DÉCISION (PESC) 2021/1026 DU CONSEIL

du 21 juin 2021

visant à soutenir le programme de cybersécurité, de cyberrésilience et d'assurance de l'information de l'Organisation pour l'interdiction des armes chimiques (OIAC) dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 28, paragraphe 1, et son article 31, paragraphe 1,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 12 décembre 2003, le Conseil européen a adopté la stratégie de l'UE contre la prolifération des armes de destruction massive (ci-après dénommée «stratégie de l'UE»), dont le chapitre III comporte une liste de mesures destinées à lutter contre cette prolifération.

(2) La stratégie de l'UE met en évidence le rôle déterminant que jouent la convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction (CAC) et l'Organisation pour l'interdiction des armes chimiques (OIAC) en faveur d'un monde exempt d'armes chimiques. Les objectifs de la stratégie de l'UE sont complémentaires de ceux poursuivis par l'OIAC, dans le cadre de ses compétences en ce qui concerne la mise en œuvre de la CAC.

(3) Le 22 novembre 2004, le Conseil a adopté l'action commune 2004/797/PESC ([1]) concernant le soutien aux activités de l'OIAC. Cette action commune étant venue à expiration, elle a été suivie par l'action commune 2005/913/PESC du Conseil ([2]) qui, à son tour, a été suivie par l'action commune 2007/185/PESC du Conseil ([3]).

L'action commune 2007/185/PESC a été suivie par les décisions 2009/569/PESC ([4]), 2012/166/PESC ([5]), 2013/726/PESC ([6]), (PESC) 2015/259 ([7]), (PESC) 2017/2302 ([8]), (PESC) 2017/2303 ([9]) et (PESC) 2019/538 ([10]) du Conseil.

([1]) Action commune 2004/797/PESC du Conseil du 22 novembre 2004 concernant le soutien aux activités de l'OIAC dans le cadre de la mise en œuvre de la stratégie de l'Union européenne contre la prolifération des armes de destruction massive (JO L 349 du 25.11.2004, p. 63).

([2]) Action commune 2005/913/PESC du Conseil du 12 décembre 2005 concernant le soutien aux activités de l'OIAC dans le cadre de la mise en œuvre de la stratégie de l'Union européenne contre la prolifération des armes de destruction massive (JO L 331 du 17.12.2005, p. 34).

([3]) Action commune 2007/185/PESC du Conseil du 19 mars 2007 concernant le soutien aux activités de l'OIAC dans le cadre de la mise en œuvre de la stratégie de l'Union européenne contre la prolifération des armes de destruction massive (JO L 85 du 27.3.2007, p. 10).

([4]) Décision 2009/569/PESC du Conseil du 27 juillet 2009 soutenant les activités de l'OIAC dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 197 du 29.7.2009, p. 96).

([5]) Décision 2012/166/PESC du Conseil du 23 mars 2012 visant à soutenir les activités de l'Organisation pour l'interdiction des armes chimiques (OIAC) dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 87 du 24.3.2012, p. 49).

([6]) Décision 2013/726/PESC du Conseil du 9 décembre 2013 à l'appui de la résolution 2118 (2013) du Conseil de sécurité des Nations unies et la décision EC-M-33/Dec 1 du Conseil exécutif de l'OIAC, dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 329 du 10.12.2013, p. 41).

([7]) Décision (PESC) 2015/259 du Conseil du 17 février 2015 visant à soutenir les activités de l'Organisation pour l'interdiction des armes chimiques (OIAC) dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 43 du 18.2.2015, p. 14).

([8]) Décision (PESC) 2017/2302 du Conseil du 12 décembre 2017 à l'appui des activités de l'OIAC visant à contribuer aux opérations de nettoyage menées sur l'ancien site de stockage d'armes chimiques en Libye dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 329 du 13.12.2017, p. 49).

([9]) Décision (PESC) 2017/2303 du Conseil du 12 décembre 2017 à l'appui de la poursuite de la mise en œuvre de la résolution 2118 (2013) du Conseil de sécurité des Nations unies et de la décision EC-M-33/DEC.1 du Conseil exécutif de l'OIAC sur la destruction des armes chimiques syriennes, dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 329 du 13.12.2017, p. 55).

([10]) Décision (PESC) 2019/538 du Conseil du 1er avril 2019 visant à soutenir les activités de l'Organisation pour l'interdiction des armes chimiques (OIAC) dans le cadre de la mise en œuvre de la stratégie de l'UE contre la prolifération des armes de destruction massive (JO L 93 du 2.4.2019, p. 3).

(4) Il est nécessaire que l'Union continue de fournir à l'OIAC une aide soutenue et ciblée dans le cadre de la mise en œuvre active du chapitre III de la stratégie de l'UE.

(5) Il est nécessaire que l'Union continue de soutenir le programme de cybersécurité, de cyberrésilience et d'assurance de l'information de l'OIAC, qui vise à renforcer la capacité de l'OIAC à maintenir des niveaux appropriés de cybersécurité et de cyberrésilience face aux défis actuels et émergents liés à la cybersécurité,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Aux fins de l'application immédiate et concrète de certains éléments de la stratégie de l'UE, l'Union apporte son soutien à un projet de l'OIAC, les objectifs étant les suivants:

— mettre à niveau les infrastructures TIC conformément au cadre institutionnel de continuité des activités de l'OIAC, en mettant fortement l'accent sur la résilience, et

— assurer la gouvernance en matière d'accès privilégiés, ainsi que la gestion et la séparation physiques, logiques et cryptographiques de l'information pour tous les réseaux stratégiques et de missions de l'OIAC.

2. Dans le cadre du paragraphe 1, les activités du projet de l'OIAC bénéficiant d'un soutien de l'Union, qui sont conformes aux mesures énoncées au chapitre III de la stratégie de l'UE, sont les suivantes:

— mise en œuvre d'un environnement propice aux efforts en cours en matière de cybersécurité et de cyberrésilience dans le cadre des opérations multisites de l'OIAC,

— conception de solutions spécifiques pour l'intégration et la configuration de systèmes sur site et dans le nuage avec les systèmes TIC de l'OIAC et des solutions de gestion des accès privilégiés (PAM), et

— lancement et test de solutions PAM.

3. Une description détaillée des activités de l'OIAC bénéficiant d'un soutien de l'Union visées au paragraphe 2 figure à l'annexe.

Article 2

1. Le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (HR) est chargé de la mise en œuvre de la présente décision.

2. La mise en œuvre technique du projet visé à l'article 1er est confiée au secrétariat technique de l'OIAC (ci-après dénommé «secrétariat technique»). Il exécute cette tâche sous la responsabilité et le contrôle du HR. À cette fin, le HR conclut les accords nécessaires avec le secrétariat technique.

Article 3

1. Le montant de référence financière pour l'exécution du projet visé à l'article 1er est de 2 151 823 EUR.

2. La gestion des dépenses financées par le montant indiqué au paragraphe 1 s'effectue conformément aux procédures et règles applicables au budget général de l'Union.

3. La Commission supervise la bonne gestion des dépenses visées au paragraphe 2. Elle conclut à cet effet la convention nécessaire avec le secrétariat technique. Cette convention prévoit que le secrétariat technique veille à ce que la contribution de l'Union bénéficie d'une visibilité adaptée à son importance et définit des mesures ayant pour but de faciliter le développement de synergies et d'éviter les activités inutilement redondantes.

4. La Commission s'efforce de conclure la convention visée au paragraphe 3 le plus tôt possible après l'entrée en vigueur de la présente décision. Elle informe le Conseil des difficultés éventuellement rencontrées dans cette démarche et de la date de la conclusion de la convention.

Article 4

Le HR rend compte au Conseil de la mise en œuvre de la présente décision sur la base de rapports périodiques établis par le secrétariat technique. Les rapports du HR constituent la base de l'évaluation effectuée par le Conseil. La Commission fournit des informations sur les aspects financiers du projet visé à l'article 1er.

Article 5

1. La présente décision entre en vigueur le jour de son adoption.

2. La présente décision expire vingt-quatre mois après la date de la conclusion de la convention visée à l'article 3, paragraphe 3. Toutefois, elle expire six mois après son entrée en vigueur si ladite convention n'a pas été conclue dans ce délai.

Fait à Luxembourg, le 21 juin 2021.

Par le Conseil
Le président
J. BORRELL FONTELLES

ANNEXE

DOCUMENT DE PROJET

1. Contexte

L'OIAC est tenue de gérer une infrastructure qui permette d'assurer la souveraineté en matière d'information d'une manière proportionnée aux classifications en matière d'accès privilégiés, aux procédures de traitement appropriées et aux menaces existantes, tout en demeurant capable d'assurer une protection contre les risques émergents. L'OIAC est constamment exposée à des risques graves et émergents liés à la cybersécurité et à la cyberrésilience. L'OIAC est la cible d'intervenants hautement qualifiés, disposant de ressources importantes et très motivés. Ces intervenants continuent de lancer de fréquentes attaques contre la confidentialité et l'intégrité des informations et des infrastructures de l'OIAC. Pour répondre aux préoccupations suscitées par les cyberattaques récentes, le contexte politique actuel et la crise liée à la COVID 19, et compte tenu des exigences spécifiques découlant de la nature des activités de l'OIAC en vue de s'acquitter du mandat de la CAC, des investissements essentiels dans les capacités techniques s'imposent manifestement.

Dans le cadre de son Fonds spécial pour la cybersécurité, la continuité des activités et la sécurité des infrastructures physiques, l'OIAC a défini un programme de cybersécurité, de cyberrésilience et d'assurance de l'information (ci après dénommé «programme de l'OIAC») qui comprend quarante-sept activités visant à relever les défis en matière de cybersécurité rencontrés récemment. Le programme de l'OIAC est aligné sur les bonnes pratiques préconisées par des entités telles que l'Agence de l'Union européenne pour la cybersécurité (ENISA) ou fait appel à des concepts liés à la directive européenne sur la sécurité des réseaux et des systèmes d'information (SRI) dans les domaines des télécommunications et de la défense. D'une manière générale, le programme de l'OIAC couvre les domaines thématiques suivants: réseaux classifiés et non classifiés; stratégie et gouvernance; détection et réaction; opérations et maintenance; et télécommunications. Fondamentalement, le programme de l'OIAC est conçu pour permettre à celle-ci de réduire les possibilités qu'ont les auteurs d'attaques dotés de ressources importantes et/ou parrainés par un État d'atteindre leurs objectifs, et pour atténuer les risques liés aux menaces externes comme internes, d'un point de vue tant humain que technique. Le soutien de l'Union prend la forme d'un projet comprenant trois activités qui correspondent à deux des quarante-sept activités du programme de l'OIAC.

2. Finalité du projet

Le projet vise d'une manière générale à faire en sorte que le secrétariat de l'OIAC ait la capacité de maintenir un niveau approprié de cybersécurité et de cyberrésilience face aux défis récurrents et émergents en matière de cyberdéfense au siège de l'OIAC et dans les installations connexes, afin que l'OIAC puisse s'acquitter de son mandat et que la CAC puisse effectivement être mise en œuvre.

3. Objectifs

— Mettre à niveau les infrastructures TIC conformément au cadre institutionnel de continuité des activités de l'OIAC, en mettant fortement l'accent sur la résilience.

— Assurer la gouvernance en matière d'accès privilégiés, ainsi que la gestion et la séparation physiques, logiques et cryptographiques de l'information pour tous les réseaux stratégiques et de missions.

4. Résultats

Les résultats escomptés auxquels le projet contribue sont les suivants:

— les équipements et services TIC assurent une bonne fiabilité des systèmes (redondance hybride/géographique) et permettent une plus grande disponibilité des systèmes et services TIC à l'appui de la continuité des activités,

— la capacité de tout facteur ou de toute personne à porter atteinte à la confidentialité et à l'intégrité des informations ou des systèmes au sein de l'OIAC est réduite autant que possible.

5. Activités

5.1. Activité 1 — Mise en œuvre d'un environnement propice aux efforts en cours en matière de cybersécurité et de cyberrésilience dans le cadre des opérations multisites de l'OIAC

Cette activité vise à créer un environnement propice au déploiement harmonieux de la planification de la continuité des activités de l'OIAC en ce qui concerne la cybersécurité et la cyberrésilience. Pour ce faire, il sera procédé à la modernisation des infrastructures – réorganisation et/ou l'archivage pour assurer la continuité des activités de l'OIAC dans le cadre d'opérations multisites. L'intégration de la gouvernance en matière d'accès privilégiés dans les processus de planification et de réaction en matière de continuité des activités sera en outre facilitée et encouragée plus avant.

5.2. Activité 2 — Conception d'une solution spécifique pour l'intégration et la configuration de systèmes sur site et dans le nuage avec les systèmes TIC de l'OIAC et des solutions de gestion des accès privilégiés (PAM)

Cette activité est axée sur la transposition de l'environnement favorable en une solution spécifique pour l'intégration et la configuration de systèmes sur site et de systèmes fondés sur le nuage avec les systèmes TIC de l'OIAC et des solutions PAM. Cela devrait accroître l'efficacité de l'infrastructure des systèmes TIC et conduire à la conception d'un système intégré de PAM pour les actifs critiques, qui soit à même d'assurer la dissuasion et la détection et corresponde à des capacités à la mesure de la recherche de menaces.

5.3. Activité 3 — Lancement et test de solutions PAM

Cette activité s'appuie sur l'infrastructure mise en œuvre et les solutions PAM conçues pour faire passer l'intégration et la configuration de la théorie à la pratique. Les systèmes doivent être cartographiés, profilés et intégrés dans les systèmes existants, compte tenu des facteurs stratégiques et humains associés. Ensuite, des tests approfondis sont menés pour vérifier et assurer la solidité du système (tous les nouveaux systèmes disposent d'une authentification renforcée pour les utilisateurs et les composants, d'une classification et d'une protection appropriées des informations et d'un système avancé de prévention des pertes de données), pendant la mise en œuvre et dans la durée, ce qui permettra au secrétariat de l'OIAC de recenser les failles et d'y remédier dans la mesure du possible.

6. Durée

La durée totale estimée des activités financées dans le cadre de ce projet devrait être de vingt-quatre mois.

7. Bénéficiaires

Les bénéficiaires du projet seront le personnel du secrétariat technique de l'OIAC, les organes chargés de la définition des politiques, les organes subsidiaires et les parties prenantes de la CAC, y compris les États parties.

8. Visibilité de l'Union

L'OIAC prend toutes les mesures appropriées, dans des conditions de sécurité raisonnables, pour faire savoir que ce projet a été financé par l'Union.