EUROPESE
COMMISSIE

Brussel, 18.5.2026
COM(2026) 239 final

2026/0118 (NLE)

Voorstel voor een

UITVOERINGSBESLUIT VAN DE RAAD

betreffende goedkeuring van steun uit de EU-cyberbeveiligingsreserve voor Oekraïne

2026/0118 (NLE)

Voorstel voor een

UITVOERINGSBESLUIT VAN DE RAAD

betreffende goedkeuring van steun uit de EU-cyberbeveiligingsreserve voor Oekraïne

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694 (verordening cybersolidariteit)[1], en met name artikel 19, lid 4,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Op 23 juni 2022 heeft de Europese Raad Oekraïne de status van kandidaat-lidstaat toegekend. Het besluit was gebaseerd op de naleving door Oekraïne van de voorwaarden in het advies van de Commissie van juni 2022 over het toetredingsverzoek van Oekraïne. Op 14 december 2023 heeft de Europese Raad, naar aanleiding van de aanbeveling van de Commissie, beslist toetredingsonderhandelingen met Oekraïne te openen.

(2) Op 19 december 2024 bevestigde de Europese Raad zijn onwrikbare steun voor de soevereiniteit en de territoriale integriteit van Oekraïne, en benadrukte dat het land zo lang als nodig politieke, financiële, economische, humanitaire, militaire en diplomatieke steun moet krijgen. Deze acties benadrukken de toewijding van de Unie om de Europese veiligheid te beschermen en tonen aan dat steun voor Oekraïne integraal deel uitmaakt van de veiligheidsdoelstellingen van de Unie.

(3) Cyberbeveiligingsincidenten blijven in de Unie en wereldwijd een economische en maatschappelijke impact veroorzaken. Cyberdreigingen evolueren bijzonder snel in bepaalde kandidaat-lidstaten van de Unie waar aanzienlijke of grootschalige cyberbeveiligingsincidenten kritieke infrastructuur kunnen verstoren en beschadigen, de goede werking van hun economie en de instellingen kunnen verstoren of ernstige risico’s kunnen vormen voor de openbare orde en de veiligheid van entiteiten en burgers. In dat verband kunnen cyberaanvallen ook verdere geopolitieke spanningen veroorzaken en een bedreiging vormen voor kritieke infrastructuur, democratische processen en verkiezingsinfrastructuur.

[1] PB L, 2025/2025, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

(4) De Russische aanvalsoorlog tegen Oekraïne heeft nadelige en ontwrichtende gevolgen gehad voor Oekraïense netwerk- en informatiesystemen van essentiële diensten, zoals de Oekraïense spoorwegen of staatsregisters. De Russiche militaire agressie ging gepaard met voortdurende cyberaanvallen op kritieke infrastructuur in Oekraïne, zoals de aanval op het satellietnetwerk KA-SAT, dat eigendom is van Viasat, aan de vooravond van de grootschalige invasie in februari 2022.

(5) Gezien de onvoorspelbare aard van cyberaanvallen, het feit dat ze vaak niet beperkt zijn tot een specifiek geografisch gebied en er een groot risico op overloopeffecten is, draagt de versterking van de weerbaarheid van buurlanden en hun capaciteit om doeltreffend te reageren op significante en grootschalige cyberbeveiligingsincidenten bij tot de bescherming van de Unie, met name de interne markt en industrie, als geheel. Daarom is in Verordening (EU) 2025/38 bepaald dat derde landen die partij zijn bij een associatieovereenkomst met de Unie, op grond waarvan ze kunnen deelnemen aan het programma Digitaal Europa ("met het programma Digitaal Europa geassocieerde derde landen"), steun kunnen krijgen uit de EU-cyberbeveiligingsreserve (de "reserve"), op hun gehele grondgebied of delen daarvan, indien dit is bepaald in de overeenkomst op grond waarvan het derde land met het programma Digitaal Europa is geassocieerd.

(6) Overeenkomstig artikel 19 van Verordening (EU) 2025/38 komt een derde land alleen in aanmerking voor steun uit de reserve indien dat specifiek is geregeld in de overeenkomst waarbij dat land met het programma Digitaal Europa wordt geassocieerd. Bovendien mogen dergelijke derde landen alleen in aanmerking blijven komen als aan de drie criteria van artikel 19, lid 3, van Verordening (EU) 2025/38 is voldaan. Ten eerste moet het derde land volledig voldoen aan de relevante bepalingen van die overeenkomst. Ten tweede moet het derde land, gezien de complementaire aard van de reserve, passende maatregelen hebben getroffen om zich voor te bereiden op significante cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten. Ten derde moet de steunverlening uit de reserve stroken met het beleid van de Unie ten aanzien van dat land en met de algemene betrekkingen met dat land, en verenigbaar zijn met ander beleid van de Unie op het gebied van veiligheid.

(7) Oekraïne is partij bij een associatieovereenkomst met de Europese Unie over de deelname aan het programma Digitaal Europa (2021-2027), die op 5 september 2022 is ondertekend. Overeenkomstig artikel 1 van de associatieovereenkomst bij het programma Digitaal Europa mag Oekraïne deelnemen aan het programma Digitaal Europa, en ook steun uit de EU-cyberbeveiligingsreserve krijgen. De overeenkomst bepaalt dat Oekraïne moet voldoen aan de verplichtingen van artikel 19, leden 2 en 9, van Verordening (EU) 2025/38.

(8) Steunverlening aan met het programma Digitaal Europa geassocieerde derde landen kan gevolgen hebben voor de betrekkingen met derde landen en het veiligheidsbeleid van de Unie, onder meer in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid. De Raad neemt een besluit op basis van een voorstel van de Commissie en houdt daarbij rekening met de beoordeling van de drie criteria van artikel 19, lid 3, van Verordening (EU) 2025/38 van de Commissie.

(9) De Unie heeft mechanismen, financieringsinstrumenten en faciliteiten opgezet om de veiligheid, defensie en weerbaarheid van Oekraïne te ondersteunen, waaronder de Europese Vredesfaciliteit, die militaire steun financiert, en het fonds voor bijstand aan

Oekraïne, dat in 2024 is opgericht. Daarnaast heeft de Unie in 2022 de militaire bijstandsmissie van de EU ter ondersteuning van Oekraïne opgestart om de Oekraïense strijdkrachten op te leiden en de adviesmissie van de Europese Unie voor de hervorming van de civiele veiligheidssector in Oekraïne, die sinds 2014 actief is, te versterken. Samen vormen die initiatieven een gecoördineerde en krachtige respons om de veiligheid, defensie en weerbaarheid van Oekraïne te versterken. In juni 2024 hebben de Unie en Oekraïne gezamenlijke toezeggingen op het gebied van veiligheid aangenomen, waarbij beide partijen onder meer hebben bevestigd de samenwerking op het gebied van weerbaarheid te versterken, met bijzondere aandacht voor de bestrijding van hybride en cyberdreigingen, buitenlandse inmenging en manipulatie van informatie, en de bescherming van kritieke infrastructuur. De in 2022 opgezette cyberdialoog tussen de EU en Oekraïne blijft een centraal platform voor politieke en technische samenwerking op het gebied van cybervraagstukken.

(10) De Commissie heeft geoordeeld dat de drie criteria van artikel 19, lid 3, van Verordening (EU) 2025/38 ten aanzien van Oekraïne zijn vervuld. Ze heeft bij die beoordeling de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid geraadpleegd.

(11) Overeenkomstig artikel 19, lid 6, van Verordening (EU) 2025/38 voldoet Oekraïne volgens de beoordeling van de Raad aan de toepasselijke bepalingen van de overeenkomst op grond waarvan dat land met het programma Digitaal Europa is geassocieerd en heeft het land passende maatregelen getroffen om zich voor te bereiden op significante cyberbeveiligingsincidenten en op aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten. Voorts strookt de steunverlening uit de reserve volgens de beoordeling van de Raad met het beleid van de Unie ten aanzien van Oekraïne en met de algemene betrekkingen met dat land, en is die steun verenigbaar met ander beleid van de Unie op het gebied van veiligheid, met name de in overweging 8 genoemde factoren.

(12) Bijgevolg moet steun voor Oekraïne uit de reserve worden goedgekeurd.

(13) Met het oog op onmiddellijke bijstand volgens de criteria van de basishandeling moet dit besluit met spoed in werking treden. Om geschikte en tijdige steun mogelijk te maken, moet het besluit gedurende één jaar van toepassing zijn,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Het verlenen van steun uit de EU-cyberbeveiligingsreserve aan Oekraïne in de zin van artikel 19 van Verordening (EU) 2025/38 wordt goedgekeurd.

Artikel 2

Dit besluit treedt in werking op de dag van de bekendmaking ervan in het Publicatieblad van de Europese Unie.

Het is van toepassing tot en met [Publications Office: please insert the date of entry into force + one year].

Gedaan te Brussel,

Voor de Raad
De voorzitter