2026/589

16.3.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/589 DU CONSEIL

du 16 mars 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 EUROPEENNE,

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'inscrire deux personnes physiques et trois entités 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. Ces personnes physiques et entités sont responsables de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres, ou sont impliqués dans de telles cyberattaques.

(3) Il y a donc lieu de modifier l'annexe I du 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 mars 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

L'annexe I du règlement (UE) 2019/796 est modifiée comme suit:

1) Les mentions ci-après sont ajoutées sous la rubrique «A. Personnes physiques»:

	Nom	Informations d'identification	Motifs de l'inscription	Date d'inscription
«18.	CHEN Cheng	陈诚 (en chinois) Alias: Jesse Chen ou lengmo ou l3n6m0 Date de naissance: 20.10.1984 Lieu de naissance: Yancheng, Jiangsu, Chine Nationalité: chinoise Sexe: masculin	Chen Cheng est un homme d'affaires chinois, cofondateur d'Anxun Information Technology Co. Ltd et l'un de ses directeurs généraux (directeur opérationnel). Il est également un représentant légal de la branche de cette société dans le Sichuan. Anxun Information Technology Co. Ltd., également connue sous le nom d'i-Soon, est une société basée en République populaire de Chine (RPC) qui propose des services de "piratage informatique". Anxun Information Technology Co. Ltd. a ciblé des infrastructures critiques et des fonctions critiques des États membres et a accédé à des informations classifiées qu'elle a vendues. En outre, Anxun Information Technology Co. Ltd. a attaqué des gouvernements de plusieurs États tiers, menaçant ainsi les objectifs de la politique étrangères et de sécurités commune (PESC) de l'Union, tels qu'ils sont énoncés à l'article 21, paragraphe 2, points a) à c), du traité sur l'Union européenne. Anxun Information Technology Co. Ltd. tire un avantage matériel important des services fournis. Anxun Information Technology Co. Ltd. est donc responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union et ses États membres ainsi que d'attaques contre des États tiers. De par ses fonctions, Chen Cheng est responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres, ainsi que de cyberattaques ayant des effets importants visant des États tiers, et est impliqué dans de telles cyberattaques.	16.3.2026

	Nom	Informations d'identification	Motifs de l'inscription	Date d'inscription
19.	WU Haibo	吴海波 (en chinois) Alias: shutdown ou shutd0wn Lieu de naissance: Chine Nationalité: chinoise Sexe: masculin	Wu Haibo est un homme d'affaires chinois, cofondateur d'Anxun Information Technology Co. Ltd. et l'un de ses directeurs généraux (Président directeur général). Il est également représentant légal, président et directeur général de la branche de Shanghaï ("maison mère") d'Anxun Information Technology Co. Ltd. En outre, il agit en tant que représentant légal de la branche de cette société dans le Sichuan. Anxun Information Technology Co. Ltd., également connue sous le nom d'i-Soon, est une société basée en République populaire de Chine (RPC) qui propose des services de "piratage informatique". Anxun Information Technology Co. Ltd. a ciblé des infrastructures critiques et des fonctions critiques des États membres et a accédé à des informations classifiées qu'elle a vendues. En outre, Anxun Information Technology Co. Ltd. a attaqué des gouvernements de plusieurs États tiers, menaçant ainsi les objectifs de la politique étrangères et de sécurités commune (PESC) de l'Union, tels qu'ils sont énoncés à l'article 21, paragraphe 2, points a) à c), du traité sur l'Union européenne. Anxun Information Technology Co. Ltd. tire un avantage matériel important des services fournis. Anxun Information Technology Co. Ltd. est donc responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres de l'UE ainsi que les attaques contre les États tiers. Wu Haibo a participé à la direction et à la promotion de tentatives de cyberattaques ayant des effets importants dirigées contre des États membres. De par ses fonctions, il est responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres, ainsi que de cyberattaques ayant des effets importants visant des États tiers, et est impliqué dans de telles cyberattaques.	16.3.2026»

2) Les mentions ci-après sont ajoutées sous la rubrique «B. Personnes morales, entités et organismes»:

	Nom	Informations d'identification	Motifs de l'inscription	Date d'inscription
«5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (en chinois) Autres dénominations: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresse: Fenghao East Road, Room 103, Building 6, No. 9, District de Haidian, Pékin, Chine Lieu d'enregistrement: Pékin, Chine Date d'enregistrement: 2.9.2010 Code de crédit social unifié: 91110108562135265P	Integrity Technology Group est une entreprise de cybersécurité basée en République populaire de Chine (RPC), qui a facilité des cyberattaques liées à la menace persistante avancée (APT) Flax Typhoon. Cette APT a utilisé les produits et la technologie d'Integrity Technology Group pour déployer ses activités d'exploitation de réseaux informatiques. Les produits d'Integrity Technology Group ont été utilisés depuis lors pour compromettre des dispositifs reposant sur l'internet des objets et y accéder dans les États membres, ainsi que dans les pays d'Europe et du monde entier. Entre 2022 et 2023, Flax Typhoon a accédé à au moins 65 600 dispositifs reposant sur l'internet des objets dans six États membres en utilisant des produits d'Integrity Technology Group. Par conséquent, les produits commerciaux et l'infrastructure d'Integrity Technology Group ont été régulièrement utilisés dans le cadre de cyberattaques visant des États membres ainsi que des États tiers. Par conséquent, en affectant les systèmes d'information relatifs aux infrastructures numériques, Integrity Technology Group fournit un soutien technique et matériel aux cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres et des États tiers.	16.3.2026

	Nom	Informations d'identification	Motifs de l'inscription	Date d'inscription
6.	Emennet Pasargad	Autres dénominations: Anzu Team ou Holy Souls ou Aria Sepehr Ayandehsazan ou Haywire Kitten Lieu d'enregistrement: Téhéran, Iran Numéro d'enregistrement: 554267 Principal établissement: Téhéran, Iran	Emennet Pasargad est un cyberacteur iranien (société) qui a ciblé de nombreuses entités, en particulier dans les États membres, ainsi qu'aux États-Unis. Emennet Pasargad, agissant sous la dénomination "Anzu Team", a ciblé l'infrastructure numérique en Suède et compromis un service de SMS suédois, affectant un grand nombre de personnes. En outre, agissant sous la dénomination "Holy Souls", l'entité a compromis la base de données des abonnés du magazine satirique français *Charlie Hebdo* et l'a mise en vente sur le dark web. Emennet Pasargad a compromis la diffusion de publicités lors des Jeux olympiques de Paris et a diffusé des campagnes de désinformation. Emennet Pasargad a également tenté d'interférer avec les élections présidentielles des États-Unis de 2020, par la même menaçant la démocratie et l'état de droit, en obtenant des informations confidentielles sur les électeurs américains, ainsi qu'un accès non autorisé au réseau informatique d'une société de médias américaine. Emennet Pasargad est donc responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres, ainsi que de cyberattaques ayant des effets importants visant un État tiers.	16.3.2026

	Nom	Informations d'identification	Motifs de l'inscription	Date d'inscription
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (en chinois) Autre dénomination: i-Soon Adresse: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, District de Minhang, Shanghaï Code de crédit social unifié: 91510105332025597A (branche du Sichuan) Code de crédit social unifié: 91310116561906136G (branche de Shanghaï) Sites internet: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Numéros de téléphone: +862161119992, +8605645893417, +8613761671735, +864000665915 Courriels: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. est une société basée en République populaire de Chine qui propose des services de "piratage informatique". Elle a ciblé des infrastructures critiques et des fonctions critiques des États membres et a accédé à des informations classifiées qu'elle a vendues. En outre, Anxun Information Technology Co. Ltd. a attaqué des gouvernements de plusieurs États tiers, menaçant ainsi les objectifs de la politique étrangères et de sécurités commune (PESC) de l'Union, tels qu'ils sont énoncés à l'article 21, paragraphe 2, points a) à c), du traité sur l'Union européenne. Anxun Information Technology Co. Ltd. tire un avantage matériel important des services fournis. Anxun Information Technology Co. Ltd. est donc responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres, ainsi que de cyberattaques ayant des effets importants visant des États tiers.	16.3.2026»