►**B**

RÈGLEMENT (UE) 2019/796 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. 1)

Modifié par:

		Journal officiel		
		n°	page	date
►**M1**	Règlement d'exécution (UE) 2020/1125 du Conseil du 30 juillet 2020	L 246	4	30.7.2020
►**M2**	Règlement d'exécution (UE) 2020/1536 du Conseil du 22 octobre 2020	L 351 I	1	22.10.2020
►**M3**	Règlement d'exécution (UE) 2020/1744 du Conseil du 20 novembre 2020	L 393	1	23.11.2020
►**M4**	Règlement d'exécution (UE) 2022/595 de la Commission du 11 avril 2022	L 114	60	12.4.2022

Rectifié par:

►**C1** Rectificatif, JO L 230 du 17.7.2020, p. 37 (2019/796)

►**C2** Rectificatif, JO L 90074 du 7.11.2023, p. 1 (2020/1125)

▼B

RÈGLEMENT (UE) 2019/796 DU CONSEIL

du 17 mai 2019

concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

Article premier

1. Le présent règlement 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 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;

▼B

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 politique étrangère et de sécurité commune (PESC) figurant dans les dispositions pertinentes de l'article 21 du traité sur l'Union européenne, des mesures restrictives au titre du présent règlement peuvent également être appliquées en réponse à des cyberattaques ayant des effets importants dirigées contre des pays tiers ou des organisations internationales.

7. Aux fins du présent règlement, 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

8. Aux fins du présent règlement, les définitions supplémentaires suivantes s'appliquent:

a) «demande»: toute demande, sous forme contentieuse ou non, introduite antérieurement ou postérieurement à la date d'entrée en vigueur du présent règlement résultant d'un contrat ou liée à l'exécution d'un contrat ou d'une opération, et notamment:

   i) une demande visant à obtenir l'exécution de toute obligation résultant d'un contrat ou d'une opération ou liée à un contrat ou à une opération;

   ii) une demande visant à obtenir la prorogation ou le paiement d'une obligation, d'une garantie ou d'une contre-garantie financières, quelle qu'en soit la forme;

   iii) une demande d'indemnisation se rapportant à un contrat ou à une opération;

   iv) une demande reconventionnelle;

▼B

v) une demande visant à obtenir, y compris par voie d'exequatur, la reconnaissance ou l'exécution d'un jugement, d'une sentence arbitrale ou d'une décision équivalente, quel que soit le lieu où ils ont été rendus;

b) «contrat ou opération»: toute opération, quelle qu'en soit la forme et quel que soit le droit qui lui est applicable, comportant un ou plusieurs contrats ou obligations similaires établis entre des parties identiques ou non; à cet effet, le terme «contrat» inclut toute obligation, toute garantie ou toute contre-garantie, notamment financières, et tout crédit, juridiquement indépendants ou non, ainsi que toute disposition y relative qui trouve son origine dans une telle opération ou qui lui est liée;

c) «autorités compétentes»: les autorités compétentes des États membres indiquées sur les sites internet dont la liste figure à l'annexe II;

d) «ressources économiques»: les actifs de toute nature, corporels ou incorporels, mobiliers ou immobiliers, qui ne sont pas des fonds, mais qui peuvent être utilisés pour obtenir des fonds, des biens ou des services;

e) «gel des ressources économiques»: toute action visant à empêcher l'utilisation de ressources économiques afin d'obtenir des fonds, des biens ou des services de quelque manière que ce soit, et notamment, mais pas exclusivement, leur vente, leur location ou leur mise sous hypothèque;

f) «gel des fonds»: toute action visant à empêcher tout mouvement, transfert, modification, utilisation, manipulation de fonds ou accès à des fonds qui aurait pour conséquence un changement de leur volume, de leur montant, de leur localisation, de leur propriété, de leur possession, de leur nature ou de leur destination ou toute autre modification qui pourrait en permettre l'utilisation, y compris la gestion de portefeuille;

g) «fonds»: des actifs financiers et des avantages économiques de toute nature, et notamment, mais pas exclusivement:

i) le numéraire, les chèques, les créances en numéraire, les traites, les ordres de paiement et autres instruments de paiement;

ii) les dépôts auprès d'établissements financiers ou d'autres entités, les soldes en compte, les créances et les titres de créance;

iii) les titres de propriété et d'emprunt, tels que les actions, les certificats représentatifs de valeurs mobilières, les obligations, les billets à ordre, les warrants, les obligations non garanties et les contrats sur produits dérivés, qu'ils soient négociés en bourse ou fassent l'objet d'un placement privé;

iv) les intérêts, les dividendes ou autres revenus d'actifs ou plus-values perçus sur des actifs;

v) le crédit, le droit à compensation, les garanties, les garanties de bonne exécution ou autres engagements financiers;

vi) les lettres de crédit, les connaissements et les contrats de vente; et

vii) tout document attestant la détention de parts d'un fonds ou de ressources financières;

▼B

h) «territoire de l'Union»: les territoires des États membres auxquels le traité est applicable, dans les conditions fixées par celui-ci, y compris leur espace aérien.

Article 2

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 3

1. Sont gelés tous les fonds et ressources économiques appartenant aux personnes physiques ou morales, entités ou organismes inscrits sur la liste qui figure à l'annexe I, de même que tous les fonds et ressources économiques que ces personnes physiques ou morales, entités ou organismes possèdent, détiennent ou contrôlent.

2. Aucun fonds 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 I, ni n'est débloqué à leur profit.

3. Figurent à l'annexe I, tels qu'ils ont été définis par le Conseil conformément à l'article 5, paragraphe 1, de la décision (PESC) 2019/797:

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.

▼B

Article 4

1. Par dérogation à l'article 3, 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 gelés, dans les conditions qu'elles jugent appropriées, après avoir établi que les fonds ou ressources économiques concernés sont:

a) ►C1 nécessaires pour répondre aux besoins fondamentaux des personnes physiques ou morales, des entités ou des organismes dont la liste figure à l'annexe I, ◄ 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.

2. L'État membre concerné informe les autres États membres et la Commission de toute autorisation accordée en vertu du paragraphe 1 dans un délai de deux semaines suivant l'autorisation.

Article 5

1. Par dérogation à l'article 3, 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 à l'article 3 a été inscrit sur la liste figurant à l'annexe I, 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) 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 I; et

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

▼B

2. L'État membre concerné informe les autres États membres et la Commission de toute autorisation accordée en vertu du paragraphe 1 dans un délai de deux semaines suivant l'autorisation.

Article 6

1. Par dérogation à l'article 3, paragraphe 1, et pour autant qu'un paiement soit dû par une personne physique ou morale, une entité ou un organisme figurant sur la liste de l'annexe I au titre d'un contrat ou d'un accord conclu ou d'une obligation contractée par la personne physique ou morale, l'entité ou l'organisme concerné avant la date à laquelle cette personne physique ou morale, cette entité ou cet organisme a été inscrit à l'annexe I, les autorités compétentes des États membres peuvent autoriser, dans les conditions qu'elles jugent appropriées, le déblocage de certains fonds ou ressources économiques gelés, pour autant que l'autorité compétente concernée ait établi que:

a) les fonds ou les ressources économiques seront utilisés par une personne physique ou morale, une entité ou un organisme inscrit sur la liste figurant à l'annexe I; et

b) le paiement n'enfreint pas l'article 3, paragraphe 2.

2. L'État membre concerné informe les autres États membres et la Commission de toute autorisation accordée en vertu du paragraphe 1 dans un délai de deux semaines suivant l'autorisation.

Article 7

1. L'article 3, paragraphe 2, n'empêche pas les établissements financiers ou de crédit de créditer les comptes gelés lorsqu'ils reçoivent des fonds versés par des tiers sur le compte d'une personne physique ou morale, d'une entité ou d'un organisme figurant sur la liste, à condition que toute somme supplémentaire versée sur ces comptes soit également gelée. L'établissement financier ou de crédit informe sans tarder l'autorité compétente concernée de toute opération de ce type.

2. L'article 3, 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 la personne physique ou morale, l'entité ou l'organisme visé à l'article 3, paragraphe 1, a été inscrit à l'annexe I; ou

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

à condition que ces intérêts, autres revenus et paiements continuent de faire l'objet des mesures prévues à l'article 3, paragraphe 1.

Article 8

1. Sans préjudice des règles applicables en matière de communication d'informations, de confidentialité et de secret professionnel, les personnes physiques ou morales, les entités et les organismes:

▼B

a) fournissent immédiatement toute information susceptible de faciliter le respect du présent règlement, notamment les informations concernant les comptes et les montants gelés conformément à l'article 3, paragraphe 1, à l'autorité compétente de l'État membre dans lequel ils résident ou sont établis et transmettent cette information à la Commission, directement ou par l'intermédiaire de l'État membre; et

b) coopèrent avec l'autorité compétente aux fins de toute vérification de l'information visée au point a).

2. Toute information supplémentaire reçue directement par la Commission est mise à la disposition des États membres.

3. Toute information fournie ou reçue conformément au présent article est utilisée aux seules fins pour lesquelles elle a été fournie ou reçue.

Article 9

Il est interdit de participer sciemment et volontairement à des activités ayant pour objet ou pour effet de contourner les mesures énoncées à l'article 3.

Article 10

1. Le gel des fonds et des ressources économiques ou le refus d'en autoriser la mise à disposition, pour autant qu'ils soient décidés de bonne foi au motif qu'une telle action est conforme au présent règlement, n'entraînent, pour la personne physique ou morale, l'entité ou l'organisme qui y procède, sa direction ou ses employés, aucune responsabilité de quelque nature que ce soit, à moins qu'il ne soit établi que le gel ou la rétention de ces fonds et ressources économiques résulte d'une négligence.

2. Les actions entreprises par des personnes physiques ou morales, des entités ou des organismes n'entraînent pour eux aucune responsabilité de quelque nature que ce soit, dès lors qu'ils ne savaient ni ne pouvaient raisonnablement soupçonner que leurs actions enfreindraient les mesures énoncées dans le présent règlement.

Article 11

1. 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 du présent règlement, 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 I;

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).

2. Dans toute procédure visant à donner effet à une demande, la charge de la preuve que la satisfaction de la demande n'est pas interdite par le paragraphe 1 incombe à la personne physique ou morale, à l'entité ou à l'organisme cherchant à donner effet à cette demande.

3. Le présent article s'applique sans préjudice du droit des personnes physiques ou morales, des entités et des organismes visés au paragraphe 1 au contrôle juridictionnel de la légalité du non-respect des obligations contractuelles conformément au présent règlement.

▼B

Article 12

1. La Commission et les États membres s'informent mutuellement des mesures prises en vertu du présent règlement et se communiquent toute autre information utile dont ils disposent en rapport avec le présent règlement, concernant en particulier:

a) les fonds gelés en vertu de l'article 3 et les autorisations accordées en vertu des articles 4, 5 et 6;

b) les problèmes liés aux violations du présent règlement et à sa mise en œuvre et les jugements rendus par les juridictions nationales.

2. Les États membres se communiquent mutuellement et immédiatement tout autre élément utile dont ils disposent et qui serait susceptible d'entraver la mise en œuvre effective du présent règlement; de même, ils en informent immédiatement la Commission.

Article 13

1. Lorsque le Conseil décide de soumettre une personne physique ou morale, une entité ou un organisme aux mesures visées à l'article 3, il modifie l'annexe I en conséquence.

2. Le Conseil communique la décision visée 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 la décision visée au paragraphe 1 et en informe la personne physique ou morale, l'entité ou l'organisme concerné en conséquence.

4. La liste figurant à l'annexe I est révisée à intervalles réguliers et au moins tous les douze mois.

5. La Commission est habilitée à modifier l'annexe II sur la base des informations fournies par les États membres.

Article 14

1. L'annexe I contient les motifs de l'inscription sur la liste des personnes physiques ou morales, des entités ou des organismes concernés.

2. L'annexe I contient, si elles sont disponibles, les informations nécessaires à l'identification des personnes physiques ou morales, des entités ou des 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 15

1. Les États membres arrêtent le régime des sanctions applicables en cas d'infraction aux dispositions du présent règlement et prennent toutes les mesures nécessaires pour en garantir l'exécution. Les sanctions prévues doivent être effectives, proportionnées et dissuasives.

▼B

2. Les États membres notifient à la Commission le régime visé au paragraphe 1 sans tarder après l'entrée en vigueur du présent règlement et lui notifient également toute modification ultérieure dudit régime.

Article 16

1. Pour mener à bien les tâches qui lui incombent au titre du présent règlement, la Commission traite des données à caractère personnel. Ces tâches comprennent notamment:

a) l'ajout du contenu de l'annexe I dans la liste électronique consolidée des personnes, groupes et entités auxquels l'Union a infligé des sanctions financières et dans la carte interactive des sanctions, toutes deux accessibles au public;

b) le traitement d'informations sur les effets des mesures prises en vertu du présent règlement, comme la valeur des fonds gelés, et d'informations relatives aux autorisations accordées par les autorités compétentes.

2. Aux fins du présent règlement, le service de la Commission indiqué à l'annexe II est désigné «responsable du traitement» pour la Commission au sens de l'article 3, paragraphe 8, du règlement (UE) 2018/1725, afin de garantir que les personnes physiques concernées peuvent exercer leurs droits en vertu dudit règlement.

Article 17

1. Les États membres désignent les autorités compétentes visées dans le présent règlement et les mentionnent sur les sites internet énumérés à l'annexe II. Ils notifient à la Commission toute modification relative aux adresses de leurs sites internet énumérés à l'annexe II.

2. Les États membres notifient à la Commission leurs autorités compétentes, ainsi que les coordonnées de ces dernières sans tarder après l'entrée en vigueur du présent règlement, ainsi que toute modification ultérieure.

3. Lorsque le présent règlement prévoit une obligation de notification ou d'information de la Commission ou de toute autre forme de communication avec la Commission, l'adresse et les autres coordonnées à utiliser à cet effet sont celles qui sont indiquées à l'annexe II.

Article 18

Le présent règlement s'applique:

a) sur le territoire de l'Union, y compris dans son espace aérien;

b) à bord de tout aéronef ou de tout navire relevant de la juridiction d'un État membre;

c) à toute personne physique, à l'intérieur ou à l'extérieur du territoire de l'Union, qui est ressortissante d'un État membre;

d) à toute personne morale, à toute entité ou à tout organisme, à l'intérieur ou à l'extérieur du territoire de l'Union, établi ou constitué selon le droit d'un État membre;

e) à toute personne morale, toute entité ou tout organisme en ce qui concerne toute opération commerciale réalisée intégralement ou en partie dans l'Union.

▼B

Article 19

Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

▼B

ANNEXE I

Liste des personnes physiques et morales, des entités et des organismes visés à l'article 3

▼M1

A. Personnes physiques

▼M3

	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. «*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.	30.7.2020

▼M3

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

▼M1

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 RussieValidité: 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

▼M1

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

▼M1

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
▼M2				
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

▼M1

B. Personnes morales, entités et organismes

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
1.	►C2 Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai) ◄	*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. «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.	30.7.2020
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.	30.7.2020

▼M1

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

▼M1

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
▼M2				
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

▼B

ANNEXE II

Sites internet contenant les informations sur les autorités compétentes et l'adresse à utiliser pour les notifications à la Commission

▼M4

BELGIQUE

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIE

https://www.mfa.bg/en/EU-sanctions

TCHÉQUIE

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DANEMARK

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

ALLEMAGNE

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTONIE

https://vm.ee/et/rahvusvahelised-sanktsioonid

IRLANDE

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRÈCE

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

ESPAGNE

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANCE

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

CROATIE

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIE

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CHYPRE

https://mfa.gov.cy/themes/

LETTONIE

http://www.mfa.gov.lv/en/security/4539

LITUANIE

http://www.urm.lt/sanctions

LUXEMBOURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

HONGRIE

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

MALTE

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

▼**M4**

PAYS-BAS

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUTRICHE

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLOGNE

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGAL

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

ROUMANIE

http://www.mae.ro/node/1548

SLOVÉNIE

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVAQUIE

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLANDE

https://um.fi/pakotteet

SUÈDE

https://www.regeringen.se/sanktioner

Adresse à utiliser pour les notifications à la Commission européenne:

Commission européenne

Direction générale de la stabilité financière, des services financiers et de l'union des marchés des capitaux (DG FISMA)

Rue de Spa 2

1049 Bruxelles, Belgique

Courriel: relex-sanctions@ec.europa.eu