur est en mesure de fournir le service dans une ou plusieurs langues officielles des institutions de l'Union ou d'un État membre, selon ce qui est exigé par, le cas échéant, les États membres ou les utilisateurs visés à l'article 14, paragraphe 3, points b) et c), là où le fournisseur peut fournir le service;
- j) dès qu'un schéma européen de certification de cybersécurité pour les services de sécurité conforme au règlement (UE) 2019/881 est en place, le fournisseur est certifié conformément à ce schéma dans un délai de deux ans à compter de la date d'application du schéma;

²³ Règlement (UE) 2024/... du Parlement européen et du Conseil du ... sur ... (JO L, ..., ELI: ...).

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 100/23 (2022/0272 (COD)) et insérer le numéro, la date, le titre, la référence au JO et la référence ELI dudit règlement dans la note de bas de page.

- k) le fournisseur inclut dans l'offre les conditions de conversion des services inutilisés de réaction aux incidents en services de préparation étroitement liés à la réaction aux incidents, tels que des exercices ou des formations.
- 3. Aux fins de l'acquisition de services pour la réserve de cybersécurité de l'Union, le pouvoir adjudicateur peut, le cas échéant, élaborer, en étroite coopération avec les États membres, des critères et des exigences supplémentaires par rapport à ceux visés au paragraphe 2.

Article 18

Mesures de soutien à l'assistance mutuelle

- 1. Le mécanisme d'urgence dans le domaine de la cybersécurité apporte une aide à l'assistance technique fournie par un État membre à un autre État membre touché par un incident de cybersécurité important ou un incident de cybersécurité majeur, y compris dans les cas visés à l'article 11, paragraphe 3, point f), de la directive (UE) 2022/2555.
- 2. L'aide à l'assistance technique mutuelle visée au paragraphe 1 du présent article est apportée sous forme de subventions et aux conditions fixées dans les programmes de travail correspondants visés à l'article 24 du règlement (UE) 2021/694.

Article 19

Aide aux pays tiers associés au programme pour une Europe numérique

1. Un pays tiers associé au programme pour une Europe numérique peut demander une aide à la réserve de cybersécurité de l'Union lorsque l'accord par lequel il est associé au programme pour une Europe numérique prévoit sa participation à la réserve de cybersécurité de l'Union. Ledit accord comprend des dispositions qui imposent au pays tiers concerné associé au programme pour une Europe numérique de se conformer aux obligations énoncées aux paragraphes 2 et 9 du présent article. Aux fins de la participation d'un pays tiers à la réserve de cybersécurité de l'Union, l'association partielle d'un pays tiers au programme pour une Europe numérique peut comprendre son association limitée à l'objectif opérationnel visé à l'article 6, paragraphe 1, point g), du règlement (UE) 2021/694.
2. Dans les trois mois suivant la conclusion de l'accord visé au paragraphe 1 et en tout état de cause avant de recevoir une aide de la réserve de cybersécurité de l'Union, le pays tiers associé au programme pour une Europe numérique fournit à la Commission des informations sur ses 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, les incidents de cybersécurité majeurs et les incidents de cybersécurité assimilés à des incidents majeurs, ainsi que des informations sur les entités nationales responsables, notamment les centres de réponse aux incidents de sécurité informatique ou entités équivalentes, leurs capacités et les ressources qui leur sont allouées. Le pays tiers associé au programme pour une Europe numérique fournit régulièrement et au moins une fois par an des mises à jour de ces informations. La Commission fournit ces informations au haut représentant et à l'ENISA afin de faciliter l'application du paragraphe 11.

3. La Commission évalue régulièrement, et au moins une fois par an, les critères suivants pour chaque pays tiers associé au programme pour une Europe numérique visé au paragraphe 1:
- a) le respect par ledit pays des dispositions de l'accord visé au paragraphe 1, dès lors qu'elles concernent la participation à la réserve de cybersécurité de l'Union;
 - b) la prise par ledit pays de mesures adéquates pour se préparer aux incidents de cybersécurité importants ou aux incidents de cybersécurité assimilés à des incidents majeurs, sur la base des informations visées au paragraphe 2; et
 - c) la compatibilité de l'octroi d'une aide avec la politique de l'Union à l'égard de ce pays et avec ses relations globales avec ce pays, ainsi qu'avec les autres actions de l'Union dans le domaine de la sécurité.

Pour réaliser l'évaluation visée au premier alinéa, la Commission consulte le haut représentant en ce qui concerne le critère visé au point c) dudit alinéa.

Lorsque la Commission parvient à la conclusion qu'un pays tiers associé au programme pour une Europe numérique remplit l'ensemble des conditions visées au premier alinéa, elle soumet au Conseil une proposition d'adoption d'un acte d'exécution conformément au paragraphe 4 afin d'autoriser l'octroi à ce pays d'une aide de la réserve de cybersécurité de l'Union.

4. Le Conseil peut adopter les actes d'exécution visés au paragraphe 3. Ces actes d'exécution s'appliquent pour une durée maximale d'un an. Ils peuvent être renouvelés. Ils peuvent prévoir une limite, qui ne peut être inférieure à 75 jours, au nombre de jours pendant lesquels l'aide peut être octroyée en réponse à une demande unique.

Le Conseil agit promptement aux fins du présent article et il adopte, en principe, les actes d'exécution visés au présent paragraphe dans un délai de huit semaines à compter de l'adoption de la proposition de la Commission pertinente en vertu du paragraphe 3, troisième alinéa.

5. Le Conseil, statuant sur proposition de la Commission, peut modifier ou abroger à tout moment un acte d'exécution adopté en vertu du paragraphe 4.

Lorsque le Conseil estime qu'il y a eu un changement important en ce qui concerne le critère visé au paragraphe 3, premier alinéa, point c), il peut, en statuant à l'initiative dûment motivée d'un ou de plusieurs États membres, modifier ou abroger un acte d'exécution adopté en vertu du paragraphe 4.

6. Dans l'exercice de ses pouvoirs d'exécution au titre du présent article, le Conseil applique le critère visé au paragraphe 3, premier alinéa, et explique son évaluation desdits critères. En particulier, lorsqu'il statue à sa propre initiative conformément au paragraphe 5, deuxième alinéa, le Conseil explique le changement majeur visé audit alinéa.

7. L'aide apportée par la réserve de cybersécurité de l'Union à un pays tiers associé au programme pour une Europe numérique respecte toutes les conditions spécifiques énoncées dans l'accord visé au paragraphe 1.
8. Les utilisateurs de pays tiers associés au programme pour une Europe numérique pouvant bénéficier de services au titre de la réserve de cybersécurité de l'Union sont des autorités compétentes telles que les centres de réponse aux incidents de sécurité informatique ou des entités équivalentes et les autorités chargées de la gestion des crises cyber.
9. Chaque pays tiers associé au programme pour une Europe numérique pouvant bénéficier d'une aide de la réserve de cybersécurité de l'Union désigne une autorité qui joue le rôle de point de contact unique aux fins du présent règlement.
10. Les demandes d'aide de la réserve de cybersécurité de l'Union au titre du présent article sont évaluées par la Commission. Le pouvoir adjudicateur ne peut octroyer de l'aide à un pays tiers que lorsque et aussi longtemps qu'un acte d'exécution du Conseil adopté en vertu du paragraphe 4 du présent article autorisant cette aide audit pays est en vigueur. Une réponse est transmise aux utilisateurs visés à l'article 14, paragraphe 3, point c), sans retard injustifié.

11. À la réception d'une demande d'aide au titre du présent article, la Commission informe immédiatement le Conseil. La Commission tient le Conseil informé de l'évaluation de la demande. La Commission coopère également avec le haut représentant en ce qui concerne les demandes reçues et la mise en œuvre de l'aide accordée aux pays tiers associés au programme pour une Europe numérique au titre de la réserve de cybersécurité de l'Union. En outre, la Commission tient également compte de tout avis fourni par l'ENISA concernant ces demandes.

Article 20

Coordination avec les mécanismes de gestion des crises de l'Union

1. Lorsqu'un incident de cybersécurité important, un incident de cybersécurité majeur ou un incident de cybersécurité assimilé à un incident majeur est la conséquence ou la cause d'une catastrophe au sens de l'article 4, point 1), de la décision n° 1313/2013/UE, l'aide apportée au titre du présent règlement pour réagir à un tel incident complète des actions entreprises conformément à, et sans préjudice de, ladite décision.
2. Dans le cas d'un incident de cybersécurité majeur ou d'un incident de cybersécurité assimilé à un incident majeur pour lequel le dispositif intégré de l'Union pour une réaction au niveau politique dans les situations de crise en vertu de la décision d'exécution (UE) 2018/1993 (ci-après dénommé "dispositif IPCR") est activé, l'aide apportée au titre du présent règlement pour réagir à cet incident est traitée conformément aux procédures applicables du dispositif IPCR.

Chapitre IV

Mécanisme européen d'analyse des incidents de cybersécurité

Article 21

Mécanisme européen d'analyse des incidents de cybersécurité

1. À la demande de la Commission ou d'EU-CyCLONe, l'ENISA, avec le soutien du réseau des CSIRT et l'approbation des États membres concernés, analyse et évalue les cybermenaces, les vulnérabilités exploitables constatées et les mesures d'atténuation relatives à un incident de cybersécurité important ou à un incident de cybersécurité majeur spécifique. Après l'analyse et l'évaluation d'un incident et dans le but de tirer les enseignements de l'expérience acquise pour éviter ou atténuer des incidents à l'avenir, l'ENISA remet un rapport d'analyse à EU-CyCLONe, au réseau des CSIRT, aux États membres concernés et à la Commission afin de les aider à s'acquitter de leurs tâches, compte tenu notamment des tâches énoncées aux articles 15 et 16 de la directive (UE) 2022/2555. Lorsqu'un incident a des effets sur un pays tiers associé au programme pour une Europe numérique, l'ENISA remet également le rapport au Conseil. Dans un tel cas, la Commission remet le rapport au haut représentant.

2. Pour préparer le rapport d'analyse visé au paragraphe 1 du présent article, l'ENISA coopère avec toutes les parties prenantes concernées, y compris les représentants des États membres, la Commission, les autres institutions, organes et organismes concernés de l'Union, les entreprises du secteur, y compris les fournisseurs de services de sécurité gérés, et les utilisateurs de services de cybersécurité, et elle recueille leurs retours d'informations. Le cas échéant, l'ENISA, en coopération avec les CSIRT et, le cas échéant, les autorités compétentes désignées ou instituées en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, coopère également avec les entités touchées par des incidents de cybersécurité importants ou des incidents de cybersécurité majeurs. Les représentants consultés déclarent tout conflit d'intérêts potentiel.
3. Le rapport d'analyse visé au paragraphe 1 du présent article comprend une analyse et un examen de l'incident de cybersécurité important ou de l'incident de cybersécurité majeur, y compris des principales causes, vulnérabilités exploitables constatées et enseignements tirés. L'ENISA veille à ce que le rapport soit conforme au droit de l'Union ou au droit national relatif à la protection des informations sensibles ou classifiées. Si les États membres concernés ou d'autres utilisateurs visés à l'article 14, paragraphe 3, qui sont touchés par l'incident, le demandent, les données et les informations contenues dans le rapport sont anonymisées. Il ne comporte pas de précisions relatives aux vulnérabilités activement exploitées qui n'ont pas encore été corrigées.

4. Le cas échéant, le rapport d'analyse formule des recommandations afin d'améliorer la posture cyber de l'Union et il peut contenir des bonnes pratiques et des enseignements tirés émanant des parties prenantes concernées.
5. L'ENISA peut produire une version publique du rapport d'analyse. Cette version du rapport ne contient que des informations publiques fiables, ou d'autres informations fiables ajoutées avec l'accord des États membres concernés et, pour les informations relatives à un utilisateur visé à l'article 14, paragraphe 3, point b) ou c), avec l'accord de ce dernier.

Chapitre V

Dispositions finales

Article 22

Modifications du règlement (UE) 2021/694

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

1) L'article 6 est modifié comme suit:

a) le paragraphe 1 est modifié comme suit:

i) le point suivant est inséré:

"a *bis*) soutenir le développement d'un système européen d'alerte en matière de cybersécurité établi par l'article 3 du règlement (UE) .../... du Parlement européen et du Conseil⁺ (ci-après dénommé "système européen d'alerte en matière de cybersécurité"), y compris la mise au point, le déploiement et l'exploitation de cyberpôles nationaux et de cyberpôles 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;

* Règlement (UE) .../... du Parlement européen et du Conseil du ... établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) (OJ L, ..., ELI: ...).";

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)) et insérer le numéro, la date, la référence JO et la référence ELI dudit règlement dans la note de bas de page.

ii) le point suivant est ajouté:

"g) mettre en place et exploiter le mécanisme d'urgence dans le domaine de la cybersécurité établi par l'article 10 du règlement (UE) .../...⁺ y compris la réserve de cybersécurité de l'Union instituée par l'article 14 dudit règlement (ci-après dénommée "réserve de cybersécurité de l'Union"), pour aider les États membres à se préparer aux incidents de cybersécurité importants et aux incidents de cybersécurité majeurs et à y réagir, en complément des ressources et capacités nationales et des autres formes de soutien disponibles au niveau de l'Union, ainsi que pour aider les autres utilisateurs à réagir aux incidents de cybersécurité assimilés à des incidents majeurs.";

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

"2. Les actions entreprises au titre de l'objectif spécifique 3 sont mises en œuvre principalement via le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, conformément au règlement (UE) 2021/887 du Parlement européen et du Conseil*. Toutefois, la réserve de cybersécurité de l'Union est mise en œuvre par la Commission et, conformément à l'article 14, paragraphe 6, du règlement (UE) .../...⁺, par l'ENISA.

* Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1)."

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

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) 1 760 806 000 EUR pour l'objectif spécifique 2 – Intelligence artificielle;

c) 1 372 020 000 EUR pour l'objectif spécifique 3 – Cybersécurité et confiance;

d) 482 640 000 EUR pour l'objectif spécifique 4 – Compétences numériques avancées;"

b) le paragraphe suivant est ajouté:

"8. Par dérogation à l'article 12, paragraphe 1, du règlement financier, les crédits d'engagement et de paiement non utilisés pour les actions menées dans le cadre de la mise en œuvre de la réserve de cybersécurité de l'Union et des mesures de soutien à l'assistance mutuelle en vertu du règlement (UE) .../...⁺, poursuivant les objectifs énoncés à l'article 6, paragraphe 1, point g), du présent règlement sont reportés de droit et peuvent être engagés et payés jusqu'au 31 décembre de l'exercice suivant. Le Parlement et le Conseil sont informés des crédits reportés en vertu de l'article 12, paragraphe 6, du règlement financier."

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

3) L'article 12 est modifié comme suit:

a) les paragraphes suivants sont insérés:

"5 *bis*. Le paragraphe 5 ne s'applique pas, en ce qui concerne les entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers, à une action de mise en œuvre du système européen d'alerte en matière de cybersécurité lorsque les deux conditions suivantes sont remplies pour ce qui est de l'action concernée:

- a) il existe un risque réel, compte tenu des résultats de la cartographie réalisée en vertu de l'article 9, paragraphe 4, du règlement (UE) .../...⁺, que les entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres ne disposent pas des outils, des infrastructures ou des services nécessaires et suffisants pour que l'action contribue de manière adéquate à l'objectif du système européen d'alerte en matière de cybersécurité;
- b) le risque de sécurité lié à une acquisition auprès de ces entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers dans le cadre du système européen d'alerte en matière de cybersécurité est proportionné aux avantages et ne porte pas atteinte aux intérêts essentiels de l'Union et de ses États membres en matière de sécurité.

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

5 *ter*. Le paragraphe 5 ne s'applique pas, en ce qui concerne les entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers, à toute action de mise en œuvre de la réserve de cybersécurité de l'Union lorsque les deux conditions suivantes sont remplies pour ce qui est de l'action concernée:

- a) il existe un risque réel, compte tenu des résultats de la cartographie réalisée en vertu de l'article 14, paragraphe 6, du règlement (UE) .../...⁺, que les entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres ne disposent pas des technologies, de l'expertise ou des capacités nécessaires et suffisantes pour que la réserve de cybersécurité de l'Union remplisse ses fonctions de manière adéquate;
- b) le risque de sécurité lié à la participation de ces entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers dans le cadre de la réserve de cybersécurité de l'Union est proportionné aux avantages et ne porte pas atteinte aux intérêts essentiels de l'Union et de ses États membres en matière de sécurité.";

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

b) le paragraphe 6 est remplacé par le texte suivant:

"6. Lorsque cela est dûment justifié pour des raisons de sécurité, le programme de travail peut aussi prévoir que les entités juridiques qui sont établies dans des pays associés et les entités juridiques qui sont établies dans l'Union mais qui sont contrôlées à partir de pays tiers peuvent être éligibles pour participer à tout ou partie des actions au titre des objectifs spécifiques 1 et 2, uniquement si elles se conforment aux exigences qui doivent être respectées par ces entités juridiques en vue de garantir la protection des intérêts essentiels de l'Union et des États membres en matière de sécurité et de garantir la protection des informations dans les documents classifiés. Ces exigences sont énoncées dans le programme de travail.

Le premier alinéa s'applique également, en ce qui concerne les entités juridiques établies dans l'Union mais contrôlées à partir de pays tiers, aux actions menées dans le cadre de l'objectif spécifique 3:

- a) pour mettre en œuvre le système européen d'alerte en matière de cybersécurité lorsque le paragraphe 5 *bis* s'applique; et
- b) pour mettre en œuvre la réserve de cybersécurité de l'Union lorsque le paragraphe 5 *ter* s'applique."

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

"2. Le programme peut octroyer un financement sous l'une ou l'autre des formes prévues dans le règlement 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* et 2014/25/UE** 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'Union, 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 du présent règlement. 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 168, paragraphe 3, du règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil^{***}, 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'Union, 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 ou 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 168, paragraphe 3, du règlement (UE, Euratom) 2024/2509, la demande d'une seule institution, d'un seul organe ou d'un seul 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.

-
- * 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).
- ** Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et abrogeant la directive 2004/17/CE (JO L 94 du 28.3.2014, p. 243).
- *** Règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil du 23 septembre 2024 relatif aux règles financières applicables au budget général de l'Union (JO L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).".

5) L'article suivant est inséré:

"Article 16 bis

Conflits de normes

Dans le cas d'actions mettant en œuvre le système européen d'alerte en matière de cybersécurité, les règles applicables sont celles énoncées aux articles 4, 5 et 9 du règlement (UE) .../...⁺. En cas de conflit entre les dispositions du présent règlement et les articles 4, 5 et 9 du règlement (UE) .../...⁺, ces derniers prévalent et s'appliquent à ces actions spécifiques.

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

En ce qui concerne la réserve de cybersécurité de l'Union⁺, l'article 19 du règlement (UE) .../...⁺ fixe des règles spécifiques pour la participation des pays tiers associés au programme. En cas de conflit entre les dispositions du présent règlement et l'article 19 du règlement (UE) .../...⁺, ce dernier prévaut et s'applique à ces actions spécifiques."

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

"Article 19

Subventions

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 États membres sélectionnés en vertu de l'article 9 du règlement (EU) .../...⁺ et au consortium d'hébergement visé à l'article 5 du règlement (EU) .../...⁺, 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 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.

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

En ce qui concerne les mesures de soutien à l'assistance mutuelle prévues à l'article 18 du règlement (UE) .../...⁺, l'ECCC informe la Commission et l'ENISA des demandes de subventions directes sans appel à propositions présentées par les États membres.

En ce qui concerne les mesures de soutien à l'assistance mutuelle prévues par l'article 18 du règlement (EU) .../...⁺, 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."

- 7) Les annexes I et II sont modifiées conformément à l'annexe du présent règlement.

Article 23

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées dans le présent article.
2. Le pouvoir d'adopter des actes délégués visé à l'article 14, paragraphe 7, est conféré à la Commission pour une période de cinq ans renouvelable à compter du ... [*date de l'entrée en vigueur du présent règlement*]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

⁺ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 94/24 (2023/0109 (COD)).

3. La délégation de pouvoir visée à l'article 14, paragraphe 7, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.
4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer".
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.
6. Un acte délégué adopté en vertu de l'article 14, paragraphe 7, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 24

Comité

1. La Commission est assistée par le comité de coordination du programme pour une Europe numérique visé à l'article 31, paragraphe 1, du règlement (UE) 2021/694. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Article 25

Évaluation et réexamen

1. Au plus tard le ... [*deux ans à compter de la date d'entrée en vigueur du présent règlement*] et au moins tous les quatre ans par la suite, la Commission évalue le fonctionnement des mesures prévues par le présent règlement et présente un rapport au Parlement européen et au Conseil.

2. L'évaluation visée au paragraphe 1 porte notamment sur:

- a) le nombre de cyberpôles nationaux et de cyberpôles transfrontières établis, l'étendue des informations partagées, y compris, si possible, les effets du partage sur les travaux du réseau des CSIRT, et la mesure dans laquelle lesdites mesures ont contribué au renforcement de la détection et de l'appréciation de la situation communes au niveau de l'Union concernant les cybermenaces et les incidents, ainsi qu'au développement de technologies de pointe, l'utilisation de fonds du programme pour une Europe numérique en vue de l'acquisition conjointe d'outils, d'infrastructures ou de services de cybersécurité, et, si cette information est disponible, le niveau de coopération entre les cyberpôles nationaux et les communautés sectorielles et transsectorielles des entités essentielles et importantes visés à l'article 3 de la directive (UE) 2022/2555;
- b) l'utilisation et l'efficacité des actions entreprises dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité en faveur de la préparation, y compris des formations, de la réaction à des incidents de cybersécurité importants, à des incidents de cybersécurité majeurs et des incidents de cybersécurité assimilés à des incidents majeurs, et du rétablissement initial suite à ceux-ci, y compris l'utilisation de fonds du programme pour une Europe numérique et les enseignements tirés et les recommandations découlant de la mise en œuvre du mécanisme d'urgence dans le domaine de la cybersécurité;

- c) l'utilisation et l'efficacité de la réserve de cybersécurité de l'Union en ce qui concerne le type d'utilisateurs, y compris l'utilisation de fonds du programme pour une Europe numérique, l'adoption des services, y compris le type de ceux-ci, le temps moyen de réponse aux demandes et de déploiement de la réserve de cybersécurité de l'Union, le pourcentage des services convertis en services de préparation liés à la prévention des incidents et à la réaction à ceux-ci et les enseignements tirés et les recommandations découlant de la mise en œuvre de la réserve de cybersécurité de l'Union;
 - d) la contribution du présent règlement au renforcement de la position concurrentielle de l'industrie et des services de l'Union dans l'ensemble de l'économie numérique, y compris les microentreprises et les petites et moyennes entreprises ainsi que les jeunes pousses, et la contribution à l'objectif global de renforcement des compétences et des capacités de la main-d'œuvre en matière de cybersécurité.
3. Sur la base des rapports visés au paragraphe 1, la Commission présente au Parlement et au Conseil, s'il y a lieu, une proposition législative de modification du présent règlement.

Article 26

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 Bruxelles, le

Par le Parlement européen

La présidente

Par le Conseil

Le président/La présidente

ANNEXE

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

- 1) À l'annexe I, la section "Objectif spécifique n° 3 – Cybersécurité et confiance" est remplacé par le texte suivant:

"Objectif spécifique 3 – Cybersécurité et confiance

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

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

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

2. L'extension des capacités technologiques existantes et la mise en réseau des centres de compétence des États membres, en veillant à ce que ces capacités répondent aux besoins du secteur public et de l'industrie, notamment par le biais de produits et services qui renforcent la cybersécurité et la confiance au sein du marché unique numérique.
3. Un large déploiement de solutions de pointe efficaces en matière de cybersécurité et de confiance dans tous les États membres. Ce déploiement comprend notamment le renforcement de la sécurité et de la sûreté des produits, depuis leur conception jusqu'à leur commercialisation.
4. Un soutien comblant le déficit de compétences en matière de cybersécurité, compte tenu de l'équilibre des genres, par exemple en alignant les programmes de compétences en matière de cybersécurité, en les adaptant aux besoins sectoriels spécifiques et en facilitant l'accès à des formations spécialisées ciblées.
5. La promotion de la solidarité entre les États membres en ce qui concerne la préparation et la réaction aux incidents de cybersécurité importants et aux incidents de cybersécurité majeurs par le déploiement de services de cybersécurité par-delà les frontières, y compris un soutien à l'assistance mutuelle entre les autorités publiques et la création d'une réserve de fournisseurs de services de sécurité gérés de confiance au niveau de l'Union."

- 2) À l'annexe II, la section "Objectif spécifique n° 3 – Cybersécurité et confiance" est remplacée par le texte suivant:

"Objectif spécifique 3 – Cybersécurité et confiance

- 3.1. Le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints, y compris dans le cadre du système européen d'alerte en matière de cybersécurité
- 3.2. Le nombre d'utilisateurs et de communautés d'utilisateurs ayant accès à des installations européennes de cybersécurité
- 3.3. Le nombre de mesures d'aide à la préparation et à la réaction aux incidents de cybersécurité dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité".

Une déclaration a été faite en ce qui concerne le présent acte et figure au ... [JO: veuillez insérer la référence au JO: JO C ... du ..., p. ...] et à l'adresse suivante: ... [JO: veuillez insérer le lien vers la déclaration].
