Parlement européen
2019-2024

Commission des affaires étrangères

2023/0109(COD)

27.10.2023

AVIS

de la commission des affaires étrangères

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

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

Rapporteur pour avis: Dragoş Tudorache

PA_Legam

Amendement 1

Proposition de règlement
Considérant 1

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

Amendement 2

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. ***Ce risque va*** au-delà de l'agression militaire de la Russie contre l'Ukraine et ***il est susceptible*** de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes	(2) L'ampleur, la fréquence et les effets des incidents de cybersécurité ne cessent de croître, notamment les attaques de la chaîne d'approvisionnement à des fins de cyberespionnage, d'attaques par rançongiciels ou de perturbation. Ces incidents représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. ***Ces menaces s'avèrent d'autant plus graves depuis le retour de la guerre sur notre continent. Ces risques vont*** au-delà de l'agression militaire de la Russie contre l'Ukraine et ***ils sont susceptibles*** de

qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays.

persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie ***et à la sécurité*** de l'Union, voire mettre en danger la santé ou la vie des personnes ***en compromettant éventuellement des installations liées à la sécurité locale ou nationale***. En outre, les incidents de cybersécurité sont imprévisibles, étant donné qu'ils surviennent et évoluent souvent dans des délais très courts, sans se limiter à une zone géographique déterminée, et qu'ils se produisent simultanément ou se propagent instantanément dans un grand nombre de pays. ***La cybersécurité est importante pour protéger nos valeurs européennes et garantit le fonctionnement de nos démocraties en protégeant nos infrastructures électorales et nos procédures démocratiques de toute ingérence étrangère.***

Amendement 3

Proposition de règlement
Considérant 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(2 bis) La cybersécurité est essentielle pour assurer la sécurité de l'Union et éviter que des acteurs malveillants, étatiques ou non, ne portent atteinte à notre démocratie, à notre économie et à notre sécurité. Il est nécessaire d'éviter un paysage fragmenté, car une telle situation ne serait pas une démarche pertinente, en particulier face au défi d'une éventuelle cyberattaque à grande échelle visant

simultanément plusieurs États membres ou infrastructures critiques transnationales. Par conséquent, il est nécessaire d'établir un organe de l'Union qui ferait office de plateforme de coordination pour tous les instruments, fonds et mécanismes présents et à venir en matière de cybersécurité.

Amendement 4

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité.	(3) Il est nécessaire de consolider la position concurrentielle de l'industrie et des services dans tous les secteurs d'activité passés au numérique dans l'Union et de soutenir leur transformation numérique, en renforçant le niveau de cybersécurité dans le marché unique numérique. Comme le recommandent trois propositions différentes de la conférence sur l'avenir de l'Europe[16], il convient d'accroître la résilience des citoyens, des entreprises et des entités exploitant des infrastructures critiques face aux menaces croissantes en matière de cybersécurité, qui peuvent avoir des conséquences dévastatrices sur la société et l'économie. Il faut donc investir dans des infrastructures et des services qui permettront de détecter les menaces et incidents de cybersécurité et d'y réagir plus rapidement, et aider les États membres à mieux se préparer aux incidents de cybersécurité importants et majeurs et à y réagir. L'Union devrait également augmenter ses capacités dans ces domaines, notamment en matière de collecte et d'analyse des données relatives aux menaces et incidents de cybersécurité***, ainsi que renforcer sa capacité à agir de manière proactive et à réagir de manière décisive face aux menaces et incidents de***

cybersécurité.

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

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

Amendement 5

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.	(4) L'Union a déjà pris un certain nombre de mesures destinées à réduire les vulnérabilités et à accroître la résilience des infrastructures et entités critiques face aux risques liés à la cybersécurité, en particulier dans le cadre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[17], de la recommandation (UE) 2017/1584 de la Commission[18], de la directive 2013/40/UE du Parlement européen et du Conseil[19] et du règlement (UE) 2019/881 du Parlement européen et du Conseil[20]. En outre, la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, ***proactive,*** solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur. ***L'Union a par ailleurs approuvé et lancé en mars 2022 sa boussole stratégique pour la sécurité et la défense, qui met notamment l'accent sur le renforcement de la cybersécurité et l'intensification de la coopération internationale avec les alliés et partenaires démocratiques partageant les mêmes valeurs, en particulier dans ce domaine. En outre, la cybersécurité constitue un point central***

dans la troisième déclaration conjointe sur la coopération UE-OTAN adoptée en janvier 2023. En particulier, le rapport d'évaluation final de l'équipe spéciale UE-OTAN recommandait de tirer pleinement parti des synergies entre l'Union et l'OTAN[1], en favorisant notamment l'échange de bonnes pratiques entre les acteurs civils et militaires en ce qui concerne la mise en œuvre des politiques et de la législation pertinentes en matière de cybersécurité.

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

---

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

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

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

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

---

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

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

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

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

la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Amendement 6

Proposition de règlement
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) La communication conjointe relative à la politique de cyberdéfense de l'UE[22], adoptée le 10 novembre 2022, a annoncé une initiative de l'UE en matière de cybersolidarité dont les objectifs sont les suivants: renforcer les capacités communes de détection, d'appréciation de la situation et de réaction de l'UE en promouvant le déploiement d'une infrastructure de centres d'opérations de sécurité (SOC) de l'UE, constituer progressivement une réserve de cybersécurité au niveau de l'Union comprenant des services de fournisseurs privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'UE.	(6) La communication conjointe relative à la politique de cyberdéfense de l'UE[22], adoptée le 10 novembre 2022, a annoncé une initiative de l'UE en matière de cybersolidarité dont les objectifs sont les suivants: renforcer les capacités communes de détection, d'appréciation de la situation et de réaction de l'UE en promouvant le déploiement d'une infrastructure de centres d'opérations de sécurité (SOC) de l'UE, constituer progressivement une réserve de cybersécurité au niveau de l'Union comprenant des services de fournisseurs privés de confiance, et soumettre les entités critiques à des tests de détection d'éventuelles vulnérabilités sur la base d'évaluations des risques de l'UE. ***En outre, l'évolution rapide du panorama des cybermenaces et la rapidité du progrès technologique démontrent également la nécessité d'une coordination et d'une coopération civilo-militaires renforcées, comme l'a souligné le Conseil dans ses conclusions sur la politique de cyberdéfense de l'UE[1].***
	[1] Conclusions du Conseil sur la politique de cyberdéfense de l'UE, approuvées par le Conseil lors de sa session du 22 mai 2023 (9618/23).

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

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

Amendement 7

Proposition de règlement
Considérant 6 bis (nouveau)

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

Amendement 8

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des menaces et incidents de cybersécurité dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités de réaction des États membres et de l'UE en cas d'incidents de cybersécurité importants et	(7) Il est nécessaire de renforcer la détection et l'appréciation de la situation des menaces et incidents de cybersécurité dans l'ensemble de l'Union ainsi que d'accroître la solidarité en améliorant la préparation et les capacités de réaction des États membres et de l'UE en cas d'incidents de cybersécurité importants et

majeurs. Par conséquent, il convient d'établir: une infrastructure paneuropéenne composée de SOC (le cyberbouclier européen), afin de mettre en place et de renforcer les capacités communes en matière de détection et d'appréciation de la situation; un mécanisme d'urgence dans le domaine de la cybersécurité, afin d'aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs et à y réagir, ainsi qu'à se rétablir immédiatement après de tels incidents; et un mécanisme d'analyse des incidents de cybersécurité, afin d'examiner et d'évaluer des incidents importants ou majeurs particuliers. Ces actions doivent s'entendre sans préjudice des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne (TFUE).

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

Amendement 9

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Aux fins de la bonne gestion financière, il convient d'établir des règles spécifiques portant sur le report des crédits d'engagement et de paiement non utilisés. Tout en respectant le principe en vertu duquel le budget de l'Union est établi sur une base annuelle, il convient que le présent règlement prévoie, compte tenu de la nature imprévisible, exceptionnelle et	(11) Aux fins de la bonne gestion financière, il convient d'établir des règles spécifiques portant sur le report des crédits d'engagement et de paiement non utilisés. Tout en respectant le principe en vertu duquel le budget de l'Union est établi sur une base annuelle, il convient que le présent règlement prévoie, compte tenu de la nature imprévisible, exceptionnelle et

spécifique de la situation en matière de cybersécurité, des possibilités de reporter des fonds non utilisés qui aillent au-delà de celles établies dans le règlement financier, afin d'optimiser la capacité du mécanisme d'urgence dans le domaine de la cybersécurité à aider les États membres à contrer efficacement les cybermenaces.

spécifique de la situation en matière de cybersécurité, des possibilités de reporter des fonds non utilisés qui aillent au-delà de celles établies dans le règlement financier, afin d'optimiser la capacité du mécanisme d'urgence dans le domaine de la cybersécurité à aider les États membres à contrer efficacement les cybermenaces. ***Ces règles spécifiques permettraient également de fournir un soutien financier à plus long terme aux fins d'une acquisition conjointe d'outils et d'infrastructures ultrasécurisés de nouvelle génération, afin d'améliorer les capacités collectives de détection en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données.***

Amendement 10

Proposition de règlement
Considérant 13

Texte proposé par la Commission	*Amendement*
(13) Chaque État membre devrait désigner un organisme public au niveau national chargé de coordonner les activités de détection des cybermenaces sur son territoire. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle.	(13) Chaque État membre devrait désigner un organisme public au niveau national chargé de coordonner les activités de détection des cybermenaces sur son territoire. Ces SOC nationaux devraient servir de point de référence et d'accès au niveau national pour la participation au cyberbouclier européen et devraient veiller à ce que les informations relatives aux cybermenaces provenant d'entités publiques et privées soient partagées et collectées au niveau national de manière efficace et rationnelle. ***Lorsque cela est possible et nécessaire, les SOC devraient également permettre la participation d'entités de défense, en mettant sur pied un «pilier de défense» en matière de gouvernance et en ce qui concerne le type d'informations transmises, tel que prévu dans la communication conjointe relative à la politique de cyberdéfense de l'UE[1],***

et avec le soutien du haut-représentant.

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

Amendement 11

Proposition de règlement
Considérant 14

Texte proposé par la Commission	*Amendement*
(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres afin de tirer pleinement parti des avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées, ***à*** l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. Ils devraient également apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les centres de réponse aux incidents de sécurité informatique (CSIRT) et sur d'autres acteurs pertinents, et en les complétant.	(14) Dans le cadre du cyberbouclier européen, il convient de créer un certain nombre de centres d'opérations de sécurité transfrontières (ci-après «SOC transfrontières»). Ceux-ci devraient regrouper les SOC nationaux d'au moins trois États membres***, notamment un «pilier en matière de défense»,*** afin de tirer pleinement parti des avantages de la détection des menaces transfrontières ainsi que du partage et de la gestion des informations. L'objectif général des SOC transfrontières devrait être de renforcer les capacités d'analyse, de prévention et de détection des cybermenaces ainsi que de contribuer à l'obtention de renseignements de haute qualité sur les cybermenaces, notamment à l'aide de l'échange de données issues de diverses sources, publiques ou privées ***et***, ***lorsque cela est nécessaire et possible, militaires avec des orientations suffisantes pour le partage d'informations, ainsi qu'à*** l'aide du partage et de l'utilisation conjointe d'outils de pointe, ainsi que du développement conjoint des capacités de détection, d'analyse et de prévention dans un environnement de confiance. Ils devraient également apporter de nouvelles capacités supplémentaires, en s'appuyant sur les SOC existants, sur les centres de réponse aux incidents de sécurité informatique (CSIRT) et sur d'autres acteurs pertinents, et en les complétant.

Amendement 12

Proposition de règlement
Considérant 15

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

Amendement 13

Proposition de règlement
Considérant 16

Texte proposé par la Commission	*Amendement*
(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures ***critiques]***. Les	(16) Les SOC transfrontières devraient servir de point central permettant de regrouper à grande échelle les données pertinentes et les renseignements sur les cybermenaces, et devraient faire en sorte que ces informations soient diffusées à un large éventail diversifié d'acteurs [par exemple les équipes d'intervention en cas d'urgence informatique (CERT), les CSIRT, les centres d'échange et d'analyse d'informations (ISAC) et les opérateurs d'infrastructures ***critiques, ainsi que la***

informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle.	***communauté de cyberdéfense]***. Les informations échangées entre les participants à un SOC transfrontières pourraient comprendre des données issues de réseaux et de capteurs, des flux de renseignements sur les menaces, des indicateurs de compromission et des informations contextualisées sur les incidents, les menaces et les vulnérabilités. En outre, les SOC transfrontières devraient également conclure des accords de coopération mutuelle ***et participer, lorsqu'il sera mis en place, au réseau opérationnel pour les CERT militaires (réseau MICNET)***.

Amendement 14

Proposition de règlement
Considérant 17

Texte proposé par la Commission	*Amendement*
(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa	(17) Une appréciation de la situation commune aux autorités compétentes est un prérequis indispensable à la préparation et à la coordination en matière d'incidents de cybersécurité importants et majeurs à l'échelle de l'Union. La directive (UE) 2022/2555 a institué EU-CyCLONe afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de cybersécurité majeurs, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. La recommandation (UE) 2017/1584 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs porte sur le rôle de tous les acteurs concernés. La directive (UE) 2022/2555 rappelle également les responsabilités qui incombent à la Commission en vertu du mécanisme de protection civile de l'Union (MPCU) institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, ainsi que sa

responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT et à la Commission. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations transmises.

responsabilité de fournir des rapports analytiques pour le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993. Par conséquent, lorsque les SOC transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient transmettre des informations pertinentes à ce propos à EU-CyCLONe, au réseau des CSIRT***, à la communauté de cyberdéfense*** et à la Commission. Selon les cas, ces informations à transmettre devraient comprendre plus particulièrement des informations techniques, des informations sur la nature et les motifs de l'attaquant ou de l'attaquant potentiel, ainsi que des informations non techniques de haut niveau sur tout incident de cybersécurité majeur potentiel ou en cours. Dans ce contexte, il convient de tenir dûment compte du besoin d'en connaître et du caractère potentiellement sensible des informations transmises.

Amendement 15

Proposition de règlement
Considérant 19

Texte proposé par la Commission	*Amendement*
(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des	(19) Aux fins de l'échange des données sur les cybermenaces issues de différentes sources, à grande échelle et dans un environnement de confiance, les entités participant au cyberbouclier européen devraient être dotées d'outils, d'équipements et d'infrastructures de pointe hautement sécurisés***, à l'exclusion des fournisseurs à haut risque de produits critiques comportant des éléments numériques***. Cela devrait permettre d'améliorer les capacités collectives de détection et les avertissements en temps utile destinés aux autorités et entités

données.	concernées, notamment en utilisant les derniers outils de l'intelligence artificielle et d'analyse des données. ***L'IA devrait faire l'objet d'un contrôle humain, et il convient de s'assurer que les personnes qui exercent cette fonction disposent du niveau de connaissance de l'outil, du soutien et de l'autorité nécessaires.***

Amendement 16

Proposition de règlement
Considérant 19 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(19 bis) Conformément au règlement [XX/XXXX (loi sur la cyberrésilience)], les entités qui participent au cyberbouclier européen devraient également satisfaire aux exigences énoncées dans le présent règlement en ce qui concerne tous les produits comportant des éléments numériques. Compte tenu des risques croissants liés aux dépendances économiques, il est nécessaire de réduire au minimum l'exposition aux fournisseurs à haut risque de produits critiques, au moyen d'un cadre stratégique commun pour assurer la sécurité économique de l'Union. La dépendance à l'égard des fournisseurs à haut risque de produits critiques comportant des éléments numériques pose un risque stratégique qui devrait être traité à l'échelle de l'Union, en particulier si un pays se livre à des activités d'espionnage économique ou exerce des pressions économiques et si sa législation impose un accès arbitraire aux opérations ou aux données de l'entreprise de quelque nature qu'elles soient, notamment lorsque les produits critiques sont destinés à être utilisés par les entités essentielles visées dans la directive (UE) nº 2022/2555.

Amendement 17

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer la souveraineté technologique de l'Union. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].	(20) En collectant, en partageant et en échangeant des données, le cyberbouclier européen devrait renforcer la souveraineté technologique de l'Union***, son autonomie stratégique, sa compétitivité et sa résilience***. La mise en commun de données de haute qualité faisant l'objet d'une curation devrait également participer au développement de technologies avancées de l'intelligence artificielle et d'analyse des données. Pour œuvrer en ce sens, il convient de connecter le cyberbouclier européen à l'infrastructure paneuropéenne de calcul à haute performance prévue par le règlement (UE) 2021/1173 du Conseil[25].
[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).	[25] Règlement (UE) 2021/1173 du Conseil du 13 juillet 2021 établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488 (JO L 256 du 19.7.2021, p. 3).

Amendement 18

Proposition de règlement
Considérant 25

Texte proposé par la Commission	*Amendement*
(25) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement immédiat en cas d'incidents de cybersécurité importants et majeurs, tels que les services fournis par l'Agence de l'Union européenne pour la cybersécurité	(25) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait apporter un soutien aux États membres en complément de leurs mesures et leurs ressources, ainsi que d'autres formes de soutien existantes pour la réaction et le rétablissement immédiat en cas d'incidents de cybersécurité importants et majeurs, tels que les services fournis par l'Agence de l'Union européenne pour la cybersécurité

(ENISA) conformément à son mandat, la réaction et l'assistance coordonnée du réseau des CSIRT, les mesures d'atténuation apportées par EU-CyCLONe, et l'assistance mutuelle que se prêtent les États membres notamment au titre de l'article 42, paragraphe 7, du TUE, ainsi que dans le contexte des équipes d'intervention rapide en cas d'incident informatique de la CSP***26*** et des équipes de réaction rapide en cas de menaces hybrides. Ce mécanisme devrait ***faire en sorte*** que des moyens ***spécialisés*** soient mis à disposition pour soutenir la préparation et la réaction aux incidents de cybersécurité dans toute l'Union et dans les pays tiers.

(ENISA) conformément à son mandat, la réaction et l'assistance coordonnée du réseau des CSIRT, les mesures d'atténuation apportées par EU-CyCLONe, et l'assistance mutuelle que se prêtent les États membres notamment au titre de l'article 42, paragraphe 7, du TUE, ainsi que dans le contexte des équipes d'intervention rapide en cas d'incident informatique de la CSP ***[1], du nouveau projet CSP relatif au Centre de coordination dans le domaine du cyber*** et ***de l'information (CIDCC) et du Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC) envisagé pour lui succéder, ainsi que*** des équipes de réaction rapide en cas de menaces hybrides. Ce mécanisme devrait ***permettre*** que des moyens ***spécifiques*** soient mis à disposition pour soutenir la préparation et la réaction aux incidents de cybersécurité dans toute l'Union et dans les pays tiers***, en particulier les pays candidats à l'adhésion à la politique étrangère et de sécurité commune et à la politique de sécurité et de défense commune de l'Union, en les aidant à renforcer leurs capacités cybernétiques et à améliorer la coopération transfrontière et régionale entre ces pays dans le domaine de la cybernétique***.

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

---

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

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

Amendement 19

Proposition de règlement
Considérant 26

Texte proposé par la Commission	*Amendement*
(26) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination de la réaction aux crises au niveau de l'Union, en particulier le MPCU[27], l'IPCR[28], et la directive (UE) 2022/2555. Il pourrait contribuer aux actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du TUE ou dans les situations définies à l'article 222 du TFUE, ou les compléter. Le recours à cet instrument devrait également être coordonné***, s'il y a lieu,*** avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatique.	(26) Le présent instrument est sans préjudice des procédures et des cadres pour la coordination de la réaction aux crises au niveau de l'Union, en particulier le MPCU[27], l'IPCR[28], et la directive (UE) 2022/2555. Il pourrait contribuer aux actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du TUE ou dans les situations définies à l'article 222 du TFUE, ou les compléter. Le recours à cet instrument devrait également être coordonné avec la mise en œuvre des mesures relatives à la boîte à outils cyberdiplomatique***, en consolidant la coopération aux niveaux stratégique, opérationnel et technique entre la communauté de cyberdéfense et les autres cybercommunautés, en particulier afin de renforcer les capacités de lutte contre les menaces de cybersécurité provenant de pays tiers, y compris par des mesures restrictives pouvant être utilisées pour prévenir les actes de cybermalveillance et y répondre***.
[27] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).	[27] Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).
[28] Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) et conformément à la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.	[28] Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) et conformément à la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

Amendement 20

Proposition de règlement
Considérant 28

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

civiles et militaires.

Amendement 21

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Dans le cadre des mesures de préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. Les secteurs ou sous-secteurs devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil	(29) Dans le cadre des mesures de préparation et dans l'optique de promouvoir une approche cohérente et de renforcer la sécurité dans toute l'Union et dans son marché intérieur, il convient d'apporter un soutien aux activités coordonnées de test et d'évaluation de la cybersécurité des entités actives dans les secteurs hautement critiques recensés en application de la directive (UE) 2022/2555. À cette fin, la Commission, avec le soutien de l'ENISA et en collaboration avec le groupe de coopération SRI institué par la directive (UE) 2022/2555, devrait recenser régulièrement les secteurs ou sous-secteurs qui devraient pouvoir bénéficier d'un soutien financier en vue de tests coordonnés au niveau de l'Union. ***Il convient de faire intervenir, s'il y a lieu, le Service européen pour l'action extérieure (SEAE), notamment par l'intermédiaire du Centre de situation et du renseignement de l'UE (IntCen) et de sa cellule de fusion contre*** les ***menaces hybrides, avec le soutien de la direction «Renseignement» de l'état-major de l'Union européenne (EMUE) dans le cadre de la capacité unique d'analyse du renseignement (SIAC), afin de fournir des évaluations à jour et ainsi contribuer au recensement des*** secteurs ou sous-secteurs ***qui*** devraient être sélectionnés à partir de l'annexe I («Secteur hautement critique») de la directive (UE) 2022/2555. Les exercices de tests coordonnés devraient s'appuyer sur des méthodes et des scénarios de risque communs***. Ces exercices devraient également jouer un rôle important dans l'amélioration de la***

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

coopération entre les entités civiles et militaires. Lorsqu'ils organisent des exercices, la Commission, le SEAE et l'ENISA devraient donc systématiquement envisager la participation de représentants d'autres cybercommunautés, telles que l'Agence européenne de défense (AED) et d'autres entités concernées. La sélection de secteurs et l'élaboration de scénarios de risque devraient prendre en compte les évaluations des risques et les scénarios de risque pertinents à l'échelle de l'UE, notamment pour éviter des doubles emplois. Par cela, on entend par exemple: l'évaluation des risques et les scénarios de risque que doivent mener la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau EU-CyCLONe, conformément aux conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne; l'évaluation des risques relatifs aux réseaux et infrastructures de communication demandée par l'appel ministériel conjoint de Nevers et réalisée par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE); l'évaluation coordonnée des risques qui doit être effectuée au titre de l'article 22 de la directive (UE) 2022/2555; et les tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du Parlement européen et du Conseil ***[1]***. La sélection des secteurs devrait également tenir compte de la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques.

[1] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du

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

Amendement 22

Proposition de règlement
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir les États membres lorsqu'ils apportent une assistance à un État membre touché par un incident de cybersécurité important ou majeur, y compris l'assistance fournie par le réseau des CSIRT en vertu de l'article 15 de la directive (UE) 2022/2555. Les États membres apportant une assistance devraient être en mesure de demander que les coûts liés à l'envoi d'équipes d'experts dans le cadre de l'assistance mutuelle soient couverts. Les coûts éligibles pourraient inclure les frais de déplacement et de logement ainsi que les indemnités journalières des experts en cybersécurité.	(32) Le mécanisme d'urgence dans le domaine de la cybersécurité devrait soutenir les États membres lorsqu'ils apportent une assistance à un État membre touché par un incident de cybersécurité important ou majeur, y compris l'assistance fournie par le réseau des CSIRT en vertu de l'article 15 de la directive (UE) 2022/2555. Les États membres apportant une assistance devraient être en mesure de demander que les coûts liés à l'envoi d'équipes d'experts dans le cadre de l'assistance mutuelle soient couverts***, en assurant une coordination efficace entre les programmes et instruments pertinents de l'Union, notamment la facilité européenne pour la paix (FEP), la politique étrangère et de sécurité commune (PESC) et l'instrument de voisinage, de coopération au développement et de coopération internationale, dans le cadre de l'assistance aux pays tiers, en particulier***

l'Ukraine et la Moldavie. Les coûts éligibles pourraient inclure les frais de déplacement et de logement ainsi que les indemnités journalières des experts en cybersécurité.

Amendement 23

Proposition de règlement
Considérant 33

Texte proposé par la Commission	*Amendement*
(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, dans des conditions similaires.	(33) Une réserve de cybersécurité au niveau de l'Union devrait être mise en place progressivement. Elle devrait comprendre des services de fournisseurs de services de sécurité gérés visant à soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants ou majeurs. La réserve de cybersécurité de l'UE devrait veiller à la disponibilité et à l'état de préparation de ces services. Les services en question devraient permettre d'aider les autorités nationales à apporter une assistance aux entités touchées actives dans des secteurs critiques ou hautement critiques, en complément des mesures prises par ces autorités au niveau national. Lorsqu'un État membre demande l'aide de la réserve de cybersécurité de l'UE, il devrait préciser de quel soutien bénéficie l'entité touchée au niveau national, soutien qu'il convient de prendre en compte lors de l'examen de la demande de l'État membre. Les services de la réserve de cybersécurité de l'UE devraient également servir à aider les institutions, organes ou organismes de l'Union, ***y compris les missions PSDC,*** dans des conditions similaires.

Amendement 24

Proposition de règlement
Considérant 34

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

Amendement 25

Proposition de règlement
Considérant 36

Texte proposé par la Commission	*Amendement*
(36) Dans le droit fil des objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents importants et majeurs poursuivis par le présent règlement, EU-CyCLONe, le réseau des CSIRT ou la Commission devraient être en mesure de demander à l'ENISA d'analyser et d'évaluer les menaces, vulnérabilités et mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique. Après l'analyse et l'évaluation d'un incident, l'ENISA devrait établir un rapport d'analyse, en collaboration avec les parties prenantes concernées, notamment les représentants du secteur privé, les États membres, la Commission ainsi que les autres institutions, organes ou organismes de	(36) Dans le droit fil des objectifs de promotion d'une appréciation commune de la situation, de renforcement de la résilience de l'Union et de réaction efficace aux incidents importants et majeurs poursuivis par le présent règlement, EU-CyCLONe, le réseau des CSIRT ou la Commission devraient être en mesure de demander à l'ENISA d'analyser et d'évaluer les menaces, vulnérabilités et mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique. ***En vue du développement d'un système de connectivité sécurisé s'appuyant sur l'infrastructure européenne de communication quantique (EuroQCI) et le programme de communication gouvernementale par satellite de l'Union européenne (Govsatcom), et notamment***

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

sur le déploiement du GALILEO GNSS pour les utilisateurs dans le domaine de la défense, tout développement futur devrait tenir compte de l'avènement de «l'hyperguerre», qui combine la vitesse et la complexité de l'informatique quantique avec des systèmes militaires hautement autonomes. Après l'analyse et l'évaluation d'un incident, l'ENISA devrait établir un rapport d'analyse, en collaboration avec les parties prenantes concernées, notamment les représentants du secteur privé, les États membres, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En ce qui concerne le secteur privé, l'ENISA met en place des canaux d'échange d'informations avec des fournisseurs spécialisés, notamment des fournisseurs de solutions de sécurité gérées et des vendeurs, afin de contribuer à sa mission, qui consiste à atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. En s'appuyant sur la collaboration avec les parties prenantes, y compris avec le secteur privé, les rapports d'analyse portant sur des incidents spécifiques devraient servir à évaluer les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits. Il convient d'accorder une attention particulière aux informations et aux enseignements transmis par les fournisseurs de services de sécurité gérés qui font preuve du plus haut niveau d'intégrité professionnelle, d'impartialité et d'expertise technique requise, comme l'exige le présent règlement. Le rapport devrait être communiqué à EU-CyCLONe, au réseau des CSIRT et à la Commission, et devrait être intégré à leurs travaux. Lorsque l'incident en question touche un pays tiers, la Commission devrait également transmettre le rapport au haut représentant***, au SEAE et aux missions PSDC dans le pays touché par l'incident, par l'intermédiaire de leur siège***.

Amendement 26

Proposition de règlement
Considérant 37

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

Amendement 27

Proposition de règlement
Article 1 – paragraphe 1 – point c

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

Amendement 28

Proposition de règlement
Article 1 – paragraphe 2 – point a

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

Amendement 29

Proposition de règlement
Article 1 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe	b) améliorer la préparation des entités actives dans des secteurs critiques et hautement critiques dans l'ensemble de l'Union et renforcer la solidarité en développant des capacités de réaction communes face aux incidents de cybersécurité importants ou majeurs, y compris en permettant aux pays tiers associés au programme pour une Europe

numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité;	numérique de bénéficier du soutien prévu par l'Union en ce qui concerne la réaction aux incidents de cybersécurité***, ou aux pays tiers qui sont candidats à l'adhésion à l'Union et ne portent pas atteinte aux intérêts de sécurité et de défense de l'Union et de ses États membres, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE; Les États membres devraient envisager d'intégrer à leur stratégie nationale de cybersécurité un programme de cyberdéfense active assorti d'exercices d'entraînement communs entre les États membres et les organisations internationales. Un tel programme devrait permettre de détecter, d'analyser et d'atténuer les menaces de manière synchronisée et en temps réel.***

Amendement 30

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

Texte proposé par la Commission	*Amendement*
	2 bis. réduire les risques systémiques en matière de cybersécurité liés à la dépendance à l'égard des équipements critiques provenant de pays qui porteraient atteinte aux intérêts de l'Union et de ses États membres en matière de sécurité et de défense, tels qu'établis dans le cadre de la PESC en vertu du titre V du traité UE;

Amendement 31

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

Texte proposé par la Commission	*Amendement*
	«communauté de cyberdéfense»: les autorités de défense des États membres, soutenues par les institutions, organes et organismes de l'Union, telle que définie

dans la communication conjointe sur la politique de cyberdéfense de l'UE[1].

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

Amendement 32

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

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

Amendement 33

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

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

Amendement 34

Proposition de règlement
Article 4 – paragraphe 1 – alinéa 2

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

Amendement 35

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux sont sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.	2. À la suite d'un appel à manifestation d'intérêt, les SOC nationaux sont sélectionnés par le Centre de compétences européen en matière de cybersécurité (ECCC) pour participer à une acquisition conjointe d'outils et d'infrastructures avec ce Centre. L'ECCC peut octroyer aux SOC nationaux sélectionnés des subventions destinées à financer le fonctionnement de ces outils et infrastructures***, à la stricte condition que ces outils et infrastructures soient fournis par des fournisseurs de confiance, conformément à l'article 16***. La contribution financière de l'Union couvre jusqu'à 50 % des coûts d'acquisition des outils et infrastructures et jusqu'à 50 % des coûts opérationnels, les coûts restants devant être couverts par l'État membre. Avant de lancer la procédure d'acquisition des outils et infrastructures, le Centre de compétences et le SOC national concluent une convention d'hébergement et d'utilisation qui régit l'utilisation des outils et infrastructures.

Amendement 36

Proposition de règlement
Article 5 – paragraphe 2

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

Amendement 37

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

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

Amendement 38

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

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

Amendement 39

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

Texte proposé par la Commission	*Amendement*
	b ter) contribue au renforcement des capacités de défense des membres participants ou permet de prévenir une menace directe et imminente à leur sécurité, en garantissant la sécurité des chaînes d'approvisionnement, au regard notamment des entités qui sont en bas de cette chaîne et qui n'ont pas besoin

d'accéder à des informations classifiées, mais qui pourraient exposer l'ensemble du secteur à des risques importants.

Amendement 40

Proposition de règlement
Article 7 – paragraphe 1

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

Amendement 41

Proposition de règlement
Article 8 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé de sécurité des données et de sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, y compris ***celle*** des données échangées par l'intermédiaire de l'infrastructure.	1. Les États membres participant au cyberbouclier européen garantissent un niveau élevé de sécurité des données et de sécurité physique de l'infrastructure du cyberbouclier européen et ils veillent à ce que l'infrastructure soit gérée et contrôlée de manière adéquate de sorte qu'il soit possible de la protéger contre les menaces et d'assurer sa sécurité et celle des systèmes, ***de réduire les risques et de promouvoir l'avantage technologique de l'Union dans les secteurs critiques,*** y compris ***des mesures visant à limiter ou à interdire les fournisseurs à haut risque, ainsi qu'à protéger la sécurité*** des données échangées par l'intermédiaire de

l'infrastructure.

Amendement 42

Proposition de règlement
Article 8 – paragraphe 2

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

Amendement 43

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires.	3. La Commission peut adopter des actes d'exécution établissant des exigences techniques applicables aux États membres afin que ceux-ci se conforment à l'obligation qui leur incombe en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 21, paragraphe 2, du présent règlement. Ce faisant, la Commission, avec le soutien du haut représentant, tient compte des normes de sécurité au niveau de la défense pertinentes, afin de faciliter la coopération avec les acteurs militaires***, en recourant de façon appropriée à l'ensemble des options de défense à la disposition des communautés civiles et militaires à des fins plus larges de sécurité et de défense***

	de l'Union, et elle en informe le Parlement.

Amendement 44

Proposition de règlement
Article 9 – paragraphe 2

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

Amendement 45

Proposition de règlement
Article 10 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union;	a) les mesures de préparation, y compris les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques, ***tels que les infrastructures publiques, les infrastructures électorales, les transports, les soins de santé, les services financiers, les télécommunications, l'approvisionnement alimentaire et la sécurité*** dans l'ensemble de l'Union;

Amendement 46

Proposition de règlement
Article 10 – paragraphe 1 – point c

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

Amendement 47

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

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

Amendement 48

Proposition de règlement
Article 11 – paragraphe 2

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

Amendement 49

Proposition de règlement
Article 12 – paragraphe 2

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

Amendement 50

Proposition de règlement
Article 12 – paragraphe 3– point b

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

Amendement 51

Proposition de règlement
Article 12 – paragraphe 4

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

sécurité, ou de fournir une assistance à cet effet et de favoriser le rétablissement immédiat.

Amendement 52

Proposition de règlement
Article 12 – paragraphe 5

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

Amendement 53

Proposition de règlement
Article 12 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA établit une autre carte similaire, après consultation de la Commission, afin	7. Afin d'aider la Commission à mettre en place la réserve de cybersécurité de l'UE, l'ENISA élabore une cartographie des services nécessaires, après consultation des États membres et de la Commission. L'ENISA***, soutenue par le SEAE,*** établit une autre carte similaire, après consultation

de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.	de la Commission, afin de recenser les besoins des pays tiers pouvant bénéficier d'une aide de la réserve de cybersécurité de l'UE en vertu de l'article 17. Le cas échéant, la Commission consulte le haut représentant.

Amendement 54

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

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

Amendement 55

Proposition de règlement
Article 15 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique. Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne.	3. En consultation avec le haut représentant, le soutien apporté au titre du mécanisme d'urgence dans le domaine de la cybersécurité peut compléter l'assistance fournie dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune, y compris par l'intermédiaire des équipes d'intervention rapide en cas d'incident informatique ***(CRRT), afin de mieux soutenir les États membres de l'Union, les missions et les opérations au titre de la PSDC ainsi que les pays tiers qui se sont alignés sur la politique étrangère et de sécurité commune et la politique de sécurité et de défense commune de l'Union dans le cadre de leurs efforts de renforcement des capacités de cyberdéfense, en particulier l'Ukraine et la Moldavie***. Il peut également s'ajouter ou contribuer à l'assistance fournie par un État membre à un autre dans le cadre de l'article 42,

paragraphe 7, du traité sur l'Union européenne.

Amendement 56

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

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

Amendement 57

Proposition de règlement
Article 16 – paragraphe 2 – point f

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

Amendement 58

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

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

Amendement 59

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

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

Amendement 60

Proposition de règlement
Article 17 – paragraphe 1

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

Amendement 61

Proposition de règlement
Article 17 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'aide apportée par la réserve de cybersécurité de l'Union est conforme au présent règlement et respecte toutes les conditions spécifiques énoncées dans les	2. L'aide apportée par la réserve de cybersécurité de l'Union est conforme au présent règlement et respecte toutes les conditions spécifiques énoncées dans les

accords d'association visés au paragraphe 1.	accords d'association visés au paragraphe 1***, excepté pour les pays tiers couverts par les dispositions énoncées au paragraphe 1, point b)***.

Amendement 62

Proposition de règlement
Article 18 – paragraphe 1

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

Amendement 63

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

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

Amendement 64

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

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

Amendement 65

Proposition de règlement
Article 20

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

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

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

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION SAISIE POUR AVIS

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

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

0	0

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