KOMISJA
EUROPEJSKA

Bruksela, dnia 18.5.2026 r.
COM(2026) 239 final

2026/0118 (NLE)

Wniosek

DECYZJA WYKONAWCZA RADY

w sprawie zezwolenia na udzielenie Ukrainie wsparcia z rezerwy cyberbezpieczeństwa UE

2026/0118 (NLE)

Wniosek

DECYZJA WYKONAWCZA RADY

w sprawie zezwolenia na udzielenie Ukrainie wsparcia z rezerwy cyberbezpieczeństwa UE

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności)[1], w szczególności jego art. 19 ust. 4,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) W dniu 23 czerwca 2022 r. Rada Europejska przyznała Ukrainie status państwa kandydującego. Decyzję tę podjęto w związku ze spełnieniem przez Ukrainę warunków określonych w opinii Komisji z czerwca 2022 r. w sprawie wniosku Ukrainy o członkostwo. W dniu 14 grudnia 2023 r. Rada Europejska podjęła, w następstwie zalecenia wydanego przez Komisję, decyzję o rozpoczęciu negocjacji akcesyjnych z Ukrainą.

(2) W dniu 19 grudnia 2024 r. Rada Europejska potwierdziła swoje niezachwiane poparcie dla suwerenności i integralności terytorialnej Ukrainy, kładąc nacisk na zapewnianie wsparcia politycznego, finansowego, gospodarczego, humanitarnego, wojskowego i dyplomatycznego tak długo, jak będzie to konieczne. Działania te podkreślają zaangażowanie Unii na rzecz utrzymania bezpieczeństwa europejskiego, pokazując, że wsparcie dla Ukrainy jest integralną częścią celów Unii w zakresie bezpieczeństwa.

(3) Incydenty w cyberbezpieczeństwie nadal wywołują skutki gospodarcze i społeczne zarówno w całej Unii, jak i w skali globalnej. Szczególnie szybko cyberzagrożenia ewoluują w niektórych państwach kandydujących do Unii, gdzie ewentualne poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę mogą prowadzić do zakłóceń lub uszkodzeń infrastruktury krytycznej, a także mogą zakłócać prawidłowe funkcjonowanie gospodarki i instytucji lub stwarzać poważne ryzyko dla bezpieczeństwa publicznego i bezpieczeństwa podmiotów i obywateli. W tym kontekście cyberataki mogą również powodować dalsze napięcia

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

geopolityczne i zagrażać infrastrukturze krytycznej, procesom demokratycznym i infrastrukturze wyborczej.

(4) Rosyjska wojna napastnicza przeciwko Ukrainie ma szkodliwy i destrukcyjny wpływ na ukraińskie systemy sieciowe i informatyczne związane z usługami kluczowymi, takimi jak ukraińska kolej lub rejestry państwowe. Agresji wojskowej towarzyszą ciągłe rosyjskie cyberataki na infrastrukturę krytyczną Ukrainy, np. ataki na satelitarną sieć KA-SAT, będącą własnością Viasat, w przeddzień pełnoskalowej inwazji w lutym 2022 r.

(5) Biorąc pod uwagę nieprzewidywalny charakter cyberataków, fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego oraz że stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii, w szczególności rynku wewnętrznego i przemysłu. W związku z tym rozporządzenie (UE) 2025/38 stanowi, że państwa trzecie, które są stronami umowy stowarzyszeniowej z Unią umożliwiającej im udział w programie „Cyfrowa Europa” (zwane dalej „państwami trzecimi stowarzyszonymi z programem »Cyfrowa Europa«”) mogą otrzymać wsparcie z rezerwy cyberbezpieczeństwa UE na całości lub części swojego terytorium, w przypadku gdy jest to przewidziane w umowie, na podstawie której dane państwo trzecie jest stowarzyszone z programem „Cyfrowa Europa”.

(6) Zgodnie z art. 19 rozporządzenia (UE) 2025/38 państwo trzecie kwalifikuje się do wsparcia z rezerwy tylko wtedy, gdy jest to wyraźnie przewidziane w umowie, na podstawie której jest ono stowarzyszone z programem „Cyfrowa Europa”. Ponadto takie państwa trzecie powinny w dalszym ciągu kwalifikować się do otrzymania wsparcia wyłącznie wtedy, gdy spełnione są trzy kryteria określone w art. 19 ust. 3 rozporządzenia (UE) 2025/38. Po pierwsze, dane państwo trzecie w pełni przestrzega odpowiednich postanowień wspomnianej umowy. Po drugie, biorąc pod uwagę komplementarny charakter rezerwy cyberbezpieczeństwa UE, państwo trzecie podjęło odpowiednie kroki, aby przygotować się na poważne incydenty w cyberbezpieczeństwie lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę. Po trzecie, udzielenie wsparcia z rezerwy cyberbezpieczeństwa UE ma być spójne z polityką Unii wobec tego państwa i ogólnymi stosunkami z tym państwem oraz z innymi politykami Unii w dziedzinie bezpieczeństwa.

(7) Ukraina jest stroną umowy o stowarzyszeniu z Unią Europejską w zakresie uczestnictwa w programie „Cyfrowa Europa” (2021–2027), podpisanej w dniu 5 września 2022 r. Zgodnie z art. 1 umowy o stowarzyszeniu z programem „Cyfrowa Europa” Ukraina może uczestniczyć w programie „Cyfrowa Europa”, w tym uzyskać wsparcie z rezerwy cyberbezpieczeństwa UE. Umowa ta zawiera postanowienia zobowiązujące Ukrainę do wypełniania obowiązków określonych w art. 19 ust. 2 i 9 rozporządzenia (UE) 2025/38.

(8) Udzielanie wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa” może mieć wpływ na stosunki z państwami trzecimi i na politykę bezpieczeństwa Unii, w tym w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony. Rada podejmuje działanie na podstawie wniosku Komisji, z należytym uwzględnieniem dokonanej

przez Komisję oceny spełnienia trzech kryteriów, o których mowa w art. 19 ust. 3 rozporządzenia (UE) 2025/38.

(9) Unia ustanowiła szereg mechanizmów, instrumentów finansowania i instrumentów wspierających bezpieczeństwo, obronę i odporność Ukrainy, w tym Europejski Instrument na rzecz Pokoju, z którego finansuje się wsparcie wojskowe, oraz Fundusz Pomocy Ukrainie, uruchomiony w 2024 r. W 2022 r. zainicjowano również misję Unii Europejskiej w zakresie pomocy wojskowej dla Ukrainy, aby przeszkolić ukraińskie siły zbrojne i wzmocnić misję doradczą Unii Europejskiej na rzecz reformy cywilnego sektora bezpieczeństwa na Ukrainie, która działa od 2014 r. Wszystkie te inicjatywy razem stanowią skoordynowaną i zdecydowaną reakcję mającą na celu wzmocnienie bezpieczeństwa, obrony i odporności Ukrainy. W czerwcu 2024 r. Unia i Ukraina przyjęły wspólne zobowiązania w zakresie bezpieczeństwa, w których obie strony potwierdziły między innymi zacieśnienie współpracy w zakresie odporności, ze szczególnym uwzględnieniem przeciwdziałania zagrożeniom hybrydowym i cyberzagrożeniom, zagranicznym manipulacjom informacjami i ingerencjom w informacje, a także ochrony infrastruktury krytycznej. Ustanowiony w 2022 r. dialog w sprawach cyberprzestrzeni między UE a Ukrainą nadal stanowi centralną platformę współpracy politycznej i technicznej w kwestiach związanych z cyberprzestrzenią.

(10) Komisja oceniła spełnienie przez Ukrainę trzech kryteriów określonych w art. 19 ust. 3 rozporządzenia (UE) 2025/38 i uznała je za spełnione. Dokonując tej oceny, Komisja skonsultowała się również z Wysokim Przedstawicielem Unii ds. Zagranicznych i Polityki Bezpieczeństwa.

(11) Zgodnie z art. 19 ust. 6 rozporządzenia (UE) 2025/38 Rada ocenia, że Ukraina przestrzega odpowiednich postanowień umowy o stowarzyszeniu Ukrainy z programem „Cyfrowa Europa” i podjęła odpowiednie kroki, by przygotować się na poważne incydenty w cyberbezpieczeństwie i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę. Ponadto Rada ocenia, że udzielenie wsparcia z rezerwy jest zgodne z polityką Unii wobec Ukrainy i ogólnie z jej stosunkami z Ukrainą oraz z innymi politykami Unii w dziedzinie bezpieczeństwa, zwłaszcza w odniesieniu do czynników określonych w motywie 8.

(12) Należy zatem zezwolić na wsparcie Ukrainy z rezerwy.

(13) Aby zapewnić możliwość natychmiastowej pomocy zgodnie z kryteriami określonymi w akcie podstawowym, niniejsza decyzja powinna wejść w życie w trybie pilnym. Aby umożliwić odpowiednie i terminowe wsparcie, niniejsza decyzja powinna mieć zastosowanie przez jeden rok,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Zezwala się na udzielenie Ukrainie wsparcia z rezerwy cyberbezpieczeństwa UE w rozumieniu art. 19 rozporządzenia (UE) 2025/38.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Stosuje się ją do dnia [Urząd Publikacji: proszę wstawić datę = data wejścia w życie + jeden rok].

Sporządzono w Brukseli dnia r.

W imieniu Rady
Przewodniczący