Journal officiel
de l'Union européenne

FR
Série L

2025/173

27.1.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/173 DU CONSEIL

du 27 janvier 2025

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 17 mai 2019 du Conseil 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) Des mesures restrictives ciblées contre les cyberattaques ayant des effets importants et constituant une menace extérieure pour l'Union ou ses États membres font partie des mesures prévues dans le cadre de l'Union pour une réponse diplomatique conjointe face aux actes de cybermalveillance, à savoir la boîte à outils cyberdiplomatique, et sont un instrument essentiel pour prévenir, dissuader, décourager et contrer de telles activités.

(3) Les actes de cybermalveillance contre les infrastructures critiques ou services essentiels, y compris par l'utilisation de rançongiciels et de logiciels malveillants d'effacement de données (wipers), le ciblage de chaînes d'approvisionnement et le cyberespionnage, y compris les activités de vol de propriété intellectuelle, sont de plus en plus nombreux, fréquents et sophistiqués. En raison de leurs effets perturbateurs et destructeurs, ces activités constituent une menace systémique pour la sécurité, l'économie et la démocratie et la société de l'Union dans son ensemble.

(4) En 2020, des cyberattaques ayant des effets importants ont été commises contre l'Estonie. Ces cyberattaques ont été menées contre des systèmes informatiques de plusieurs institutions, dans le but d'utiliser les données pour compromettre la sécurité de l'Estonie. Ces cyberattaques concernaient le stockage d'informations classifiées.

(5) Dans le cadre d'une action continue, adaptée et coordonnée de l'Union contre les acteurs persistants de cybermenaces, il convient d'inscrire trois personnes physiques 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 sont responsables de cyberattaques ayant des effets importants et constituant une menace extérieure pour l'Union ou ses États membres, ou y participent.

(6) 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 27 janvier 2025.

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, les mentions ci-après sont ajoutées sous la rubrique «A. Personnes physiques»:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Date de naissance: 16.9.1997 Nationalité: russe Sexe: masculin Entités associées: Direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie	Nikolay Korchagin est responsable de cyberattaques ayant des effets importants et y participe en menant des activités de renseignement dirigées contre l'Estonie et en accédant illégalement à un système informatique. Nikolay Korchagin est un officier de l'unité militaire 29155 de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GRU). À ce titre, il est responsable de cyberattaques contre des systèmes informatiques, et y participe, dans le but de collecter des informations dans les systèmes de données de plusieurs institutions, qui, de manière indépendante ou combinée, donnent une vue d'ensemble de la politique de cybersécurité de l'Estonie, des cybercapacités de l'État, ainsi que des données à caractère personnel sensibles et autres données sensibles, dans le but de les utiliser pour compromettre la sécurité de l'Estonie. Les attaques touchent donc au stockage d'informations classifiées. Ces attaques ont concerné des alliés et des partenaires de l'Estonie. Par conséquent, Nikolay Korchagin est responsable de cyberattaques ayant des effets importants et constituant une menace extérieure pour un État membre, et y participe.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Date de naissance: 1.9.1997 Nationalité: russe Sexe: masculin Entités associées: Direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie	Vitaly Shevchenko est responsable de cyberattaques ayant des effets importants et y participe en menant des activités de renseignement dirigées contre l'Estonie et en accédant illégalement à un système informatique. Vitaly Shevchenko est un officier de l'unité militaire 29155 de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GRU). À ce titre, il est responsable de cyberattaques contre des systèmes informatiques, et y participe, dans le but de collecter des informations dans les systèmes de données de plusieurs institutions, qui, de manière indépendante ou combinée, donnent une vue d'ensemble de la politique de cybersécurité de l'Estonie, des cybercapacités de l'État, ainsi que des données à caractère personnel sensibles et autres données sensibles, dans le but de les utiliser pour compromettre la sécurité de l'Estonie. Les attaques touchent donc au stockage d'informations classifiées. Ces attaques ont concerné des alliés et des partenaires de l'Estonie. Par conséquent, Vitaly Shevchenko est responsable de cyberattaques ayant des effets importants et constituant une menace extérieure pour un État membre, et y participe.	27.1.2025

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Date de naissance: 17.6.1980 Nationalité: russe Sexe: masculin Entités associées: Direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie	Yuriy Denisov est responsable de cyberattaques ayant des effets importants et y participe en menant des activités de renseignement dirigées contre l'Estonie et en accédant illégalement à un système informatique. Yuriy Denisov est un officier de l'unité militaire 29155 de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GRU). À ce titre, il est responsable de cyberattaques contre des systèmes informatiques, et y participe, dans le but de collecter des informations dans les systèmes de données de plusieurs institutions, qui, de manière indépendante ou combinée, donnent une vue d'ensemble de la politique de cybersécurité de l'Estonie, des cybercapacités de l'État, ainsi que des données à caractère personnel sensibles et autres données sensibles, dans le but d'utiliser les données pour compromettre la sécurité de l'Estonie. Les attaques touchent donc au stockage d'informations classifiées. Ces attaques ont concerné des alliés et des partenaires de l'Estonie. Par conséquent, Yuriy Denisov est responsable de cyberattaques ayant des effets importants et constituant une menace extérieure pour un État membre, et y participe.	27.1.2025»