



COMMISSION
EUROPÉENNE

Bruxelles, le 18.5.2026
COM(2026) 239 final

2026/0118 (NLE)

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

autorisant l'octroi d'une aide de la réserve de cybersécurité de l'Union à l'Ukraine

Proposition de

DÉCISION D'EXÉCUTION DU CONSEIL

autorisant l'octroi d'une aide de la réserve de cybersécurité de l'Union à l'Ukraine

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694¹ (ci-après le «règlement sur la cybersolidarité»), et notamment son article 19, paragraphe 4,

vu la proposition de la Commission européenne,

considérant ce qui suit:

- (1) Le 23 juin 2022, le Conseil européen a accordé à l'Ukraine le statut de pays candidat. La décision était fondée sur le respect par l'Ukraine des conditions énoncées dans l'avis de la Commission de juin 2022 sur la demande d'adhésion de l'Ukraine. Le 14 décembre 2023, le Conseil européen a décidé d'ouvrir des négociations d'adhésion avec l'Ukraine, à la suite de la recommandation émise par la Commission.
- (2) Le 19 décembre 2024, le Conseil européen a réaffirmé son soutien sans faille à la souveraineté et à l'intégrité territoriale de l'Ukraine, en insistant sur la fourniture d'un soutien politique, financier, économique, humanitaire, militaire et diplomatique aussi longtemps que nécessaire. Ces actions soulignent l'attachement de l'Union au maintien de la sécurité européenne, démontrant que le soutien à l'Ukraine fait partie intégrante des objectifs de l'Union en matière de sécurité.
- (3) Les répercussions économiques et sociétales des incidents de cybersécurité continuent de se faire sentir tant au sein de l'Union qu'à l'échelle mondiale. Les cybermenaces évoluent de manière particulièrement rapide dans certains pays candidats à l'adhésion à l'Union où d'éventuels incidents de cybersécurité importants ou majeurs sont susceptibles de perturber et d'endommager des infrastructures critiques, d'interférer avec le bon fonctionnement de leurs économies et de leurs institutions, ou d'exposer les entités et les citoyens à des risques graves pour la sûreté et la sécurité publiques. Dans ce contexte, les cyberattaques pourraient également provoquer de nouvelles tensions géopolitiques et menacer les infrastructures critiques, les processus démocratiques et l'infrastructure électorale.

¹ JO L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>.

- (4) La guerre d'agression menée par la Russie contre l'Ukraine a eu un effet préjudiciable et perturbateur sur les réseaux et les systèmes d'information ukrainiens de services essentiels tels que les voies ferroviaires ou les registres d'État ukrainiens. L'agression militaire s'est accompagnée de cyberattaques constantes de la Russie contre les infrastructures critiques de l'Ukraine, y compris le ciblage du réseau satellitaire KA-SAT, détenu par Viasat, à la veille de l'invasion à grande échelle de février 2022.
- (5) Compte tenu de la nature imprévisible des cyberattaques, du fait qu'elles ne se limitent souvent pas à une zone géographique déterminée et qu'elles présentent un risque élevé de propagation, le renforcement de la résilience des pays voisins et leur capacité à réagir efficacement à des incidents de cybersécurité importants et majeurs contribuent à la protection de l'Union dans son ensemble, en particulier de son marché intérieur et de ses entreprises. Par conséquent, le règlement (UE) 2025/38 dispose que les pays tiers parties à un accord d'association avec l'Union autorisant leur participation au programme pour une Europe numérique peuvent bénéficier d'une aide de la réserve de cybersécurité de l'Union (ci-après dénommée «réserve»), sur tout ou partie de leurs territoires, lorsque l'accord associant le pays tiers au programme pour une Europe numérique le stipule.
- (6) Conformément à l'article 19 du règlement (UE) 2025/38, un pays tiers ne peut demander une aide de la réserve que lorsque cela est spécifiquement prévu dans l'accord d'association entre ce pays et le programme pour une Europe numérique. En outre, ce pays tiers ne devrait pouvoir bénéficier de l'aide que lorsque trois critères énoncés à l'article 19, paragraphe 3, du règlement (UE) 2025/38 sont remplis. Premièrement, le pays tiers doit se conformer pleinement aux dispositions pertinentes de cet accord. Deuxièmement, compte tenu du caractère complémentaire de la réserve, le pays tiers doit avoir pris des mesures adéquates pour se préparer aux incidents de cybersécurité importants ou assimilés à des incidents majeurs. Troisièmement, l'octroi d'une aide de la réserve doit être compatible avec la politique de l'Union à l'égard de ce pays et avec ses relations globales avec ce pays, ainsi qu'avec les autres actions de l'Union dans le domaine de la sécurité.
- (7) L'Ukraine est partie à un accord d'association relatif à la participation au programme pour une Europe numérique (2021-2027) signé le 5 septembre 2022 avec l'Union européenne. Conformément à l'article 1^{er} de cet accord d'association, l'Ukraine est autorisée à participer au programme pour une Europe numérique, et notamment à bénéficier d'un soutien de la réserve de cybersécurité de l'Union. L'accord comprend des dispositions exigeant de l'Ukraine qu'elle se conforme aux obligations énoncées à l'article 19, paragraphes 2 et 9, du règlement (UE) 2025/38.
- (8) L'octroi d'une aide aux pays tiers associés au programme pour une Europe numérique peut avoir une incidence sur les relations avec les pays tiers et la politique de sécurité de l'Union, notamment dans le contexte de la politique étrangère et de sécurité commune et de la politique de défense et de sécurité commune. Le Conseil agit sur la base d'une proposition de la Commission, en tenant dûment compte de l'évaluation des trois critères visés à l'article 19, paragraphe 3, du règlement (UE) 2025/38 par la Commission.
- (9) L'Union a mis en place une série de mécanismes, d'instruments de financement et de facilités pour soutenir la sécurité, la défense et la résilience de l'Ukraine, notamment la facilité européenne pour la paix, qui finance le soutien militaire, et le Fonds d'assistance à l'Ukraine, lancé en 2024. Elle a également lancé la mission d'assistance militaire de l'UE en Ukraine en 2022 afin de former les forces armées ukrainiennes et

de renforcer la mission de conseil de l'Union européenne sur la réforme du secteur de la sécurité civile en Ukraine, opérationnelle depuis 2014. Ensemble, toutes ces initiatives constituent une réponse coordonnée et solide pour renforcer la sécurité, la défense et la résilience de l'Ukraine. En juin 2024, l'Union et l'Ukraine ont adopté des engagements conjoints en matière de sécurité, dans le cadre desquels les deux parties se sont notamment engagées à renforcer leur coopération en matière de résilience, en mettant l'accent sur la lutte contre les menaces hybrides et les cybermenaces et contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, ainsi que sur la protection des infrastructures critiques. Le dialogue UE-Ukraine sur le cyberspace établi en 2022 reste une plateforme centrale pour aborder la coopération politique et technique sur les questions liées au cyberspace.

- (10) La Commission a évalué, en ce qui concerne l'Ukraine, les trois critères énoncés à l'article 19, paragraphe 3, du règlement (UE) 2025/38 et considère qu'ils sont remplis. Pour réaliser cette évaluation, elle a également consulté le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité.
- (11) Conformément à l'article 19, paragraphe 6, du règlement (UE) 2025/38, le Conseil considère que l'Ukraine respecte les dispositions pertinentes de l'accord associant ce pays au programme pour une Europe numérique et a pris les mesures adéquates pour se préparer aux incidents de cybersécurité importants et aux incidents de cybersécurité assimilés à des incidents majeurs. En outre, le Conseil estime que l'octroi d'une aide de la réserve est compatible avec la politique de l'Union à l'égard de l'Ukraine et avec ses relations globales avec ce pays, ainsi qu'avec les autres actions de l'Union dans le domaine de la sécurité, notamment à la lumière des facteurs exposés au considérant 8.
- (12) Il convient donc d'autoriser un soutien à l'Ukraine au titre de la réserve.
- (13) Afin de permettre une assistance immédiate selon les critères énoncés dans l'acte de base, la présente décision devrait entrer en vigueur de toute urgence. Afin de permettre un soutien adéquat et en temps utile, la décision devrait s'appliquer pendant un an.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'octroi à l'Ukraine d'une aide de la réserve de cybersécurité de l'Union au sens de l'article 19 du règlement (UE) 2025/38 est autorisé.

Article 2

La présente décision entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable jusqu'au [Office des publications: insérer la date d'entrée en vigueur + un an].

Fait à Bruxelles, le

*Par le Conseil
Le président/la présidente*