Parlement européen
2019-2024

Commission des affaires étrangères

2020/0359(COD)

15.7.2021

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 directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148
2020/0359(COD))

Rapporteure pour avis: Markéta Gregorová

PA_Legam

AMENDEMENTS

La commission des affaires étrangères invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les amendements suivants:

Amendement 1

Proposition de directive
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) Depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés concernant l'amélioration du niveau de cyber-résilience de l'Union. Le réexamen de cette directive a montré qu'elle avait joué le rôle de catalyseur dans l'approche institutionnelle et réglementaire de la cybersécurité dans l'Union, ouvrant la voie à une évolution importante des mentalités. Cette directive a veillé à ce que les cadres nationaux soient achevés en définissant des stratégies nationales en matière de cybersécurité, en créant des capacités nationales et en mettant en œuvre des mesures réglementaires couvrant les infrastructures et les acteurs essentiels recensés par chacun des États membres. Elle a également contribué à la coopération au niveau de l'Union par la création du groupe de coopération[12] et du réseau des centres de réponse aux incidents de sécurité informatique (ci-après le «réseau des CSIRT»)[13]. En dépit de ces accomplissements, le réexamen de la directive (UE) 2016/1148 a montré que certaines insuffisances intrinsèques l'empêchaient de répondre efficacement aux défis actuels et émergents liés à la cybersécurité.	(2) Depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés concernant l'amélioration du niveau de cyber-résilience de l'Union. Le réexamen de cette directive a montré qu'elle avait joué le rôle de catalyseur dans l'approche institutionnelle et réglementaire de la cybersécurité dans l'Union, ouvrant la voie à une évolution importante des mentalités. Cette directive a veillé à ce que les cadres nationaux soient achevés en définissant des stratégies nationales en matière de cybersécurité, en créant des capacités nationales et en mettant en œuvre des mesures réglementaires couvrant les infrastructures et les acteurs essentiels recensés par chacun des États membres. Elle a également contribué à la coopération au niveau de l'Union par la création du groupe de coopération[12] et du réseau des centres de réponse aux incidents de sécurité informatique (ci-après le «réseau des CSIRT»)[13]***. La directive (UE) 2016/1148, premier acte législatif de l'Union sur la cybersécurité, prévoit des mesures juridiques pour renforcer le niveau global de cyber-résilience, y compris dans le domaine de la sécurité et de la défense de l'Union, en garantissant la coopération des États membres et une culture de la sécurité dans tous les secteurs***. En dépit de ces accomplissements, le réexamen de la directive (UE) 2016/1148 a montré que

certaines insuffisances intrinsèques l'empêchaient de répondre efficacement aux défis actuels et émergents liés à la cybersécurité***, lesquels ont très souvent une origine extérieure à l'Union, ce qui représente une grave menace pour la sécurité intérieure et extérieure au niveau de l'Union***.

[12] Article 11 de la directive (UE) 2016/1148.

[13] Article 12 de la directive (UE) 2016/1148.

[12] Article 11 de la directive (UE) 2016/1148.

[13] Article 12 de la directive (UE) 2016/1148.

Amendement 2

Proposition de directive
Considérant 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(3 bis) Pour l'Union, les campagnes hybrides «sont multidimensionnelles: combinant des mesures coercitives et des mesures subversives, elles utilisent des outils et des tactiques aussi bien conventionnels que non conventionnels (diplomatiques, militaires, économiques et technologiques) pour déstabiliser l'adversaire. Elles sont conçues de manière à être difficiles à détecter ou à "attribuer" et sont mises en œuvre aussi bien par des acteurs étatiques que non étatiques»[1a]. Grâce à l'internet et aux réseaux en ligne, les acteurs étatiques et non étatiques disposent de nouveaux moyens pour mener des actions agressives. Ceux-ci peuvent être utilisés pour pirater des infrastructures critiques et des processus démocratiques, lancer des campagnes de désinformation et de propagande convaincantes, voler des données et divulguer des données sensibles. Dans le pire des cas, les cyberattaques permettent à un adversaire de prendre le contrôle de ressources telles que des systèmes militaires et des

structures de commandement[1b]. Dans le même temps, un dispositif solide de coopération avec le secteur privé et les parties prenantes civiles, y compris les industries et les entités participant à la gestion des infrastructures critiques, est essentiel, et il convient de le renforcer compte tenu des caractéristiques intrinsèques du cyberespace, dans lequel l'innovation technologique est principalement portée par des entreprises privées qui ne sont souvent pas actives dans le domaine militaire; Ces incidents et crises de cybersécurité de grande ampleur au niveau de l'Union devraient être correctement préparés et protégés par des exercices de formation conjoints, étant donné qu'ils sont susceptibles d'invoquer l'article 222 du TFUE (la «clause de solidarité»).

_____

[1a] Commission européenne/haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, communication conjointe au Parlement européen, au Conseil européen et au Conseil, «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides», JOIN(2018) 16 final, Brussels, 13.6.2018, p. 1.

[1b]

https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Amendement 3

Proposition de directive
Considérant 3 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(3 ter) Les incidents et crises de cybersécurité majeurs au niveau de l'Union exigent, du fait de la forte interdépendance entre les secteurs et les pays, une action coordonnée pour garantir une réaction rapide et efficace,

ainsi qu'une amélioration de la prévention et de la préparation pour faire face à des situations similaires à l'avenir. La cyber-résilience des réseaux et des systèmes d'information ainsi que la disponibilité, la confidentialité et l'intégrité des données sont indispensables pour garantir la sécurité de l'Union, à l'intérieur comme à l'extérieur de ses frontières. L'ambition de l'Union de jouer un rôle géopolitique plus important repose aussi sur des capacités de cyberdéfense et de dissuasion crédibles, y compris sur la capacité à détecter des actes malveillants de manière effective et en temps opportun ainsi qu'à y répondre de manière appropriée. 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. Il en va de même pour les opérations et missions menées par l'Union dans le cadre de la politique de sécurité et de défense commune (PSDC) afin d'assurer la paix et la stabilité dans son voisinage et au-delà. À cet égard, les orientations stratégiques sur la sécurité et la défense de l'Union devraient renforcer et guider la mise en œuvre de l'ambition de l'Union dans le domaine de la sécurité et de la défense, et traduire cette ambition en besoins capacitaires dans le domaine de la cyberdéfense, renforçant ainsi la capacité de l'Union et des États membres à prévenir, décourager et dissuader les actes de cybermalveillance, à y répondre et à s'en remettre, en renforçant sa posture, sa connaissance de la situation, ses outils, ses procédures et ses partenariats. La coopération de l'Union avec des organisations internationales telles que l'OTAN contribue aux discussions sur les moyens de prévenir et de décourager les attaques hybrides et les cyberattaques et d'y réagir, et d'étudier les moyens de mettre en place une analyse commune des

cybermenaces.

Amendement 4

Proposition de directive
Considérant 6

Texte proposé par la Commission	*Amendement*
(6) La présente directive ne modifie pas la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité, assurer l'action publique et la sécurité publique et permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. À cet égard, les règles nationales et européennes visant à protéger les informations classifiées, les accords de non-divulgation et les accords informels de non-divulgation, tels que le protocole d'échange d'information «Traffic Light Protocol»[14], sont pertinentes.	(6) La présente directive ne modifie pas la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité, assurer l'action publique et la sécurité publique et permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union ***et des droits fondamentaux. Indépendamment de l'environnement technologique, il est essentiel de veiller au respect plein et entier de la légalité et d'autres garanties, en particulier les droits fondamentaux, tels que le droit au respect de la vie privée et de la confidentialité des communications ainsi que le droit à la protection des données à caractère personnel. De même, afin d'assurer une résilience globale, il est nécessaire non seulement de renforcer les infrastructures technologiques et de posséder des capacités de réaction, mais aussi de sensibiliser le public aux risques et à la sécurité informatiques.*** Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. À cet égard, les règles nationales et européennes visant à protéger les informations classifiées, les accords de non-divulgation et les accords informels de non-divulgation, tels que le protocole d'échange d'information «Traffic Light Protocol»[14], sont pertinentes.
[14] Le protocole «Traffic Light Protocol»	[14] Le protocole «Traffic Light Protocol»

permet à une personne partageant des informations d'indiquer à son public des limitations applicables à la diffusion plus large de ces informations: il est utilisé par la quasi-totalité des communautés des CSIRT et par certains centres d'échange et d'analyse d'informations (ISAC).	permet à une personne partageant des informations d'indiquer à son public des limitations applicables à la diffusion plus large de ces informations: il est utilisé par la quasi-totalité des communautés des CSIRT et par certains centres d'échange et d'analyse d'informations (ISAC).

Amendement 5

Proposition de directive
Considérant 14 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(14 bis) En vue de mettre en place un système de connectivité sécurisé et de s'appuyer sur l'infrastructure européenne de communication quantique (EuroQCI) et le programme de communication gouvernementale par satellite de l'Union européenne (Govsatcom), et notamment du déploiement du GNSS GALILEO pour les utilisateurs dans le domaine de la défense, lorsque le développement futur devrait tenir compte, entre autres, de l'incidence de la fusion de la vitesse et de la complexité de l'informatique quantique avec des systèmes militaires hautement autonomes, les États membres devraient veiller à la protection de l'ensemble des infrastructures de communications électroniques, telles que les systèmes de réseaux spatiaux, terrestres et sous-marins. Dans le même temps, il convient d'établir une vision commune de la stratégie d'adoption de l'informatique en nuage pour les secteurs sensibles, dans le but de définir une approche de l'Union fondée sur des normes communes entre pays partenaires partageant les mêmes valeurs.

Amendement 6

Proposition de directive
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.	(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. ***Les infrastructures qui sont détenues, gérées ou exploitées par l'Union ou en son nom dans le cadre de ses programmes spatiaux sont particulièrement importantes pour la sécurité de l'Union et de ses États membres et pour le bon fonctionnement des missions relevant de la PSDC. Ces infrastructures doivent bénéficier d'une protection adéquate conformément au règlement (UE) 2021/696 du Parlement européen et du Conseil***[18a]. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur ***et menaçant la sécurité des citoyens de l'Union***. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.
	[18a] Règlement (UE) 2021/696 du Parlement européen et du Conseil du

28 avril 2021 établissant le programme spatial de l'Union et l'Agence de l'Union européenne pour le programme spatial et abrogeant les règlements (UE) nº 912/2010, (UE) nº 1285/2013 et (UE) nº 377/2014 et la décision nº 541/2014/UE (JO L 170 du 12.5.2021, p. 69).

Amendement 7

Proposition de directive
Considérant 26

Texte proposé par la Commission	*Amendement*
(26) Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive.	(26) Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive***, afin de contribuer à l'élaboration de normes de l'Union susceptibles de façonner le paysage de la cybersécurité à l'échelle internationale. Les États membres pourraient également étudier la possibilité de renforcer la coopération avec des pays partenaires partageant les mêmes valeurs et des organisations internationales telles que le Conseil de l'Europe, l'Organisation du traité de l'Atlantique Nord, l'Organisation de coopération et de développement économiques, l'Organisation pour la sécurité et la coopération en Europe et les Nations unies, en vue de parvenir à des accords multilatéraux sur les normes en matière de cybersécurité, le comportement responsable des États et des acteurs non étatiques dans le cyberespace et une gouvernance numérique mondiale efficace, ainsi que de créer un cyberespace ouvert, libre, stable et sûr fondé sur le droit international.***

Amendement 8

Proposition de directive

Considérant 27

Texte proposé par la Commission	*Amendement*
(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»)[20], un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union.	(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»)[20], un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur ***ou menaçant la sécurité des citoyens ainsi que les intérêts économiques et financiers de l'Union***. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union. ***L'Union et les États membres devraient également encourager davantage les exercices de simulation et les discussions fondées sur des scénarios en matière de gestion de crise afin de garantir la cohérence des politiques intérieures et extérieures et de parvenir à une conception commune des procédures de mise en œuvre de la clause de solidarité.***
[20] 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).	[20] 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).

Amendement 9

Proposition de directive

Considérant 36

Texte proposé par la Commission	*Amendement*
(36) L'Union devrait, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération et du réseau des CSIRT. De tels accords ***devraient*** assurer un niveau suffisant de protection des données.	(36) L'Union devrait, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération et du réseau des CSIRT. De tels accords ***doivent*** assurer un niveau suffisant de protection des données***, et ils devraient promouvoir l'accès au marché, remédier aux risques en matière de sécurité, renforcer la résilience à l'échelon mondial et sensibiliser aux cybermenaces et aux actes de cybermalveillance***. ***L'Union devrait également continuer à soutenir le renforcement des capacités dans les pays tiers. Les États membres devraient, s'il y a lieu, encourager la participation de pays partenaires, qui ont des vues analogues et partagent les valeurs de l'Union, aux projets pertinents de la CSP. Par conséquent, la Commission devrait étudier la possibilité de relancer des processus visant à établir un cadre formel et structuré de coopération dans ce domaine.***

Amendement 10

Proposition de directive
Considérant 37

Texte proposé par la Commission	*Amendement*
(37) Les États membres devraient contribuer à la création du cadre de l'Union européenne pour la réaction aux crises de cybersécurité défini dans la recommandation (UE) 2017/1584 via les réseaux de coopération existants, notamment le réseau européen d'organisations de liaison en cas de crises	(37) Les États membres devraient contribuer à la création du cadre de l'Union européenne pour la réaction aux crises de cybersécurité défini dans la recommandation (UE) 2017/1584 via les réseaux de coopération existants, notamment le réseau européen d'organisations de liaison en cas de crises

de cybersécurité (UE - CyCLONe), le réseau des CSIRT et le groupe de coopération. EU-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération. Le règlement intérieur d'UE-CyCLONe devrait préciser plus en détail les modalités selon lesquelles le réseau devrait fonctionner, y compris, mais sans s'y limiter, les rôles, les modes de coopération, les interactions avec les autres acteurs pertinents et les modèles de partage d'informations, ainsi que les moyens de communication. Pour la gestion des crises au niveau de l'Union, les parties concernées devraient s'appuyer sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR). La Commission devrait avoir recours au processus intersectoriel de premier niveau ARGUS pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la ***politique de sécurité et de défense commune (***PSDC***)***, le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE) devrait être activé.	de cybersécurité (UE - CyCLONe), le réseau des CSIRT et le groupe de coopération***, le Centre européen de lutte contre la cybercriminalité et le Centre de situation et du renseignement de l'UE (INTCEN), afin de développer la coopération stratégique en matière de renseignement sur les cybermenaces et les actes de cybermalveillance pour soutenir l'Union dans l'appréciation de la situation et la prise de décision en vue d'une réponse diplomatique commune***. EU-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération. Le règlement intérieur d'UE-CyCLONe devrait préciser plus en détail les modalités selon lesquelles le réseau devrait fonctionner, y compris, mais sans s'y limiter, les rôles, les modes de coopération, les interactions avec les autres acteurs pertinents et les modèles de partage d'informations, ainsi que les moyens de communication. Pour la gestion des crises au niveau de l'Union, les parties concernées devraient s'appuyer sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR)***, qui favorise également la coordination au niveau politique de la réaction à l'invocation de la clause de solidarité***. La Commission devrait avoir recours au processus intersectoriel de premier niveau ARGUS pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la PSDC, le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE) devrait être activé***, de même que toute mesure visant à protéger les missions et opérations de la PSDC et les délégations de l'Union. En outre, l'Union devrait exploiter pleinement sa boîte à outils cyberdiplomatique.***

Amendement 11

Proposition de directive

Considérant 40 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(40 bis) 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. Ce programme devrait permettre de détecter, d'analyser et d'atténuer les menaces de manière synchronisée et en temps réel. La cyberdéfense active fonctionne à la vitesse du réseau et utilise des capteurs, des logiciels et des renseignements pour détecter et stopper les activités malveillantes, idéalement avant qu'elles n'affectent les réseaux et systèmes. En outre, les États membres devraient améliorer sensiblement la méthode de partage d'information, afin de définir une norme commune de communication qui pourrait être utilisée pour les informations classifiées et non classifiées, afin de renforcer l'intervention rapide. L'Union et les États membres devraient également renforcer leur capacité à imputer des cyberattaques pour une dissuasion efficace et une réaction proportionnée, conformément au droit international.

Amendement 12

Proposition de directive
Considérant 40 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(40 ter) Les États membres devraient proposer un programme de cyberdéfense active dans le cadre de leur stratégie nationale en matière de cybersécurité. La cyberdéfense active est la détection, l'analyse et l'atténuation précoces, en temps réel, d'atteintes à la

sécurité du réseau, associées à l'utilisation de ressources déployées en dehors du réseau attaqué. Elle repose sur une stratégie défensive qui exclut les mesures offensives contre des infrastructures civiles critiques des adversaires, lesquelles seraient contraires au droit international (tel que le protocole additionnel de 1977 aux conventions de Genève). La capacité à partager et à comprendre rapidement et automatiquement les informations et analyses concernant les menaces ainsi que les alertes relatives à des cyberactivités malveillantes et les mesures prises en réaction à celles-ci sont d'une importance vitale pour unir les efforts afin de réussir à détecter et à prévenir les cyberattaques. Les mesures de cyberdéfense active pourraient notamment porter sur la configuration des configurations de serveurs de messagerie électronique, la configuration de sites web, la journalisation et le filtrage par DNS. Les États membres devraient adopter des dispositifs pour garantir l'accès le plus large possible aux outils de cybersécurité les plus performants à l'appui des entreprises, des petites et moyennes entreprises et les entreprises aux moyens financiers limités, par des prestations, des subventions, des prêts ou des avantages fiscaux affectés à l'acquisition de produits et de services de cybersécurité de pointe, afin que le coût de ceux-ci ne soit pas un élément de discrimination. Les États membres devraient également s'efforcer de promouvoir des partenariats avec des établissements universitaires et d'autres instituts de recherche dans l'optique de développer la R-D en matière de cybersécurité afin de mettre au point des technologies, des outils et des savoir-faire communs applicables tant dans le secteur civil que dans le secteur de la défense, grâce à une démarche pluridisciplinaire. Les partenariats devraient être financés par des outils existants aussi bien que par

de nouveaux outils de financement, sous la tutelle de la Commission européenne.

Amendement 13

Proposition de directive
Considérant 43

Texte proposé par la Commission	*Amendement*
(43) Il est tout particulièrement important de répondre aux risques de cybersécurité découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers. Les entités devraient donc évaluer et prendre en compte la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et fournisseurs de services, y compris de leurs procédures de développement sécurisées.	(43) Il est tout particulièrement important de répondre aux risques de cybersécurité découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers. Les entités devraient donc évaluer et prendre en compte la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et fournisseurs de services, y compris ***de leurs systèmes de gestion des risques,*** de leurs procédures de développement sécurisées ***conformément aux normes de cybersécurité de l'Union***.

Amendement 14

Proposition de directive
Considérant 43 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(43 bis) Les éventuels facteurs de risque non techniques, tels que l'influence injustifiée d'un pays tiers sur des fournisseurs et prestataires de services, en particulier dans le cas d'autres modèles de gouvernance, peuvent être des vulnérabilités cachées ou des portes dérobées ou encore d'éventuelles ruptures d'approvisionnement

systémiques, en particulier en cas de verrouillage technologique ou de dépendance à l'égard de fournisseurs. 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 15

Proposition de directive
Considérant 46

Texte proposé par la Commission	*Amendement*
(46) Afin de mieux répondre aux risques principaux liés aux chaînes d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission ***et*** l'ENISA, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21], dans le but	(46) Afin de mieux répondre aux risques principaux liés aux chaînes d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission***,*** l'ENISA ***et le Service européen pour l'action extérieure***, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la

de déterminer, secteur par secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21], dans le but de déterminer, secteur par secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

Amendement 16

Proposition de directive
Considérant 68

Texte proposé par la Commission	*Amendement*
(68) Les entités devraient être encouragées à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données.	(68) Les entités devraient être encouragées à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. ***En outre, les États membres pourraient également étudier la possibilité de nouer le dialogue avec des pays partenaires partageant les mêmes valeurs.*** Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données. ***De même, les États membres devraient aider les autorités compétentes et les CSIRT à mettre en place des programmes gratuits***

	ou accessibles d'assistance, de formation et d'audit en matière de cybersécurité pour les entités qui ne relèvent pas du champ d'application de la présente directive, en particulier les jeunes pousses, les PME et les organisations non gouvernementales (ONG).

Amendement 17

Proposition de directive
Considérant 68 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(68 bis) Étant donné que la cybersécurité revêt une dimension à la fois civile et militaire, l'échange d'informations entre les secteurs (relevant de la défense, du civil, de la répression et de l'action extérieure) devrait également être encouragé. L'unité conjointe de cybersécurité pourrait jouer un rôle important dans la protection de l'Union contre les cyberattaques en aidant les acteurs à établir une compréhension commune du paysage des menaces et à coordonner leur action.

Amendement 18

Proposition de directive
Considérant 73

Texte proposé par la Commission	*Amendement*
(73) Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant	(73) Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant

approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. L'imposition d'une amende administrative n'affecte pas l'exercice d'autres pouvoirs par les autorités compétentes ou l'imposition d'autres sanctions prévues dans les dispositions nationales transposant la présente directive.	approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause***, sans préjudice des objectifs de la présente directive***. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. L'imposition d'une amende administrative n'affecte pas l'exercice d'autres pouvoirs par les autorités compétentes ou l'imposition d'autres sanctions prévues dans les dispositions nationales transposant la présente directive.

Amendement 19

Proposition de directive
Article 5 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
a) une politique traitant de la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités essentielles et importantes pour la fourniture de leurs services;	a) une politique traitant de la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités essentielles et importantes pour la fourniture de leurs services***, sur la base d'une évaluation complète des menaces potentielles pour les chaînes d'approvisionnement***;

Amendement 20

Proposition de directive
Article 5 – paragraphe 2 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) une politique visant à promouvoir l'interopérabilité et le respect de normes communes de l'Union en matière de cybersécurité;

Amendement 21

Proposition de directive
Article 5 – paragraphe 2 – point d

Texte proposé par la Commission	*Amendement*
d) une politique liée au maintien de la disponibilité générale et de l'intégrité du noyau public de l'internet ouvert;	d) une politique liée au maintien de la disponibilité générale et de l'intégrité du noyau public de l'internet ouvert, ***y compris, le cas échéant, la cybersécurité des câbles de communications sous-marins***;

Amendement 22

Proposition de directive
Article 5 – paragraphe 2 – point f

Texte proposé par la Commission	*Amendement*
f) une politique de soutien aux institutions universitaires et de recherche ***visant à développer des*** outils de cybersécurité et à sécuriser les infrastructures de réseau;	f) une politique de soutien aux institutions universitaires et de recherche ***en matière de cybersécurité et de développement d'***outils de cybersécurité et d'infrastructures de réseau sures;

Amendement 23

Proposition de directive
Article 5 – paragraphe 2 – point h

Texte proposé par la Commission	*Amendement*
h) une politique répondant aux besoins spécifiques des PME, en particulier de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux menaces de cybersécurité**.**	h) une politique répondant aux besoins spécifiques ***des jeunes pousses,*** des PME ***et des ONG***, en particulier de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux menaces de cybersécurité***, la réponse aux incidents de cybersécurité et la recherche d'une assistance en matière de cybersécurité;***

Amendement 24

Proposition de directive

Article 5 – paragraphe 2 – point h bis (nouveau)

Texte proposé par la Commission	*Amendement*
	h bis) une politique pour promouvoir l'utilisation et le développement de logiciels ouverts.

Amendement 25

Proposition de directive
Article 6 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Chaque État membre désigne l'un de ses CSIRT visés à l'article 9 comme coordinateur aux fins de la divulgation ***coordonnée*** des vulnérabilités. Le CSIRT désigné doit agir comme intermédiaire de confiance, en facilitant, si nécessaire, les interactions entre l'entité effectuant le signalement et le fabricant ou le fournisseur de produits ou de services TIC. Lorsque la vulnérabilité signalée concerne plusieurs fabricants ou fournisseurs de produits ou services TIC dans l'Union, le CSIRT désigné de chaque État membre concerné coopère avec le réseau CSIRT.	1. Chaque État membre désigne l'un de ses CSIRT visés à l'article 9 comme coordinateur aux fins de la divulgation ***responsable et obligatoire*** des vulnérabilités. Le CSIRT désigné doit agir comme intermédiaire de confiance, en facilitant, si nécessaire, les interactions entre l'entité effectuant le signalement et le fabricant ou le fournisseur de produits ou de services TIC. Lorsque la vulnérabilité signalée concerne plusieurs fabricants ou fournisseurs de produits ou services TIC dans l'Union, le CSIRT désigné de chaque État membre concerné coopère avec le réseau CSIRT.

Amendement 26

Proposition de directive
Article 6 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités. À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer	2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités. À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer

les vulnérabilités présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations sur les vulnérabilités contenues dans le registre. Le registre comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.	les vulnérabilités présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations sur les vulnérabilités contenues dans le registre. ***Conformément à l'article 10, paragraphe 2, les CSIRT facilitent l'accès aux informations sur les vulnérabilités enregistrées dans le registre européen des vulnérabilités et, dans le même temps, apporter un appui en matière d'atténuation des risques, aux entités qui ne relèvent pas du champ d'application de la présente directive, en particulier aux jeunes entreprises, aux PME et aux ONG.*** Le registre comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.

Amendement 27

Proposition de directive
Article 7 – paragraphe 3 – point f

Texte proposé par la Commission	*Amendement*
f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union.	f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union***, y compris au regard des réponses aux demandes au titre de la clause de solidarité***.

Amendement 28

Proposition de directive
Article 7 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les États membres communiquent à la Commission la désignation de leurs autorités compétentes visées au paragraphe 1 et soumettent leurs plans nationaux d'intervention en cas d'incident et de crise de cybersécurité visés au paragraphe 3 dans les trois mois suivant cette désignation et l'adoption de ces plans. Les États membres peuvent exclure certaines informations du plan lorsque et dans la mesure où cela est strictement nécessaire pour préserver la sécurité nationale.	4. Les États membres communiquent à la Commission la désignation de leurs autorités compétentes visées au paragraphe 1 et soumettent leurs plans nationaux d'intervention en cas d'incident et de crise de cybersécurité visés au paragraphe 3 dans les trois mois suivant cette désignation et l'adoption de ces plans. Les États membres peuvent exclure certaines informations du plan lorsque et dans la mesure où cela est strictement nécessaire pour préserver la sécurité nationale. ***En cas d'incident ou de crise de cybersécurité majeur qui implique plus d'un État membre et qui est pertinent à l'échelon de l'Union, des structures de gestion de crise et de gouvernance doivent être mises en place. Ces structures organisent 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.***

Amendement 29

Proposition de directive
Article 9 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Les CSIRT coopèrent et échangent des informations pertinentes avec les institutions nationales chargées du maintien de la sécurité publique, de la défense et de la sécurité nationale.

Amendement 30

Proposition de directive
Article 9 – paragraphe 4 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	4 ter. Les CSIRT coopèrent et, sans préjudice du droit de l'Union, en particulier du règlement (UE) 2016/679, échangent des informations pertinentes sur les cybermenaces, les vulnérabilités, les bonnes pratiques et les normes avec des pays tiers de confiance et des organisations internationales.

Amendement 31

Proposition de directive
Article 9 – paragraphe 4 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	4 quater. Sans préjudice du droit de l'Union, en particulier du règlement (UE) 2016/679, les CSIRT apportent une assistance en matière de cybersécurité aux CSIRT ou à des structures équivalentes dans les pays candidats à l'adhésion à l'Union et aux autres pays tiers des Balkans occidentaux et du partenariat oriental.

Amendement 32

Proposition de directive
Article 10 – paragraphe 2 – point e bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) la mise en place des programmes gratuits ou accessibles d'assistance, de formation et d'audit en matière de cybersécurité pour les entités qui ne relèvent pas du champ d'application de la présente directive, en particulier les jeunes pousses, les PME et les ONG;

Amendement 33

Proposition de directive
Article 11 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une coopération appropriée entre les autorités compétentes et les points de contact uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre.	4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une coopération appropriée entre les autorités compétentes et les points de contact uniques et les services répressifs, les autorités chargées de la protection des données***, les autorités nationales de surveillance de l'intelligence artificielle, les autorités nationales chargées de la gouvernance des données*** et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre.
[39] [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]	[39] [insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]

Amendement 34

Proposition de directive
Article 12 – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3. Le groupe de coopération est composé de représentants des États membres, de la Commission ***et*** de l'ENISA. Le service européen pour l'action extérieure participe aux activités du groupe de coopération en qualité	3. Le groupe de coopération est composé de représentants des États membres, de la Commission***, d'EU–CyCLONe,*** de l'ENISA ***et de l'Agence européenne de défense***. Le service européen pour l'action extérieure participe

d'observateur. Les autorités européennes de surveillance (AES), conformément à l'article 17, paragraphe 5, point c), du règlement (UE) XXXX/XXXX [le règlement sur la résilience opérationnelle numérique du secteur financier], ***peuvent participer*** aux activités du groupe de coopération.	aux activités du groupe de coopération en qualité d'observateur. Les ***autorités nationales de surveillance de l'intelligence artificielle, les autorités nationales chargées de la gouvernance des données et les*** autorités européennes de surveillance (AES), conformément à l'article 17, paragraphe 5, point c), du règlement (UE) XXXX/XXXX [le règlement sur la résilience opérationnelle numérique du secteur financier], ***participent*** aux activités du groupe de coopération.

Amendement 35

Proposition de directive
Article 12 – paragraphe 4 – point e bis (nouveau)

Texte proposé par la Commission	*Amendement*
	e bis) sans préjudice du droit de l'Union, la coopération, l'assistance mutuelle et l'échange de bonnes pratiques et d'informations avec des pays tiers de confiance et des organisations internationales;

Amendement 36

Proposition de directive
Article 13 – paragraphe 3 – point k

Texte proposé par la Commission	*Amendement*
k) la coopération et l'échange d'informations avec les centres d'opérations de sécurité (COS) régionaux et au niveau de l'Union afin d'améliorer la connaissance commune de la situation concernant les incidents et les menaces dans toute l'Union;	k) la coopération et l'échange d'informations avec les centres d'opérations de sécurité (COS) régionaux et au niveau de l'Union ***et, s'il y a lieu, des CERT militaires,*** afin d'améliorer la connaissance commune de la situation concernant les incidents et les menaces dans toute l'Union;

Amendement 37

Proposition de directive
Article 14 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le réseau UE-CyCLONe est composé des représentants de la Commission, de l'ENISA et des autorités des États membres chargées de la gestion des crises désignées conformément à l'article 7. L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations.	2. Le réseau UE-CyCLONe est composé des représentants de la Commission, ***du SEAE,*** de l'ENISA et des autorités des États membres chargées de la gestion des crises désignées conformément à l'article 7. L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations. ***Les autorités nationales chargées de la gestion des crises sont conseillées par un groupe consultatif de la société civile. Pour les incidents ou crises de cybersécurité majeurs au niveau de l'Union qui implique plus d'un État membre, une structure de gestion de crise associant tous les acteurs concernés est mise en place au niveau de l'Union. Cette structure comprend est composée de l'unité conjointe de cybersécurité, de CSIRT, du réseau des CSIRT, du groupe de coordination, de la Commission, du SEAE et de l'ENISA. Elle se charge également de la préparation et de la mise en œuvre des activités liées à l'invocation et à la mise en application de la clause de solidarité.***

Amendement 38

Proposition de directive
Article 14 – paragraphe 3 – point a

Texte proposé par la Commission	*Amendement*
a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs;	a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs***, et d'assurer la liaison avec les agences des États membres chargées de la sécurité intérieure et de la défense territoriale***;

Amendement 39

Proposition de directive
Article 17 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que les membres de l'organe de direction suivent régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer les risques et les pratiques de gestion en matière de cybersécurité et leur incidence sur les activités de l'entité.	2. Les États membres veillent à ce que les membres de l'organe de direction suivent régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer les risques et les pratiques de gestion en matière de cybersécurité et leur incidence sur les activités de l'entité. ***Les États membres encouragent les entités essentielles et importantes à évaluer régulièrement les membres des organes de direction visés au paragraphe 1 du présent article au regard de l'adéquation de leurs compétences en vue de garantir le respect de l'article 18.***

Amendement 40

Proposition de directive
Article 18 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.	3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé***, en tenant compte des normes et de la législation de l'Union en matière de cybersécurité et des facteurs de risque non techniques potentiels, tels que les vulnérabilités cachées ou les portes dérobées et les éventuelles ruptures d'approvisionnement systémiques***.

Amendement 41

Proposition de directive
Article 19 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le groupe de coopération, en coopération avec la Commission ***et*** l'ENISA, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.	1. Le groupe de coopération, en coopération avec la Commission**,** l'ENISA ***et le Service européen pour l'action extérieure***, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.

Amendement 42

Proposition de directive
Article 19 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission, après avoir consulté le groupe de coopération ***et*** l'ENISA, détermine les services, systèmes ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques visée au paragraphe 1.	2. La Commission, après avoir consulté le groupe de coopération**,** l'ENISA ***et le Service européen pour l'action extérieure***, détermine les services, systèmes ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques visée au paragraphe 1.

Amendement 43

Proposition de directive
Article 19 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Lors de l'identification de risques pour des services, systèmes ou chaînes d'approvisionnement informatiques critiques, la Commission, après consultation du groupe de coopération, de

	l'ENISA et du Service européen pour l'action extérieure, formule des recommandations à l'intention des États membres et des autorités nationales compétentes définies dans le présent règlement en vue de remédier aux risques recensés et de renforcer leur résilience à l'égard de ceux-ci.

Amendement 44

Proposition de directive
Article 25 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) des informations sur l'organe de direction responsable des mesures de gestion des risques en matière de cybersécurité prévues à l'article 18, conformément à l'article 17;

Amendement 45

Proposition de directive
Article 29 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;	c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques***, y compris aux risques liés aux chaînes d'approvisionnement visés à l'article 18, paragraphe 3***;

Amendement 46

Proposition de directive
Article 30 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux	b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux

risques;	risques***, y compris aux risques liés aux chaînes d'approvisionnement visés à l'article 18, paragraphe 3***;

Amendement 47

Proposition de directive
Annexe I – ENTITÉS ESSENTIELLES: SECTEURS, SOUS-SECTEURS ET TYPES D'ENTITÉS – Secteur 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Éducation et recherche – Établissements d'enseignement supérieur et instituts de recherche

Amendement 48

Proposition de directive
Annexe I – ENTITÉS ESSENTIELLES: SECTEURS, SOUS-SECTEURS ET TYPES D'ENTITÉS – Secteur 9 Administration publique – Type d'entité

Texte proposé par la Commission	*Amendement*
– Entités de l'administration publique des pouvoirs publics centraux	– Entités de l'administration publique des pouvoirs publics centraux
– Entités de l'administration publique des régions de niveau NUTS 1 énumérées à l'annexe I du règlement (CE) nº 1059/2003([27])	– Entités de l'administration publique des régions de niveau NUTS 1 énumérées à l'annexe I du règlement (CE) nº 1059/2003 ([27]***, 27 bis (nouveau)***)
– Entités de l'administration publique des régions de niveau NUTS 2 énumérées à l'annexe I du règlement (CE) nº 1059/2003	– Entités de l'administration publique des régions de niveau NUTS 2 énumérées à l'annexe I du règlement (CE) nº 1059/2003 ***(27 ter (nouveau))***
[27] Règlement (CE) nº 1059/2003 du Parlement européen et du Conseil du 26 mai 2003 relatif à l'établissement d'une nomenclature commune des unités territoriales statistiques (NUTS) (JO L 154 du 21.6.2003, p. 1).	[27] Règlement (CE) nº 1059/2003 du Parlement européen et du Conseil du 26 mai 2003 relatif à l'établissement d'une nomenclature commune des unités territoriales statistiques (NUTS) (JO L 154 du 21.6.2003, p. 1).
	27 bis (nouveau) ***Ou les unités administratives équivalentes, dans les États membres où la classification NUTS n'a pas encore été***

prise en compte dans la structure institutionnelle de l'administration.

27 ter (nouveau) ***Ou les unités administratives équivalentes, dans les États membres où la classification NUTS n'a pas encore été prise en compte dans la structure institutionnelle de l'administration.***

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Mesures en vue d'un niveau commun élevé de cybersécurité à travers l'Union, abrogation de la directive (UE) 2016/1148
Références	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 21.1.2021
Avis émis par Date de l'annonce en séance	AFET 21.1.2021
Rapporteur(e) pour avis Date de la nomination	Markéta Gregorová 22.2.2021
Examen en commission	25.5.2021 16.6.2021 17.6.2021
Date de l'adoption	14.7.2021
Résultat du vote final	+: 59 –: 5 0: 6
Membres présents au moment du vote final	Alviina Alametsä, Alexander Alexandrov Yordanov, Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk, David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergei Stanishev, Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Suppléants présents au moment du vote final	Ioan-Rareş Bogdan, Andrey Kovatchev, Marisa Matias, Gabriel Mato, Milan Zver

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION SAISIE POUR AVIS

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
Renew	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

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