EUROPEISKA
KOMMISSIONEN

Bryssel den 18.5.2026
COM(2026) 239 final

2026/0118 (NLE)

Förslag till

RÅDETS GENOMFÖRANDEBESLUT

om godkännande av stöd från EU-cybersäkerhetsreserven till Ukraina

2026/0118 (NLE)

Förslag till

RÅDETS GENOMFÖRANDEBESLUT

om godkännande av stöd från EU-cybersäkerhetsreserven till Ukraina

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsförordningen)[1], särskilt artikel 19.4,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Den 23 juni 2022 beviljade Europeiska rådet Ukraina status som kandidatland. Beslutet grundades på att Ukraina uppfyllde villkoren i kommissionens yttrande från juni 2022 om Ukrainas ansökan om medlemskap. Den 14 december 2023 beslutade Europeiska rådet, efter kommissionens rekommendation, att inleda anslutningsförhandlingar med Ukraina.

(2) Den 19 december 2024 bekräftade Europeiska rådet återigen sitt orubbliga stöd för Ukrainas suveränitet och territoriella integritet och betonade tillhandahållandet av politiskt, finansiellt, ekonomiskt, humanitärt, militärt och diplomatiskt stöd så länge som det behövs. Dessa åtgärder understryker unionens fasta vilja att upprätthålla säkerheten i Europa och visar att stödet till Ukraina är en integrerad del av unionens säkerhetsmål.

(3) Cybersäkerhetsincidenter fortsätter att orsaka ekonomiska och samhälleliga konsekvenser i hela unionen och även globalt. Cyberhoten utvecklas särskilt snabbt i vissa EU-kandidatländer, där möjliga betydande eller storskaliga cybersäkerhetsincidenter potentiellt kan störa och skada kritisk infrastruktur, hindra deras ekonomi och institutioner från att fungera korrekt eller medföra allvarliga risker för den allmänna säkerheten och tryggheten för entiteter och medborgare. I detta sammanhang kan cybersäkerhetsattacker även orsaka ytterligare geopolitiska spänningar och hota kritisk infrastruktur, demokratiska processer och valinfrastruktur.

(4) Rysslands anfallskrig mot Ukraina har haft en skadlig och störande inverkan på Ukrainas nätverks- och informationssystem för samhällsviktiga tjänster, såsom Ukrainas järnväg och statliga register. Den militära aggressionen har åtföljts av konstanta ryska cyberattacker riktade mot Ukrainas kritiska infrastruktur, däribland

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

satellitnätet Ka-Sat, som ägs av Viasat, kvällen före den fullskaliga invasionen i februari 2022.

(5) Med tanke på att cybersäkerhetsangrepp är oförutsägbara, att de sällan är begränsade till ett visst geografiskt område och att de har en hög risk för spridningseffekter, bidrar en förstärkning av grannländernas resiliens och deras kapacitet att hantera betydande och storskaliga cybersäkerhetsincidenter på ett ändamålsenligt sätt till skyddet av unionen, särskilt den inre marknaden och industrin. I förordning (EU) 2025/38 anges därför att ett tredjeland som är part i ett associeringsavtal med unionen som möjliggör dess deltagande i programmet för ett digitalt Europa (*tredjeländer som är associerade till programmet för ett digitalt Europa*) kan få stöd från EU-cybersäkerhetsreserven (*reserven*), i hela eller delar av sitt territorium, om detta föreskrivs i det avtal genom vilket det är associerat till programmet för ett digitalt Europa.

(6) I enlighet med artikel 19 i förordning (EU) 2025/38 får ett tredjeland som är associerat till programmet för ett digitalt Europa endast begära stöd från reserven om det avtal genom vilket det är associerat till programmet för ett digitalt Europa föreskriver detta. Vidare behåller dessa tredjeländer endast den rätten om de tre kriterier som anges i artikel 19.3 i förordning (EU) 2025/38 uppfylls. För det första ska tredjelandet till fullo uppfylla de relevanta villkoren i det avtalet. För det andra ska tredjelandet, med tanke på reservens kompletterande karaktär, ha vidtagit lämpliga åtgärder som förberedelse inför betydande eller storskaliga cybersäkerhetsincidenter. För det tredje ska stödet från reserven vara förenligt med unionens politik gentemot, och de övergripande förbindelserna med, det landet och med annan unionspolitik på säkerhetsområdet.

(7) Ukraina är part i ett associeringsavtal med Europeiska union om deltagande i programmet för ett digitalt Europa (2021–2027), undertecknat den 5 september 2022. I enlighet med artikel 1 i associeringsavtalet till programmet för ett digitalt Europa har Ukraina rätt att delta i det programmet och att få stöd från reserven. Avtalet innehåller bestämmelser som kräver att Ukraina uppfyller de skyldigheter som anges i artikel 19.2 och 19.9 i förordning (EU) 2025/38.

(8) Tillhandahållandet av stöd till tredjeländer som är associerade till programmet för ett digitalt Europa kan påverka förbindelserna med tredjeländer och unionens säkerhetspolitik, inbegripet inom ramen för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken. Rådet agerar på grundval av ett förslag från kommissionen, med vederbörligt beaktande av kommissionens bedömning av de tre kriterier som anges i artikel 19.3 i förordning (EU) 2025/38.

(9) Unionen har inrättat en rad mekanismer, finansieringsinstrument och faciliteter för att stödja Ukrainas säkerhet, försvar och resiliens, däribland den europeiska fredsfaciliteten, som finansierar militärt stöd, och stödfonden för Ukraina, som lanserades 2024. Unionen inledde 2022 också Europeiska unionens uppdrag för militärt bistånd till Ukraina, för att utbilda den ukrainska försvarsmakten och stärka Europeiska unionens rådgivande uppdrag för reform av den civila säkerhetssektorn i Ukraina, vilket varit verksamt sedan 2014. Tillsammans utgör alla dessa initiativ en samordnad och robust svarsåtgärd för att stärka Ukrainas säkerhet, försvar och resiliens. I juni 2024 antog unionen och Ukraina gemensamma säkerhetsåtaganden, som innebar att båda parterna bekräftade sin avsikt att bland annat stärka samarbetet om resiliens, med fokus på att motverka hybridhot och cyberhot samt utländsk informationsmanipulering och inblandning, och att skydda kritisk infrastruktur.

Cyberdialogen mellan EU och Ukraina, som inrättades 2022, fortsätter att fungera som en central plattform för det politiska och tekniska samarbetet om cyberfrågor.

(10) Kommissionen har med avseende på Ukraina bedömt de tre kriterier som anges i artikel 19.3 i förordning (EU) 2025/38 och anser att de är uppfyllda. I samband med denna bedömning har kommissionen också samrått med unionens höga representant för utrikes frågor och säkerhetspolitik.

(11) I enlighet med artikel 19.6 i förordning (EU) 2025/38 har rådet bedömt att Ukraina uppfyller de relevanta villkoren i det avtal genom vilket Ukraina är associerat till programmet för ett digitalt Europa och att Ukraina har vidtagit lämpliga åtgärder som förberedelse inför betydande cybersäkerhetsincidenter och incidenter som är likvärdiga med storskaliga cybersäkerhetsincidenter. Dessutom har rådet bedömt att stödet från reserven är förenligt med unionens politik gentemot, och de övergripande förbindelserna med, Ukraina, och att det är förenligt med annan unionspolitik på säkerhetsområdet, särskilt de faktorer som anges i skäl 8.

(12) Stöd till Ukraina från reserven bör därför godkännas.

(13) För att säkerställa att omedelbart bistånd möjliggörs enligt de kriterier som anges i den grundläggande rättsakten bör detta beslut träda i kraft så snart som möjligt. För att möjliggöra lämpligt stöd i rätt tid bör beslutet gälla i ett år.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Tillhandahållande av stöd från EU-cybersäkerhetsreserven till Ukraina i den mening som avses i artikel 19 i förordning (EU) 2025/38 godkänns härmed.

Artikel 2

Detta beslut träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

Det ska tillämpas till och med [Publikationsbyrån: för in datumet för detta besluts ikraftträdande + ett år]

Utfärdat i Bryssel den

På rådets vägnar
Ordförande