LUTTE CONTRE LES CYBERATTAQUES

Décision (PESC) 2019/797 consolidée
concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres

Consolidation prenant en compte :

Décision (PESC) 2019/797 du 17 mai 2019
Décision (PESC) 2020/651 du 14 mai 2020
Décision (PESC) 2020/1127 du 30 juillet 2020 (voir le registre national des gels)
Décision (PESC) 2020/1537 du 22 octobre 2020 (voir registre national de gels)
Décision (PESC) 2020/1748 du 20 novembre 2020 (voir registre national de gels)
Décision (PESC) 2021/796 du 17 mai 2021
Décision (PESC) 2022/754 du 16 mai 2022

Lien vers le registre national des gels de la Direction générale du Trésor

en rouge : dernière mise à jour
en bleu : mises à jour antérieures

considérant ce qui suit :

(1) Le 19 juin 2017, le Conseil a adopté les conclusions relatives à un cadre pour une réponse diplomatique conjointe face aux actes de cybermalveillance (ci-après dénommé «boîte à outils cyberdiplomatique»), dans lesquelles il s'est déclaré préoccupé par la capacité et la volonté accrues d'acteurs étatiques et non étatiques à poursuivre leurs objectifs en menant des activités cybermalveillantes, et a indiqué qu'il est de plus en plus nécessaire de protéger l'intégrité et la sécurité de l'Union, de ses États membres et de leurs citoyens contre les menaces informatiques et les actes de cybermalveillance.

(2) Le Conseil a souligné que le fait de signaler clairement les conséquences possibles d'une réponse diplomatique conjointe de l'Union face à de telles activités cybermalveillantes influence le comportement des cyberagresseurs potentiels dans le cyberespace, renforçant ainsi la sécurité de l'Union et de ses États membres. Il a également affirmé que les mesures relevant de la politique étrangère et de sécurité commune (PESC), y compris, si nécessaire, les mesures restrictives, adoptées

dans le cadre des dispositions pertinentes des traités, conviennent à un cadre pour une réponse diplomatique conjointe de l'Union face aux actes de cybermalveillance, le but étant d'encourager la coopération, de faciliter la réduction des menaces immédiates et à long terme, et d'influencer le comportement d'agresseurs potentiels à long terme.

(3) Le 11 octobre 2017, les lignes directrices relatives à la mise en œuvre de la boîte à outils cyberdiplomatique ont été approuvées par le Comité politique et de sécurité. Les lignes directrices relatives à la mise en œuvre portent sur cinq catégories de mesures, y compris les mesures restrictives, figurant dans la boîte à outils cyberdiplomatique, ainsi que sur la procédure pour recourir à ces mesures.

(4) Dans ses conclusions du 16 avril 2018 sur les actes de cybermalveillance, le Conseil a condamné fermement l'utilisation à des fins malveillantes de technologies de l'information et de la communication (TIC) et souligné que l'utilisation des TIC à des fins malveillantes est inacceptable parce qu'elle met à mal la stabilité, la sécurité, ainsi que les avantages qu'offrent l'internet et les TIC. Le Conseil a rappelé que la boîte à outils cyberdiplomatique concourt à la prévention des conflits, à la coopération et à la stabilité dans le cyberespace en précisant les mesures pouvant être décidées dans le cadre de la PESC, y compris les mesures restrictives, pour prévenir les actes de cybermalveillance et y répondre. Il a déclaré que l'Union n'aurait de cesse d'affirmer avec force que le droit international existant s'applique au cyberespace et a souligné que le respect du droit international, en particulier de la charte des Nations unies, est indispensable pour préserver la paix et la stabilité. Le Conseil a également souligné que les États ne doivent pas faire appel à des intermédiaires pour commettre des actes internationalement illicites à l'aide des TIC et qu'ils devraient veiller à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes, comme indiqué dans le rapport établi en 2015 par le groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

(5) Le 28 juin 2018, le Conseil européen a adopté des conclusions dans lesquelles il souligne la nécessité de renforcer les capacités de lutte contre les menaces sur la cybersécurité qui proviennent de l'extérieur de l'Union. Le Conseil européen a invité les institutions et les États membres à mettre en œuvre les mesures visées dans la communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 13 juin 2018 intitulée « Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides », y compris l'utilisation pratique de la boîte à outils cyberdiplomatique.

(6) Le 18 octobre 2018, le Conseil européen a adopté des conclusions invitant à poursuivre les travaux sur la capacité de réaction aux cyberattaques et de dissuasion de ces attaques par des mesures restrictives de l'Union, à la suite des conclusions du Conseil du 19 juin 2017.

(7) Dans ce contexte, la présente décision établit un cadre pour des mesures restrictives ciblées visant à dissuader et contrer les cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres. 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, la présente décision permet également d'appliquer des mesures restrictives en réponse à des cyberattaques ayant des effets importants dirigées contre des pays tiers ou des organisations internationales.

(8) Afin d'avoir un effet dissuasif, les mesures restrictives ciblées devraient se concentrer sur les cyberattaques entrant dans le champ d'application de la présente décision qui sont menées délibérément.

(9) Les mesures restrictives ciblées devraient être différenciées de l'imputation de responsabilité pour des cyberattaques à un État tiers. L'application de mesures restrictives ciblées n'équivaut pas à une telle imputation, qui constitue une décision politique souveraine prise au cas par cas. Chaque État membre est libre de procéder à sa propre appréciation en ce qui concerne l'imputation de cyberattaques à un État tiers.

(10) Une nouvelle action de l'Union est nécessaire pour mettre en œuvre certaines mesures,

A ADOPTÉ LA PRÉSENTE DÉCISION :

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 bienêtre 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 ;

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.

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.

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.

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) nécessaires pour répondre aux besoins fondamentaux des personnes physiques 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) 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.

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.

Article 10 [1][2][3]

La présente décision est applicable jusqu'au 18 mai 2025 et fait l'objet d'un suivi constant. Les mesures énoncées aux articles 4 et 5 s'appliquent à l'égard des personnes physiques et morales, des entités et des organismes dont la liste figure à l'annexe jusqu'au 18 mai 2023

~~La présente décision s'applique jusqu'au 18 mai 2022 2021 2020 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.~~

Article 11

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

Fait à Bruxelles, le 17 mai 2019.

Par le Conseil Le président E.O. TEODOROVIC

[1] Modifié par la décision (PESC) 2020/651 du 14/05/2020
[2] Modifié par la décision (PESC) 2021/796 du 17/05/2021
[3] Modifié par la décision (PESC) 2022/754 du 16/05/2022

ANNEXE

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

[…]

Consulter le registre national des gels de la Direction Générale du Trésor