EURÓPSKA
KOMISIA

V Bruseli 18. 5. 2026
COM(2026) 239 final

2026/0118 (NLE)

Návrh

VYKONÁVACIE ROZHODNUTIE RADY

o povolení podpory z rezervy EÚ na účely kybernetickej bezpečnosti pre Ukrajinu

2026/0118 (NLE)

Návrh

VYKONÁVACIE ROZHODNUTIE RADY

o povolení podpory z rezervy EÚ na účely kybernetickej bezpečnosti pre Ukrajinu

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite)[1], a najmä na jeho článok 19 ods. 4,

so zreteľom na návrh Európskej komisie,

keďže:

(1) Európska rada 23. júna 2022 udelila Ukrajine štatút kandidátskej krajiny. Príslušné rozhodnutie bolo založené na tom, že Ukrajina splnila podmienky uvedené v stanovisku Komisie z júna 2022 k žiadosti Ukrajiny o členstvo. Európska rada v nadväznosti na odporúčanie Komisie 14. decembra 2023 rozhodla o začatí prístupových rokovaní s Ukrajinou.

(2) Európska rada 19. decembra 2024 opätovne potvrdila svoju neochvejnú podporu zvrchovanosti a územnej celistvosti Ukrajiny, pričom zdôraznila poskytovanie politickej, finančnej, hospodárskej, humanitárnej, vojenskej a diplomatickej podpory tak dlho, ako to bude potrebné. Tieto kroky zdôrazňujú odhodlanie Únie zachovať európsku bezpečnosť a dokazujú, že podpora Ukrajiny je neoddeliteľnou súčasťou bezpečnostných cieľov Únie.

(3) Kybernetické incidenty majú naďalej hospodársky a spoločenský vplyv v celej Únii, ako aj na celosvetovej úrovni. Kybernetické hrozby sa v určitých kandidátskych krajinách Únie vyvíjajú obzvlášť rýchlo, pričom významné alebo rozsiahle kybernetické incidenty majú potenciál narušiť a poškodiť kritickú infraštruktúru, negatívne vplývať na riadne fungovanie ekonomiky a inštitúcií alebo predstavovať vážne riziká v oblasti verejnej bezpečnosti a ochrany pre subjekty a občanov. V tejto súvislosti by kybernetické útoky mohli ďalej zvyšovať geopolitické napätie a ohrozovať kritickú infraštruktúru, demokratické procesy a volebnú infraštruktúru.

(4) Útočná vojna Ruska proti Ukrajine má nepriaznivý a narúšajúci vplyv na ukrajinské sieťové a informačné systémy základných služieb, ako sú ukrajinské železnice alebo štátne registre. Vojenskú agresiu sprevádzali nepretržité kybernetické útoky Ruska na kritickú infraštruktúru Ukrajiny vrátane útoku na satelitnú sieť KA-SAT vo vlastníctve spoločnosti Viasat v predvečer rozsiahlej invázie vo februári 2022.

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

(5) S ohľadom na nepredvídateľnú povahu kybernetických útokov a na skutočnosť, že tieto útoky často nie sú obmedzené na konkrétnu geografickú oblasť a predstavujú vysoké riziko presahu, zvýšenie odolnosti susedných krajín a posilnenie ich kapacity účinne reagovať na významné a rozsiahle kybernetické bezpečnostné incidenty prispieva k ochrane celej Únie, najmä vnútorného trhu a priemyslu ako celku. V nariadení (EÚ) 2025/38 sa preto stanovuje, že tretie krajiny, ktoré sú zmluvnou stranou dohody o pridružení s Úniou, ktorá im umožňuje účasť na programe Digitálna Európa (ďalej len „tretie krajiny pridružené k programu Digitálna Európa“), môžu byť podporované z rezervy EÚ na účely kybernetickej bezpečnosti (ďalej len „rezerva“) na celom svojom území alebo jeho časti, ak sa tak stanovuje v dohode, ktorou je tretia krajina pridružená k programu Digitálna Európa.

(6) V súlade s článkom 19 nariadenia (EÚ) 2025/38 je tretia krajina oprávnená na podporu z rezervy len vtedy, ak je to osobitne stanovené v dohode o pridružení danej krajiny k programu Digitálna Európa. Okrem toho by takéto tretie krajiny mali zostať oprávnené len pokým sú splnené tri kritériá stanovené v článku 19 ods. 3 nariadenia (EÚ) 2025/38. Po prvé, tretia krajina má v plnej miere dodržiavať príslušné podmienky uvedenej dohody. Po druhé, vzhľadom na komplementárnu povahu rezervy má tretia krajina prijať primerané kroky na prípravu na významné alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty. Po tretie, poskytovanie podpory z rezervy má byť v súlade s politikou Únie voči tejto krajine a celkovými vzťahmi s ňou, ako aj s inými politikami Únie v oblasti bezpečnosti.

(7) Ukrajina je zmluvnou stranou dohody o pridružení s Európskou úniou k účasti na programe Digitálna Európa (2021 – 2027), ktorá bola podpísaná 5. septembra 2022. V súlade s článkom 1 dohody o pridružení k programu Digitálna Európa sa Ukrajina môže zúčastňovať na programe Digitálna Európa a získať podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Dohoda obsahuje ustanovenia, ktorými sa od Ukrajiny vyžaduje, aby dodržiavala povinnosti stanovené v článku 19 ods. 2 a 9 nariadenia (EÚ) 2025/38.

(8) Poskytovanie podpory tretím krajinám pridruženým k programu Digitálna Európa môže ovplyvniť vzťahy s tretími krajinami a bezpečnostnú politiku Únie, a to aj v kontexte spoločnej zahraničnej a bezpečnostnej politiky a spoločnej bezpečnostnej a obrannej politiky. Rada koná na základe návrhu Komisie, pričom náležite zohľadňuje posúdenie troch kritérií uvedených v článku 19 ods. 3 nariadenia (EÚ) 2025/38 zo strany Komisie.

(9) Únia zriadila celý rad mechanizmov, nástrojov financovania a opatrení na podporu bezpečnosti, obrany a odolnosti Ukrajiny vrátane Európskeho mierového nástroja, z ktorého sa financuje vojenská podpora, a Fondu pomoci pre Ukrajinu zriadeného v roku 2024. Okrem toho v roku 2022 zriadila vojenskú pomocnú misiu EÚ na podporu Ukrajiny s cieľom vycvičiť ukrajinské ozbrojené sily a posilniť poradnú misiu Európskej únie pre reformu sektora civilnej bezpečnosti na Ukrajine, ktorá funguje od roku 2014. Tieto iniciatívy spoločne predstavujú koordinovanú a ráznu reakciu s cieľom posilniť bezpečnosť, obranu a odolnosť Ukrajiny. V júni 2024 Únia a Ukrajina prijali spoločné bezpečnostné záväzky, v ktorých obe strany okrem iného potvrdili zámer posilniť spoluprácu v oblasti odolnosti so zameraním na boj proti hybridným a kybernetickým hrozbám, zahraničnej manipulácii s informáciami a zahraničnému zasahovaniu, ako aj na ochranu kritickej infraštruktúry. Kybernetický dialóg medzi EÚ a Ukrajinou zriadený v roku 2022 je naďalej kľúčovou platformou na riešenie politickej a technickej spolupráce v kybernetických otázkach.

(10) Komisia vo vzťahu k Ukrajine posúdila tri kritériá stanovené v článku 19 ods. 3 nariadenia (EÚ) 2025/38 a považuje ich za splnené. Pri tomto posúdení konzultovala aj s vysokou predstaviteľkou Únie pre zahraničné veci a bezpečnostnú politiku.

(11) Podľa posúdenia Rady v súlade s článkom 19 ods. 6 nariadenia (EÚ) 2025/38 Ukrajina dodržiava relevantné podmienky dohody, ktorou je táto krajina pridružená k programu Digitálna Európa, a podnikla primerané kroky na prípravu na významné kybernetickobezpečnostné incidenty a incidenty rovnocenné rozsiahlym kybernetickobezpečnostným incidentom. Navyše, poskytnutie podpory z rezervy je podľa posúdenia Rady v súlade s politikou Únie voči Ukrajine, jej celkovými vzťahmi s Ukrajinou a s ostatnými politikami Únie v oblasti bezpečnosti, najmä vzhľadom na faktory uvedené v odôvodnení 8.

(12) Podpora z rezervy pre Ukrajinu by sa preto mala povoliť.

(13) S cieľom zabezpečiť poskytovanie okamžitej pomoci v súlade s kritériami stanovenými v základnom akte by toto rozhodnutie malo nadobudnúť účinnosť čo najskôr. S cieľom zabezpečiť primeranú a včasnú podporu by sa toto rozhodnutie malo uplatňovať jeden rok,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Týmto sa povoľuje poskytovanie podpory Ukrajine z rezervy EÚ na účely kybernetickej bezpečnosti v zmysle článku 19 nariadenia (EÚ) 2025/38.

Článok 2

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

Uplatňuje sa do [Úrad pre publikácie: vložte dátum nadobudnutia účinnosti + jeden rok].

V Bruseli

Za Radu
predseda