Raad van de Europese Unie

Brussel, 22 mei 2026
(OR. en)

9399/26

Interinstitutionele dossiers:
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

NOTA

van:	het secretariaat-generaal van de Raad
aan:	het Comité van permanente vertegenwoordigers/de Raad
Betreft:	Voorstel voor een verordening van het Europees Parlement en de Raad inzake het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees kader voor cyberbeveiligingscertificering en de beveiliging van de ICT-toeleveringsketen, en tot intrekking van Verordening (EU) 2019/881 (cyberbeveiligingsverordening 2) Voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2022/2555 wat betreft vereenvoudigingsmaatregelen en afstemming op het [voorstel voor de cyberbeveiligingsverordening] – Voortgangsverslag

Het voorzitterschap heeft een voortgangsverslag opgesteld over het voorstel voor een verordening van het Europees Parlement en de Raad inzake het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees kader voor cyberbeveiligingscertificering en de beveiliging van de ICT-toeleveringsketen, en tot intrekking van Verordening (EU) 2019/881 (cyberbeveiligingsverordening 2), teneinde verslag uit te brengen over de tot dusver door de voorbereidende instanties van de Raad verrichte werkzaamheden en over de stand van zaken bij de bespreking van het voorstel.

INLEIDING

1. Op 20 januari 2026 heeft de Commissie een nieuw cyberbeveiligingspakket voorgesteld om de veerkracht en capaciteiten van de EU op het gebied van cyberbeveiliging te versterken. Het pakket bestaat uit een **verordening** inzake het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees kader voor cyberbeveiligingscertificering en de beveiliging van de toeleveringsketen van informatie- en communicatietechnologie (ICT), en trekt Verordening (EU) 2019/881 (cyberbeveiligingsverordening) in. Deze verordening ("cyberbeveiligingsverordening 2") wordt aangevuld met een **richtlijn** tot wijziging van Richtlijn (EU) 2022/2555 (NIS 2-richtlijn) wat betreft vereenvoudigingsmaatregelen en afstemming op het [voorstel voor de cyberbeveiligingsverordening].

2. Voorafgaand aan het voorstel had de Raad in zijn conclusies over Enisa van 6 december 2024[1] de Commissie verzocht de rol van Enisa bij de ondersteuning van de operationele samenwerking op EU-niveau en tussen de lidstaten bij het vergroten van de cyberweerbaarheid te onderzoeken en verder te versterken, waarbij rekening wordt gehouden met de bevoegdheden van de lidstaten op dit gebied. De Commissie werd ook opgeroepen ervoor te zorgen dat het mandaat van Enisa om de lidstaten te ondersteunen, toegespitst en duidelijk omschreven zou worden, met concrete strategische doelstellingen en prioritaire taken, naast een preciezere verdeling van taken en bevoegdheden ten opzichte van andere actoren. De Raad heeft de Commissie ook aangespoord de evaluatie van de cyberbeveiligingsverordening aan te grijpen om manieren te vinden voor een eenvoudiger, op risico's gebaseerde en tevens transparantere en snellere aanpak voor het ontwikkelen van EU-regelingen voor de certificering van cyberbeveiliging. Voorts benadrukte de Raad in zijn conclusies[2] van 21 mei 2024 over de toekomst van cyberbeveiliging zijn toezegging om de beveiliging van ICT-toeleveringsketens te waarborgen en wees hij op het belang van niet-technische risicofactoren, zoals ongepaste invloed van een derde staat op leveranciers en aanbieders. Tot slot werd in de conclusies van de Raad[3] van 17 oktober 2022 over de beveiliging van ICT-toeleveringsketens benadrukt dat de weerbaarheid en beveiliging van ICT-toeleveringsketens moeten worden versterkt, gezien de gevolgen van geopolitieke spanningen en afhankelijkheden van ICT-producten en -diensten.

---

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

3. Doel van het voorstel voor een verordening, dat gebaseerd is op artikel 114 VWEU, is het cyberbeveiligingskader van de Unie te versterken. Het versterkt de rol en de taken van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) om de lidstaten en de entiteiten van de Unie te ondersteunen bij het bereiken van een hoog cyberbeveiligingsniveau, veerkracht en vertrouwen in de Unie. Het moet het Europees kader voor cyberbeveiligingscertificering (ECCF) doeltreffender en efficiënter maken om een snellere ontwikkeling en uitvoering van de regeling mogelijk te maken. Het voorstel omvat ook een Uniekader voor betrouwbare beveiliging van ICT-toeleveringsketens, waarin niet-technische risicofactoren en afhankelijkheden worden aangepakt die van invloed zijn op de beveiliging van kritieke ICT-infrastructuur en -diensten. Het gaat gepaard met gerichte vereenvoudigingsmaatregelen in verband met de uitvoering van de NIS 2-richtlijn[4], die tot doel hebben de nalevingsvereisten te vereenvoudigen, onnodige administratieve lasten te verminderen en de juridische duidelijkheid te vergroten.

4. In de routekaart "Eén Europa, één markt"[5], die is ondertekend in de marge van de informele bijeenkomst van de staatshoofden en regeringsleiders van 24 april 2026 in Cyprus, is dit voorstel opgenomen als een van de prioritaire doelstellingen.

5. Het Europees Parlement benoemde Gregorová Markéta (Verts/ALE) tot rapporteur van de bevoegde Commissie ITRE.

6. Op 29 april 2026 heeft het Europees Economisch en Sociaal Comité een advies betreffende het voorstel[6] aangenomen.

---

4 PB L 333 van 27.12.2022, blz. 80.
5 Doc. 8473/26.
6 Doc. 8980/26.

STAND VAN DE BESPREKINGEN IN DE VOORBEREIDENDE INSTANTIES VAN DE RAAD

7. Er werd een algemene presentatie van het cyberbeveiligingspakket gegeven op de vergadering van de Horizontale Groep cybervraagstukken van 26 januari 2026 en die van het Comité van permanente vertegenwoordigers van 28 januari 2026.

8. De Horizontale Groep cybervraagstukken is op 2 februari 2026 begonnen met de bespreking van het voorstel en kreeg een gedetailleerde presentatie van de Commissie. Daarbij presenteerde de Commissie ook de bevindingen van het evaluatieverslag, het financieel memorandum en de effectbeoordeling.

9. De groep is op 23 februari 2026 begonnen met de lezing van de voorgestelde verordening.

10. De lidstaten waren ingenomen met het voorstel en steunden in het algemeen de algemene doelstellingen ervan, met name de versterking van de steun van Enisa voor de operationele samenwerking tussen de lidstaten en de stroomlijning van het certificeringskader. Uit de besprekingen is echter ook gebleken dat een aantal aspecten van het voorstel nader moet worden besproken. De delegaties verzochten om verdere verduidelijking van de beoogde grotere operationele rol en taken voor Enisa, zoals de afgifte van vroegtijdige waarschuwingen, de oprichting van een ransomware-helpdesk en de rol van Enisa in het CSIRT-netwerk. Verscheidene delegaties plaatsten vraagtekens bij de gevolgen voor de middelen van de lidstaten in verband met de voorgestelde bijdrage van twee gedetacheerde nationale deskundigen (GND's) per lidstaat om de taken van Enisa te ondersteunen. De stemregels van de raad van bestuur moeten ook verder worden besproken. De delegaties benadrukten dat er behoefte is aan meer duidelijkheid en nauwkeurigheid met betrekking tot de definities en de begrippen in het voorstel. De samenstelling van de begroting van Enisa, met name de heffing van vergoedingen, moest ook verder worden verduidelijkt.

11. De nieuwe bepalingen voor een doeltreffender en efficiënter certificeringsproces werden over het algemeen positief onthaald, hoewel er een algemene behoefte werd vastgesteld aan een grotere deelname van de lidstaten aan het hele certificeringsproces. Het vrijwillige karakter van de certificering werd over het algemeen toegejuicht. De delegaties plaatsten echter vraagtekens bij een aantal van de voorgestelde termijnen in het certificeringskader.

12. Bij de besprekingen over het kader voor betrouwbare ICT-toeleveringsketens kwamen verschillende punten van zorg onder de lidstaten naar voren. De delegaties verzochten om verdere verduidelijking van de methode en de procedures voor de identificatie van belangrijke ICT-activa en leveranciers met een hoog risico, en van het toepassingsgebied en het mogelijke effect van de voorgestelde maatregelen. De delegaties benadrukten het belang van een passend niveau van betrokkenheid van de lidstaten.

13. Verscheidene delegaties maakten een studievoorbehoud bij verschillende delen van het voorstel, met name wat betreft governanceaspecten, het gebruik van uitvoeringshandelingen en het voorgestelde mechanisme voor de identificatie van leveranciers met een hoog risico en de beveiliging van ICT-toeleveringsketens.

14. Na de besprekingen in de Horizontale Groep cybervraagstukken werd de lidstaten verzocht schriftelijke opmerkingen in te dienen over de bepalingen met betrekking tot Titel I “algemene bepalingen” en titel II “Enisa”. 23 lidstaten hebben bijdragen ingediend. Later werd de lidstaten ook verzocht schriftelijke opmerkingen in te dienen over titel III “Europees kader voor cyberbeveiligingscertificering”. 20 lidstaten namen de gelegenheid te baat om hun standpunten schriftelijk in te dienen.

15. Op basis van deze schriftelijke bijdragen van de lidstaten en de werkzaamheden in de Horizontale Groep cybervraagstukken zal het voorzitterschap een compromistekst opstellen over Titel II “Enisa” en Titel III “Europees kader voor cyberbeveiligingscertificering”, die begin juni 2026 tijdens de vergadering van de groep zal worden gepresenteerd.

16. Verscheidene lidstaten hebben de Juridische dienst van de Raad verzocht de juistheid van de rechtsgrondslag te onderzoeken.

17. Het voorzitterschap zal eind mei 2026 beginnen met de lezing van de vereenvoudigingsmaatregelen van de NIS 2-richtlijn.

18. De Horizontale Groep cybervraagstukken zal onder het Cypriotische voorzitterschap uiteindelijk in totaal 15 vergaderingen hebben gehouden over het voorstel voor cyberbeveiligingsverordening 2.

19. Voortbouwend op de vooruitgang die door het Cypriotische voorzitterschap is geboekt, is het aantredende Ierse voorzitterschap van plan om voort te werken aan dit belangrijke dossier.

20. In het licht van het bovenstaande worden het Comité van permanente vertegenwoordigers en de Raad verzocht kennis te nemen van de voortgang bij de bespreking van het verordeningsvoorstel.