BESLUIT (GBVB) 2021/1026 VAN DE RAAD

van 21 juni 2021

ter ondersteuning van het programma voor cyberbeveiliging, veerkracht en informatieborging van de Organisatie voor het verbod van chemische wapens (OPCW) in het kader van de uitvoering van de EU-strategie tegen de verspreiding van massavernietigingswapens

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de Europese Unie, en met name artikel 28, lid 1, en artikel 31, lid 1,

Gezien het voorstel van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid,

Overwegende hetgeen volgt:

(1) Op 12 december 2003 heeft de Europese Raad de EU-strategie tegen de verspreiding van massavernietigingswapens ("de EU-strategie") aangenomen, met in hoofdstuk III een lijst van maatregelen ter bestrijding van die verspreiding.

(2) In de EU-strategie wordt de cruciale rol benadrukt die het Verdrag tot verbod van de ontwikkeling, de productie, de aanleg van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens (Chemical Weapons Convention — het "CWC") en de Organisatie voor het verbod van chemische wapens (Organisation for the Prohibition of Chemical Weapons — de "OPCW") vervullen bij het tot stand brengen van een wereld zonder chemische wapens. De doelstellingen van de EU-strategie zijn complementair aan die van de OPCW, die immers verantwoordelijk is voor de uitvoering van het CWC.

(3) Op 22 november 2004 heeft de Raad Gemeenschappelijk Optreden 2004/797/GBVB ([1]) betreffende de ondersteuning van OPCW-activiteiten vastgesteld. Dat Gemeenschappelijk Optreden is na het verstrijken ervan opgevolgd door Gemeenschappelijk Optreden 2005/913/GBVB van de Raad ([2]), dat op zijn beurt is opgevolgd door Gemeenschappelijk Optreden 2007/185/GBVB van de Raad ([3]).

Gemeenschappelijk Optreden 2007/185/GBVB werd opgevolgd door de Besluiten 2009/569/GBVB ([4]), 2012/166/GBVB ([5]), 2013/726/CFSP ([6]), (GBVB) 2015/259 ([7]), (GBVB) 2017/2302 ([8]), (GBVB) 2017/2303 ([9]) en (GBVB) 2019/538 ([10]) van de Raad.

([1]) Gemeenschappelijk Optreden 2004/797/GBVB van de Raad van 22 november 2004 betreffende de ondersteuning van OPCW-activiteiten in het kader van de uitvoering van maatregelen van de strategie van de EU tegen de verspreiding van massavernietigingswapens (PB L 349 van 25.11.2004, blz. 63).

([2]) Gemeenschappelijk Optreden 2005/913/GBVB van de Raad van 12 december 2005 betreffende de ondersteuning van OPCW-activiteiten in het kader van de uitvoering van maatregelen van de strategie van de EU tegen de verspreiding van massavernietigingswapens (PB L 331 van 17.12.2005, blz. 34).

([3]) Gemeenschappelijk Optreden 2007/185/GBVB van de Raad van 19 maart 2007 betreffende de ondersteuning van OPCW-activiteiten in het kader van de uitvoering van maatregelen van de strategie van de EU tegen de verspreiding van massavernietigingswapens (PB L 85 van 27.3.2007, blz. 10).

([4]) Besluit 2009/569/GBVB van de Raad van 27 juli 2009 betreffende de ondersteuning van OPCW-activiteiten in het kader van de uitvoering van de strategie van de EU ter bestrijding van de verspreiding van massavernietigingswapens (PB L 197 van 29.7.2009, blz. 96).

([5]) Besluit 2012/166/GBVB van de Raad van 23 maart 2012 betreffende de ondersteuning van OPCW-activiteiten in het kader van de uitvoering van maatregelen van de EU-strategie tegen de verspreiding van massavernietigingswapens (PB L 87 van 24.3.2012, blz. 49).

([6]) Besluit 2013/726/GBVB van de Raad van 9 december 2013 ter ondersteuning van UNSCR 2118 (2013) en van EC-M-33/Dec 1 van de uitvoerende raad van de OPCW, in het kader van de tenuitvoerlegging van de EU-strategie tegen de verspreiding van massavernietigingswapens (PB L 329 van 10.12.2013, blz. 41).

([7]) Besluit (GBVB) 2015/259 van de Raad van 17 februari 2015 ter ondersteuning van activiteiten van de Organisatie voor het verbod van chemische wapens (OPCW) in het kader van de uitvoering van de strategie van de EU tegen de verspreiding van massavernietigingswapens (PB L 43 van 18.2.2015, blz. 14).

([8]) Besluit (GBVB) 2017/2302 van de Raad van 12 december 2017 ter ondersteuning van de OPCW-activiteiten die bijdragen tot de sanering van de voormalige opslagplaats voor chemische wapens in Libië in het kader van de uitvoering van de EU-strategie tegen de verspreiding van massavernietigingswapens (PB L 329 van 13.12.2017, blz. 49.

([9]) Besluit (GBVB) 2017/2303 van de Raad van 12 december 2017 ter ondersteuning van de verdere uitvoering van Resolutie 2118 (2013) van de VN-Veiligheidsraad en Besluit EC-M-33/DEC.1 van de uitvoerende raad van de OPCW inzake de vernietiging van de Syrische chemische wapens, in het kader van de tenuitvoerlegging van de EU-strategie tegen de verspreiding van massavernietigingswapens (PB L 329 van 13.12.2017, blz. 55).

([10]) Besluit (GBVB) 2019/538 van de Raad van 1 april 2019 ter ondersteuning van activiteiten van de Organisatie voor het verbod van chemische wapens (OPCW) in het kader van de uitvoering van de strategie van de EU tegen de verspreiding van massavernietigingswapens (PB L 93 van 2.4.2019, blz. 3).

(4) Voor de actieve uitvoering van hoofdstuk III van de EU-strategie is het noodzakelijk dat die intensieve en gerichte steun van de EU aan de OPCW wordt voortgezet.

(5) Er is verdere steun van de Unie nodig voor het programma voor cyberbeveiliging, veerkracht en informatieborging van de OPCW, dat erop gericht is de OPCW beter in staat te stellen een gepast niveau van cyberbeveiliging en veerkracht in stand te houden bij het aanpakken van bestaande en nieuwe uitdagingen op het gebied van cyberbeveiliging,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

1. Om onmiddellijk praktische uitvoering te geven aan bepaalde elementen van de EU-strategie, steunt de Unie een project van de OPCW dat erop gericht is:

— de ICT-infrastructuur te verbeteren overeenkomstig het institutionele bedrijfscontinuïteitskader van de OPCW, met veel aandacht voor veerkracht, en

— governance inzake bevoorrechte toegang te waarborgen, samen met de fysieke, logische en cryptografische verwerking en scheiding van informatie voor alle strategische netwerken en missienetwerken van de OPCW.

2. In de context van lid 1 ondersteunt de Unie de volgende activiteiten van het OPCW-project, die in overeenstemming zijn met de in hoofdstuk III van de EU-strategie vermelde maatregelen:

— het bevorderen van een gunstig klimaat voor permanente inspanningen op het gebied van cyberbeveiliging en veerkracht in het kader van OPCW-operaties op meerdere locaties;

— het ontwerpen van op maat gesneden oplossingen voor de integratie en configuratie van lokale en cloudgebaseerde systemen in de ICT-systemen van de OPCW, en oplossingen voor het beheer van bevoorrechte toegang (Privileged Access Management, PAM), en

— het in werking stellen en testen van PAM-oplossingen.

3. Een gedetailleerde beschrijving van de in lid 2 bedoelde door de Unie ondersteunde OPCW-activiteiten is in de bijlage opgenomen.

Artikel 2

1. De hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid ("de HV") draagt de verantwoordelijkheid voor de uitvoering van dit besluit.

2. De technische uitvoering van het in artikel 1 genoemde project is een taak van het technisch secretariaat van de OPCW ("het technisch secretariaat"). Het voert die taak uit onder verantwoordelijkheid en toezicht van de HV. Daartoe treft de HV de nodige regelingen met het technisch secretariaat.

Artikel 3

1. Het financieel referentiebedrag voor de uitvoering van het in artikel 1 bedoelde project bedraagt 2 151 823 EUR.

2. De door het bedrag in lid 1 gefinancierde uitgaven worden beheerd overeenkomstig de procedures en voorschriften die van toepassing zijn op de algemene begroting van de Unie.

3. De Commissie houdt toezicht op het correcte beheer van de in lid 2 bedoelde uitgaven. Daartoe sluit zij de nodige overeenkomst met het technisch secretariaat. In die overeenkomst wordt bepaald dat het technisch secretariaat er zorg voor moet dragen dat de bijdrage van de Unie zichtbaar is in een mate die evenredig is aan haar omvang en maatregelen moet vaststellen die het ontwikkelen van synergieën en het vermijden van overlappingen bevorderen.

4. De Commissie stelt alles in het werk om de in lid 3 bedoelde overeenkomst zo spoedig mogelijk na de inwerkingtreding van dit besluit te sluiten. Zij stelt de Raad in kennis van eventuele moeilijkheden en van de datum van sluiting van de overeenkomst.

Artikel 4

De HV brengt aan de Raad verslag uit over de uitvoering van dit besluit, op basis van de periodieke verslagen die worden opgesteld door het technisch secretariaat. De verslagen van de HV vormen de basis voor de evaluatie door de Raad. De Commissie verstrekt informatie over de financiële aspecten van het in artikel 1 bedoelde project.

Artikel 5

1. Dit besluit treedt in werking op de datum waarop het wordt vastgesteld.

2. Dit besluit verstrijkt 24 maanden na de sluiting van de in artikel 3, lid 3, bedoelde overeenkomst. Het verstrijkt echter zes maanden nadat het in werking is getreden indien die overeenkomst op dat moment nog niet is gesloten.

Gedaan te Luxemburg, 21 juni 2021.

Voor de Raad
De voorzitter
J. BORRELL FONTELLES

BIJLAGE

PROJECTDOCUMENT

1. Achtergrond

De OPCW moet infrastructuur die informatiesoevereiniteit mogelijk maakt, in stand houden op zodanige wijze dat de rubriceringen met bevoorrechte toegang, geschikte verwerkingsroutines en bestaande gevaren in acht worden genomen, en moet tegelijkertijd in staat blijven bescherming te bieden tegen nieuwe risico's. De OPCW blijft voortdurend te maken krijgen met ernstige en nieuwe risico's op het gebied van cyberbeveiliging en cyberveerkracht. De OPCW is het doelwit van uiterst bedreven, zeer goed uitgeruste en bijzonder gemotiveerde actoren. Die actoren blijven de vertrouwelijkheid en integriteit van de informatie- en infrastructuurvoorzieningen van de OPCW regelmatig aanvallen. Om tegemoet te komen aan de bezorgdheid naar aanleiding van de recente cyberaanvallen, de huidige politieke context en de COVID-19-crisis, en gezien de unieke vereisten die voortvloeien uit de aard van de werkzaamheden van de OPCW om het mandaat van het CWC te vervullen, zijn onmiskenbaar essentiële investeringen in technische capaciteit noodzakelijk.

In het kader van haar speciale fonds voor cyberbeveiliging, bedrijfscontinuïteit en veiligheid van fysieke infrastructuur heeft de OPCW haar programma voor cyberbeveiliging, veerkracht en informatieborging (het "OPCW-programma") opgesteld, met daarin 47 activiteiten om problemen op het gebied van cyberbeveiliging aan te pakken die zich de laatste tijd hebben voorgedaan. Het OPCW-programma is gebaseerd op goede praktijken die worden aanbevolen door organisaties zoals het EU-Agentschap voor cyberbeveiliging (Enisa), en maakt gebruik van concepten die verband houden met de Europese richtlijn betreffende netwerk- en informatiebeveiliging (NIB) op het gebied van telecommunicatie en defensie. Algemeen beschouwd bestrijkt het OPCW-programma de volgende thematische gebieden: gerubriceerde en niet-gerubriceerde netwerken; beleid en governance; detectie en respons; exploitatie en onderhoud; en telecommunicatie. Het OPCW-programma is in wezen bedoeld om de OPCW in staat te stellen te verhinderen dat goed uitgeruste en/of door een staat gesteunde aanvallers hun doel bereiken, en om de risico's van externe en van interne bedreigingen vanuit zowel menselijk als technisch oogpunt te beperken. De steun van de Unie is opgezet als een project van drie activiteiten, die overeenkomen met twee van de 47 activiteiten van het OPCW-programma.

2. Doel van het project

Het algemene doel van het project is te waarborgen dat het secretariaat van de OPCW over de nodige capaciteit beschikt om een passend niveau van cyberbeveiliging en veerkracht in stand te houden bij het aanpakken van steeds terugkerende en nieuwe problemen op het gebied cyberbeveiliging en -defensie, zowel in het hoofdkantoor als in andere vestigingen van de OPCW, zodat de OPCW haar mandaat kan vervullen en het CWC doeltreffend kan uitvoeren.

3. Doelstellingen

— De ICT-infrastructuur verbeteren overeenkomstig het institutionele bedrijfscontinuïteitskader van de OPCW, met veel aandacht voor veerkracht;

— governance inzake bevoorrechte toegang waarborgen, samen met de fysieke, logische en cryptografische verwerking en scheiding van informatie voor alle strategische netwerken en missienetwerken.

4. Resultaten

De verwachte resultaten waaraan het project bijdraagt, zijn de volgende:

— de ICT-apparatuur en -diensten bieden een hoge systeembetrouwbaarheid (hybride/geografische redundantie) en zorgen voor een betere beschikbaarheid van de ICT-systemen en -diensten ter ondersteuning van de bedrijfscontinuïteit;

— de mogelijkheden van elke factor of persoon om de vertrouwelijkheid en integriteit van informatie of systemen binnen de OPCW aan te tasten, worden tot een minimum beperkt.

5. Activiteiten

5.1. Activiteit 1 — Het bevorderen van een gunstig klimaat voor permanente inspanningen op het gebied van cyberbeveiliging en veerkracht in het kader van OPCW-operaties op meerdere locaties

Deze activiteit heeft tot doel een gunstig klimaat te waarborgen voor een vlotte uitrol van de bedrijfscontinuïteitsplanning van de OPCW op het gebied van cyberbeveiliging en veerkracht. Dit vereist een modernisering van de infrastructuur, een nieuwe architectuur en/of archivering om de bedrijfscontinuïteit van alle OPCW-operaties op meerdere locaties te waarborgen. Ook moet de integratie van governance inzake bevoorrechte toegang in de bedrijfscontinuïteitsplanning en responsprocessen verder gefaciliteerd en bevorderd worden.

5.2. Activiteit 2 — Het ontwerpen van op maat gesneden oplossingen voor de integratie en configuratie van lokale en cloudgebaseerde systemen in de ICT-systemen van de OPCW, en van oplossingen voor het beheer van bevoorrechte toegang (Privileged Access Management, PAM)

Deze activiteit is erop gericht dat gunstige klimaat om te zetten in een ontwerp op maat voor de integratie en configuratie van lokale en cloudgebaseerde systemen in de ICT-systemen van de OPCW en PAM-oplossingen. Dat zal naar verwachting leiden tot een verhoogde doeltreffendheid van de ICT-systeeminfrastructuur en tot het ontwerp van een geïntegreerd PAM-systeem voor kritieke middelen, dat afschrikking en detectie waarborgt en voldoende capaciteit biedt voor het naspeuren van bedreigingen.

5.3. Activiteit 3 — Het in werking stellen en testen van PAM-oplossingen

Deze activiteit bouwt voort op de geïmplementeerde infrastructuur en de PAM-oplossingen om de integratie en configuratie van theorie naar praktijk te brengen. De systemen moeten in kaart worden gebracht, worden afgebakend en in de bestaande systemen worden ingebed, een en ander rekening houdend met de relevante beleids- en menselijke factoren. Vervolgens wordt de soliditeit van het systeem tijdens de werking ervan en over een bepaalde tijdspanne gecontroleerd en gewaarborgd aan de hand van grondige tests (alle nieuwe systemen beschikken over strikte authenticatiemechanismen voor gebruikers en apparatuur, adequate classificatie en bescherming van informatie en een geavanceerd systeem voor de preventie van gegevensverlies), zodat het secretariaat van de OPCW lacunes kan opsporen en, voor zover mogelijk, verhelpen.

6. Duur

De geschatte totale duur van de via dit project gefinancierde activiteiten bedraagt 24 maanden.

7. Begunstigden

De begunstigden van het project zijn het personeel van het technisch secretariaat van de OPCW, beleidsvormingsorganen, ondergeschikte organen en stakeholders bij het CWC, met inbegrip van staten.

8. Zichtbaarheid van de EU

De OPCW doet, met inachtneming van redelijke veiligheidsoverwegingen, al het nodige om er ruchtbaarheid aan te geven dat dit project door de Unie wordt gefinancierd.