Conseil de
l'Union européenne

Bruxelles, le 22 janvier 2026
(OR. en)

5611/26
ADD 2

Dossiers interinstitutionnels:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	21 janvier 2026
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	SWD(2026) 12 final
Objet:	DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT accompagnant les documents: Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2) et Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2]

Les délégations trouveront ci-joint le document SWD(2026) 12 final.

p.j.: SWD(2026) 12 final

COMMISSION
EUROPÉENNE

Strasbourg, le 20.1.2026
SWD(2026) 12 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

accompagnant les documents:

Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2)

et

Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Résumé de l'analyse d'impact

Objectif

L'objectif premier de la présente analyse d'impact est d'évaluer l'adéquation des réglementations actuelles pour faire face à l'évolution des menaces de cybersécurité dans l'ensemble de l'Union. L'analyse propose un ensemble intégré d'options stratégiques visant à renforcer l'Agence de l'Union européenne pour la cybersécurité (ENISA), à réformer le cadre européen de certification de cybersécurité (ECCF) et à simplifier le respect du cadre législatif existant en matière de cybersécurité. Cette évaluation souligne l'importance de moduler la gouvernance de la cybersécurité afin de l'harmoniser avec les progrès technologiques et les exigences du marché, tout en garantissant la compétitivité et en tenant compte des incidences sur l'environnement.

Énoncé du problème

Malgré les efforts existants, le paysage de la cybersécurité de l'Union reste confronté à des défis importants dans un contexte de menaces de plus en plus complexes. Le manque de coordination entre les États membres et les autres acteurs au niveau de l'Union, le blocage de la mise en œuvre des outils stratégiques ainsi que les obstacles réglementaires et la complexité entravent une gestion efficace de la cybersécurité. Ces problèmes entraînent une hausse des coûts pour les entreprises et les pouvoirs publics, une augmentation des risques d'incidents de cybersécurité et des niveaux incohérents de protection des citoyens.

Justification de l'action de l'UE

Les menaces de cybersécurité dépassent les frontières nationales; une approche unifiée est donc essentielle pour apporter une réponse solide. Une intervention au niveau de l'Union garantit une protection cohérente, renforce la compétitivité en offrant des conditions de concurrence équitables et facilite la libre circulation des services et produits numériques au sein du marché unique. L'harmonisation au niveau de l'Union réduit également les charges administratives grâce à la simplification des obligations liées au respect des règles et à la rationalisation des procédures.

Options envisageables et option privilégiée

Le présent rapport analyse quatre domaines d'intervention, qui comportent chacun un ensemble d'options stratégiques envisagées au regard des objectifs spécifiques à atteindre: 1) le mandat de l'ENISA (qui fait également partie de l'actuel règlement sur la cybersécurité); 2) l'ECCF (qui fait lui aussi partie de l'actuel règlement sur la cybersécurité); et 3) des modifications ciblées de la directive SRI 2, dans le but de simplifier le mandat de l'ENISA et de l'ECCF, mais aussi de les relier entre eux, Chacun de ces ensembles d'options représente un domaine d'intervention à part entière. Tous les groupes d'options sont néanmoins interconnectés et pertinents les uns pour les autres.

Options pour remédier au décalage entre le cadre d'action de l'Union en matière de cybersécurité et les besoins des parties prenantes dans un environnement de plus en plus hostile

Option A.1: *clarification du mandat de l'ENISA et établissement de priorités* - Cette option fournirait un cadre clair et stable pour les tâches de l'ENISA en intégrant les tâches définies par d'autres actes législatifs.

Option A.2: *réforme du mandat de l'ENISA* – Cette option abrogerait et remplacerait le règlement sur la cybersécurité, en révisant le mandat de l'Agence.

Option A.3: *réforme du mandat de l'ENISA avec une priorité résolument accordée au soutien opérationnel* – Cette option s'appuierait sur l'option A.2. En outre, l'ENISA développerait des capacités pour aider directement les entités relevant de la directive SRI 2, à la demande d'un État membre, à réagir aux incidents de cybersécurité et à s'en remettre.

Options pour le cadre européen de certification de cybersécurité

Option B.1: *clarification du champ d'application, des éléments et des objectifs de l'ECCF et introduction d'un mécanisme de maintenance* – Cette option prévoirait un nouveau mécanisme de maintenance des schémas, après leur adoption, à mettre en œuvre par l'ENISA.

Option B.2: *réforme de l'ECCF au moyen d'une révision de ses procédures et d'un élargissement de son champ d'application afin de faciliter la simplification des contraintes réglementaires* – Cette option abrogerait le règlement sur la cybersécurité et le remplacerait par un nouveau règlement. Outre l'option B.1, les procédures relatives à la demande, à l'élaboration et à l'adoption de schémas seraient révisées afin d'améliorer la responsabilité et l'efficacité.

Option B.3: *réforme de l'ECCF telle qu'envisagée dans l'option B.2 et introduction d'une certification obligatoire pour la posture de cybersécurité* – Cette option s'appuierait sur l'option B.2, mais vise à accroître encore l'incidence du cadre en introduisant une certification obligatoire des entités essentielles couvertes par la directive SRI 2 en tenant compte de scénarios de risque spécifiques, au lieu de s'appuyer uniquement sur la certification volontaire des entités.

Options de simplification

Option C.1: *adoption d'une approche fondée sur des instruments non contraignants et non législatifs, y compris en ayant recours aux habilitations existantes (adoption d'actes d'exécution au titre de l'article 21, paragraphe 5, et de l'article 23, paragraphe 11, de la directive SRI 2)* – Cette option envisage l'adoption d'actes d'exécution en utilisant les habilitations existantes au titre de la directive SRI 2 afin de garantir un degré plus élevé d'harmonisation des mesures de gestion des risques de cybersécurité, des seuils de notification des incidents ainsi que des informations, des formats et des procédures de notification, ainsi que l'adoption d'une série de lignes directrices afin d'améliorer la sécurité juridique et d'harmoniser davantage la mise en œuvre.

Option C.2: *Intervention ciblée – mesures visant à simplifier davantage le respect du cadre législatif pertinent de l'Union en matière de cybersécurité* – Cette option implique une intervention limitée au moyen de modifications apportées au règlement sur la cybersécurité et à la directive SRI 2 dans le but de simplifier certains aspects du cadre de cybersécurité, y compris des adaptations du champ d'application, une harmonisation maximale des actes d'exécution, la démonstration de la conformité au moyen d'une certification et l'adoption de l'ensemble de lignes directrices envisagé dans le cadre de l'option C1.

Option C.3: *harmonisation des mesures liées à la cybersécurité énoncées dans la législation de l'Union* – Cette option s'appuierait sur l'option C.2 et supprimerait toutes les mesures de gestion des risques de cybersécurité et les habilitations relatives à ces mesures qui figurent dans la législation sectorielle. En lieu et place, l'écosystème de la directive SRI 2 serait modifié afin de prévoir des exigences rationalisées pour tous les types d'entités, ce qui permettrait d'accroître l'harmonisation.

Options pour la sécurité de la chaîne d'approvisionnement des TIC

Option D.1: *adoption d'une approche non contraignante pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC* – Cette option ne prévoirait pas d'intervention réglementaire au niveau de l'Union. En lieu et place, la Commission augmenterait le nombre d'évaluations coordonnées des risques et de boîtes à outils volontaires.

Option D.2: *intervention réglementaire ad hoc codifiant la boîte à outils 5G* – Cette option codifierait les mesures de la boîte à outils 5G. Elle introduirait l'obligation pour les États membres de veiller à ce que les composants provenant de fournisseurs à haut risque ne soient pas utilisés dans les actifs essentiels du réseau.

Option D.3: *cadre global et horizontal pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC* – Cette option établirait un cadre réglementaire horizontal et neutre sur le plan technologique et sectoriel afin de faire face aux risques de cybersécurité non techniques dans les chaînes d'approvisionnement des TIC.

Après des analyses approfondies, le train de mesures privilégié comprend: l'option A.2 (réforme du mandat de l'ENISA); l'option B.2 (réforme de l'ECCF au moyen d'une révision de ses procédures et d'un élargissement de son champ d'application afin de faciliter la simplification du respect des obligations réglementaires); l'option C.2 (intervention ciblée – poursuite de la simplification du respect du cadre législatif pertinent de l'Union en matière de cybersécurité); et l'option D.3 (cadre global et horizontal pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC).

Cette combinaison offre une réponse équilibrée aux défis stratégiques recensés, en renforçant considérablement l'efficacité, l'efficience et la cohérence dans l'ensemble de l'Union.

Principales incidences

Analyse coûts-avantages: la transition vers le cadre réglementaire proposé entraînera des coûts, tant pour l'ENISA, qui, selon les estimations, devrait payer jusqu'à 161,3 millions d'euros sur cinq ans pour s'acquitter de ses nouvelles tâches, que pour les autorités publiques dans toute l'Union, qui devraient payer jusqu'à 80 millions d'euros sur cinq ans pour la supervision (en tenant compte des économies de coûts pertinentes). En ce qui concerne les entreprises, pendant une période de transition de trois ans, la suppression progressive de certains équipements à haut risque pourrait entraîner des coûts annuels de 3,4 à 4,3 milliards d'euros pour les opérateurs de réseaux mobiles, tandis que les investissements dans des fournisseurs de confiance pourraient atteindre simultanément 2 milliards d'euros par an. En outre, la rationalisation et la réduction des obligations de conformité devraient permettre aux entreprises de réaliser jusqu'à 14,6 milliards d'euros d'économies. Par ailleurs, l'amélioration de la posture de cybersécurité globale et de la souveraineté technologique de l'Union, ainsi que la stimulation de l'innovation et de la compétitivité devraient amener des bénéfices considérables pour les citoyens, les autorités publiques et les entreprises, qui devraient largement compenser les dépenses initiales à long terme.

Compétitivité: en réduisant la fragmentation du marché et en harmonisant la réglementation, les options privilégiées renforcent l'égalité concurrentielle dans l'ensemble de l'Union, en offrant aux entreprises des trajectoires plus claires en matière de conformité et d'innovation.

Vérification de la cohérence climatique: l'évaluation a porté sur les incidences potentielles de chaque option sur l'environnement. Une attention particulière a été accordée à l'efficacité énergétique, aux émissions liées aux déplacements et à la consolidation des infrastructures. Les options privilégiées A.2, B.2 et C.2 ont une incidence limitée sur l'environnement, tandis que l'option D.3 tient compte de la neutralité environnementale, en prenant en considération le cycle de vie des produits et des périodes de transition pour le remplacement des actifs essentiels. Cela est conforme à l'engagement de l'Union en faveur de la durabilité.

Numérique par défaut: l'accent mis sur des processus numériques rationalisés témoigne de l'engagement de l'Union en faveur d'une approche consistant à donner la priorité au numérique, garantissant un échange de données et une prise de décision plus rapides et plus fiables. L'option D.3 pourrait également avoir une forte incidence sur la numérisation, car elle impliquerait le remplacement de composants provenant d'entités établies dans des pays tiers ou contrôlées par des entités de pays tiers suscitant des préoccupations en matière de cybersécurité.

Simplification et allégement des contraintes: Les options privilégiées contribuent à la simplification en introduisant des précisions sur le champ d'application et des mesures visant à rationaliser la conformité et la supervision, en réduisant ainsi les charges administratives. Le principe «un ajout, un retrait» est pris en considération en veillant à ce que les nouvelles obligations soient contrebalancées par des réductions dans d'autres domaines.

Conclusion

La présente analyse d'impact présente une stratégie globale visant à renforcer la cybersécurité de l'Union, à remédier aux inefficacités réglementaires et à préparer le paysage numérique

aux défis à venir. Elle recommande une approche collaborative et cohérente, fondant les réformes politiques sur les cadres existants tout en s'adaptant aux nouvelles réalités technologiques. Grâce à ces mesures, l'UE vise à garantir une économie numérique résiliente, compétitive et durable.