Arrêté Ministériel 2020-568 du 3 septembre 2020 portant application de l'Ordonnance Souveraine n° 1.675 du 10 juin 2008 relative aux procédures de gel des fonds mettant en œuvre des sanctions économiques visant à lutter contre les cyberattaques

Nous, Ministre d'État de la Principauté,

Vu l'Ordonnance Souveraine n° 1.675 du 10 juin 2008 relative aux procédures de gel des fonds mettant en œuvre des sanctions économiques ;

Vu la délibération du Conseil de Gouvernement en date du 2 septembre 2020 ;

ARRÊTONS :

ARTICLE PREMIER.

En vertu de l'article premier de l'Ordonnance Souveraine n° 1.675 du 10 juin 2008 relative aux procédures de gel des fonds mettant en œuvre des sanctions économiques, les établissements de crédit et autres institutions financières, les entreprises d'assurance et tout organisme, entité ou personne sont tenus de procéder au gel des fonds et des ressources économiques appartenant, possédés ou détenus par les personnes physiques, entités ou les organismes énumérés à l'annexe du présent arrêté visant :

a) les personnes physiques ou morales, les entités ou les organismes qui sont responsables de cyberattaques ou de tentatives de cyberattaques ;

b) les personnes physiques ou morales, entités ou organismes qui apportent un soutien financier, technique ou matériel, aux cyberattaques ou tentatives de cyberattaques, ou sont impliqués de toute autre manière dans celles-ci, notamment en planifiant, en préparant, en dirigeant, en aidant à préparer, en encourageant de telles attaques, en y participant ou en les facilitant par action ou omission ;

c) les personnes physiques ou morales, entités ou organismes qui sont associés aux personnes physiques ou morales, aux entités ou aux organismes visés aux points a) et b) du présent paragraphe.

Sont constitutives de cyberattaques, les actions suivantes :

a) l'accès aux systèmes d'information ;

b) les atteintes à l'intégrité d'un système d'information ;

c) les atteintes à l'intégrité des données ; ou

d) l'interception de données,

lorsque ces actions ne sont pas dûment autorisées par le propriétaire de tout ou partie du système ou des données ou par une personne détenant tout ou partie des droits sur le système ou les données..

ART. 2.

La liste figurant à l'annexe au présent arrêté pourra être modifiée ou complétée.

ART. 3.

Le Conseiller de Gouvernement-Ministre des Finances et de l'Économie est chargé de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le trois septembre deux mille vingt.

Le Ministre d'État,
P. DARTOUT.

ANNEXE

Annexe à l'Arrêté Ministériel n° 2020-568 du 3 septembre 2020 portant application de l'Ordonnance Souveraine n° 1.675 du 10 juin 2008 relative aux procédures de gel des fonds mettant en œuvre des sanctions économiques visant à lutter contre les cyberattaques

Liste des personnes physiques et morales, entités et organismes visés par l'arrêté ministériel susvisé :

A. Personnes physiques

	Nom	Informations d'identification	Motifs de la désignation
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. « Operation Cloud Hopper » a ciblé les systèmes d'information d'entreprises multinationales sur six continents, 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.
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. « Operation Cloud Hopper » a ciblé les systèmes d'information d'entreprises multinationales sur six continents 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 ». 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.

	Nom	Informations d'identification	Motifs de la désignation
3.	Alexey Valeryevich MININ	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.
4.	Aleksei Sergeyvich MORENETS	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.

	Nom	Informations d'identification	Motifs de la désignation
5.	Evgenii Mikhaylovich SEREBRIAKOV	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.
6.	Oleg Mikhaylovich SOTNIKOV	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 Inlichtingenen Veiligheidsdienst – MIVD) a perturbé la tentative de cyberattaque, évitant ainsi de graves dommages à l'OIAC.

B. Personnes morales, entités et organismes

	Nom	Informations d'identification	Motifs de la désignation
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 et l'a facilitée. « Operation Cloud Hopper » a ciblé les systèmes d'information d'entreprises multinationales sur six continents, 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, 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 relatifs à des services nécessaires à la maintenance de services et d'activités économiques essentiels au sein de divers États, 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.

	Nom	Informations d'identification	Motifs de la désignation
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, 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. « NotPetya » ou « EternalPetya » a rendu des données inaccessibles dans un certain nombre d'entreprises au sein 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.