KOMISJA
EUROPEJSKA

Bruksela, dnia 24.6.2025 r.
COM(2025) 342 final

2025/0187 (NLE)

Wniosek

DECYZJA WYKONAWCZA RADY

zezwalająca na udzielenie Mołdawii wsparcia z rezerwy cyberbezpieczeństwa UE

(Tekst mający znaczenie dla EOG)

2025/0187 (NLE)

Wniosek

DECYZJA WYKONAWCZA RADY

zezwalająca na udzielenie Mołdawii wsparcia z rezerwy cyberbezpieczeństwa UE

(Tekst mający znaczenie dla EOG)

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 swoich konkluzjach z dnia 15 grudnia 2022 r. Rada Europejska potwierdziła, że Unia będzie w dalszym ciągu zapewniać wszelkie stosowne wsparcie Republice Mołdawii (określanej dalej jako Mołdawia), ponieważ państwo to zmaga się z wieloaspektowymi skutkami rosyjskiej wojny napastniczej przeciwko Ukrainie.

(2) W dniu 23 czerwca 2022 r. Rada Europejska przyznała Mołdawii status kraju kandydującego. Decyzję tę podjęto w związku ze spełnieniem przez Mołdawię warunków określonych w opinii Komisji z czerwca 2022 r. w sprawie wniosku Mołdawii o członkostwo. W dniu 14 grudnia 2023 r. Rada Europejska podjęła, w następstwie zalecenia wydanego przez Komisję Europejską, decyzję o rozpoczęciu negocjacji akcesyjnych z Mołdawią.

(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 krajach kandydujących do UE, 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 lub obywateli. Dzieje się tak szczególnie w Mołdawii, gdzie Rosja prowadzi kampanie

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

hybrydowe i dokonuje cyberataków, które są ukierunkowane na infrastrukturę krytyczną, procesy demokratyczne i infrastrukturę wyborczą.

(4) Biorąc pod uwagę nieprzewidywalny charakter cyberataków oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i 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, a szczególnie jej rynku wewnętrznego i przemysłu. W związku z tym rozporządzenie (UE) 2025/38 stanowi, że państwa trzecie stowarzyszone z programem „Cyfrowa Europa" mogą otrzymać – w odniesieniu do całości lub części swojego terytorium – wsparcie z rezerwy cyberbezpieczeństwa UE, w przypadku gdy przewiduje to umowa, na podstawie której dane państwo trzecie jest stowarzyszone z programem „Cyfrowa Europa".

(5) Jak przewidziano w art. 19 rozporządzenia (UE) 2025/38, państwa trzecie stowarzyszone z programem „Cyfrowa Europa" powinny mieć możliwość wystąpienia o wsparcie z rezerwy cyberbezpieczeństwa UE, w przypadku gdy podmioty, które potrzebują wsparcia z tej rezerwy, są podmiotami działającymi w sektorach kluczowych lub w innych sektorach krytycznych oraz w przypadku gdy wykryte incydenty prowadzą do znaczących zakłóceń operacyjnych lub mogą mieć skutki uboczne w Unii. Państwa trzecie stowarzyszone z programem „Cyfrowa Europa" powinny kwalifikować się do otrzymania wsparcia tylko wtedy, gdy umowa, na podstawie której są one stowarzyszone z programem „Cyfrowa Europa", wyraźnie przewiduje takie wsparcie. Ponadto takie państwa trzecie powinny w dalszym ciągu kwalifikować się do otrzymania wsparcia wyłącznie wówczas, gdy nadal spełnione są trzy kryteria. Po pierwsze, dane państwo trzecie powinno w pełni przestrzegać odpowiednich postanowień wspomnianej umowy. Po drugie, biorąc pod uwagę komplementarny charakter rezerwy cyberbezpieczeństwa UE, państwo trzecie powinno było podjąć 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 powinno być spójne z polityką Unii wobec tego państwa i ogólnymi stosunkami z tym państwem oraz z innymi politykami Unii w dziedzinie bezpieczeństwa.

(6) 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. W związku z tym i zgodnie z art. 19 ust. 4 rozporządzenia (UE) 2025/38 akt wykonawczy Rady może określać maksymalną liczbę dni, nie mniejszą niż 75, przez które takie wsparcie może być udzielane w odpowiedzi na złożony wniosek. Rada powinna podjąć działanie na podstawie wniosku Komisji, z należytym uwzględnieniem dokonanej przez Komisję oceny trzech kryteriów.

(7) Mołdawia dotkliwie odczuwa skutki rosyjskiej wojny napastniczej przeciwko Ukrainie, a jednocześnie stanowi bezpośredni cel prowadzonych przez Rosję działań hybrydowych mających na celu destabilizację tego kraju i osłabienie jego starań na drodze do członkostwa w UE. W tym kontekście Unia udzieliła Mołdawii kompleksowego wsparcia mającego ułatwić sprostanie wyzwaniom, przed którymi kraj ten stoi w związku z rosyjską wojną napastniczą przeciwko Ukrainie, oraz

mającego wzmocnić odporność, bezpieczeństwo i stabilność tego kraju w obliczu bezpośrednich destabilizujących działań Rosji.

(8) W dniu 24 kwietnia 2023 r. Rada zatwierdziła ustanowienie, w ramach wspólnej polityki bezpieczeństwa i obrony, cywilnej partnerskiej misji Unii Europejskiej w Mołdawii w celu zapewnienia doradztwa strategicznego i wsparcia operacyjnego w obszarach zarządzania kryzysowego i przeciwdziałania zagrożeniom hybrydowym. Od 2021 r. UE udziela również, za pośrednictwem Europejskiego Instrumentu na rzecz Pokoju, konsekwentnego wsparcia mającego wzmocnić zdolności Mołdawii w obszarze wojskowo-obronnym. Podpisany w dniu 21 maja 2024 r. dokument ustanawiający partnerstwo UE i Mołdawii w dziedzinie bezpieczeństwa i obrony usprawnił strukturę współpracy UE z Mołdawią w kluczowych obszarach pokoju, bezpieczeństwa i obrony. Ponadto przyjęty przez Komisję w dniu 10 października 2024 r. komunikat w sprawie Planu wzrostu gospodarczego dla Mołdawii ma na celu wsparcie reform społeczno-gospodarczych w Mołdawii oraz zwiększenie dostępu tego kraju do jednolitego rynku UE, przy czym założono konkretne reformy w obszarze zarządzania cyberbezpieczeństwem.

(9) Komisja oceniła trzy kryteria określone w art. 19 ust. 3 rozporządzenia (UE) 2025/38 w odniesieniu do Mołdawii i uznała je za spełnione. Dokonując tej oceny, Komisja skonsultowała się również z Wysokim Przedstawicielem Unii ds. Zagranicznych i Polityki Bezpieczeństwa,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Niniejszym zezwala się na udzielenie Republice Mołdawii wsparcia z rezerwy cyberbezpieczeństwa UE w rozumieniu art. 19 rozporządzenia (UE) 2025/38, zgodnie z wnioskiem Komisji przedłożonym na podstawie art. 19 ust. 3 rozporządzenia (UE) 2025/38.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia i decyzję tę stosuje się nie dłużej niż przez rok.

Sporządzono w Brukseli dnia r.

W imieniu Rady
Przewodniczący