►**B**

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)

Modifiée par:

		Journal officiel		
		n°	page	date
►**M1**	Décision (PESC) 2020/651 du Conseil du 14 mai 2020	L 153	4	15.5.2020
►**M2**	Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020	L 246	12	30.7.2020
►**M3**	Décision (PESC) 2020/1537 du Conseil du 22 octobre 2020	L 351 I	5	22.10.2020
►**M4**	Décision (PESC) 2020/1748 du Conseil du 20 novembre 2020	L 393	19	23.11.2020

Rectifiée par:

►**C1**	Rectificatif, JO L 230 du 17.7.2020, p. 36 (2019/797)

▼B

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

Article premier

1. La présente décision s'applique aux cyberattaques ayant des effets importants, y compris les tentatives de cyberattaques ayant des effets potentiels importants, qui constituent une menace extérieure pour l'Union ou ses États membres.

2. Les cyberattaques constituant une menace extérieure sont notamment celles qui:

a) ont leur origine ou sont menées à l'extérieur de l'Union;

b) utilisent des infrastructures situées à l'extérieur de l'Union;

c) sont menées par toute personne physique ou morale, toute entité ou tout organisme établi ou agissant à l'extérieur de l'Union; ou

d) sont menées avec l'appui, sur les instructions ou sous le contrôle de toute personne physique ou morale, entité ou organisme agissant à l'extérieur de l'Union.

3. À cette fin, les cyberattaques sont des actions faisant intervenir l'un ou l'autre des éléments suivants:

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 du système ou des données ou d'une partie du système ou des données ou par une autre personne détenant des droits sur le système ou les données ou une partie du système ou des données, ou sont en contravention avec le droit de l'Union ou de l'État membre concerné.

4. Les cyberattaques constituant une menace pour les États membres sont notamment celles qui portent atteinte aux systèmes d'information en ce qui concerne, notamment:

a) les infrastructures critiques, y compris les câbles sous-marins et les objets lancés dans l'espace extra-atmosphérique, qui sont indispensables au maintien des fonctions vitales de la société, ou à la santé, la sûreté, la sécurité et au bien-être économique ou social des citoyens;

b) les services nécessaires au maintien d'activités sociales et/ou économiques critiques, en particulier dans les secteurs de l'énergie (électricité, pétrole et gaz); des transports (aériens, ferroviaires, fluviaux, maritimes et routiers); des activités bancaires; des infrastructures des

▼B

marchés financiers; de la santé (prestataires de soins, hôpitaux et cliniques privées); de l'approvisionnement en eau potable et sa distribution; des infrastructures numériques; et tout autre secteur essentiel pour l'État membre concerné;

c) les fonctions critiques des États, en particulier dans les domaines de la défense, de la gouvernance et du fonctionnement des institutions, y compris pour ce qui est des élections publiques ou de la procédure de vote, du fonctionnement de l'infrastructure économique et civile, de la sécurité intérieure et des relations extérieures, y compris dans le cadre de missions diplomatiques;

d) le stockage ou le traitement des informations classifiées; ou

e) les équipes d'intervention d'urgence mises en place par les pouvoirs publics.

5. Les cyberattaques constituant une menace pour l'Union sont notamment celles qui sont dirigées contre ses institutions, organes et organismes, ses délégations auprès de pays tiers ou d'organisations internationales, ses opérations et missions organisées dans le cadre de la politique de sécurité et de défense commune (PSDC) et ses représentants spéciaux.

6. Lorsque cela est jugé nécessaire pour réaliser les objectifs de la PESC figurant dans les dispositions pertinentes de l'article 21 du traité sur l'Union européenne, des mesures restrictives au titre de la présente décision peuvent également être appliquées en réponse à des cyberattaques ayant des effets importants dirigées contre des pays tiers ou des organisations internationales.

Article 2

Aux fins de la présente décision, on entend par:

a) «système d'information»: un dispositif isolé ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci;

b) «atteinte à l'intégrité d'un système d'information»: le fait d'entraver ou d'interrompre le fonctionnement d'un système d'information en introduisant, en transmettant, en endommageant, en effaçant, en détériorant, en altérant ou en supprimant des données numériques, ou en les rendant inaccessibles;

c) «atteinte à l'intégrité des données»: l'effacement, l'endommagement, la détérioration, l'altération ou la suppression de données numériques dans un système d'information, ou le fait de rendre ces données inaccessibles; cette notion couvre également le vol de données, de fonds, de ressources économiques ou de droits de propriété intellectuelle;

d) «interception de données»: le fait d'intercepter, par des moyens techniques, des transmissions privées de données numériques à destination, à partir ou au sein d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données numériques.

▼B

Article 3

Les facteurs qui déterminent si une cyberattaque a un effet important au sens de l'article 1er, paragraphe 1, comprennent l'un ou l'autre des éléments suivants:

a) la portée, l'ampleur, l'incidence ou la gravité des perturbations causées, notamment sur les activités économiques et sociétales, les services essentiels, les fonctions critiques de l'État, l'ordre public ou la sécurité publique;

b) le nombre de personnes physiques ou morales, d'entités ou d'organismes touchés;

c) le nombre d'États membres concernés;

d) l'ampleur des pertes économiques causées, notamment par le pillage de fonds, de ressources économiques ou de propriété intellectuelle;

e) l'avantage économique acquis par l'auteur de l'infraction, à son profit ou au profit de tiers;

f) la quantité ou la nature des données volées ou l'ampleur des violations de l'intégrité des données; ou

g) la nature des données sensibles sur le plan commercial auxquelles il a été accédé.

Article 4

1. Les États membres prennent les mesures nécessaires pour empêcher l'entrée ou le passage en transit sur leur territoire:

a) des personnes physiques qui sont responsables de cyberattaques ou de tentatives de cyberattaques;

b) des personnes physiques qui apportent un soutien financier, technique ou matériel aux cyberattaques ou aux tentatives de cyberattaques, ou sont impliquées 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) des personnes physiques qui sont associées aux personnes visées aux points a) et b),

dont la liste figure en annexe.

2. Un État membre n'est pas tenu, en vertu du paragraphe 1, de refuser l'entrée sur son territoire à ses propres ressortissants.

3. Le paragraphe 1 s'applique sans préjudice des cas où un État membre est lié par une obligation de droit international, à savoir:

a) en tant que pays hôte d'une organisation internationale intergouvernementale;

b) en tant que pays hôte d'une conférence internationale convoquée par les Nations unies ou tenue sous leurs auspices;

c) en vertu d'un accord multilatéral conférant des privilèges et immunités; ou

d) en vertu du traité de réconciliation (accords du Latran) conclu en 1929 par le Saint-Siège (État de la Cité du Vatican) et l'Italie.

▼B

4. Le paragraphe 3 est considéré comme applicable également aux cas où un État membre est pays hôte de l'Organisation pour la sécurité et la coopération en Europe (OSCE).

5. Le Conseil est tenu dûment informé dans chacun des cas où un État membre accorde une dérogation au titre du paragraphe 3 ou 4.

6. Les États membres peuvent accorder des dérogations aux mesures instituées en vertu du paragraphe 1, lorsque le déplacement d'une personne se justifie pour des raisons humanitaires urgentes ou lorsque la personne se déplace pour assister à des réunions intergouvernementales ou à des réunions dont l'initiative a été prise par l'Union ou qui sont organisées par celle-ci, ou à des réunions organisées par un État membre assurant la présidence de l'OSCE, lorsqu'il y est mené un dialogue politique visant directement à promouvoir les objectifs politiques des mesures restrictives, y compris la sécurité et la stabilité dans le cyberespace.

7. Les États membres peuvent également accorder des dérogations aux mesures instituées en vertu du paragraphe 1 lorsque l'entrée ou le passage en transit est justifié aux fins d'une procédure judiciaire.

8. Tout État membre souhaitant accorder des dérogations visées au paragraphe 6 ou 7 en informe le Conseil par écrit. La dérogation est réputée accordée sauf si un ou plusieurs membres du Conseil soulèvent une objection par écrit dans les deux jours ouvrables qui suivent la réception de la notification de la dérogation proposée. Si un ou plusieurs membres du Conseil soulèvent une objection, le Conseil, statuant à la majorité qualifiée, peut décider d'accorder la dérogation proposée.

9. Lorsque, en application des paragraphes 3, 4, 6, 7 ou 8, un État membre autorise des personnes énumérées à l'annexe à entrer ou à passer en transit sur son territoire, cette autorisation est strictement limitée à l'objectif pour lequel elle est accordée et aux personnes qu'elle concerne directement.

Article 5

1. Sont gelés tous les fonds et ressources économiques appartenant:

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

b) aux personnes physiques ou morales, entités ou organismes qui apportent un soutien financier, technique ou matériel, aux cyberattaques ou aux 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) aux personnes physiques ou morales, entités ou organismes qui sont associés aux personnes physiques ou morales, aux entités et aux organismes visés aux points a) et b);

dont la liste figure en annexe, de même que tous les fonds et ressources économiques que ces personnes, entités ou organismes possèdent, détiennent ou contrôlent.

▼B

2. Aucun fond ni aucune ressource économique n'est mis à la disposition, directement ou indirectement, des personnes physiques ou morales, des entités ou des organismes dont la liste figure à l'annexe, ni n'est débloqué à leur profit.

3. Par dérogation aux paragraphes 1 et 2, les autorités compétentes des États membres peuvent autoriser le déblocage de certains fonds ou ressources économiques gelés, ou la mise à disposition de certains fonds ou ressources économiques, dans les conditions qu'elles jugent appropriées, après avoir établi que les fonds ou les ressources économiques concernés sont:

a) ►C1 nécessaires pour répondre aux besoins fondamentaux des personnes physiques ou morales, entités ou organismes dont la liste figure à l'annexe ◄, ainsi que des membres de la famille de ces personnes physiques qui sont à leur charge, notamment les dépenses consacrées à l'achat de vivres, au paiement de loyers ou au remboursement de prêts hypothécaires, à l'achat de médicaments et au paiement de frais médicaux, d'impôts, de primes d'assurance et de redevances de services publics;

b) destinés exclusivement au règlement d'honoraires d'un montant raisonnable ou au remboursement de dépenses correspondant à des services juridiques;

c) destinés exclusivement au paiement de charges ou de frais correspondant à la garde ou à la gestion courante de fonds ou de ressources économiques gelés;

d) nécessaires pour faire face à des dépenses extraordinaires, pour autant que l'autorité compétente concernée ait notifié, au moins deux semaines avant l'autorisation, aux autorités compétentes des autres États membres et à la Commission les motifs pour lesquels elle estime qu'une autorisation spéciale devrait être accordée; ou

e) destinés à être versés sur ou depuis le compte d'une mission diplomatique ou consulaire ou d'une organisation internationale bénéficiant d'immunités conformément au droit international, dans la mesure où ces versements sont destinés à être utilisés à des fins officielles par la mission diplomatique ou consulaire ou l'organisation internationale.

L'État membre concerné informe les autres États membres et la Commission de toute autorisation accordée en vertu du présent paragraphe.

4. Par dérogation au paragraphe 1, les autorités compétentes des États membres peuvent autoriser le déblocage de certains fonds ou ressources économiques gelés, pour autant que les conditions suivantes soient réunies:

a) les fonds ou ressources économiques font l'objet d'une décision arbitrale rendue avant la date à laquelle la personne physique ou morale, l'entité ou l'organisme visé au paragraphe 1 a été inscrit sur la liste figurant à l'annexe, ou d'une décision judiciaire ou administrative rendue dans l'Union, ou d'une décision judiciaire exécutoire dans l'État membre concerné, avant ou après cette date;

▼B

b) les fonds ou ressources économiques seront exclusivement utilisés pour faire droit aux demandes garanties par une telle décision ou dont la validité a été établie par une telle décision, dans les limites fixées par les lois et règlements applicables régissant les droits des personnes titulaires de telles demandes;

c) la décision ne bénéficie pas à une personne physique ou morale, une entité ou un organisme inscrit sur la liste figurant à l'annexe; et

d) la reconnaissance de la décision n'est pas contraire à l'ordre public de l'État membre concerné.

L'État membre concerné informe les autres États membres et la Commission de toute autorisation accordée en vertu du présent paragraphe.

5. Le paragraphe 1 n'interdit pas à une personne physique ou morale, à une entité ou un organisme inscrit sur la liste figurant à l'annexe d'effectuer un paiement dû au titre d'un contrat conclu avant la date à laquelle cette personne physique ou morale, cette entité ou cet organisme a été inscrit sur ladite liste, dès lors que l'État membre concerné s'est assuré que le paiement n'est pas reçu, directement ou indirectement, par une personne physique ou morale, une entité ou un organisme visé au paragraphe 1.

6. Le paragraphe 2 ne s'applique pas au versement sur les comptes gelés:

a) d'intérêts ou d'autres rémunérations de ces comptes;

b) de paiements dus en vertu de contrats ou d'accords conclus ou d'obligations contractées avant la date à laquelle ces comptes ont été soumis aux mesures prévues aux paragraphes 1 et 2; ou

c) de paiements dus en vertu de décisions judiciaires, administratives ou arbitrales rendues dans l'Union ou exécutoires dans l'État membre concerné,

à condition que ces intérêts, autres revenus et paiements continuent de faire l'objet des mesures prévues au paragraphe 1.

Article 6

1. Le Conseil, statuant à l'unanimité sur proposition d'un État membre ou du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, établit la liste qui figure à l'annexe et la modifie.

2. Le Conseil communique les décisions visées au paragraphe 1, y compris les motifs de son inscription sur la liste, à la personne physique ou morale, à l'entité ou à l'organisme concerné, soit directement si son adresse est connue, soit par la publication d'un avis, en donnant à cette personne physique ou morale, cette entité ou cet organisme la possibilité de présenter des observations.

3. Lorsque des observations sont formulées, ou lorsque de nouveaux éléments de preuve substantiels sont présentés, le Conseil revoit les décisions visées au paragraphe 1 et en informe la personne physique ou morale, l'entité ou l'organisme concerné en conséquence.

▼B

Article 7

1. L'annexe indique les motifs de l'inscription sur la liste des personnes physiques et morales, des entités et des organismes visés aux articles 4 et 5.

2. L'annexe contient, si elles sont disponibles, les informations nécessaires à l'identification des personnes physiques ou morales, des entités ou organismes concernés. En ce qui concerne les personnes physiques, ces informations peuvent comprendre les noms, prénoms et pseudonymes, la date et le lieu de naissance, la nationalité, les numéros de passeport et de carte d'identité, le sexe, l'adresse, si elle est connue, ainsi que la fonction ou la profession. En ce qui concerne les personnes morales, les entités ou les organismes, ces informations peuvent comprendre les dénominations, le lieu et la date d'enregistrement, le numéro d'enregistrement et l'adresse professionnelle.

Article 8

Il n'est fait droit à aucune demande liée à tout contrat ou à toute opération dont l'exécution a été affectée, directement ou indirectement, en totalité ou en partie, par les mesures instituées en vertu de la présente décision, y compris à des demandes d'indemnisation ou à toute autre demande de ce type, telle qu'une demande de compensation ou une demande à titre de garantie, en particulier une demande visant à obtenir la prorogation ou le paiement d'une obligation, d'une garantie ou d'une contre-garantie, notamment financières, quelle qu'en soit la forme, présentée par:

a) des personnes physiques ou morales, des entités ou des organismes désignés inscrits sur la liste figurant à l'annexe;

b) toute personne physique ou morale, toute entité ou tout organisme agissant par l'intermédiaire ou pour le compte de l'une des personnes physiques ou morales, entités ou de l'un des organismes visés au point a).

Article 9

Afin que les mesures énoncées dans la présente décision aient le plus grand impact possible, l'Union encourage les États tiers à adopter des mesures restrictives analogues à celles prévues par la présente décision.

▼M1

Article 10

La présente décision est applicable jusqu’au 18 mai 2021 et fait l’objet d’un suivi constant. Elle est renouvelée, ou modifiée, le cas échéant, si le Conseil estime que ses objectifs n’ont pas été atteints.

▼B

Article 11

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

▼B

ANNEXE

Liste des personnes physiques et morales, des entités et des organismes visés aux articles 4 et 5

▼M2

A. Personnes physiques

▼M4

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
1.	GAO Qiang	Date de naissance: 4 octobre 1983 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	Date de naissance: 10 septembre 1981 Lieu de naissance: Chine 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.	30.7.2020

▼M4

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			«*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*». 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.	

▼M2

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

▼M2

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
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

▼M2

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
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
▼M3 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

▼M3

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
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

▼M2

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

▼M2

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			«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

▼M2

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
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. «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.	30.7.2020

▼M3

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.	22.10.2020

▼M3

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			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.	