DÉCISIONS

DÉCISION (PESC) 2020/1537 DU CONSEIL

du 22 octobre 2020

modifiant la décision (PESC) 2019/797 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 l'Union européenne, et notamment son article 29,

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 la décision (PESC) 2019/797 ([1]).

(2) Des mesures restrictives ciblées contre les cyberattaques ayant des effets importants qui constituent 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 (la boîte à outils cyberdiplomatique) et sont un instrument essentiel pour dissuader et contrer de telles activités.

(3) Afin d'empêcher, de décourager et de prévenir la poursuite et l'augmentation des actes de cybermalveillance ainsi que d'y faire face, il convient d'inscrire deux personnes physiques et un organisme sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe de la décision (PESC) 2019/797. Ces personnes et cet organisme sont responsables de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres, notamment de la cyberattaque contre le parlement fédéral allemand («*Deutscher Bundestag*») qui s'est déroulée en avril et mai 2015, ou y ont participé.

(4) Il y a donc lieu de modifier la décision (PESC) 2019/797 en conséquence,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'annexe de la décision (PESC) 2019/797 est modifiée conformément à l'annexe de la présente décision.

Article 2

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

Fait à Bruxelles, le 22 octobre 2020.

Par le Conseil
Le président
M. ROTH

([1]) Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 129 I du 17.5.2019, p. 13).

ANNEXE

Les mentions ci-après sont ajoutés à la liste des personnes physiques et morales, des entités et des organismes figurant à l'annexe de la décision (PESC) 2019/797:

A. Personnes physiques

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Date de naissance: 15 novembre 1990 Lieu de naissance: Koursk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Nationalité: russe Sexe: masculin	Dmitry Badin a participé à une cyberattaque ayant des effets importants dirigée contre le parlement fédéral allemand ("*Deutscher Bundestag*"). En tant que membre du renseignement militaire du 85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Dmitry Badin a fait partie d'une équipe de membres du renseignement militaire russe qui a mené une cyberattaque contre le parlement fédéral allemand ("*Deutscher Bundestag*") en avril et mai 2015. Cette cyberattaque a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de la chancelière Angela Merkel, ont été affectés.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Date de naissance: 21 février 1961 Nationalité: russe Sexe: masculin	Igor Kostyukov est actuellement le chef de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), dont il a précédemment été le premier chef adjoint. L'une des unités sous son commandement est le 85e Centre principal des services spéciaux (GTsSS), également appelé unité militaire 26165 (alias techniques: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" et "Strontium"). À ce titre, Igor Kostyukov est responsable des cyberattaques menées par le GTsSS, y compris de celles ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres. En particulier, des membres du renseignement militaire du GTsSS ont participé à la cyberattaque contre le parlement fédéral allemand ("*Deutscher Bundestag*") qui s'est déroulée en avril et mai 2015 et à la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas en avril 2018. La cyberattaque contre le parlement fédéral allemand a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de la chancelière Angela Merkel, ont été affectés.	22.10.2020»

B. Personnes morales, entités et organismes

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«4.	85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU)	Adresse: Komsomol'skiy Prospekt, 20, Moscou, 119146, Fédération de Russie	Le 85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), également appelé "unité militaire 26165" (alias techniques: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" et "Strontium") est responsable de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres. En particulier, des membres du renseignement militaire du GTsSS ont participé à la cyberattaque contre le parlement fédéral allemand ("*Deutscher Bundestag*") qui s'est déroulée en avril et mai 2015 et à la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas en avril 2018. La cyberattaque contre le parlement fédéral allemand a ciblé le système d'information du parlement et en a perturbé le fonctionnement pendant plusieurs jours. Une importante quantité de données a été volée et les comptes de courrier électronique de plusieurs parlementaires, ainsi que de la chancelière Angela Merkel, ont été affectés.	22.10.2020»