Conseil de
l'Union européenne

Bruxelles, le 22 mai 2026
(OR. en)

9399/26

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

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents/Conseil
Objet:	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) 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] - Rapport sur l'état des travaux

La présidence a élaboré un rapport sur l'état des travaux concernant la 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 sécurité 2), afin de rendre compte des travaux effectués jusqu'à présent par les instances préparatoires du Conseil et de l'état d'avancement de l'examen de la proposition.

INTRODUCTION

1. Le 20 janvier 2026, la Commission a proposé un nouveau train de mesures sur la cybersécurité visant à renforcer la résilience et les capacités de l'UE en matière de cybersécurité. Le train de mesures comprend un **règlement** 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 technologies de l'information et de la communication (TIC), et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité). Ce règlement (ci-après dénommé "règlement sur la cybersécurité 2") est complété par une **directive** modifiant la directive (UE) 2022/2555 (ci-après dénommée "directive SRI 2") en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2].

2. Avant que la proposition soit élaborée, le Conseil avait, dans ses conclusions sur l'ENISA du 6 décembre 2025[1], invité la Commission à examiner et à renforcer encore le rôle de l'ENISA pour ce qui est de soutenir la coopération opérationnelle menée au niveau de l'UE et entre les États membres pour renforcer la cyberrésilience, en tenant compte des compétences des États membres dans ce domaine. La Commission a également été invitée à veiller à ce que le mandat de l'ENISA visant à soutenir les États membres soit ciblé et clairement défini, et assorti d'objectifs stratégiques concrets et de tâches hiérarchisées, en plus d'une répartition plus précise des tâches et des compétences par rapport aux autres acteurs. Le Conseil a en outre invité instamment la Commission à saisir l'occasion qu'offre l'évaluation du règlement sur la cybersécurité pour trouver des moyens d'adopter une approche plus souple, plus transparente, plus rapide et fondée sur les risques pour l'élaboration de schémas de certification de cybersécurité de l'UE. De plus, dans ses conclusions du 21 mai 2024 sur l'avenir de la cybersécurité[2], le Conseil a souligné sa détermination à assurer la sécurité des chaînes d'approvisionnement des TIC et a mis l'accent sur l'importance des facteurs de risque non techniques, y compris l'influence injustifiée exercée par les pays tiers sur les fournisseurs et prestataires. Enfin, les conclusions du Conseil[3] du 17 octobre 2022 sur la sécurité de la chaîne d'approvisionnement des TIC ont souligné la nécessité de renforcer la résilience et la sécurité des chaînes d'approvisionnement des TIC, compte tenu de l'incidence des tensions géopolitiques et des dépendances aux produits et services TIC.

---

1 Doc. 16527/24.
2 Doc. 10133/24.
3 Doc. 13664/22.

3. La proposition de règlement, qui se fonde sur l'article 114 du TFUE, vise à consolider le cadre de l'Union en matière de cybersécurité. Elle approfondit le rôle et les tâches de l'Agence de l'Union européenne pour la sécurité (ENISA) afin d'aider les États membres et les entités de l'Union à atteindre un niveau élevé de cybersécurité, de résilience et de confiance dans l'Union. Elle vise à rendre le cadre européen de certification de cybersécurité plus efficace et effectif pour permettre une élaboration et une mise en œuvre plus rapides des schémas. La proposition établit en outre un cadre de l'Union digne de confiance pour la sécurité de la chaîne d'approvisionnement des TIC, qui traite des facteurs de risque non techniques et des dépendances affectant la sécurité des infrastructures critiques et des services dans le domaine des TIC. Elle s'accompagne de mesures de simplification ciblées en lien avec la mise en œuvre de la directive SRI 2[4], visant à simplifier les exigences de conformité, à réduire la charge administrative inutile et à accroître la clarté juridique.

4. La feuille de route "Une Europe, un marché"[5], signée en marge de la réunion informelle des chefs d'État ou de gouvernement qui s'est tenue à Chypre le 24 avril 2026, inclut cette proposition dans sa liste de résultats à atteindre en priorité.

5. Le Parlement européen a nommé M[me] Gregorová Markéta (Verts/ALE) rapporteure de la commission ITRE, compétente au fond.

6. Le 29 avril 2026, le Comité économique et social européen a rendu son avis sur la proposition[6].

---

4 JO L 333 du 27.12.2022, p. 80.
5 Doc. 8473/26.
6 Doc. 8980/26.

ÉTAT D'AVANCEMENT DES TRAVAUX AU SEIN DES INSTANCES PRÉPARATOIRES DU CONSEIL

7. Une présentation générale du train de mesures sur la cybersécurité a eu lieu lors de la réunion du groupe horizontal "Questions cyber" (GHQC) du 26 janvier 2026 et de la réunion du Comité des représentants permanents du 28 janvier 2026.

8. L'examen de la proposition par le GHQC a débuté le 2 février 2026 par une présentation détaillée de la Commission. Au cours de cette présentation, la Commission a en outre évoqué les conclusions du rapport d'évaluation, de la fiche financière et de l'analyse d'impact.

9. Le GHQC a commencé la lecture complète de la proposition de règlement le 23 février 2026.

10. Les États membres ont accueilli favorablement la proposition et ont globalement soutenu ses objectifs généraux, notamment le renforcement du soutien apporté par l'ENISA à la coopération opérationnelle des États membres et la simplification du cadre de certification. Toutefois, les discussions ont aussi montré que plusieurs aspects de la proposition appelaient un examen approfondi. Les délégations ont demandé des éclaircissements concernant l'approfondissement envisagé du rôle opérationnel et des tâches de l'ENISA, notamment la diffusion d'alertes précoces, la création d'un service d'assistance en matière de rançongiciels et son rôle au sein du réseau des CSIRT. Plusieurs délégations se sont interrogées sur les implications pour les États membres, sur le plan des ressources, de la contribution proposée de deux experts nationaux détachés (END) par État membre à l'appui des tâches de l'ENISA. Les règles de vote du conseil d'administration doivent également être examinées plus avant. Les délégations ont souligné la nécessité de clarifier et de préciser les définitions et concepts utilisés dans l'ensemble de la proposition. La composition du budget de l'ENISA, notamment la perception de redevances, doit elle aussi être clarifiée.

11. Les nouvelles dispositions visant à rendre le processus de certification plus efficace et effectif ont été globalement bien accueillies, même si la nécessité générale d'une participation accrue des États membres tout au long du processus de certification a été mise en évidence. Le caractère volontaire de la certification a reçu un accueil généralement favorable. Cependant, des délégations ont remis en cause certaines des échéances proposées concernant le cadre de certification.

12. Les discussions sur le cadre digne de confiance pour la chaîne d'approvisionnement des TIC ont fait ressortir plusieurs préoccupations parmi les États membres. Les délégations ont demandé des précisions supplémentaires sur la méthode et les procédures utilisées pour recenser les actifs de TIC essentiels et les fournisseurs à haut risque, ainsi que sur la portée et l'incidence éventuelle des mesures proposées. Les délégations ont souligné qu'il importe d'assurer un niveau adéquat d'association des États membres.

13. Plusieurs délégations ont émis des réserves d'examen sur différentes parties de la proposition, en particulier concernant les aspects relatifs à la gouvernance, le recours aux actes d'exécution et le mécanisme proposé visant à recenser les fournisseurs à haut risque et la sécurité de la chaîne d'approvisionnement des TIC.

14. À la suite des discussions au sein du GHQC, les États membres ont été invités à présenter des observations écrites sur les dispositions du titre I, relatif aux dispositions générales, et du titre II, relatif à l'ENISA. Vingt-trois États membres ont présenté des contributions. Par la suite, les États membres ont été invités à formuler des observations écrites sur le titre III, relatif au cadre européen de certification de cybersécurité. Vingt États membres ont saisi la possibilité de soumettre leur point de vue par écrit.

15. Sur la base de ces contributions écrites des États membres et des travaux menés au sein du GHQC, la présidence élaborera un texte de compromis sur le titre II (ENISA) et le titre III (Cadre européen de certification de cybersécurité), qui sera présenté lors de la réunion que le GHQC tiendra début juin 2026.

16. Plusieurs États membres ont demandé au service juridique du Conseil d'examiner la pertinence de la base juridique.

17. La présidence entamera fin mai 2026 la lecture complète des mesures de simplification de la directive SRI 2.

18. Au total, le GHQC aura consacré, sous la présidence chypriote, un total de quinze réunions à la proposition de règlement sur la cybersécurité 2.

19. Sur la base des progrès réalisés sous la présidence chypriote, la future présidence irlandaise prévoit de poursuivre les travaux sur cet important dossier.

20. Compte tenu de ce qui précède, le Comité des représentants permanents et le Conseil sont invités à prendre note des progrès accomplis dans le cadre de l'examen de la proposition de règlement.