DÉCISION (PESC) 2020/1127 DU CONSEIL

du 30 juillet 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. Des mesures restrictives peuvent également être appliquées en réponse à des cyberattaques ayant des effets importants dirigées contre des pays tiers ou des organisations internationales, lorsque cela est jugé nécessaire à la réalisation des objectifs de la politique étrangère et de sécurité commune énoncés dans les dispositions pertinentes de l'article 21 du traité sur l'Union européenne.

(3) Le 16 avril 2018, le Conseil a adopté des conclusions dans lesquelles il condamne fermement l'utilisation à des fins malveillantes de technologies de l'information et de la communication, y compris les cyberattaques connues sous les noms de «WannaCry» et de «NotPetya», qui ont causé des dommages et des pertes économiques considérables dans l'Union et ailleurs. Le 4 octobre 2018, les présidents du Conseil européen et de la Commission européenne, ainsi que le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après dénommé «haut représentant»), ont fait part de leurs vives préoccupations dans une déclaration commune concernant une tentative de cyberattaque visant à porter atteinte à l'intégrité de l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas, un acte agressif qui témoigne d'un mépris pour l'objectif solennel de l'OIAC. Dans une déclaration faite au nom de l'Union le 12 avril 2019, le haut représentant a exhorté les acteurs à mettre un terme aux actes de cybermalveillance qui visent à saper l'intégrité, la sécurité et la compétitivité économique de l'Union, y compris aux actes de vol de propriété intellectuelle facilités par les technologies de l'information et de la communication. Parmi ces vols de propriété intellectuelle facilités par les technologies de l'information et de la communication figurent ceux commis par l'acteur connu sous le nom de «APT10» («*Advanced Persistent Threat 10*»).

(4) Dans ce contexte, et 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 six personnes physiques et trois entités ou organismes 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 entités ou organismes sont responsables de cyberattaques ou de tentatives de cyberattaques, y compris la tentative de cyberattaque contre l'OIAC et les cyberattaques connues sous les noms de «WannaCry», «NotPetya» et «Operation Cloud Hopper», y ont apporté leur soutien, y ont participé ou les ont facilitées.

(5) 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.

([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 129I du 17.5.2019, p. 13).

Article 2

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

Fait à Bruxelles, le 30 juillet 2020.

Par le Conseil
Le président
M. ROTH

ANNEXE

Les personnes et entités ou organismes 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
1.	GAO Qiang	Lieu de naissance: Province de Shandong, Chine Adresse: Chambre 1102, Guanfu Mansion, 46 Xinkai Road, District de Hedong, Tianjin, Chine Nationalité: chinoise Sexe: masculin	Gao Qiang est impliqué dans "Operation Cloud Hopper", une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers. "Operation Cloud Hopper" a ciblé les systèmes d'information d'entreprises multinationales sur six continents, y compris d'entreprises établies dans l'Union, et a permis d'obtenir un accès non autorisé à des données sensibles sur le plan commercial, causant ainsi d'importantes pertes économiques. L'acteur connu sous le nom de "APT10" ("*Advanced Persistent Threat 10*") (*alias* "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") a mené "Operation Cloud Hopper". Gao Qiang peut être relié à APT10, y compris par son association avec l'infrastructure de commandement et de contrôle de APT10. De plus, Gao Qiang a été employé par Huaying Haitai, une entité désignée comme apportant un soutien à "Operation Cloud Hopper" et facilitant celle-ci. Il a des liens avec Zhang Shilong, qui est également désigné en liaison avec "Operation Cloud Hopper". Gao Qiang est donc associé à la fois à Huaying Haitai et à Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Adresse: Hedong, Yuyang Road n° 121, Tianjin, Chine Nationalité: chinoise Sexe: masculin	Zhang Shilong est impliqué dans "Operation Cloud Hopper", une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers. "Operation Cloud Hopper" a ciblé les systèmes d'information d'entreprises multinationales sur six continents, y compris d'entreprises établies dans l'Union, et a permis d'obtenir un accès non autorisé à des données sensibles sur le plan commercial, causant ainsi d'importantes pertes économiques. L'acteur connu sous le nom de "APT10" ("*Advanced Persistent Threat 10*") (*alias* "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") a mené "Operation Cloud Hopper".	30.7.2020

			Zhang Shilong peut être relié à "APT10", y compris par le logiciel malveillant qu'il a développé et testé en liaison avec les cyberattaques menées par "APT10". De plus, Zhang Shilong a été employé par Huaying Haitai, une entité désignée comme apportant un soutien à "Operation Cloud Hopper" et facilitant celle-ci. Il a des liens avec Gao Qiang, qui est également désigné en liaison avec "Operation Cloud Hopper". Zhang Shilong est donc associé à la fois à Huaying Haitai et à Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Date de naissance: 27 mai 1972 Lieu de naissance: Oblast de Perm, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 120017582 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17 avril 2017 au 17 avril 2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Alexey Minin a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. En tant qu'agent de soutien en matière de renseignement humain au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Alexey Minin a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Date de naissance: 31 juillet 1977 Lieu de naissance: Oblast de Mourmansk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 100135556 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17 avril 2017 au 17 avril 2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Aleksei Morenets a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. En tant que cyber-opérateur au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Aleksei Morenets a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Date de naissance: 26 juillet 1981 Lieu de naissance: Koursk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 100135555 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17 avril 2017 au 17 avril 2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Evgenii Serebriakov a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. En tant que cyber-opérateur au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Evgenii Serebriakov a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau WiFi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Date de naissance: 24 août 1972 Lieu de naissance: Oulianovsk, République socialiste fédérative soviétique de Russie (aujourd'hui Fédération de Russie) Numéro de passeport: 120018866 Délivré par le ministère des affaires étrangères de la Fédération de Russie Validité: du 17 avril 2017 au 17 avril 2022 Lieu: Moscou, Fédération de Russie Nationalité: russe Sexe: masculin	Oleg Sotnikov a participé à une tentative de cyberattaque ayant des effets potentiels importants dirigée contre l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. En tant qu'agent de soutien en matière de renseignement humain au sein de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), Oleg Sotnikov a fait partie d'une équipe de quatre membres du renseignement militaire russe qui ont tenté d'obtenir un accès non autorisé au réseau Wi-Fi de l'OIAC à La Haye (Pays-Bas) en avril 2018. Si elle avait été couronnée de succès, la tentative de cyberattaque, qui visait le piratage du réseau Wi-Fi de l'OIAC, aurait compromis la sécurité du réseau et les travaux d'enquête en cours de l'OIAC. Le Service du renseignement et de la sécurité militaires des Pays-Bas (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC.	30.7.2020

B. Personnes morales, entités et organismes

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haiti)	*Alias*: Haitai Technology Development Co. Ltd Lieu: Tianjin, Chine	Huaying Haitai a apporté un soutien financier, technique ou matériel à "Operation Cloud Hopper", une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers, et l'a facilitée.	30.7.2020

			"Operation Cloud Hopper" a ciblé les systèmes d'information d'entreprises multinationales sur six continents, y compris d'entreprises établies dans l'Union, et a permis d'obtenir un accès non autorisé à des données sensibles sur le plan commercial, causant ainsi d'importantes pertes économiques. L'acteur connu sous le nom de "APT10" ("*Advanced Persistent Threat 10*") (*alias* "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") a mené "Operation Cloud Hopper". Huaying Haitai peut être reliée à "APT10". De plus, Huaying Haitai a employé Gao Qiang et Zhang Shilong, tous deux désignés en liaison avec "Operation Cloud Hopper". Huaying Haitai est donc associée à Gao Qiang et à Zhang Shilong.	
2.	Chosun Expo	*Alias*: Chosen Expo; Korea Export Joint Venture Lieu: RPDC	Chosun Expo a apporté un soutien financier, technique ou matériel à une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers, y compris les cyberattaques connues sous le nom de "WannaCry" et les cyberattaques lancées contre l'Autorité polonaise de surveillance financière et Sony Pictures Entertainment, ainsi que le cyber-braquage de la banque centrale du Bangladesh et la tentative de cyber-braquage de la banque vietnamienne Tiên Phong, et les a facilitées. "WannaCry" a perturbé des systèmes d'information dans le monde entier en les ciblant au moyen d'un rançongiciel et en bloquant l'accès aux données. Les systèmes d'information d'entreprises présentes dans l'Union, y compris des systèmes d'information relatifs à des services nécessaires à la maintenance de services et d'activités économiques essentiels au sein des États membres, en ont été affectés. L'acteur connu sous le nom de "APT38" ("*Advanced Persistent Threat 38*") ou le "Lazarus Group" ont mené "WannaCry". Chosun Expo peut être reliée à APT38/"Lazarus Group", y compris au moyen des comptes utilisés pour les cyberattaques.	30.7.2020
3.	Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU)	Adresse: 22 Kirova Street, Moscou, Fédération de Russie	Le Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU), également connu par son numéro de poste de campagne 74455, est responsable de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers, y compris les cyberattaques de juin 2017 connues sous les noms de "NotPetya" ou "EternalPetya" et les cyberattaques lancées contre un réseau électrique ukrainien pendant l'hiver 2015-2016.	30.7.2020"

			"NotPetya" ou "EternalPetya" a rendu des données inaccessibles dans un certain nombre d'entreprises au sein de l'Union, de l'Europe au sens large et du monde entier, en ciblant les ordinateurs au moyen d'un rançongiciel et en bloquant l'accès aux données, ce qui a entraîné, entre autres, d'importantes pertes économiques. La cyberattaque lancée contre un réseau électrique ukrainien a provoqué l'arrêt d'une partie de celui-ci pendant l'hiver. L'acteur connu sous le nom de Sandworm (*alias* "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer", ou "Telebots"), qui est également à l'origine de l'attaque lancée contre le réseau électrique ukrainien, a mené "NotPetya" ou "EternalPetya". Le Centre principal des technologies spéciales de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie joue un rôle actif dans les cyberactivités menées par Sandworm et peut être relié à celui-ci.	