Journal officiel
de l'Union européenne

FR
Série L

2026/2550

16.11.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/2550 DU CONSEIL

du 16 novembre 2026

mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

LE CONSEIL DE L'UNION EUROPÉENNE,

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

vu le règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres [1], et notamment son article 13, paragraphe 1,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 17 mai 2019, le Conseil a adopté le règlement (UE) 2019/796.

(2) Dans le cadre d'une action continue, adaptée et coordonnée de l'Union contre les acteurs persistants de cybermenaces, il convient d'ajouter une entité sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe I du règlement (UE) 2019/796. Cette entité est responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union et ses États membres, ainsi que de cyberattaques ayant des effets importants contre des États tiers.

(3) Il y a donc lieu de modifier le règlement (UE) 2019/796 en conséquence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

L'annexe I du règlement (UE) 2019/796 est modifiée conformément à l'annexe du présent règlement.

Article 2

Le présent règlement entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 16 novembre 2026.

Par le Conseil

La présidente

K. KALLAS

[1] JO L 129 I du 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANNEXE

À l'annexe I du règlement (UE) 2019/796, la mention suivante est ajoutée sous la rubrique «B. Personnes morales, entités et organismes»:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«12.	NoName057(16)	Autres dénominations: 05716nnm, Nnm05716, NoName057, NoName05716	NoName057(16) est un groupe de hackers pro-russe apparu pour la première fois en mars 2022 et qui revendique des cyberattaques ciblant des organismes gouvernementaux, des infrastructures critiques et des entreprises privées d'Ukraine, des États-Unis et de l'UE. NoName057(16) utilise l'outil DDoSia au moyen duquel elle mène des attaques par déni de service en adressant de façon répétée des requêtes réseau aux sites internet ciblés. Après ces attaques, le groupe les revendique, traite les cibles et adresse des menaces sur le dark web ou sur des chaînes Telegram. NoName057(16) se livre à des cyberattaques ayant un impact significatif qui constituent une menace extérieure pesant sur l'Union ou ses États membres. NoName057(16) a pris pour cible des services nécessaires au maintien d'activités sociales et économiques essentielles et de fonctions étatiques critiques d'États membres, y compris des portails gouvernementaux, des services de renseignement militaire, des partis politiques et des candidats au cours de processus électoraux, le secteur énergétique et industriel, des infrastructures de transport, des installations d'alimentation en eau, des banques, des institutions financières et des services de paiement en ligne, et des bureaux de poste nationaux. NoName057(16) est donc responsable de cyberattaques ayant un impact significatif qui constituent une menace extérieure pesant sur les États membres. Cette entité est également responsable de cyberattaques ayant un impact significatif contre des États tiers.	16.11.2026»