Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

Arrêté du 22 octobre 2020 portant application des articles L. 562-3, L. 745-13, L. 755-13 et L. 765-13 du code monétaire et financier

NOR : *ECOT2028707A*

Par arrêté du ministre de l'économie, des finances et de la relance en date du 22 octobre 2020, vu la décision 2019/797/PESC du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats, modifiée notamment par la décision (PESC) 2020/1537 du 22 octobre 2020 ; vu le code monétaire et financier, notamment ses articles L. 562-3, L. 745-13, L. 755-13 et L. 765-13.

A Saint-Barthélemy, Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises, les fonds et ressources économiques qui appartiennent à, sont possédés, détenus ou contrôlés par les personnes mentionnées dans l'annexe sont gelés.

Le présent arrêté entre en vigueur à la date de sa publication au *Journal officiel* de la République française pour une durée de six mois.

Notification des voies et délais de recours

Le présent arrêté peut être contesté dans les deux mois à compter de sa notification, soit par recours gracieux adressé au ministère de l'économie, des finances et de la relance au 139, rue de Bercy, 75572 Paris Cedex 12, télédoc 233, ou à sanctions-gel-avoirs@dgtresor.gouv.fr, soit par recours contentieux auprès du tribunal administratif de Paris, 7, rue de Jouy, 75181 Paris Cedex 04, téléphone : 01-44-59-44-00, télécopie : 01-44-59-46-46, urgences télécopie référés : 01-44-59-44-99, greffe.ta-paris@juradm.fr. En l'absence de réponse à un recours gracieux dans les deux mois qui suivent la date du recours, il y a rejet implicite de la demande et le tribunal administratif de Paris pourra être saisi dans les deux mois suivant le rejet implicite.

ANNEXE

* 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

Renseignements complémentaires : 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 Etats 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.

Désigné par le règlement (UE) 2020/1536 du 22/10/2020

* KOSTYUKOV Igor Olegovich

Date de naissance : 21/02/1961

Nationalité : russe - sexe : masculin

Renseignement complémentaires : 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 »). A 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 Etats 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.

Désigné par le règlement (UE) 2020/1536 du 22/10/2020

* BADIN

Dmitry Sergeyevich

Date de naissance : 15/11/1990

Lieu de naissance : Koursk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie)

Nationalité : russe - sexe : masculin

Renseignements complémentaires : 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.

Désigné par le règlement (UE) 2020/1536 du 22/10/2020