Raad van de
Europese Unie

Brussel, 14 september 2018
(OR. en)

12104/18

Interinstitutioneel dossier:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

BEGELEIDENDE NOTA

van:	de heer Jordi AYET PUIGARNAU, directeur, namens de secretaris-generaal van de Europese Commissie
ingekomen:	12 september 2018
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
Nr. Comdoc.:	COM(2018) 630 final
Betreft:	Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

Hierbij gaat voor de delegaties document COM(2018) 630 final.

Bijlage: COM(2018) 630 final

EUROPESE
COMMISSIE

Brussel, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

Een bijdrage van de Europese Commissie aan de bijeenkomst van leiders in Salzburg op 19-20 september 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Nu het dagelijks leven en de economie steeds meer op digitale technologieën steunen, stijgt ook het risico op ernstige cyberincidenten. Om de veiligheid in de toekomst te waarborgen, zal de Unie zich beter moeten kunnen weren tegen cyberdreigingen, aangezien zowel de civiele infrastructuur als de militaire capaciteit afhankelijk zijn van veilige digitale systemen.

Om de grotere uitdagingen aan te kunnen, heeft de Unie haar activiteiten op dit gebied gestaag opgevoerd. Daarbij bouwt zij voort op de cyberbeveiligingsstrategie van 2013[1] en de daarin opgenomen doelstellingen en beginselen ter bevordering van een betrouwbaar, veilig en open cyber-ecosysteem. In 2016 heeft de Unie voor het eerst maatregelen op het gebied van cyberbeveiliging vastgesteld in Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[2] voor de beveiliging van netwerk- en informatiesystemen.

Aangezien het cyberbeveiligingslandschap snel verandert, hebben de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid in september 2017 een gezamenlijke mededeling[3] voorgesteld over "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" om de weerbaarheid, het afschrikkingseffect en het reactievermogen van de EU ten opzichte van cyberaanvallen te versterken. In de gezamenlijke mededeling wordt ook op eerdere initiatieven voortgebouwd en worden een aantal maatregelen voorgesteld, zoals de versterking van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), de oprichting van een vrijwillig en Uniebreed kader voor cyberbeveiligingscertificering met het oog op betere cyberbeveiliging van digitale producten en diensten, alsook een blauwdruk om snel en gecoördineerd op grootschalige cyberincidenten en -crises te reageren.

In de gezamenlijke mededeling werd erkend dat het ook in het strategische belang van de Unie is om essentiële technologische capaciteiten op het gebied van cyberbeveiliging te behouden en te ontwikkelen voor de beveiliging van de digitale eengemaakte markt, en met name de bescherming van kritieke netwerken en informatiesystemen, alsook voor de verlening van essentiële diensten op het gebied van cyberbeveiliging. De Unie moet in staat zijn zelfstandig haar digitale activa veilig te stellen en te concurreren op de mondiale cyberbeveiligingsmarkt.

De Unie is momenteel een netto-importeur van cyberbeveiligingsproducten en -oplossingen en is grotendeels afhankelijk van niet-Europese aanbieders[4]. De cyberbeveiligingsmarkt is wereldwijd goed voor 600 miljard euro en zal de komende vijf jaar naar verwachting gemiddeld met zo'n 17 % groeien wat betreft de verkoop, het aantal bedrijven en de

---

1 Gezamenlijke mededeling aan het Europees Parlement en de Raad: Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace (JOIN(2013) 1 final).

2 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB L 194 van 19.7.2016, blz. 1.

3 Gezamenlijke mededeling aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" (JOIN(2017) 450 final).

4 Ontwerp van het eindverslag over de studie van de cyberbeveiligingsmarkt, 2018

werkgelegenheid. In de top 20 van landen die vanuit marktperspectief op kop lopen wat cyberbeveiliging betreft, staan echter maar zes lidstaten[5].

Tegelijkertijd is er in de Unie een schat aan deskundigheid en ervaring op het gebied van cyberbeveiliging – bij de recente inventarisatie door de Commissie van expertisecentra op het gebied van cyberbeveiliging zijn 660 organisaties uit de hele Unie in kaart gebracht[6]. Indien deze knowhow in verhandelbare producten en oplossingen zou worden omgezet, zou dit de Unie in staat stellen de gehele waardeketen op het gebied van cyberbeveiliging te bestrijken. De onderzoeksgemeenschap en de industriële gemeenschappen leveren echter los van elkaar inspanningen die daardoor niet op elkaar zijn afgestemd en geen gezamenlijk doel nastreven, waardoor de EU op dit gebied minder concurrerend is en haar digitale troeven minder goed kan veiligstellen. De betrokken cyberbeveiligingssectoren (zoals energie, ruimtevaart, defensie, vervoer) en subdomeinen worden momenteel onvoldoende ondersteund[7]. In Europa worden de synergieën tussen de civiele en militaire cyberbeveiligingssectoren niet ten volle benut.

Toen in 2016 het publiek-private partnerschap voor cyberbeveiliging ("cPPP") in de Unie werd opgezet, was dit een eerste grote stap om de onderzoeksgemeenschap, de industrie en de publieke sector samen te brengen om onderzoek en innovatie op het gebied van cyberbeveiliging te vergemakkelijken. Dit zou binnen de grenzen van het meerjarig financieel kader voor de periode 2014-2020 goede, meer gerichte resultaten op het gebied van onderzoek en innovatie moeten opleveren. Dankzij het cPPP konden industriële partners toezeggingen doen over hun individuele uitgaven met betrekking tot gebieden die in de strategische agenda voor onderzoek en innovatie van het partnerschap zijn vastgesteld.

De Unie kan echter op veel grotere schaal investeringen nastreven en heeft behoefte aan een doeltreffender mechanisme om blijvende capaciteit op te bouwen, inspanningen en bevoegdheden te bundelen en een stimulans te geven aan de ontwikkeling van innovatieve oplossingen voor cyberbeveiligingsuitdagingen van het bedrijfsleven op het gebied van nieuwe multifunctionele technologieën (bv. kunstmatige intelligentie, kwantumcomputers, blockchaintechnologie en veilige digitale identiteiten) en in cruciale sectoren (bv. vervoer, energie, gezondheid, financiën, de overheid, telecommunicatie, de maakindustrie, defensie, ruimtevaart).

In de gezamenlijke mededeling werd de mogelijkheid overwogen om de cyberbeveiligingscapaciteit van de Unie te versterken door middel van een netwerk van kenniscentra voor cyberbeveiliging met een centraal Europees kenniscentrum voor cyberbeveiliging. Dit zou een aanvulling zijn op de bestaande inspanningen voor een dergelijke capaciteitsopbouw op het niveau van de Unie en van de lidstaten. In de gezamenlijke mededeling wordt gewag gemaakt van het voornemen van de Commissie om in 2018 de effecten te beoordelen van de beschikbare opties voor de op te zetten structuur. Als eerste stap – en als bijdrage aan het toekomstige denkproces – heeft de Commissie in het kader van Horizon 2020 een proeffase opgestart om de nationale centra samen te brengen in een netwerk en zo een nieuwe impuls te geven aan de ontwikkeling van kennis en technologie op het gebied van cyberbeveiliging.

---

5 Ontwerp van het eindverslag over de studie van de cyberbeveiligingsmarkt, 2018

6 Technische verslagen JRC: European Cybersecurity Centres of Expertise, 2018

7 Technisch verslag JRC: Outcomes of the Mapping Exercise (meer details in de bijlagen 4 en 5)

De staatshoofden en regeringsleiders hebben op de digitale top van Tallinn in september 2017 opgeroepen om van Europa uiterlijk in 2025 een leider in cyberbeveiliging te maken, zodat de burgers, consumenten en bedrijven vol vertrouwen online kunnen gaan en bescherming genieten, en een vrij en aan het recht onderworpen internet mogelijk wordt.

In de conclusies van de Raad[8] van november 2017 werd de Commissie verzocht om snel een effectbeoordeling van de mogelijke opties te maken en medio 2018 het toepasselijke rechtsinstrument voor de uitvoering van het initiatief voor te stellen.

Het programma Digitaal Europa, dat in juni 2018 door de Commissie is voorgesteld[9]*,* is bedoeld om de voordelen van de digitale transformatie voor Europese burgers en bedrijven op alle relevante beleidsgebieden van de EU te vergroten en te maximaliseren door het beleid te versterken en de ambities van de digitale eengemaakte markt te ondersteunen. In het programma wordt een coherente en overkoepelende aanpak voorgesteld met het oog op de optimale benutting van geavanceerde technologieën en de juiste combinatie van technische capaciteit en menselijke competentie bij de digitale transformatie – niet alleen op het gebied van cyberbeveiliging, maar ook met betrekking tot slimme data-infrastructuur, kunstmatige intelligentie, geavanceerde vaardigheden en toepassingen in de industrie en op gebieden van openbaar belang. Deze elementen hangen samen, versterken elkaar en kunnen, wanneer zij gelijktijdig worden gestimuleerd, de omvang bereiken die nodig is om een data-economie te laten gedijen[10]. Ook in het programma *Horizon Europa*[11], het volgende EU-kaderprogramma voor O&I, is cyberbeveiliging een prioriteit.

In deze verordening wordt voorgesteld om tegelijk met een netwerk van nationale coördinatiecentra een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging op te richten. Om het Europese technologische en industriële ecosysteem op het gebied van cyberbeveiliging te stimuleren, moet dit op maat gemaakte samenwerkingsmodel als volgt functioneren: Het kenniscentrum bevordert de werkzaamheden van het netwerk, helpt deze te coördineren, en helpt de kennisgemeenschap voor cyberbeveiliging vooruit door de agenda voor cyberbeveiligingstechnologie te stimuleren en de toegang tot de opgedane knowhow te vergemakkelijken. Het kenniscentrum doet dit met name door de relevante onderdelen van de programma's Digitaal Europa en Horizon Europa ten uitvoer te leggen door subsidies toe te kennen en aanbestedingen uit te schrijven. Aangezien in andere delen van de wereld aanzienlijk in cyberbeveiliging wordt geïnvesteerd en er in Europa behoefte is aan een betere coördinatie en bundeling van de middelen, wordt het kenniscentrum voorgesteld als een Europees partnerschap[12], wat een gezamenlijke investering door de Unie, de lidstaten en/of de industrie vergemakkelijkt. Daarom moeten de lidstaten volgens dit voorstel in gelijke mate financieel bijdragen aan de

---

8 Conclusies van de Raad over de Gezamenlijke mededeling aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan een sterke cyberbeveiliging voor de EU", goedgekeurd door de Raad Algemene zaken op 20 november 2017.

9 COM(2018) 434 Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van het programma Digitaal Europa voor de periode 2021-2027

10 Zie SWD (2018) 305.

11 COM(2018) 435 Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van Horizon Europa – het kaderprogramma voor onderzoek en innovatie, en tot vaststelling van de regels voor deelname en verspreiding

12 Zoals gedefinieerd in het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van Horizon Europa – het kaderprogramma voor onderzoek en innovatie, en tot vaststelling van de regels voor deelname en verspreiding (COM(2018) 435), en zoals bedoeld in het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van het programma Digitaal Europa voor de periode 2021-2027 (COM(2018) 434).

acties van het kenniscentrum en het netwerk. Het voornaamste besluitvormingsorgaan is de raad van bestuur, waarin alle lidstaten vertegenwoordigd zijn, maar waarin alleen de lidstaten die een financiële bijdrage leveren, stemrecht hebben. In de raad van bestuur wordt er gestemd volgens het beginsel van dubbele meerderheid, wat betekent dat 75 % van de financiële bijdragen en 75 % van de stemmen nodig zijn. Aangezien de Commissie verantwoordelijk is voor de begroting van de Unie, beschikt zij over 50 % van de stemmen. Voor haar werkzaamheden in de raad van bestuur zal de Commissie, waar nodig, gebruikmaken van de expertise van de Europese Dienst voor extern optreden. Om regelmatig overleg met de privésector, consumentenorganisaties en andere relevante belanghebbenden te waarborgen, wordt de raad van bestuur bijgestaan door een industrieel en wetenschappelijk adviescomité.

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zou nauw samenwerken met het netwerk van nationale coördinatiecentra en de kennisgemeenschap voor cyberbeveiliging die bij deze verordening worden opgericht (bestaande uit een grote en diverse groep van actoren die zich bezighouden met de ontwikkeling van cyberbeveiligingstechnologie, zoals onderzoeksinstellingen, industrieën aan de vraagzijde en aan de aanbodzijde, en de publieke sector); dit kenniscentrum zou het voornaamste uitvoeringsorgaan zijn voor de financiële middelen van de EU die in het kader van de voorgestelde programma's *Digitaal Europa* en *Horizon Europa* voor cyberbeveiliging worden uitgetrokken.

Door deze alomvattende aanpak zou cyberbeveiliging in de hele waardeketen kunnen worden ondersteund, van het onderzoek tot de uitrol en het gebruik van cruciale technologieën. De financiële bijdragen van de lidstaten moeten in verhouding staan tot de financiële bijdrage van de EU aan dit initiatief en zijn een onontbeerlijk element voor het welslagen ervan.

De European Cybersecurity Organisation (Europese organisatie voor cyberbeveiliging), de tegenhanger van de Commissie voor het contractuele publiek-private partnerschap voor cyberbeveiliging in het kader van Horizon 2020, moet, gezien haar bijzondere deskundigheid en ruime en relevante vertegenwoordiging van belanghebbenden, worden uitgenodigd om bij te dragen aan de werkzaamheden van het kenniscentrum en het netwerk.

Ook moet het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging manieren zoeken om de synergieën tussen de civiele en defensieaspecten van cyberbeveiliging te versterken. Het kenniscentrum moet de lidstaten en andere relevante actoren ondersteunen door advies te verstrekken, expertise te delen en de samenwerking bij projecten en acties te vergemakkelijken. Op verzoek van de lidstaten zou het ook kunnen optreden als projectbeheerder, met name met betrekking tot het Europees Defensiefonds. Dit initiatief beoogt bij te dragen tot de aanpak van de volgende problemen:

- **Onvoldoende samenwerking tussen de vraagzijde en de aanbodzijde in de cyberbeveiligingsindustrie.** De Europese bedrijven staan voor de uitdaging dat ze zowel voor hun eigen beveiliging moeten zorgen als veilige producten en diensten aan hun klanten moeten aanbieden. Ze zijn echter vaak niet in staat om hun bestaande producten, diensten en activa afdoende te beveiligen of om veilige innovatieve producten en diensten te ontwerpen. Voor individuele spelers voor wie cyberbeveiliging buiten de kernactiviteiten valt, is het vaak te duur om cruciale activa met betrekking tot cyberbeveiliging te ontwikkelen en toe te passen. Tegelijkertijd worden de banden tussen de vraag- en de aanbodzijde van de cyberbeveiligingsmarkt onvoldoende aangehaald, wat leidt tot een suboptimaal aanbod van Europese producten en oplossingen die zijn aangepast

aan de behoeften van de verschillende sectoren, en tot onvoldoende vertrouwen bij de marktdeelnemers.

- **Geen efficiënt mechanisme voor samenwerking tussen de lidstaten voor de opbouw van industriële capaciteit.** Op dit moment is er ook geen doeltreffend mechanisme dat de lidstaten toelaat samen te werken aan de opbouw van de nodige capaciteiten ter ondersteuning van innovatie op het gebied van cyberbeveiliging in alle bedrijfssectoren en de aanwending van geavanceerde Europese oplossingen op het gebied van cyberbeveiliging. De bestaande mechanismen voor samenwerking tussen de lidstaten op het gebied van cyberbeveiliging krachtens Richtlijn (EU) 2016/1148 voorzien niet in dit soort activiteiten.
- **Onvoldoende samenwerking binnen en tussen onderzoeks- en industriële gemeenschappen.** Hoewel Europa theoretisch over het vermogen beschikt om de volledige cyberbeveiligingswaardeketen te dekken, zijn er relevante cyberbeveiligingssectoren (bv. energie, ruimtevaart, defensie, vervoer) en subdomeinen die tegenwoordig slecht worden ondersteund door de onderzoeksgemeenschap of slechts worden ondersteund door een beperkt aantal centra (bv. postkwantum- en kwantumcryptografie, vertrouwen en cyberbeveiliging bij kunstmatige intelligentie). Hoewel er hiervoor kennelijk wordt samengewerkt, gaat het zeer vaak om consultancyachtige kortetermijnafspraken, waardoor er geen langetermijnplannen worden gemaakt om industriële uitdagingen op het gebied van cyberbeveiliging op te lossen.
- **Onvoldoende samenwerking op het gebied van cyberbeveiliging tussen civiele en militaire onderzoeks- en innovatiegemeenschappen.** Het probleem van de ontoereikende samenwerking heeft ook betrekking op de civiele en militaire gemeenschappen. De bestaande synergieën worden niet ten volle benut omdat er geen efficiënte mechanismen zijn waardoor deze gemeenschappen efficiënt zouden kunnen samenwerken en vertrouwen kunnen opbouwen, hetgeen – meer nog dan op andere gebieden – een voorwaarde is voor succesvolle samenwerking. Tegelijk beschikt de EU-markt voor cyberbeveiling slechts over beperkte financiële mogelijkheden en zijn er onder meer onvoldoende financiële middelen voor innovatie.
- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Het kennisnetwerk voor cyberbeveiliging en het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zullen een extra ondersteuning zijn voor de bestaande beleidsbepalingen en spelers op het gebied van cyberbeveiliging. Het mandaat van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal een aanvulling vormen op de inspanningen van het Enisa, maar legt een andere nadruk en vereist andere vaardigheden. Terwijl het mandaat van het Enisa voorziet in een adviserende rol inzake onderzoek en innovatie op het gebied van cyberbeveiliging in de EU, is het voorgestelde mandaat van het kenniscentrum vooral gericht op andere taken die cruciaal zijn voor de versterking van de weerbaarheid van de EU op het gebied van cyberbeveiliging. Bovendien komen de kernactiviteiten in het mandaat van het Enisa niet overeen met de kerntaken van het kenniscentrum en het netwerk, namelijk het stimuleren van de ontwikkeling en invoering van cyberbeveiligingstechnologie en het aanvullen van de inspanningen voor capaciteitsopbouw op EU- en nationaal niveau.

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal samen met het kennisnetwerk voor cyberbeveiliging ook werken aan de ondersteuning van onderzoek om de standaardiserings- en certificeringsprocessen te

vergemakkelijken en te versnellen, met name die met betrekking tot regelingen voor cyberbeveiligingscertificering in de zin van de voorgestelde cyberbeveiligingsverordening[13][14].

Dit initiatief is een feitelijke uitbreiding van het publiek-private partnerschap voor cyberbeveiliging (cPPP), de eerste EU-brede poging om de cyberbeveiligingsbranche, de vraagzijde (kopers van cyberbeveiligingsproducten en -oplossingen, met inbegrip van openbare besturen en kritieke sectoren zoals de vervoers-, gezondheids-, energie- en financiële sector) en de onderzoeksgemeenschap bijeen te brengen om een platform voor duurzame dialoog op te zetten en voorwaarden te scheppen voor vrijwillige gezamenlijke investeringen. Het cPPP werd in 2016 opgezet en zal tegen 2020 tot 1,8 miljard EUR aan investeringen hebben geleid. De omvang van de investeringen in andere delen van de wereld (de VS hebben in 2017 alleen al 19 miljard dollar geïnvesteerd in cyberbeveiliging) toont aan dat de EU meer moet doen om een kritische massa aan investeringen te bereiken en de versnippering van de capaciteiten in de hele EU te verhelpen.

- **Verenigbaarheid met andere beleidsterreinen van de Unie**

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal optreden als één uitvoerend orgaan voor diverse EU-programma's ter ondersteuning van cyberbeveiliging (de programma's "Digitaal Europa" en "Horizon Europa") en zal de samenhang en de synergieën tussen deze programma's verbeteren.

Dit initiatief kan ook een aanvulling bieden op de inspanningen van de lidstaten door makers van onderwijsbeleid passende input te geven voor de verbetering van de vaardigheden op het gebied van cyberbeveiliging (bv. door voor de civiele en militaire onderwijsstelsels leerplannen voor cyberbeveiliging te ontwikkelen). Dat zou ertoe bijdragen dat de EU op termijn over gekwalificeerd cyberbeveiligingspersoneel beschikt, wat van cruciaal belang is voor cyberbeveiligingsbedrijven en andere branches met een belang in cyberbeveiliging. Wat onderwijs en opleiding in cyberdefensie betreft, strookt dit initiatief met de lopende werkzaamheden van het platform voor onderwijs, opleiding, evaluatie en oefeningen op cybergebied dat is opgericht in het kader van de Europese Veiligheids- en defensieacademie.

Dit initiatief zal de inspanningen van de digitale-innovatiehubs in het kader van het programma "Digitaal Europa" aanvullen en ondersteunen. Digitale-innovatiehubs zijn non-profitorganisaties die bedrijven – vooral startups, kmo's en midcaps – helpen hun concurrentievermogen te vergroten door de bedrijfsprocessen/productieprocessen, maar ook de producten en diensten zelf, te verbeteren door middel van slimme innovatie met digitale technologie. Digitale-innovatiehubs bieden bedrijfsgerichte innovatiediensten aan, zoals marktonderzoek, financieringsadvies, toegang tot relevante test- en experimenteerfaciliteiten, opleidingen en de ontwikkeling van vaardigheden, om nieuwe producten of diensten met succes op de markt te brengen of om betere productieprocessen in te voeren. Sommige

---

[13] Voorstel voor een Verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening" – COM(2017) 477 final/3)

[14] Dit doet geen afbreuk aan de certificeringsmechanismen van de algemene verordening gegevensbescherming waarin gegevensbeschermingsautoriteiten een rol moeten spelen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG ("algemene verordening gegevensbescherming").

digitale-innovatiehubs met specifieke deskundigheid op het gebied van cyberbeveiliging zouden rechtstreeks kunnen worden betrokken bij de kennisgemeenschap voor cyberbeveiliging die bij dit initiatief wordt opgericht. In de meeste gevallen zouden de digitale-innovatiehubs, die zelf geen specifiek cyberbeveiligingsprofiel hebben, er echter voor zorgen dat hun clientèle toegang heeft tot de expertise, de kennis en de capaciteiten op het gebied van cyberbeveiliging waarover de kennisgemeenschap voor cyberbeveiliging beschikt. Ze zouden hiervoor nauw samenwerken met het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging. Digitale-innovatiehubs zouden ook ondersteuning bieden bij de aanwending van innovatieve cyberbeveiligingsproducten en -oplossingen die tegemoetkomen aan de behoeften van de bedrijven en andere eindgebruikers die bij hen zijn aangesloten. Tot slot zouden sectorspecifieke digitale-innovatiehubs hun kennis over bestaande sectorale behoeften kunnen delen met het netwerk en het kenniscentrum en zo input geven voor de discussie om de onderzoeks- en innovatieagenda op één lijn te brengen met de industriële behoeften.

Er zal worden gestreefd naar synergieën met relevante kennis- en innovatiegemeenschappen van het Europees Instituut voor innovatie en technologie, en in het bijzonder met EIT Digital.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

Door zijn aard en specifieke doelstellingen moet het kenniscentrum worden vastgesteld op basis van een dubbele rechtsgrondslag. Op grond van artikel 187 VWEU, waarin structuren in het leven worden geroepen die noodzakelijk zijn voor de goede uitvoering van programma's voor onderzoek en technologische ontwikkeling en demonstratie in de Unie, kan het kenniscentrum synergieën creëren en middelen bundelen om in de nodige capaciteit op het niveau van de lidstaten te investeren en Europese gedeelde activa te ontwikkelen (bv. door de gezamenlijke aanbesteding van de nodige infrastructuur voor tests en experimenten op het gebied van cyberbeveiliging). In de eerste alinea van artikel 188 wordt voorzien in de vaststelling van dergelijke maatregelen. Met artikel 188, eerste alinea, als enige rechtsgrondslag zouden de activiteiten echter niet verder mogen gaan dan onderzoek en ontwikkeling, hetgeen wel nodig is om alle in deze verordening vastgestelde doelstellingen van het kenniscentrum te verwezenlijken om de marktintroductie van cyberbeveiligingsproducten en -oplossingen te ondersteunen, het concurrentievermogen en het marktaandeel van de Europese cyberbeveiligingsbranche te helpen versterken, en toegevoegde waarde te bieden ten opzichte van de nationale inspanningen om de vaardigheidskloof op het gebied van cyberbeveiliging te dichten. Om deze doelstellingen te verwezenlijken is het daarom noodzakelijk artikel 173, lid 3, VWEU als rechtsgrondslag toe te voegen, zodat de Unie maatregelen kan vaststellen om het concurrentievermogen van de industrie te ondersteunen.

• Motivering van het voorstel aan de hand van de subsidiariteits- en evenredigheidsbeginselen

Cyberbeveiliging is een zaak van gemeenschappelijk belang voor de Unie, zoals ook is bevestigd in de hierboven vermelde conclusies van de Raad. Goede voorbeelden zijn de omvang en het grensoverschrijdende karakter van incidenten zoals *WannaCry* en *NonPetya*. Gezien de aard en de omvang van de technologische uitdagingen op het gebied van cyberbeveiliging, en aangezien de inspanningen in het bedrijfsleven, de overheidssector en de onderzoeksgemeenschappen, alsook tussen deze sectoren onderling, onvoldoende worden gecoördineerd, moet de EU de coördinatie-inspanningen verder ondersteunen, zowel om een

kritische massa aan middelen bijeen te brengen als om een beter beheer van kennis en activa te garanderen. Dit is noodzakelijk aangezien er middelen nodig zijn voor bepaalde capaciteiten voor het onderzoek naar en de ontwikkeling en invoering van cyberbeveiligingstechnologieën, aangezien er toegang moet worden verleend tot interdisciplinaire kennis op het gebied van cyberbeveiliging in verschillende disciplines (vaak slechts gedeeltelijk beschikbaar op nationaal niveau) en aangezien de industriële waardeketens een mondiaal karakter hebben en de concurrenten overal ter wereld op allerlei markten actief zijn.

Hiervoor zijn middelen en expertise vereist van een niveau dat moeilijk kan worden bereikt met afzonderlijke maatregelen van een lidstaat. Zo zou een pan-Europees kwantumcommunicatienetwerk een investering van ongeveer 900 miljoen EUR van de EU vergen, afhankelijk van de investeringen van de lidstaten (te koppelen / aan te vullen) en de mate waarin voor de technologie bestaande infrastructuren kunnen worden hergebruikt. Het initiatief zal een grote rol spelen bij het bundelen van de financiering en het mogelijk maken van dit soort investeringen in de Unie.

De doelstellingen van dit initiatief kunnen niet volledig door de lidstaten alleen worden verwezenlijkt. Zoals hierboven is aangetoond, kunnen de doelstellingen beter worden verwezenlijkt op het niveau van de Unie door de inspanningen te bundelen en overlappingen te voorkomen, door bij te dragen tot het bereiken van een kritische massa aan investeringen en door ervoor te zorgen dat de overheidsfinanciering optimaal wordt gebruikt. Tegelijk gaat deze verordening, overeenkomstig het evenredigheidsbeginsel, niet verder dan nodig is om dit doel te verwezenlijken. Maatregelen op EU-niveau zijn daarom gerechtvaardigd om redenen van subsidiariteit en evenredigheid.

Dit instrument voorziet niet in nieuwe wettelijke verplichtingen voor bedrijven. Tegelijkertijd zullen voor ondernemingen, en met name kleine en middelgrote ondernemingen, naar alle waarschijnlijk de kosten met betrekking tot het ontwerp van innovatieve cyberbeveiligde producten afnemen, aangezien dit initiatief het mogelijk maakt om middelen te bundelen voor investeringen in de nodige capaciteiten op lidstaatniveau of om Europese gedeelde activa te ontwikkelen (bv. door de gezamenlijke aanbesteding van de nodige infrastructuur voor tests en experimenten op het gebied van cyberbeveiliging). Deze activa zouden door industrieën en kmo's in verschillende sectoren kunnen worden gebruikt om ervoor te zorgen dat hun producten cyberbeveiligd zijn en dat cyberbeveiliging concurrentievoordeel oplevert.

- **Keuze van het instrument**

Het voorgestelde instrument voorziet in de oprichting van een orgaan voor de uitvoering van maatregelen op het gebied van cyberbeveiliging in het kader van de programma's "Digitaal Europa" en "Horizon Europa". Het bevat een beschrijving van het mandaat, de taken en de bestuurlijke structuur van dit orgaan. De oprichting van een dergelijk orgaan van de Unie, moet in een verordening worden vastgesteld.

3. RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

Het voorstel tot oprichting van een kennisnetwerk voor cyberbeveiliging met een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging is een nieuw initiatief. Het is een voortzetting en opschaling van het contractuele publiek-private partnerschap voor cyberbeveiliging dat in 2016 in het leven is geroepen.

- **Raadpleging van belanghebbenden**

Cyberbeveiliging is een breed, sectoroverschrijdend thema. De Commissie heeft verschillende raadplegingsmethoden gebruikt om ervoor te zorgen dat het algemeen belang van de Unie – en niet dat van een beperkte groep belanghebbenden – duidelijk tot uiting komt in dit initiatief. Met deze methode wordt gezorgd voor transparantie en verantwoordingsplicht in het kader van de werkzaamheden van de Commissie. Hoewel er gezien de doelgroep (de industrie, de onderzoeksgemeenschap en de lidstaten) voor dit initiatief geen specifieke openbare raadpleging is gehouden, werd het thema al geregeld door een aantal andere openbare raadplegingen aangesneden:

- In 2018 werd een algemene openbare raadpleging gehouden over investeringen, onderzoek en innovatie, kleine en middelgrote ondernemingen en de interne markt.
- In 2017 werd online een twaalf weken durende openbare raadpleging gehouden om te peilen naar de mening van het grote publiek (ongeveer 90 respondenten) over de evaluatie en herziening van het Enisa.
- In 2016 werd online een twaalf weken durende openbare raadpleging gehouden naar aanleiding van de start van het contractuele publiek-private partnerschap voor cyberbeveiliging (ongeveer 240 respondenten).

De Commissie heeft ook gerichte raadplegingen over dit initiatief georganiseerd, waaronder workshops, vergaderingen en gerichte verzoeken om input (van het Enisa en het Europees Defensieagentschap). De raadplegingsperiode duurde zes maanden en liep van november 2017 tot en met maart 2018. De Commissie heeft ook de expertisecentra in kaart gebracht, waardoor bij 665 centra voor cyberbeveiliging informatie kon worden verzameld over hun knowhow, activiteiten, werkterreinen en internationale samenwerking. De enquête werd in januari opgestart en voor de analyse in het verslag zijn de antwoorden in aanmerking genomen die uiterlijk op 8 maart 2018 zijn ingediend.

Belanghebbenden uit de onderzoeks- en industriële gemeenschappen waren van mening dat het kenniscentrum en het netwerk een toegevoegde waarde zouden kunnen bieden voor de huidige inspanningen op nationaal niveau door te helpen een EU-breed ecosysteem voor cyberbeveiliging in het leven te roepen dat een betere samenwerking tussen de onderzoeks- en industriële gemeenschappen mogelijk maakt. Zij vonden het ook noodzakelijk dat de EU en de lidstaten het industriebeleid voor cyberbeveiliging proactief, met een langetermijnperspectief en vanuit strategisch oogpunt uitstippelen en daarbij verder gaan dan alleen onderzoek en innovatie. De belanghebbenden vermeldden ook dat er behoefte is aan toegang tot essentiële capaciteiten zoals test- en experimenteerfaciliteiten en aan meer ambitie bij het dichten van de kloof op het gebied van cyberbeveiligingsvaardigheden, bijvoorbeeld door grootschalige Europese projecten op te zetten die het grootste talent aantrekken. Al het bovenstaande werd ook gezien als noodzakelijk als de EU wereldwijd een leider op het gebied van cyberbeveiliging wil worden.

In het kader van de sinds september verrichte raadplegingsactiviteiten[15] en in de specifieke conclusies van de Raad[16] hebben de lidstaten positief gereageerd op het voornemen om een kennisnetwerk voor cyberbeveiliging op te richten om de ontwikkeling en toepassing van

[15] Bijv. de rondetafelconferentie op hoog niveau met de lidstaten, vicevoorzitter Ansip en commissaris Gabriel, 5 december 2017.

[16] Raad Algemene zaken: Conclusies van de Raad over de Gezamenlijke mededeling aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan een sterke cyberbeveiliging voor de EU" (20 november 2017).

cyberbeveiligingstechnologieën te bevorderen, waarbij de nadruk wordt gelegd op het belang om inclusief te zijn voor alle lidstaten en hun bestaande excellentie- en kenniscentra en bijzondere aandacht te schenken aan complementariteit. De lidstaten benadrukten met name het belang van de coördinerende rol van het toekomstige kenniscentrum ter ondersteuning van het netwerk. De in maart 2018 door de Europese Dienst voor extern optreden uitgevoerde inventarisatie van de behoeften op het gebied van cyberdefensie heeft aangetoond dat de meeste lidstaten vinden dat de EU een meerwaarde kan bieden op het vlak van opleiding en onderwijs en bij de ondersteuning van de industrie door middel van onderzoek en ontwikkeling[17]. Het initiatief zou inderdaad samen met de lidstaten of met door hen gesteunde entiteiten ten uitvoer worden gelegd. Door samenwerkingsverbanden op te zetten tussen de industrie, de onderzoeksgemeenschap en/of de openbare sector zouden de bestaande entiteiten en inspanningen kunnen worden gebundeld in plaats van dat er nieuwe worden gecreëerd. De lidstaten zouden ook worden betrokken bij het vaststellen van specifieke acties die gericht zijn op de overheidssector als een directe gebruiker van cyberbeveiligingstechnologie en -knowhow.

- **Effectbeoordeling**

Een effectbeoordeling ter ondersteuning van dit initiatief is op 11 april 2017 voorgelegd aan de Raad voor regelgevingstoetsing en kreeg een positief advies met punten van voorbehoud. De effectbeoordeling is vervolgens opnieuw bekeken aan de hand van de opmerkingen van de Raad voor regelgevingstoetsing. Het advies van de raad voor regelgevingstoetsing en de bijlage waarin wordt uitgelegd op welke manier rekening is gehouden met de opmerkingen van de raad, worden samen met dit voorstel gepubliceerd.

In de effectbeoordeling zijn een aantal wetgevende en niet-wetgevende beleidsopties in overweging genomen. De volgende opties zijn meegenomen voor een diepgaande beoordeling:

- Het basisscenario – de samenwerkingsoptie – gaat uit van de voortzetting van de huidige aanpak om de industriële en technologische capaciteiten op het gebied van cyberbeveiliging in de EU verder op te bouwen door middel van onderzoek en innovatie en daarmee verband houdende samenwerkingsmechanismen in het kader van KP9.
- Optie 1: Een kennisnetwerk voor cyberbeveiliging en een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging met een dubbel mandaat om maatregelen te nemen ter ondersteuning van industriële technologieën, alsook op het gebied van onderzoek en innovatie.
- Optie 2: Een kennisnetwerk voor cyberbeveiliging met een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging, gericht op onderzoek en innovatie.

De opties die in een vroeg stadium werden verworpen, waren 1) de optie om helemaal geen actie te ondernemen, 2) de optie om uitsluitend een kennisnetwerk voor cyberbeveiliging op te richten, 3) de optie om alleen een gecentraliseerde structuur te creëren en 4) de optie om een bestaand agentschap te gebruiken (het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), het Uitvoerend Agentschap onderzoek (REA) of het Uitvoerend Agentschap innovatie en netwerken (INEA)).

[17] EDEO, maart 2018.

De conclusie van de analyse luidde dat optie 1 het best geschikt is om de doelstellingen van het initiatief te verwezenlijken, om optimale economische, maatschappelijke en milieueffecten te bereiken en de belangen van de Unie het best te waarborgen. De voornaamste argumenten vóór deze optie waren de mogelijkheid om een echt industriebeleid op het gebied van cyberbeveiliging uit te werken door ondersteuning te bieden aan activiteiten die niet alleen verband houden met onderzoek en ontwikkeling, maar ook met marktintroductie, de flexibiliteit van het netwerk van kenniscentra om met verschillende samenwerkingsmodellen het gebruik van bestaande kennis en middelen te optimaliseren en de mogelijkheid om structuur aan te brengen in de samenwerkingsverbanden en gezamenlijke toezeggingen van publieke en private belanghebbenden uit alle relevante sectoren, met inbegrip van defensie. Tot slot maakt optie 1 het mogelijk om ook meer synergieën te creëren en biedt deze optie een uitvoeringsmechanisme voor twee verschillende EU-financieringsstromen op het gebied van cyberbeveiliging in het kader van het volgende meerjarig financieel kader (de programma's "Digitaal Europa" en "Horizon Europa").

- **Grondrechten**

Dankzij dit initiatief kunnen overheden en industrieën in de lidstaten cyberdreigingen voortaan beter voorkomen en er beter op reageren, door beter beveiligde producten en oplossingen te bieden en aan te schaffen. Dit is met name van belang voor de beveiliging van de toegang tot essentiële diensten (zoals vervoers-, gezondheids-, bancaire en financiële diensten).

Als de Europese Unie meer capaciteit heeft om zelfstandig haar producten en diensten te beveiligen, zal dit de burgers ook helpen om van hun democratische rechten en waarden te genieten (bv. betere bescherming van de in het Handvest van de grondrechten verankerde rechten op informatie, met name het recht op bescherming van persoonsgegevens en het privéleven) zodat ook het vertrouwen in de digitale maatschappij en economie groter wordt.

4. GEVOLGEN VOOR DE BEGROTING

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal, in samenwerking met het kennisnetwerk voor cyberbeveiliging, het voornaamste uitvoeringsorgaan zijn voor de financiële middelen van de EU die in het kader van Digitaal Europa en Horizon Europa voor cyberbeveiliging worden uitgetrokken.

De budgettaire gevolgen van de uitvoering van Digitaal Europa zijn in detail beschreven in het financieel memorandum bij dit voorstel. De bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21, lid 1, onder b), zal door de Commissie worden voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt. Het voorstel zal worden gebaseerd op de resultaten van het in artikel 6, lid 6, van Verordening XXX [kaderprogramma Horizon Europa] omschreven strategische planningsproces.

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

In dit voorstel (artikel 38) wordt expliciet voorzien in een evaluatieclausule op grond waarvan de Commissie een onafhankelijke evaluatie zal maken. De Commissie zal vervolgens aan het Europees Parlement en de Raad verslag uitbrengen over haar evaluatie en, in voorkomend geval, een voorstel tot herziening doen, teneinde de impact en de toegevoegde waarde van het

instrument te meten. De evaluatiemethodiek van de Commissie inzake betere regelgeving zal worden toegepast.

Zoals bepaald in artikel 17 van dit voorstel, moet de uitvoerend directeur elke twee jaar een ex-postevaluatie van de activiteiten van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk aan de raad van bestuur voorleggen. De uitvoerend directeur moet ook een actieplan als follow-up van ex-postevaluaties en tweejaarlijks een voortgangsrapportage voor de Commissie opstellen. De raad van bestuur moet erop toezien dat gepast gevolg wordt gegeven aan die conclusies, zoals bepaald in artikel 16 van dit voorstel.

Overeenkomstig de bepalingen van artikel 228 van het Verdrag kunnen vermeende gevallen van wanbeheer bij de activiteiten van de juridische entiteit worden onderzocht door de Europese Ombudsman.

2018/0328 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

Een bijdrage van de Europese Commissie aan de bijeenkomst van leiders in Salzburg op 19-20 september 2018

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 173, lid 3, en artikel 188, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Gezien het advies van het Europees Economisch en Sociaal Comité[18],

Gezien het advies van het Comité van de Regio's[19],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

1) Nu we als burgers in ons dagelijkse leven en in onze economieën steeds meer op digitale technologieën steunen, stijgt ook het risico op ernstige cyberincidenten. Om de veiligheid in de toekomst te waarborgen, zal de Unie zich onder meer beter moeten kunnen weren tegen cyberdreigingen op technologisch en industrieel gebied, aangezien zowel civiele infrastructuur als militaire capaciteiten afhankelijk zijn van veilige digitale systemen.

2) Als gevolg van de strategie inzake cyberbeveiliging[20] van 2013, die tot doel heeft een betrouwbaar, veilig en open cyber-ecosysteem tot stand te brengen, heeft de Unie haar activiteiten met betrekking tot de toenemende uitdagingen op het gebied van cyberbeveiliging stelselmatig uitgebreid. In 2016 heeft de Unie de eerste maatregelen op het gebied van cyberbeveiliging vastgesteld in Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[21] voor de beveiliging van netwerk- en informatiesystemen.

---

18 PB C ... van ..., blz. ...

19 PB C , blz. .

20 Gezamenlijke mededeling aan het Europees Parlement en de Raad: Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace (JOIN(2013) 1 final).

21 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

3) De Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid hebben in september 2017 een gezamenlijke mededeling[22] voorgesteld over "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" om de weerbaarheid, het afschrikkingseffect en het reactievermogen van de EU ten opzichte van cyberaanvallen te versterken.

4) De staatshoofden en regeringsleiders hebben op de digitale top van Tallinn in september 2017 opgeroepen om van Europa uiterlijk in 2025 een leider in cyberbeveiliging te maken, zodat de burgers, consumenten en bedrijven vol vertrouwen online kunnen gaan en bescherming genieten, en zodat een vrij en aan het recht onderworpen internet mogelijk wordt.

5) Ernstige verstoringen van netwerk- en informatiesystemen kunnen gevolgen hebben voor individuele lidstaten en voor de Unie als geheel. De beveiliging van netwerk- en informatiesystemen is daarom essentieel voor de goede werking van de interne markt. Voor cyberbeveiliging is de Unie momenteel afhankelijk van niet-Europese aanbieders. Het is echter in het strategische belang van de Unie om essentiële technologische capaciteiten op het gebied van cyberbeveiliging te behouden en te ontwikkelen voor de beveiliging van de digitale eengemaakte markt, en met name de bescherming van kritieke netwerken en informatiesystemen, alsook voor de verlening van essentiële diensten op het gebied van cyberbeveiliging.

6) In de Unie is er een schat aan deskundigheid en ervaring als het gaat om onderzoek, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging, maar de inspanningen van de industrie- en onderzoeksgemeenschappen zijn versnipperd, zijn onvoldoende op elkaar afgestemd en hebben geen gezamenlijke missie, hetgeen het concurrentievermogen op dit gebied belemmert. Deze inspanningen en deskundigheid moeten op een efficiënte manier worden gebundeld, onderling verbonden en gebruikt om bestaande onderzoeks-, technologische en industriële capaciteiten op Unieniveau en nationaal niveau te versterken en aan te vullen.

7) In de in november 2017 aangenomen conclusies van de Raad werd de Commissie verzocht om een snelle effectbeoordeling van de mogelijke opties om tegelijk met het Europees onderzoeks- en kenniscentrum een netwerk van kenniscentra voor cyberbeveiliging op te richten en medio 2018 het relevante rechtsinstrument voor te stellen.

8) Het kenniscentrum moet het belangrijkste instrument van de Unie zijn om investeringen in onderzoek, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging te bundelen en om samen met het kennisnetwerk voor cyberbeveiliging relevante projecten en initiatieven uit te voeren. Het kenniscentrum moet voor cyberbeveiliging financiële steun uit de programma's Horizon Europa en Digitaal Europa verstrekken en in voorkomend geval ook beschikbaar zijn voor het Europees Fonds voor Regionale Ontwikkeling en andere programma's. Deze aanpak moet bijdragen tot synergieën en coördinatie van financiële steun voor onderzoek, innovatie, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging en moet vermijden dat er dubbel werk wordt verricht.

9) Rekening houdend met het feit dat de doelstellingen van dit initiatief het best kunnen worden bereikt als alle of zoveel mogelijk lidstaten deelnemen, en om de lidstaten aan

[22] Gezamenlijke mededeling aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" (JOIN(2017) 450 final).

te moedigen deel te nemen, moeten alleen lidstaten die financieel bijdragen aan de administratieve en operationele kosten van het kenniscentrum, stemrecht hebben.

10) De financiële bijdrage van de deelnemende lidstaten moet in verhouding staan tot de financiële bijdrage van de Unie aan dit initiatief.

11) Het kenniscentrum moet de werkzaamheden van het kennisnetwerk voor cyberbeveiliging ("het netwerk"), dat bestaat uit nationale coördinatiecentra in elke lidstaat, vergemakkelijken en helpen coördineren. Nationale coördinatiecentra moeten directe financiële steun van de Unie ontvangen, met inbegrip van subsidies die zonder oproep tot het indienen van voorstellen worden toegekend, om activiteiten uit te voeren die verband houden met deze verordening.

12) De nationale coördinatiecentra moeten door de lidstaten worden geselecteerd. Naast de noodzakelijke administratieve capaciteit moeten de centra beschikken over, of directe toegang hebben tot, technologische expertise op het gebied van cyberbeveiliging, met name op gebieden als cryptografie, ICT-beveiligingsdiensten, indringerdetectie, systeembeveiliging, netwerkbeveiliging, beveiliging van software en toepassingen, of de menselijke en maatschappelijke aspecten van beveiliging en privacy. Zij moeten ook over de capaciteit beschikken om effectief in dialoog te gaan en samen te werken met de industrie, de onderzoeksgemeenschap en de overheidssector, met inbegrip van overeenkomstig Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[23] aangewezen autoriteiten.

13) Wanneer financiële steun wordt verleend aan nationale coördinatiecentra om derden op nationaal niveau te ondersteunen, gebeurt dit via overeenkomsten voor de doorgifte van subsidies aan de betrokken belanghebbenden.

14) Opkomende technologieën, zoals kunstmatige intelligentie (KI), het internet der dingen, high-performance computing (HPC) en kwantumcomputers, blockchain en concepten zoals veilige digitale identiteiten, bieden oplossingen en brengen tegelijk nieuwe cyberbeveiligingsuitdagingen met zich mee. Om de robuustheid van bestaande of toekomstige ICT-systemen te beoordelen en te valideren, zullen beveiligingsoplossingen voor aanvallen op HPC- en kwantumcomputers moeten worden getest. Het kenniscentrum, het netwerk en de kennisgemeenschap voor cyberbeveiliging moeten bijdragen aan de bevordering en verspreiding van de nieuwste cyberbeveiligingsoplossingen. Tegelijkertijd moeten het kenniscentrum en het netwerk ten dienste staan van ontwikkelaars en exploitanten in kritieke sectoren zoals vervoer, energie, gezondheidszorg, financiën, telecommunicatie, maakindustrie, defensie en ruimtevaart, en hen helpen hun uitdagingen op het gebied van cyberbeveiliging op te lossen.

15) Het kenniscentrum moet verschillende sleutelfuncties hebben. Ten eerste moet het kenniscentrum de werkzaamheden van het Europees kennisnetwerk voor cyberbeveiliging bevorderen en helpen coördineren, alsook de kennisgemeenschap voor cyberbeveiliging vooruithelpen. Het kenniscentrum moet een drijvende kracht zijn achter de agenda voor cyberbeveiligingstechnologie en de toegang tot de bij het netwerk en de kennisgemeenschap voor cyberbeveiliging verzamelde knowhow vergemakkelijken. Ten tweede moet het uitvoering geven aan de desbetreffende

[23] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

onderdelen van de programma's Digitaal Europa en Horizon Europa door subsidies toe te kennen, doorgaans na een oproep tot het indienen van voorstellen. Ten derde moet het kenniscentrum gezamenlijke investeringen door de Unie, de lidstaten en/of de industrie vergemakkelijken.

16) Het kenniscentrum moet een stimulans geven en ondersteuning bieden voor samenwerking en coördinatie van de activiteiten van de kennisgemeenschap voor cyberbeveiliging, die bestaat uit een grote, open en diverse groep actoren die zich met cyberbeveiligingstechnologie bezighouden. Die kennisgemeenschap moet met name onderzoeksorganen, industrieën aan de aanbod- en vraagzijde, en de publieke sector omvatten. De kennisgemeenschap voor cyberbeveiliging moet input leveren voor de activiteiten en het werkplan van het kenniscentrum en moet ook profiteren van de gemeenschapsvormende activiteiten van het kenniscentrum en het netwerk, maar mag verder geen voorkeursbehandeling krijgen bij oproepen tot het indienen van voorstellen en aanbestedingen.

17) Om tegemoet te komen aan de behoeften van de industrieën aan zowel de vraag- als de aanbodzijde, moet het kenniscentrum zich bij de uitvoering van zijn taak om industrieën kennis en technische bijstand op het gebied van cyberbeveiliging te verlenen, zowel richten op ICT-producten en -diensten als op alle andere industriële en technologische producten en oplossingen waarin cyberbeveiligingstechnologie wordt ingebouwd.

18) Terwijl het kenniscentrum en het netwerk moeten streven naar synergieën op het vlak van cyberbeveiliging tussen de civiele en de defensie-industrie, worden de in het kader van het programma Horizon Europa gefinancierde projecten uitgevoerd overeenkomstig Verordening XXX [Verordening Horizon Europa], waarin is bepaald dat onderzoeks- en innovatieactiviteiten in het kader van Horizon Europa op civiele toepassingen zijn gericht.

19) Om te zorgen voor gestructureerde en duurzame samenwerking moeten de relaties tussen het kenniscentrum en de nationale coördinatiecentra op een contractuele overeenkomst worden gebaseerd.

20) Er moet worden voorzien in passende regelingen inzake de aansprakelijkheid en de transparantie van het kenniscentrum.

21) Zowel het Gemeenschappelijk Centrum voor Onderzoek van de Commissie als het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) moeten, gezien hun respectieve expertise op het gebied van cyberbeveiliging, een actieve rol spelen in de kennisgemeenschap voor cyberbeveiliging en in het industrieel en wetenschappelijk adviescomité.

22) Wanneer zij een financiële bijdrage uit de algemene begroting van de Unie ontvangen, moeten de nationale coördinatiecentra en de entiteiten die deel uitmaken van de kennisgemeenschap voor cyberbeveiliging, bekendmaken dat de respectieve activiteiten in het kader van dit initiatief worden ondernomen.

23) De bijdrage van de Unie aan het kenniscentrum moet de helft van de kosten van de activiteiten met betrekking tot de oprichting, administratie en coördinatie ervan financieren. Om dubbele financiering te vermijden, mogen deze activiteiten niet tegelijkertijd genieten van een bijdrage uit andere programma's van de Unie.

24) De raad van bestuur van het kenniscentrum, die is samengesteld uit vertegenwoordigers van de lidstaten en van de Commissie, moet de algemene richting van de werkzaamheden van het kenniscentrum vaststellen en garanderen dat het zijn

taken overeenkomstig deze verordening uitvoert. De raad van bestuur dient de noodzakelijke bevoegdheden toegewezen te krijgen voor de vaststelling van de begroting, de controle op de uitvoering ervan, de vaststelling van passende financiële regels, de opstelling van transparante werkprocedures voor besluitvorming door het kenniscentrum, de goedkeuring van het werkplan en het strategisch meerjarenplan van het kenniscentrum waarin de prioriteiten voor de verwezenlijking van de doelen en taken van het kenniscentrum hun weerslag vinden, de vaststelling van het reglement van orde, de benoeming van de uitvoerend directeur en de besluitvorming over de verlenging van de ambtstermijn van de uitvoerend directeur en de beëindiging ervan.

25) Omwille van de goede en doeltreffende werking van het kenniscentrum moeten de Commissie en de lidstaten erop toezien dat personen die worden benoemd tot lid van de raad van bestuur over passende professionele deskundigheid en ervaring op functionele gebieden beschikken. De Commissie en de lidstaten dienen zich tevens in te spannen om het verloop onder hun respectievelijke vertegenwoordigers in de raad van bestuur te beperken om de continuïteit van zijn werk zeker te stellen.

26) Voor een goede werking van het kenniscentrum is het noodzakelijk dat de uitvoerend directeur wordt benoemd op grond van zowel verdiensten en aantoonbare administratieve en bestuurskundige vaardigheden, als van bekwaamheid en ervaring die relevant is voor cyberbeveiliging; daarnaast dient hij of zij de taken op volledig onafhankelijke wijze uit te voeren.

27) Het kenniscentrum moet beschikken over een industrieel en wetenschappelijk adviescomité als adviserend orgaan teneinde regelmatig overleg met de private sector, consumentenorganisaties en andere relevante belanghebbenden te waarborgen. Het industrieel en wetenschappelijk adviescomité moet zich richten op kwesties die relevant zijn voor de belanghebbenden en deze onder de aandacht van de raad van bestuur van het kenniscentrum brengen. Dankzij de samenstelling van het industrieel en wetenschappelijk adviescomité en de daaraan toegewezen taken, zoals advies geven over het werkplan, moeten de belanghebbenden voldoende vertegenwoordigd zijn bij de werkzaamheden van het kenniscentrum.

28) Het kenniscentrum moet, via het industrieel en wetenschappelijk adviescomité, profiteren van de specifieke deskundigheid en de brede en relevante vertegenwoordiging van belanghebbenden die gedurende de looptijd van Horizon 2020 is opgebouwd door middel van het contractuele publiek-private partnerschap voor cyberbeveiliging.

29) In het kenniscentrum moeten er regels gelden ter voorkoming en beheersing van belangenconflicten. Het kenniscentrum moet verder de relevante bepalingen van de Unie inzake publieke toegang tot documenten toepassen, zoals uiteengezet in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad[24]. Op de verwerking van persoonsgegevens door het kenniscentrum is Verordening (EU) nr. XXX/2018 van het Europees Parlement en de Raad van toepassing. Het kenniscentrum dient in het bijzonder de bepalingen na te leven die van toepassing zijn op de EU-instellingen alsmede de nationale wetgeving inzake de behandeling van informatie, in het bijzonder gevoelige niet-gerubriceerde informatie en gerubriceerde EU-informatie.

---

[24] Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

30) De financiële belangen van de Unie en de lidstaten moeten gedurende de gehele uitgavencyclus worden beschermd door middel van evenredige maatregelen, waaronder preventie, opsporing en onderzoek van onregelmatigheden, de terugvordering van verloren gegane, ten onrechte betaalde of oneigenlijk gebruikte bedragen en, indien nodig, administratieve en financiële sancties overeenkomstig Verordening (EU, Euratom) XXX van het Europees Parlement en de Raad[25] ("Financieel Reglement").

31) Het kenniscentrum dient op een open en transparante manier te functioneren door alle relevante informatie tijdig ter beschikking te stellen en zijn activiteiten, waaronder informatie- en verspreidingsactiviteiten, bij het bredere publiek te bevorderen. Het reglement van orde van de organen van het kenniscentrum moet openbaar worden gemaakt.

32) De intern controleur van de Commissie moet ten aanzien van het kenniscentrum dezelfde bevoegdheden uitoefenen als die welke hij met betrekking tot de Commissie uitoefent.

33) De Commissie, het kenniscentrum, de Rekenkamer en het Europees Bureau voor fraudebestrijding moeten toegang krijgen tot alle nodige informatie en alle locaties om audits en onderzoeken uit te voeren met betrekking tot de subsidies, contracten en overeenkomsten die door het kenniscentrum zijn ondertekend.

34) Aangezien de doelstellingen van deze verordening, namelijk het behouden en verder ontwikkelen van de technologische en industriële capaciteiten van de Unie op het gebied van cyberbeveiliging, het vergroten van het concurrentievermogen van de cyberbeveiligingsbranche van de Unie en het omzetten van cyberbeveiliging in een concurrentievoordeel voor andere bedrijfstakken in de Unie, niet in voldoende mate door de lidstaten kunnen worden verwezenlijkt omdat de bestaande, beperkte middelen versnipperd zijn en omdat de benodigde investeringen aanzienlijk zijn, maar beter op het niveau van de Unie kunnen worden verwezenlijkt omdat zo dubbel werk wordt vermeden, er een kritische massa van investeringen kan worden bereikt en de overheidsfinanciering optimaal wordt benut, kan de Unie maatregelen treffen overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstelling te verwezenlijken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN EN BEGINSELEN VAN HET KENNISCENTRUM EN HET NETWERK

Artikel 1

Voorwerp

1. Bij deze verordening worden het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (het "kenniscentrum") en het

[25] [voeg titel en PB-referentie toe]

netwerk van nationale coördinatiecentra opgericht en worden regels vastgesteld voor de aanwijzing van nationale coördinatiecentra en voor de oprichting van de kennisgemeenschap voor cyberbeveiliging.

2. Het kenniscentrum draagt bij aan de uitvoering van het onderdeel cyberbeveiliging van het bij Verordening XXX vastgestelde programma Digitaal Europa, en met name aan acties met betrekking tot artikel 6 van Verordening (EU) XXX [programma Digitaal Europa], alsook van het bij Verordening XXX vastgestelde programma Horizon Europa, en met name punt 2.2.6 van pijler II van bijlage I bij Besluit nr. XXX tot vaststelling van het specifieke programma tot uitvoering van Horizon Europa – het kaderprogramma voor onderzoek en innovatie [referentienummer van het specifieke programma].

3. De zetel van het kenniscentrum bevindt zich in [Brussel, België].

4. Het kenniscentrum heeft rechtspersoonlijkheid. In elke lidstaat bezit het de ruimste handelingsbevoegdheid die door de wetgeving van de betrokken lidstaat aan rechtspersonen wordt verleend. Het kan met name roerende en onroerende goederen verkrijgen of vervreemden en in rechte optreden.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "cyberbeveiliging": de bescherming van netwerk- en informatiesystemen, de gebruikers ervan en andere personen tegen cyberdreigingen;

(2) "cyberbeveiligingsproducten en -oplossingen": ICT-producten, -diensten of -processen met het specifieke doel om netwerk- en informatiesystemen, de gebruikers ervan en getroffen personen tegen cyberdreigingen te beschermen;

(3) "overheidsinstantie": elke regering of andere overheidsdienst, met inbegrip van publieke adviesorganen, op nationaal, regionaal of lokaal niveau, of elke natuurlijke persoon of rechtspersoon die overeenkomstig het nationale recht publieke bestuursfuncties vervult, met inbegrip van specifieke taken;

(4) "deelnemende lidstaat": een lidstaat die vrijwillig financieel bijdraagt aan de administratieve en operationele kosten van het kenniscentrum.

Artikel 3

Opdracht van het kenniscentrum en het netwerk

1. Het kenniscentrum en het netwerk helpen de Unie om:

   (a) de technologische en industriële capaciteiten op het gebied van cyberbeveiliging die nodig zijn voor de beveiliging van de digitale eengemaakte markt, te behouden en te ontwikkelen;

   (b) het concurrentievermogen van de cyberbeveiligingsbranche in de Unie te vergroten en van cyberbeveiliging een concurrentievoordeel te maken voor andere industrieën in de Unie.

2. In voorkomend geval voert het kenniscentrum zijn taken uit in samenwerking met het netwerk van nationale coördinatiecentra en met een kennisgemeenschap voor cyberbeveiliging.

Artikel 4

Doelstellingen en taken van het kenniscentrum

Het kenniscentrum heeft de volgende doelstellingen en bijbehorende taken:

1. de werkzaamheden van het in artikel 6 bedoelde netwerk van nationale coördinatiecentra ("het netwerk") en de in artikel 8 bedoelde kennisgemeenschap voor cyberbeveiliging vergemakkelijken en helpen coördineren;

2. bijdragen aan de uitvoering van het onderdeel cyberbeveiliging van het bij Verordening XXX[26] vastgestelde programma Digitaal Europa, en met name aan acties met betrekking tot artikel 6 van Verordening (EU) XXX [programma Digitaal Europa], alsook van het bij Verordening XXX[27] vastgestelde programma Horizon Europa, en met name punt 2.2.6 van pijler II van bijlage I bij Besluit nr. XXX tot vaststelling van het specifieke programma tot uitvoering van Horizon Europa – het kaderprogramma voor onderzoek en innovatie [referentienummer van het specifieke programma], en van andere programma's van de Unie indien hierin wordt voorzien in rechtshandelingen van de Unie;

3. de capaciteit, de kennis en de infrastructuur op het gebied van cyberbeveiliging verbeteren ten behoeve van de industrie, de publieke sector en de onderzoeksgemeenschappen, door de volgende taken uit te voeren:

    (a) wat de geavanceerde industriële en onderzoeksinfrastructuren en aanverwante diensten op het gebied van cyberbeveiliging betreft, dergelijke infrastructuren en aanverwante diensten aankopen, upgraden, exploiteren en beschikbaar stellen aan een grote groep gebruikers uit de publieke sector, de onderzoeks- en wetenschapsgemeenschap en de industrie, waaronder het MKB, in de hele Unie;

    (b) wat de geavanceerde industriële en onderzoeksinfrastructuren en aanverwante diensten op het gebied van cyberbeveiliging betreft, ondersteuning bieden, ook financieel, aan andere entiteiten om dergelijke infrastructuren en aanverwante diensten aan te kopen, te upgraden, te exploiteren en beschikbaar te stellen aan een grote groep gebruikers uit de publieke sector, de onderzoeks- en wetenschapsgemeenschap en de industrie, waaronder het MKB, in de hele Unie;

    (c) kennis over cyberbeveiliging verstrekken en technische bijstand leveren aan de industrie en overheidsinstanties, met name door steun te verlenen aan maatregelen voor een gemakkelijkere toegang tot de in het netwerk en de kennisgemeenschap voor cyberbeveiliging beschikbare expertise;

4. bijdragen tot de ruime aanwending van geavanceerde cyberbeveiligingsproducten en -oplossingen in de hele economie, door:

    (a) onderzoek op het gebied van cyberbeveiliging, ontwikkeling en aanwending van cyberbeveiligingsproducten en -oplossingen in de Unie door overheidsinstanties en verwerkende industrieën te stimuleren;

---

26 [voeg volledige titel en PB-referentie toe]

27 [voeg volledige titel en PB-referentie toe]

(b) overheidsinstanties, industrieën aan de vraagzijde en andere gebruikers te helpen om de meest recente cyberbeveiligingsoplossingen te gebruiken en te integreren;

(c) ondersteuning te bieden aan met name overheidsinstanties bij het plaatsen van overheidsopdrachten, of namens overheidsinstanties opdrachten voor geavanceerde cyberbeveiligingsproducten en -oplossingen te plaatsen;

(d) startende, kleine en middelgrote ondernemingen in de cyberbeveiligingsbranche financieel en technisch bij te staan zodat zij aansluiting vinden bij potentiële markten en investeringen aantrekken;

5. zorgen voor een beter begrip van cyberbeveiliging en helpen om het gebrek aan cyberbeveiligingsvaardigheden in de Unie aan te pakken door:

(a) de verdere ontwikkeling van cyberbeveiligingsvaardigheden te ondersteunen, in voorkomend geval samen met de relevante EU-agentschappen en -organen, waaronder het Enisa;

6. bijdragen aan de versterking van het onderzoek en de ontwikkeling op het gebied van cyberbeveiliging in de Unie door:

(a) financiële steun te verlenen voor onderzoek op het gebied van cyberbeveiliging, op basis van een gemeenschappelijke, voortdurend geëvalueerde en verbeterde meerjarige strategische, industriële, agenda voor technologie en onderzoek;

(b) in samenwerking met de industrie en het netwerk steun te verlenen aan grootschalige onderzoeks- en demonstratieprojecten voor technologische vermogens op het gebied van cyberbeveiliging van de volgende generatie;

(c) steun te verlenen aan onderzoek en innovatie op het gebied van de standaardisatie van cyberbeveiligingstechnologie;

7. de samenwerking tussen de civiele en de defensieindustrie verbeteren als het gaat om cyberbeveiligingstechnologieën en -toepassingen voor tweeërlei gebruik, door:

(a) de lidstaten en belanghebbenden uit het bedrijfsleven en de onderzoekswereld te ondersteunen op het vlak van onderzoek, ontwikkeling en aanwending;

(b) bij te dragen aan de samenwerking tussen de lidstaten door middel van steun voor onderwijs, opleiding en oefeningen;

(c) belanghebbenden samen te brengen om synergieën te bevorderen tussen civiel en militair cyberbeveiligingsonderzoek en de civiele en de militaire cyberbeveiligingsmarkt;

8. de synergieën tussen de civiele en de defensiedimensie van cyberbeveiliging versterken in verband met het Europees Defensiefonds, door:

(a) advies te verstrekken, expertise te delen en samenwerking te bevorderen tussen relevante belanghebbenden;

(b) op verzoek van de lidstaten multinationale cyberdefensieprojecten te beheren en op die manier op te treden als projectmanager in de zin van

Verordening XXX [Verordening tot oprichting van het Europees Defensiefonds].

Artikel 5

Investeringen in en gebruik van infrastructuur, capaciteit, producten of oplossingen

1. Terwijl het kenniscentrum financiering voor infrastructuur, capaciteit, producten of oplossingen overeenkomstig artikel 4, punten 3 en 4, verstrekt in de vorm van een subsidie of een prijs, kan in het werkplan van het kenniscentrum met name het volgende worden gespecificeerd:

   (a) regels voor de exploitatie van infrastructuur of capaciteit, waarbij eventueel de exploitatie aan een onderbrengende entiteit kan worden toevertrouwd op basis van door het kenniscentrum te bepalen criteria;

   (b) regels voor de toegang tot en het gebruik van infrastructuur of capaciteit.

2. Het kenniscentrum kan verantwoordelijk zijn voor de algemene uitvoering van relevante gezamenlijke aanbestedingsacties, waaronder precommerciële aanbestedingen, namens leden van het netwerk, leden van de kennisgemeenschap voor cyberbeveiliging, of andere derde partijen die gebruikers van cyberbeveiligingsproducten en -oplossingen vertegenwoordigen. Daartoe kan het kenniscentrum worden bijgestaan door een of meer nationale coördinatiecentra of leden van de kennisgemeenschap voor cyberbeveiliging.

Artikel 6

Aanwijzing van nationale coördinatiecentra

1. Uiterlijk op [datum] wijst elke lidstaat de entiteit aan die optreedt als nationaal coördinatiecentrum voor de toepassing van deze verordening en stelt de lidstaat de Commissie hiervan in kennis.

2. Op basis van een beoordeling van de vraag of die entiteit aan de in lid 4 vastgelegde criteria voldoet, besluit de Commissie binnen zes maanden na de aanwijzing door de lidstaat of de entiteit geaccrediteerd wordt als nationaal coördinatiecentrum, dan wel of de aanwijzing wordt afgewezen. De Commissie maakt de lijst van nationale coördinatiecentra bekend.

3. De lidstaten kunnen te allen tijde een nieuwe entiteit als nationaal coördinatiecentrum aanwijzen voor de toepassing van deze verordening. De leden 1 en 2 zijn van toepassing op de aanwijzing van elke nieuwe entiteit.

4. Het aangewezen nationale coördinatiecentrum beschikt over het vermogen om het kenniscentrum en het netwerk te ondersteunen bij de uitvoering van hun taken als bedoeld in artikel 3 van deze verordening. Het beschikt over of heeft rechtstreekse toegang tot technologische expertise op het gebied van cyberbeveiliging en kan effectief in dialoog gaan en samenwerken met de industrie, de overheidssector en de onderzoeksgemeenschap.

5. De betrekkingen tussen het kenniscentrum en de nationale coördinatiecentra worden onderhouden op basis van een contractuele overeenkomst tussen het kenniscentrum en elk van de nationale coördinatiecentra. De overeenkomst omvat de regels voor de betrekkingen en de verdeling van taken tussen het kenniscentrum en elk nationaal coördinatiecentrum.

6. Het netwerk van nationale coördinatiecentra bestaat uit alle door de lidstaten aangewezen nationale coördinatiecentra.

Artikel 7

Taken van de nationale coördinatiecentra

1. De nationale coördinatiecentra vervullen de volgende taken:

   (a) ze ondersteunen het kenniscentrum bij de verwezenlijking van zijn doelstellingen en in het bijzonder bij de coördinatie van de kennisgemeenschap voor cyberbeveiliging;

   (b) ze bevorderen op lidstaatniveau de deelname van de industrie en andere actoren aan grensoverschrijdende projecten;

   (c) samen met het kenniscentrum dragen ze bij aan de identificatie en de aanpak van sectorspecifieke industriële uitdagingen op het gebied van cyberbeveiliging;

   (d) ze treden op nationaal niveau op als contactpunt voor de kennisgemeenschap voor cyberbeveiliging en voor het kenniscentrum;

   (e) ze streven naar synergieën met relevante activiteiten op nationaal en regionaal niveau;

   (f) ze voeren specifieke acties uit waaraan het kenniscentrum subsidies heeft toegekend, bijvoorbeeld door middel van financiële steun aan derden overeenkomstig artikel 204 van Verordening XXX [nieuw Financieel Reglement] onder de in de betrokken subsidieovereenkomsten gespecificeerde voorwaarden;

   (g) ze bevorderen en verspreiden de relevante resultaten van de werkzaamheden van het netwerk, de kennisgemeenschap voor cyberbeveiliging en het kenniscentrum op nationaal of regionaal niveau;

   (h) ze beoordelen verzoeken van een in dezelfde lidstaat als het coördinatiecentrum opgerichte entiteit om deel te gaan uitmaken van de kennisgemeenschap voor cyberbeveiliging.

2. Voor de toepassing van punt f) kan de financiële steun aan derden in een van de in artikel 125 van Verordening XXX [nieuw Financieel Reglement] genoemde vormen worden verleend, ook in de vorm van vaste bedragen.

3. Nationale coördinatiecentra kunnen overeenkomstig artikel 195, onder d), van Verordening XXX [nieuw Financieel Reglement] van de Unie een subsidie ontvangen voor de uitvoering van de in dit artikel omschreven taken.

4. De nationale coördinatiecentra werken waar nodig via het netwerk samen om de in lid 1, onder a), b), c), e) en g) bedoelde taken uit te voeren.

Artikel 8

De kennisgemeenschap voor cyberbeveiliging

1. De kennisgemeenschap voor cyberbeveiliging draagt bij aan de in artikel 3 vastgelegde opdracht van het kenniscentrum en versterkt en verspreidt expertise over cyberbeveiliging in de hele Unie.

2. De kennisgemeenschap voor cyberbeveiliging bestaat uit industriële en academische organisaties, onderzoeksorganisaties zonder winstoogmerk, en uit verenigingen, publieke en andere entiteiten die zich bezighouden met operationele en technische aangelegenheden. De kennisgemeenschap brengt de voornaamste partijen bijeen die belang hebben bij de technologische en industriële capaciteit op het gebied van cyberbeveiliging in de Unie. Nationale coördinatiecentra en instellingen en organen van de Unie met relevante deskundigheid worden erbij betrokken.

3. Alleen entiteiten die in de Unie gevestigd zijn, kunnen als lid van de kennisgemeenschap voor cyberbeveiliging worden geaccrediteerd. Zij tonen aan dat zij over deskundigheid op het gebied van cyberbeveiliging beschikken met betrekking tot ten minste één van de volgende domeinen:

   (a) onderzoek;

   (b) industriële ontwikkeling;

   (c) opleiding en onderwijs.

4. Het kenniscentrum accrediteert entiteiten die naar nationaal recht zijn opgericht als lid van de kennisgemeenschap voor cyberbeveiliging, nadat het nationaal coördinatiecentrum van de lidstaat waar de entiteit is gevestigd, heeft geoordeeld over de vraag of die entiteit voldoet aan de criteria van lid 3. Een accreditatie is niet in de tijd beperkt, maar kan te allen tijde door het kenniscentrum worden ingetrokken als het relevante nationale coördinatiecentrum of het kenniscentrum zelf van oordeel is dat de entiteit niet aan de criteria van lid 3 voldoet of onder de relevante bepalingen van artikel 136 van Verordening XXX [nieuw financieel reglement] valt.

5. Het kenniscentrum accrediteert de relevante organen, agentschappen en bureaus van de Unie als leden van de kennisgemeenschap voor cyberbeveiliging, nadat het heeft beoordeeld of die entiteit aan de criteria van lid 3 voldoet. Een accreditatie is niet in de tijd beperkt, maar kan te allen tijde door het kenniscentrum worden ingetrokken als het van oordeel is dat de entiteit niet aan de criteria van lid 3 voldoet of onder de relevante bepalingen van artikel 136 van Verordening XXX [nieuw financieel reglement] valt.

6. De vertegenwoordigers van de Commissie kunnen aan de werkzaamheden van de kennisgemeenschap deelnemen.

Artikel 9

Taken van de leden van de kennisgemeenschap voor cyberbeveiliging

De leden van de kennisgemeenschap voor cyberbeveiliging:

(1) ondersteunen het kenniscentrum bij de verwezenlijking van de in de artikelen 3 en 4 genoemde opdracht en doelstellingen, en werken hiertoe nauw samen met het kenniscentrum en de betrokken nationale coördinatiecentra;

(2) nemen deel aan activiteiten die door het kenniscentrum en de nationale coördinatiecentra worden gepromoot;

(3) nemen in voorkomend geval deel aan werkgroepen die door de raad van bestuur van het kenniscentrum zijn opgericht voor de uitvoering van specifieke activiteiten zoals voorzien in het werkplan van het kenniscentrum;

(4) bieden waar relevant ondersteuning aan het kenniscentrum en de nationale coördinatiecentra bij de promotie van specifieke projecten;

(5) bevorderen en verspreiden de relevante resultaten van de binnen de gemeenschap uitgevoerde activiteiten en projecten.

Artikel 10

Samenwerking van het kenniscentrum met instellingen, organen, bureaus en agentschappen van de Unie

1. Het kenniscentrum werkt samen met relevante instellingen, organen, bureaus en agentschappen van de Unie, waaronder het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging, het computercrisisresponsteam (CERT-EU), de Europese Dienst voor extern optreden, het Gemeenschappelijk Centrum voor onderzoek van de Commissie, het Uitvoerend Agentschap onderzoek, het Uitvoerend Agentschap innovatie en netwerken, het Europees Centrum voor de bestrijding van cybercriminaliteit bij Europol en het Europees Defensieagentschap.
2. Dergelijke samenwerking vindt plaats op basis van werkafspraken. Deze afspraken worden vooraf ter goedkeuring aan de Commissie voorgelegd.

HOOFDSTUK II

ORGANISATIE VAN HET KENNISCENTRUM

Artikel 11

Lidmaatschap en structuur

1. De leden van het kenniscentrum zijn de Unie, vertegenwoordigd door de Commissie, en de lidstaten.
2. De structuur van het kenniscentrum omvat:
   (a) een raad van bestuur, die de in artikel 13 vastgestelde taken uitoefent;
   (b) een uitvoerend directeur, die de in artikel 16 vastgestelde taken uitoefent;
   (c) een industrieel en wetenschappelijk adviescomité, dat de in artikel 20 vastgestelde taken uitvoert.

AFDELING I

RAAD VAN BESTUUR

Artikel 12

Samenstelling van de raad van bestuur

1. De raad van bestuur bestaat uit één vertegenwoordiger van elke lidstaat en vijf vertegenwoordigers van de Commissie namens de Unie.
2. Elk lid van de raad van bestuur heeft een plaatsvervanger om het lid te vertegenwoordigen in geval van afwezigheid.
3. De leden van de raad van bestuur en hun plaatsvervangers worden benoemd op grond van hun kennis op het gebied van technologie en op grond van hun relevante bestuurlijke, administratieve en budgettaire vaardigheden. De Commissie en de lidstaten spannen zich ter wille van de continuïteit van het werk van de raad van bestuur in om het verloop onder hun vertegenwoordigers in de raad van bestuur te

beperken. De Commissie en de lidstaten streven naar een evenwichtige deelname van mannen en vrouwen in de raad van bestuur.

4. De ambtstermijn van de leden van de raad van bestuur en hun plaatsvervangers bedraagt vier jaar. Die termijn kan worden verlengd.

5. De leden van de raad van bestuur handelen onafhankelijk en op transparante wijze in het belang van het kenniscentrum en staan in voor de doelstellingen, opdracht, identiteit, autonomie en samenhang ervan.

6. De Commissie kan indien nodig waarnemers uitnodigen, waaronder vertegenwoordigers van relevante organen, bureaus en agentschappen van de Unie, om deel te nemen aan de vergaderingen van de raad van bestuur.

7. Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) is een permanente waarnemer in de raad van bestuur.

Artikel 13

Taken van de raad van bestuur

1. De raad van bestuur draagt de volledige verantwoordelijkheid voor de strategische koers en de werkzaamheden van het kenniscentrum en houdt toezicht op de uitvoering van zijn activiteiten.

2. De raad van bestuur stelt zijn reglement van orde vast. Dat reglement voorziet in specifieke procedures om belangenconflicten te identificeren en te voorkomen en de vertrouwelijkheid van alle gevoelige informatie te waarborgen.

3. De raad van bestuur neemt de noodzakelijke strategische besluiten en moet met name:

   (a) een strategisch meerjarenplan vaststellen dat een overzicht bevat van de belangrijkste prioriteiten en geplande initiatieven van het kenniscentrum, met inbegrip van een raming van de financieringsbehoeften en -bronnen;

   (b) op basis van een voorstel van de uitvoerend directeur het werkplan, de jaarrekeningen en balans, alsook het jaarlijks activiteitenverslag van het kenniscentrum vaststellen;

   (c) de specifieke financiële regels van het kenniscentrum vaststellen overeenkomstig [artikel 70 van het Financieel Reglement];

   (d) een procedure voor de benoeming van de uitvoerend directeur vaststellen;

   (e) de criteria en procedures vaststellen voor de beoordeling en accreditatie van de entiteiten als leden van de kennisgemeenschap voor cyberbeveiliging;

   (f) de uitvoerend directeur benoemen, ontslaan, zijn of haar ambtstermijn verlengen, hem of haar begeleiden en toezicht houden op zijn of haar prestaties, en de rekenplichtige benoemen;

   (g) de jaarlijkse begroting van het kenniscentrum goedkeuren, met inbegrip van de daarmee overeenstemmende personeelsformatie waarin, uitgedrukt in voltijdsequivalenten, het aantal tijdelijke ambten per functiegroep en per rang, het aantal arbeidscontractanten en het aantal gedetacheerde nationale deskundigen is aangegeven;

   (h) regels inzake belangenconflicten vaststellen;

(i) werkgroepen oprichten met leden van de kennisgemeenschap voor cyberbeveiliging;

(j) leden van het industrieel en wetenschappelijk adviescomité benoemen;

(k) in overeenstemming met Gedelegeerde Verordening (EG, Euratom) nr. 1271/2013 van de Commissie[28] een interne auditfunctie oprichten;

(l) het kenniscentrum in de hele wereld promoten om de aantrekkelijkheid ervan te vergroten en ervoor te zorgen dat het een instelling voor cyberbeveiliging van wereldklasse wordt;

(m) het communicatiebeleid van het kenniscentrum vaststellen op aanbeveling van de uitvoerend directeur;

(n) er toezicht op houden dat passend gevolg wordt gegeven aan de conclusies van evaluaties achteraf;

(o) in voorkomend geval, regels vaststellen ter uitvoering van het Statuut en de Regeling die van toepassing is op de andere personeelsleden van de Unie overeenkomstig artikel 31, lid 3;

(p) in voorkomend geval, regels vaststellen voor de detachering van nationale deskundigen naar het kenniscentrum en voor het inzetten van stagiairs overeenkomstig artikel 32, lid 2;

(q) beveiligingsvoorschriften voor het kenniscentrum vaststellen;

(r) een fraudebestrijdingsstrategie vaststellen die in verhouding staat tot de frauderisico's, rekening houdend met een kosten-batenanalyse van de uit te voeren maatregelen;

(s) de methode voor de berekening van de financiële bijdrage van de lidstaten vaststellen;

(t) de verantwoordelijkheid dragen voor elke taak die niet specifiek aan een bepaald orgaan van het kenniscentrum is toegewezen; de raad van bestuur kan dergelijke taken opdragen aan iedere persoon in het kenniscentrum.

Artikel 14

Voorzitter en vergaderingen van de raad van bestuur

1. De raad van bestuur kiest onder zijn stemgerechtigde leden een voorzitter en een vicevoorzitter voor een periode van twee jaar. De raad van bestuur kan ertoe besluiten het mandaat van de voorzitter en de vicevoorzitter eenmaal te verlengen. Indien hun lidmaatschap van de raad van bestuur echter tijdens hun ambtstermijn afloopt, loopt hun ambtstermijn automatisch op diezelfde datum af. De vicevoorzitter vervangt ambtshalve de voorzitter wanneer deze is verhinderd zijn of haar taken te verrichten. De voorzitter neemt aan de stemming deel.

2. De raad van bestuur belegt ten minste driemaal per jaar een gewone vergadering. De raad van bestuur kan buitengewone vergaderingen beleggen op verzoek van de Commissie, op verzoek van een derde van al zijn leden, op verzoek van de voorzitter

[28] Gedelegeerde Verordening (EU) nr. 1271/2013 van de Commissie van 30 september 2013 houdende de financiële kaderregeling van de organen, bedoeld in artikel 208 van Verordening (EU, Euratom) nr. 966/2012 van het Europees Parlement en de Raad (PB L 328 van 7.12.2013, blz. 42).

of op verzoek van de uitvoerend directeur met het oog op de vervulling van zijn of haar taken.

3. De uitvoerend directeur neemt deel aan de beraadslagingen, tenzij de raad van bestuur daar anders over beslist, maar heeft geen stemrecht. De raad van bestuur kan per geval andere personen uitnodigen om de vergaderingen als waarnemers bij te wonen.

4. Op uitnodiging van de voorzitter kunnen leden van het industrieel en wetenschappelijk adviescomité zonder stemrecht deelnemen aan de vergaderingen van de raad van bestuur.

5. De leden van de raad van bestuur en hun plaatsvervangers kunnen zich overeenkomstig de bepalingen van het reglement van orde tijdens de vergaderingen laten bijstaan door adviseurs of deskundigen.

6. Het kenniscentrum vervult de secretariaatstaken voor de raad van bestuur.

Artikel 15

Stemprocedure in de raad van bestuur

1. De Unie heeft een aandeel van 50 % in de stemmen. De stemrechten van de Unie zijn ondeelbaar.

2. Elke deelnemende lidstaat heeft één stem.

3. De raad van bestuur neemt besluiten met een meerderheid van ten minste 75 % van alle stemmen, met inbegrip van de stemmen van de afwezige leden, die ten minste 75 % van de totale financiële bijdragen aan het kenniscentrum vertegenwoordigt. De financiële bijdrage wordt berekend op basis van de door de lidstaten voorgestelde geraamde uitgaven, als bedoeld in artikel 17, lid 2, onder c), en gebaseerd op het in artikel 22, lid 5, bedoelde verslag over de hoogte van de bijdragen van de deelnemende lidstaten.

4. Alleen de vertegenwoordigers van de Commissie en de vertegenwoordigers van de deelnemende lidstaten hebben stemrecht.

5. De voorzitter neemt aan de stemming deel.

AFDELING II

UITVOEREND DIRECTEUR

Artikel 16

Benoeming, ontslag of verlenging van de ambtstermijn van de uitvoerend directeur

1. De uitvoerend directeur beschikt over grote deskundigheid en heeft een goede reputatie op de gebieden waarop het kenniscentrum opereert.

2. De uitvoerend directeur wordt in dienst genomen als een tijdelijke functionaris van het kenniscentrum overeenkomstig artikel 2, onder a), van de Regeling die van toepassing is op de andere personeelsleden.

3. De uitvoerend directeur wordt na een open en transparante selectieprocedure door de raad van bestuur aangesteld uit een lijst van door de Commissie voorgedragen kandidaten.

4. Voor de sluiting van het contract met de uitvoerend directeur wordt het kenniscentrum vertegenwoordigd door de voorzitter van de raad van bestuur.

5. De ambtstermijn van de uitvoerend directeur bedraagt vier jaar. Aan het eind van deze termijn voert de Commissie een beoordeling uit waarin rekening wordt gehouden met de evaluatie van de prestaties van de uitvoerend directeur en de toekomstige taken en uitdagingen van het kenniscentrum.

6. Op voorstel van de Commissie, die rekening houdt met de in lid 5 bedoelde beoordeling, kan de raad van bestuur de ambtstermijn van de uitvoerend directeur eenmaal verlengen met ten hoogste vier jaar.

7. Een uitvoerend directeur wiens ambtstermijn is verlengd, mag niet deelnemen aan een andere selectieprocedure voor dezelfde betrekking.

8. De uitvoerend directeur wordt uitsluitend uit zijn of haar functie ontheven bij besluit van de raad van bestuur op voorstel van de Commissie.

Artikel 17

Taken van de uitvoerend directeur

1. De uitvoerend directeur is verantwoordelijk voor de werkzaamheden en de dagelijkse leiding en is de wettelijke vertegenwoordiger van het kenniscentrum. De uitvoerend directeur legt verantwoording af aan de raad van bestuur en verricht zijn of haar taken in alle onafhankelijkheid binnen de grenzen van de hem of haar verleende bevoegdheden.

2. De uitvoerend directeur voert op onafhankelijke wijze met name de volgende taken uit:

   (a) de besluiten van de raad van bestuur uitvoeren;

   (b) de werkzaamheden van de raad van bestuur ondersteunen, het secretariaat van de vergaderingen verzorgen en alle informatie verstrekken die voor de vervulling van de taken van de raad van bestuur nodig is;

   (c) na overleg met de raad van bestuur en de Commissie, het ontwerp van strategisch meerjarenplan en het ontwerp van jaarlijks werkplan van het kenniscentrum opstellen en ter goedkeuring voorleggen aan de raad van bestuur, en in dat werkplan een omschrijving geven van het toepassingsgebied van de oproepen tot het indienen van voorstellen, de oproepen tot het indienen van blijken van belangstelling en de aanbestedingen die nodig zijn voor de uitvoering van het werkplan en de bijbehorende uitgavenramingen, zoals voorgesteld door de lidstaten en de Commissie;

   (d) de ontwerpjaarbegroting opstellen en ter goedkeuring voorleggen aan de raad van bestuur, met inbegrip van de bijbehorende personeelsformatie, waarin het aantal tijdelijke aanstellingen per functiegroep en per rang en het aantal contractmedewerkers en gedetacheerde nationale deskundigen wordt vermeld, uitgedrukt in voltijdequivalenten;

   (e) het werkplan uitvoeren en hierover verslag uitbrengen aan de raad van bestuur;

   (f) het ontwerp van jaarlijks activiteitenverslag van het kenniscentrum, met daarin de informatie over de overeenkomstige uitgaven, opstellen;

(g) zorgen voor de uitvoering van doeltreffende toezichts- en evaluatieprocedures met betrekking tot de prestaties van het kenniscentrum;

(h) een actieplan opstellen voor de follow-up van de conclusies van de beoordelingen achteraf, en om de twee jaar aan de Commissie verslag uitbrengen over de geboekte vooruitgang;

(i) de overeenkomsten met de nationale coördinatiecentra voorbereiden, erover onderhandelen en deze sluiten;

(j) de verantwoordelijkheid dragen voor administratieve en financiële zaken en personeelsaangelegenheden, met inbegrip van de uitvoering van de begroting van het kenniscentrum, waarbij naar behoren rekening wordt gehouden met het advies van de interne auditfunctie, binnen de grenzen van de delegatie door de raad van bestuur;

(k) de uitschrijving van oproepen tot het indienen van voorstellen goedkeuren en beheren in overeenstemming met het werkplan, en de subsidieovereenkomsten en -besluiten administreren;

(l) de lijst met acties goedkeuren die voor financiering zijn geselecteerd op basis van de door een panel van onafhankelijke deskundigen opgestelde ranglijst;

(m) de uitschrijving van aanbestedingen goedkeuren en beheren in overeenstemming met het werkplan, en de contracten administreren;

(n) de voor financiering geselecteerde offertes goedkeuren;

(o) het ontwerp van jaarrekening en jaarbalans voorleggen aan de interne auditfunctie, en vervolgens aan de raad van bestuur;

(p) ervoor zorgen dat risicoanalyses en risicobeheer worden toegepast;

(q) afzonderlijke subsidieovereenkomsten, besluiten en contracten ondertekenen;

(r) contracten voor opdrachten ondertekenen;

(s) een actieplan opstellen voor de follow-up van de conclusies van interne of externe auditverslagen, alsook van onderzoeken van het Europees Bureau voor fraudebestrijding (OLAF), en verslag uitbrengen over de geboekte vooruitgang, tweemaal per jaar aan de Commissie en op regelmatige tijdstippen aan de raad van bestuur;

(t) een ontwerp van financiële regeling opstellen die van toepassing is op het kenniscentrum;

(u) een doeltreffend en efficiënt internecontrolesysteem instellen, toezien op de werking ervan en elke ingrijpende wijziging aan de raad van bestuur melden;

(v) zorgen voor doeltreffende communicatie met de instellingen van de Unie;

(w) alle andere maatregelen nemen die nodig zijn voor de beoordeling van de voortgang die het kenniscentrum boekt bij de verwezenlijking van zijn opdracht en de in de artikelen 3 en 4 van deze verordening vastgestelde doelstellingen;

(x) alle andere taken uitvoeren die de raad van bestuur aan hem of haar heeft toevertrouwd of gedelegeerd.

AFDELING III

INDUSTRIEEL EN WETENSCHAPPELIJK ADVIESCOMITÉ

Artikel 18

Samenstelling van het industrieel en wetenschappelijk adviescomité

1. Het industrieel en wetenschappelijk adviescomité bestaat uit maximaal 16 leden. De raad van bestuur kiest de leden uit de vertegenwoordigers van de entiteiten van de kennisgemeenschap voor cyberbeveiliging.
2. De leden van het industrieel en wetenschappelijk adviescomité beschikken over deskundigheid met betrekking tot onderzoek op het gebied van cyberbeveiliging, industriële ontwikkeling, professionele diensten of de aanwending daarvan. De vereisten met betrekking tot dergelijke deskundigheid worden nader gespecificeerd door de raad van bestuur.
3. De procedures voor de benoeming van de leden door de raad van bestuur en de werking van het adviescomité worden vastgesteld in het reglement van orde van het kenniscentrum en worden openbaar gemaakt.
4. De ambtstermijn van de leden van het industrieel en wetenschappelijk adviescomité bedraagt drie jaar. Die termijn kan worden verlengd.
5. Vertegenwoordigers van de Commissie en van het Europees Agentschap voor netwerk- en informatiebeveiliging kunnen deelnemen en ondersteuning verlenen aan de werkzaamheden van het industrieel en wetenschappelijk adviescomité.

Artikel 19

Werking van het industrieel en wetenschappelijk adviescomité

1. Het industrieel en wetenschappelijk adviescomité komt ten minste tweemaal per jaar bijeen.
2. Het industrieel en wetenschappelijk adviescomité kan de raad van bestuur adviseren over de oprichting van werkgroepen voor specifieke kwesties die van belang zijn voor de werkzaamheden van het kenniscentrum, waarbij een of meer leden van het industrieel en wetenschappelijk adviescomité eventueel instaan voor de algemene coördinatie.
3. Het industrieel en wetenschappelijk adviescomité kiest zijn voorzitter.
4. Het industrieel en wetenschappelijk adviescomité stelt haar reglement van orde vast, met daarin onder meer de regels voor de benoeming van de vertegenwoordigers die het adviescomité vertegenwoordigen, alsook de duur van hun benoeming.

Artikel 20

Taken van het industrieel en wetenschappelijk adviescomité

Het industrieel en wetenschappelijk adviescomité geeft het kenniscentrum advies met betrekking tot de uitoefening van de activiteiten van het kenniscentrum en heeft ook de volgende taken:

(1) het biedt de uitvoerend directeur en de raad van bestuur strategisch advies en input voor het opstellen van het werkplan en het strategisch meerjarenplan binnen de door de raad van bestuur vastgestelde termijnen;

(2) het organiseert openbare raadplegingen waaraan alle publieke en private belanghebbenden op het gebied van cyberbeveiliging kunnen deelnemen, teneinde de input voor het in lid 1 bedoelde strategische advies te verzamelen;

(3) het bevordert het werkplan en het strategische meerjarenplan van het kenniscentrum en verzamelt er feedback over.

HOOFDSTUK III
FINANCIËLE BEPALINGEN

Artikel 21

Financiële bijdrage van de Unie

1. De bijdrage van de Unie voor de administratieve en operationele kosten van het kenniscentrum omvat:

   (a) 1 981 668 000 EUR uit het programma Digitaal Europa, waaronder tot 23 746 000 EUR voor administratieve kosten;

   (b) een bedrag uit het programma Horizon Europa, onder meer voor administratieve kosten, dat moet worden bepaald met inachtneming van het strategische planningsproces dat moet worden uitgevoerd overeenkomstig artikel 6, lid 6, van Verordening XXX [Verordening Horizon Europa].

2. De maximale bijdrage van de Unie wordt betaald uit de kredieten van de algemene begroting van de Unie die zijn toegewezen aan het [programma Digitaal Europa] en aan het specifieke programma tot uitvoering van Horizon Europa, vastgesteld bij Besluit XXX.

3. Het kenniscentrum voert overeenkomstig artikel 62, onder c), punt iv), van Verordening (EU, Euratom) XXX[29] [het Financieel Reglement] maatregelen uit van [het programma Digitaal Europa] en [het programma Horizon Europa] op het gebied van cyberbeveiliging.

4. De financiële bijdrage van de Unie dekt de in artikel 4, lid 8, onder b), bedoelde taken niet.

Artikel 22

Bijdragen van de deelnemende lidstaten

1. De deelnemende lidstaten leveren een totale bijdrage aan de operationele en administratieve kosten van het kenniscentrum van ten minste dezelfde hoogte als genoemd in artikel 21, lid 1, van deze verordening.

2. Voor de beoordeling van de in lid 1 en artikel 23, lid 3, onder b), punt ii), bedoelde bijdragen worden de kosten vastgesteld overeenkomstig de gebruikelijke kostenberekeningsmethoden van de desbetreffende lidstaten, overeenkomstig de boekhoudkundige normen die van toepassing zijn in de lidstaat en overeenkomstig de van toepassing zijnde internationale boekhoudnormen en internationale normen voor financiële verslaglegging (IFRS). De kosten worden gecertificeerd door een onafhankelijke externe auditor die is aangewezen door de betrokken lidstaat. De

[29] [voeg volledige titel en PB-referentie toe]

waarderingsmethode van de bijdragen kan door het kenniscentrum worden geverifieerd indien er enige onduidelijkheid is ontstaan door de certificering.

3. Wanneer een deelnemende lidstaat zijn verplichtingen in verband met zijn financiële bijdrage niet nakomt, maakt de uitvoerend directeur daarvan schriftelijk melding en stelt hij een redelijke termijn vast waarbinnen de betalingsachterstand moet worden weggewerkt. Indien de betalingsachterstand niet binnen die termijn is weggewerkt, roept de uitvoerend directeur een vergadering van de raad van bestuur bijeen om te besluiten of het stemrecht van de in gebreke blijvende lidstaat moet worden ingetrokken, dan wel of andere maatregelen moeten worden genomen tot deze zijn verbintenissen wel nakomt. Het stemrecht van de in gebreke blijvende lidstaat wordt opgeschort totdat zijn betalingsachterstand is weggewerkt.

4. De Commissie kan de financiële bijdrage van de Unie aan het kenniscentrum beëindigen, evenredig verlagen of schorsen, indien de deelnemende lidstaten de in lid 1 bedoelde bijdragen niet, slechts gedeeltelijk of te laat verstrekken.

5. De deelnemende lidstaten brengen jaarlijks uiterlijk op 31 januari aan de raad van bestuur verslag uit over de hoogte van de bijdragen die zij in elk van de voorgaande begrotingsjaren overeenkomstig lid 1 hebben geleverd.

Artikel 23

Kosten en middelen van het kenniscentrum

1. Het kenniscentrum wordt door de Unie en de lidstaten gezamenlijk gefinancierd door middel van in tranches betaalde financiële bijdragen en bijdragen die bestaan uit kosten die door de nationale coördinatiecentra en begunstigden worden gemaakt bij de uitvoering van acties die niet door het kenniscentrum worden vergoed.

2. De administratieve kosten van het kenniscentrum bedragen niet meer dan [getal] EUR en worden bekostigd uit financiële bijdragen die op jaarbasis gelijkelijk worden verdeeld over de Unie en de deelnemende lidstaten. Indien een deel van de bijdragen voor de administratieve kosten niet wordt gebruikt, kan het ter beschikking worden gesteld om de operationele kosten van het kenniscentrum te dekken.

3. De operationele kosten van het kenniscentrum worden gedekt door:

   (a) de financiële bijdrage van de Unie;

   (b) bijdragen van de deelnemende lidstaten in de vorm van:

      i) financiële bijdragen; en

      ii) in voorkomend geval, bijdragen in natura van de deelnemende lidstaten bestaande uit de kosten die door de nationale coördinatiecentra en de begunstigden worden gemaakt bij de uitvoering van indirecte acties, verminderd met de bijdrage van het kenniscentrum en andere bijdragen van de Unie in die kosten;

4. De in de begroting van het kenniscentrum opgenomen middelen bestaan uit de volgende bijdragen:

   (a) de financiële bijdragen van de deelnemende lidstaten aan de administratieve kosten;

   (b) de financiële bijdragen van de deelnemende lidstaten aan de operationele kosten;

(c) alle inkomsten die door het kenniscentrum worden gegenereerd;

(d) alle andere financiële bijdragen, middelen en inkomsten.

5. Intresten op de bijdragen die door de deelnemende lidstaten aan het kenniscentrum worden betaald, gelden als inkomsten.

6. Alle middelen van het kenniscentrum en zijn activiteiten zijn erop gericht de in artikel 4 genoemde doelstellingen te bereiken.

7. Het kenniscentrum is eigenaar van alle activa die het genereert of die eraan zijn overgedragen voor de verwezenlijking van zijn doelstellingen.

8. Behalve bij ontbinding van het kenniscentrum, worden de inkomsten, voor zover zij meer bedragen dan de uitgaven, niet aan de deelnemende leden van het kenniscentrum uitbetaald.

Artikel 24

Financiële verbintenissen

De financiële verbintenissen van het kenniscentrum mogen het bedrag van de beschikbare of door zijn leden voor zijn begroting vastgelegde financiële middelen niet overschrijden.

Artikel 25

Begrotingsjaar

Het begrotingsjaar begint op 1 januari en eindigt op 31 december.

Artikel 26

Opstelling van de begroting

1. De uitvoerend directeur stelt jaarlijks een ontwerpraming op van de ontvangsten en uitgaven van het kenniscentrum voor het volgende begrotingsjaar en zendt die, samen met een ontwerpoverzicht van de personeelsformatie, aan de raad van bestuur. De ontvangsten en uitgaven zijn in evenwicht. De uitgaven van het kenniscentrum omvatten de personele, administratieve, infrastructurele en operationele uitgaven. De administratieve uitgaven worden tot een minimum beperkt.

2. De raad van bestuur stelt jaarlijks de raming van de ontvangsten en uitgaven van het kenniscentrum voor het volgende begrotingsjaar vast op basis van de in lid 1 bedoelde opgestelde ontwerpraming van de ontvangsten en uitgaven.

3. Uiterlijk op 31 januari van elk jaar stuurt de raad van bestuur de in lid 2 bedoelde raming, die deel uitmaakt van het ontwerp van het enig programmeringsdocument, naar de Commissie.

4. Op basis van deze raming voert de Commissie in het ontwerp van algemene begroting van de Europese Unie, dat zij overeenkomstig de artikelen 313 en 314 VWEU bij het Europees Parlement en de Raad indient, de ramingen op die zij nodig acht voor het overzicht van de personeelsformatie en voor de bijdrage ten laste van de algemene begroting.

5. Het Europees Parlement en de Raad keuren de kredieten voor de bijdrage aan het kenniscentrum goed.

6. Het Europees Parlement en de Raad stellen de personeelsformatie van het kenniscentrum vast.

7. De raad van bestuur stelt, samen met het werkplan, de begroting van het kenniscentrum vast. De begroting wordt definitief na de definitieve vaststelling van de algemene begroting van de Unie. Voor zover van toepassing past de raad van bestuur de begroting en het werkplan van het kenniscentrum aan in overeenstemming met de algemene begroting van de Unie.

Artikel 27

Indiening van de rekeningen van het kenniscentrum en kwijting

De indiening van de voorlopige en definitieve rekeningen van het kenniscentrum en de kwijting verlopen volgens de regels en het tijdschema van het Financieel Reglement en de overeenkomstig artikel 29 vastgestelde financiële regels.

Artikel 28

Operationele en financiële verslaglegging

1. De uitvoerend directeur brengt jaarlijks verslag uit aan de raad van bestuur over de uitvoering van zijn/haar taken in overeenstemming met de financiële regels van het kenniscentrum.

2. Binnen twee maanden na de sluiting van elk begrotingsjaar legt de uitvoerend directeur de raad van bestuur ter goedkeuring een jaarlijks activiteitenverslag voor over de door het kenniscentrum in het voorafgaande kalenderjaar gemaakte vorderingen, met name in vergelijking met het werkplan voor dat jaar. Dit verslag bevat informatie over onder meer de volgende zaken:

   (a) uitgevoerde operationele acties en de daarmee verband houdende uitgaven;

   (b) de ingediende acties, met inbegrip van een opsplitsing per soort deelnemer, waaronder kmo's, en per lidstaat;

   (c) de voor financiering aangewezen acties, met inbegrip van een opsplitsing per soort deelnemer, waaronder kmo's, en per lidstaat, met vermelding van de bijdrage van het kenniscentrum aan de afzonderlijke deelnemers en acties;

   (d) vorderingen met de verwezenlijking van de in artikel 4 omschreven doelstellingen, en voorstellen voor verdere noodzakelijke werkzaamheden ter verwezenlijking van die doelstellingen.

3. Na goedkeuring door de raad van bestuur wordt het jaarlijkse activiteitenverslag openbaar gemaakt.

Artikel 29

Financiële regels

Het kenniscentrum stelt zijn specifieke financiële regels vast overeenkomstig artikel 70 van Verordening XXX [nieuw Financieel Reglement].

Artikel 30

Bescherming van de financiële belangen

1. Het kenniscentrum neemt passende maatregelen om ervoor te zorgen dat bij de uitvoering van uit hoofde van deze verordening gefinancierde acties, de financiële belangen van de Unie via de toepassing van preventieve maatregelen tegen fraude, corruptie en andere onwettige activiteiten worden beschermd door middel van doeltreffende controles en, indien onregelmatigheden worden ontdekt, door middel van terugvordering van de onverschuldigd betaalde bedragen en, voor zover van toepassing, door middel van doeltreffende, evenredige en afschrikkende bestuurlijke sancties.

2. Het kenniscentrum verleent personeelsleden van de Commissie en andere door haar gemachtigde personen alsmede de Rekenkamer toegang tot zijn terreinen en gebouwen en tot alle informatie, ook in elektronisch formaat, die benodigd is voor het verrichten van hun controles.

3. Het Europees Bureau voor fraudebestrijding (OLAF) kan overeenkomstig de bepalingen en procedures vastgesteld in Verordening (Euratom, EG) nr. 2185/96 van de Raad[30] en Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad[31] onderzoeken, waaronder controles en verificaties ter plaatse, uitvoeren om vast te stellen of er sprake is van fraude, corruptie of andere onwettige activiteiten waardoor de financiële belangen van de Unie worden geschaad in verband met een direct of indirect uit hoofde van deze verordening gefinancierde subsidieovereenkomst dan wel een contract.

4. Onverminderd de leden 1, 2 en 3 van dit artikel bevatten de contracten en subsidieovereenkomsten die uit de toepassing van deze verordening voortvloeien, bepalingen die de Commissie, het kenniscentrum, de Rekenkamer en OLAF uitdrukkelijk de bevoegdheid geven dergelijke controles en onderzoeken binnen hun respectieve bevoegdheden te verrichten. Wanneer de uitvoering van een actie geheel of gedeeltelijk uitbesteed of verder gedelegeerd wordt, of wanneer hiervoor een overheidsopdracht moet worden geplaatst of financiële steun moet worden verleend aan een derde, wordt in het contract of de subsidieovereenkomst bepaald dat de contractant of de begunstigde ervan verplicht is van elke betrokken derde te verlangen dat deze uitdrukkelijk de bevoegdheid van de Commissie, het kenniscentrum, de Rekenkamer en OLAF aanvaardt.

HOOFDSTUK IV

PERSONEEL VAN HET KENNISCENTRUM

Artikel 31

Personeel

1. Het Statuut van de ambtenaren en de Regeling die van toepassing is op de andere personeelsleden van de Europese Unie, vastgesteld bij Verordening (EEG, Euratom,

---

30 Verordening (Euratom, EG) nr. 2185/96 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Europese Gemeenschappen tegen fraudes en andere onregelmatigheden (PB L 292 van 15.11.1996, blz. 2).

31 Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11 september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) en tot intrekking van Verordening (EG) nr. 1073/1999 van het Europees Parlement en de Raad en Verordening (Euratom) nr. 1074/1999 van de Raad (PB L 248 van 18.9.2013, blz. 1).

EGKS) nr. 259/68 van de Raad[32] ("het Statuut" en "de Regeling die van toepassing is op andere personeelsleden"), en de door de instellingen van de Europese Unie gezamenlijk vastgestelde regelingen ter uitvoering van het Statuut en de Regeling die van toepassing is op andere personeelsleden, zijn van toepassing op het personeel van het kenniscentrum.

2. De raad van bestuur oefent met betrekking tot het personeel van het kenniscentrum de bevoegdheden tot aanstelling uit die krachtens het Statuut aan het tot aanstelling bevoegde gezag zijn toegekend en de bevoegdheden krachtens de Regeling die van toepassing is op de andere personeelsleden zijn toegekend aan het tot het sluiten van arbeidscontracten bevoegde gezag (de "bevoegdheden tot aanstelling").

3. Overeenkomstig artikel 110 van het Statuut stelt de raad van bestuur, op grond van artikel 2, lid 1, van het Statuut en van artikel 6 van de Regeling die van toepassing is op de andere personeelsleden, een besluit vast om de bevoegdheden tot aanstelling te delegeren aan de uitvoerend directeur en de voorwaarden vast te stellen waaronder die delegatie kan worden geschorst. De uitvoerend directeur mag deze bevoegdheid op zijn beurt subdelegeren.

4. Indien uitzonderlijke omstandigheden dit vereisen, kan de raad van bestuur een besluit nemen om de delegatie van de bevoegdheden tot aanstelling aan de uitvoerend directeur en elke door deze laatste verleende subdelegatie tijdelijk te schorsen. In een dergelijk geval oefent de raad van bestuur de bevoegdheden tot aanstelling zelf uit of worden deze gedelegeerd aan een van zijn leden of aan een ander personeelslid van het kenniscentrum dan de uitvoerend directeur.

5. De raad van bestuur stelt overeenkomstig artikel 110 van het Statuut bepalingen vast voor de tenuitvoerlegging van het Statuut en de Regeling die van toepassing is op de andere personeelsleden.

6. De personele middelen worden bepaald in de personeelsformatie van het kenniscentrum, waarin het aantal tijdelijke aanstellingen per functiegroep en per rang alsmede het aantal arbeidscontractanten worden vermeld uitgedrukt in voltijdequivalenten, in overeenstemming met de jaarbegroting van het kenniscentrum.

7. Het personeel van het kenniscentrum bestaat uit tijdelijke functionarissen en arbeidscontractanten.

8. Alle personeelskosten zijn ten laste van het kenniscentrum.

Artikel 32

Gedetacheerde nationale deskundigen en andere personeel

1. Het kenniscentrum kan gebruikmaken van gedetacheerde nationale deskundigen of ander personeel dat niet in dienst is van het kenniscentrum.

2. In overleg met de Commissie stelt de raad van bestuur een besluit vast met regels voor de detachering van nationale deskundigen bij het kenniscentrum.

---

[32] Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad van 29 februari 1968 tot vaststelling van het Statuut van de ambtenaren van de Europese Gemeenschappen en de regeling welke van toepassing is op de andere personeelsleden van deze Gemeenschappen, alsmede van bijzondere maatregelen welke tijdelijk op de ambtenaren van de Commissie van toepassing zijn (PB L 56 van 4.3.1968, blz. 1).

Artikel 33

Voorrechten en immuniteiten

Protocol nr. 7 inzake voorrechten en immuniteiten van de Europese Unie, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht, is van toepassing op het kenniscentrum en zijn personeelsleden.

HOOFDSTUK V

GEMEENSCHAPPELIJKE BEPALINGEN

Artikel 34

Beveiligingsvoorschriften

1. Artikel 12, lid 7, van Verordening (EU) XXX [programma Digitaal Europa] is van toepassing bij deelname aan alle door het kenniscentrum gefinancierde acties.

2. Voor uit Horizon Europa gefinancierde acties gelden de volgende specifieke beveiligingsvoorschriften:

   (a) voor de toepassing van artikel 34, lid 1 [Eigendom en bescherming] van Verordening (EU) XXX [Horizon Europa] kan, indien het werkplan hierin voorziet, de verlening van niet-exclusieve licenties worden beperkt tot derde partijen die zijn gevestigd of geacht worden te zijn gevestigd in de lidstaten en waarover door lidstaten en/of onderdanen van lidstaten zeggenschap wordt uitgeoefend;

   (b) voor de toepassing van artikel 36, lid 4, onder b), [Overdracht en licentieverlening] van Verordening (EU) XXX [Horizon Europa], is de overdracht of licentieverlening aan een in een geassocieerd land of in de Unie gevestigde juridische entiteit waarover vanuit derde landen zeggenschap wordt uitgeoefend, ook een grond om bezwaar te maken tegen de overdracht van de eigendom van resultaten of tegen de verlening van een exclusieve licentie voor resultaten;

   (c) voor de toepassing van artikel 37, lid 3 [Toegangsrechten] van Verordening (EU) XXX [Horizon Europa] kan, indien het werkplan hierin voorziet, de verlening van toegang tot resultaten en background alleen worden beperkt tot juridische entiteiten die zijn gevestigd of geacht worden te zijn gevestigd in de lidstaten en waarover door lidstaten en/of onderdanen van lidstaten zeggenschap wordt uitgeoefend.

Artikel 35

Transparantie

1. Het kenniscentrum verricht zijn werkzaamheden met een hoge mate van transparantie.

2. Het kenniscentrum ziet erop toe dat geïnteresseerden en alle belanghebbenden van passende, objectieve, betrouwbare en gemakkelijk toegankelijke informatie worden voorzien, in het bijzonder met betrekking tot de resultaten van zijn werkzaamheden. Tevens maakt het de overeenkomstig artikel 41 afgelegde belangenverklaringen openbaar.

3. De raad van bestuur kan op voorstel van de uitvoerend directeur belanghebbenden toestemming geven om de uitvoering van activiteiten van het kenniscentrum te observeren.

4. Het kenniscentrum legt in zijn reglement van orde de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde transparantiebepalingen vast. Voor uit Horizon Europa gefinancierde acties zal hiervoor naar behoren rekening worden gehouden met de bepalingen van bijlage III bij de verordening betreffende Horizon Europa.

Artikel 36

Beveiligingsvoorschriften voor de bescherming van gerubriceerde informatie en gevoelige niet-gerubriceerde informatie

1. Onverminderd artikel 35 onthult het kenniscentrum aan derden geen verwerkte of ontvangen informatie waarvoor een met redenen omkleed verzoek om gehele of gedeeltelijke vertrouwelijke behandeling is ingediend.

2. De leden van de raad van bestuur, de uitvoerend directeur, de leden van het industrieel en wetenschappelijk adviescomité, de externe deskundigen die deelnemen aan ad-hocwerkgroepen en de personeelsleden van het kenniscentrum houden zich ook na het beëindigen van hun functie aan de geheimhoudingsplicht uit hoofde van artikel 339 van het Verdrag betreffende de werking van de Europese Unie.

3. De raad van bestuur van het kenniscentrum stelt, na goedkeuring door de Commissie, de beveiligingsvoorschriften van het kenniscentrum vast op basis van de beginselen en regels die zijn vastgelegd in de beveiligingsvoorschriften van de Commissie voor de bescherming van gerubriceerde EU-informatie (EUCI) en gevoelige niet-gerubriceerde informatie, waaronder voorschriften betreffende de verwerking en opslag van dergelijke informatie, zoals omschreven in Besluiten (EU, Euratom) 2015/443[33] en 2015/444[34].

4. Het kenniscentrum kan alle nodige maatregelen nemen om de uitwisseling van voor zijn taken relevante informatie met de Commissie en de lidstaten en, indien van toepassing, de relevante agentschappen en organen van de Unie, te vergemakkelijken. Voor elke administratieve regeling inzake het delen van EUCI of, bij het ontbreken van een dergelijke regeling, voor elke uitzonderlijke ad-hocvrijgave van EUCI is voorafgaande toestemming van de Commissie vereist.

Artikel 37

Toegang tot documenten

1. Verordening (EG) nr. 1049/2001 is van toepassing op de documenten die bij het kenniscentrum berusten.

---

33 Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie (PB L 72 van 17.3.2015, blz. 41).

34 Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

2. De raad van bestuur stelt binnen zes maanden na de oprichting van het kenniscentrum regelingen voor de uitvoering van Verordening (EG) nr. 1049/2001 vast.

3. Tegen besluiten van het kenniscentrum uit hoofde van artikel 8 van Verordening (EG) nr. 1049/2001 kan een klacht bij de ombudsman worden ingediend uit hoofde van artikel 228 van het Verdrag betreffende de werking van de Europese Unie of een beroep bij het Hof van Justitie van de Europese Unie worden ingesteld uit hoofde van artikel 263 van het Verdrag betreffende de werking van de Europese Unie.

Artikel 38

Toezicht, evaluatie en toetsing

1. Het kenniscentrum zorgt ervoor dat zijn activiteiten, met inbegrip van de activiteiten die door de nationale coördinatiecentra en het netwerk worden beheerd, onderworpen zijn aan permanent en systematisch toezicht en periodieke evaluatie. Het kenniscentrum zorgt ervoor dat de gegevens voor het toezicht op de uitvoering en de resultaten van het programma efficiënt, doeltreffend en tijdig worden verzameld en dat evenredige verslagleggingsvereisten worden opgelegd aan de ontvangers van middelen van de Unie en de lidstaten. De resultaten van de evaluatie worden bekendgemaakt.

2. Zodra voldoende informatie over de uitvoering van deze verordening beschikbaar is, maar uiterlijk drie jaar nadat met de uitvoering ervan is begonnen, voert de Commissie een tussentijdse evaluatie van het kenniscentrum uit. De Commissie stelt een verslag over die evaluatie op en zendt dat uiterlijk op 31 december 2024 aan het Europees Parlement en de Raad toe. Het kenniscentrum en de lidstaten verstrekken de Commissie de informatie die zij voor de opstelling van dat verslag nodig heeft.

3. De in lid 2 bedoelde evaluatie omvat een beoordeling van de door het kenniscentrum behaalde resultaten met betrekking tot zijn doelstellingen, mandaat en taken. Indien de Commissie van oordeel is dat de voortzetting van het kenniscentrum gezien de daaraan toegewezen doelstellingen, taken en mandaat gerechtvaardigd is, kan zij voorstellen de in artikel 46 genoemde looptijd van het mandaat van het kenniscentrum te verlengen.

4. Op grond van de conclusies van de in lid 2 bedoelde tussentijdse evaluatie kan de Commissie handelen in overeenstemming met [artikel 22, lid 5,] of andere passende maatregelen treffen.

5. Het toezicht, de evaluatie, de uitfasering en de verlenging van de bijdrage uit Horizon Europa gebeuren overeenkomstig de bepalingen van de artikelen 8, 45 en 47 en bijlage III van de verordening betreffende Horizon Europa en de overeengekomen uitvoeringsbepalingen.

6. Het toezicht, de verslaglegging en de evaluatie van de bijdrage uit Digitaal Europa gebeuren overeenkomstig de bepalingen van de artikelen 24 en 25 van het programma Digitaal Europa.

7. In geval van ontbinding van het kenniscentrum verricht de Commissie binnen zes maanden na de ontbinding van het kenniscentrum, maar niet later dan twee jaar na de inleiding van de in artikel 46 van deze verordening bedoelde ontbindingsprocedure, een eindevaluatie van het kenniscentrum. De resultaten van deze eindevaluatie worden bij het Europees Parlement en de Raad ingediend.

Artikel 39

Aansprakelijkheid van het kenniscentrum

1. De contractuele aansprakelijkheid van het kenniscentrum valt onder het recht dat van toepassing is op de overeenkomst, het besluit of het contract in kwestie.
2. In geval van niet-contractuele aansprakelijkheid vergoedt het kenniscentrum, overeenkomstig de algemene beginselen die de wetgevingen van de lidstaten gemeen hebben, alle schade die door zijn personeel bij de uitoefening van hun taken is veroorzaakt.
3. Elke betaling door het kenniscentrum in verband met de aansprakelijkheid als bedoeld in de leden 1 en 2 en de daarmee verband houdende kosten en uitgaven worden beschouwd als uitgaven van het kenniscentrum en worden door zijn middelen gedekt.
4. Het kenniscentrum is als enige verantwoordelijk voor het nakomen van zijn verplichtingen.

Artikel 40

Bevoegdheid van het Hof van Justitie van de Europese Unie en toepasselijk recht

1. Het Hof van Justitie van de Europese Unie is bevoegd uitspraak te doen:
   (1) wanneer door het kenniscentrum gesloten overeenkomsten, besluiten en contracten een arbitragebeding bevatten;
   (2) in geschillen over de vergoeding van schade die door personeelsleden van het kenniscentrum wordt veroorzaakt bij de uitoefening van hun taken;
   (3) in elk geschil tussen het kenniscentrum en zijn personeel binnen de grenzen en onder de voorwaarden vastgelegd in het Statuut.
2. In alle aangelegenheden die niet bij deze verordening of bij andere rechtshandelingen van de Unie zijn geregeld, is het recht van de lidstaat waar de zetel van het kenniscentrum zich bevindt, van toepassing.

Artikel 41

Aansprakelijkheid van leden en verzekering

1. De financiële aansprakelijkheid van de leden voor de schulden van het kenniscentrum is beperkt tot de door hen reeds betaalde bijdrage aan de administratieve kosten.
2. Het kenniscentrum sluit de nodige verzekeringen af en houdt deze aan.

Artikel 42

Belangenconflicten

De raad van bestuur van het kenniscentrum kan regels vaststellen om belangenconflicten met betrekking tot zijn leden, zijn organen en zijn personeel te voorkomen en te beheersen. Deze regels omvatten de bepalingen ter voorkoming van belangenconflicten met betrekking tot de vertegenwoordigers van de leden die zitting hebben in de raad van bestuur, alsook in het industrieel en wetenschappelijk adviescomité, overeenkomstig Verordening XXX [nieuw Financieel Reglement].

Artikel 43

Bescherming van persoonsgegevens

1. Op de verwerking van persoonsgegevens door het kenniscentrum is Verordening (EU) XXX/2018 van het Europees Parlement en de Raad van toepassing.
2. De raad van bestuur stelt uitvoeringsvoorschriften als bedoeld in artikel xx, lid 3, van Verordening (EU) xxx/2018 vast. De raad van bestuur kan aanvullende maatregelen vaststellen met het oog op de toepassing van Verordening (EU) xxx/2018 door het kenniscentrum.

Artikel 44

Ondersteuning door de onderbrengende lidstaat

Tussen het kenniscentrum en de lidstaat [België] waar zijn zetel zich bevindt, kan een administratieve overeenkomst worden gesloten betreffende voorrechten, immuniteiten en andere ondersteuning die door die lidstaat aan het kenniscentrum worden verleend.

HOOFDSTUK VII

SLOTBEPALINGEN

Artikel 45

Initiële acties

1. De Commissie is belast met de oprichting en de initiële werking van het kenniscentrum totdat het over voldoende operationele capaciteit beschikt om zijn eigen begroting uit te voeren. Overeenkomstig het recht van de Unie betrekt de Commissie de bevoegde organen van het kenniscentrum bij de uitvoering van alle nodige maatregelen.
2. Voor de toepassing van lid 1 kan de Commissie, totdat de uitvoerend directeur zijn of haar taken opneemt na zijn of haar benoeming door de raad van bestuur in overeenstemming met artikel 16, een tijdelijk uitvoerend directeur aanstellen en de taken waarmee de uitvoerend directeur belast is uitvoeren; deze kan worden bijgestaan door een beperkt aantal ambtenaren van de Commissie. De Commissie kan tijdelijk een beperkt aantal van haar ambtenaren toewijzen.
3. De tijdelijk uitvoerend directeur kan alle betalingen binnen de kredieten van de jaarbegroting van het kenniscentrum goedkeuren wanneer deze zijn goedgekeurd door de raad van bestuur, en kan besluiten aannemen en overeenkomsten en

contracten sluiten, met inbegrip van personeelscontracten, wanneer de personeelsformatie van het kenniscentrum is vastgesteld.

4. De tijdelijk uitvoerend directeur bepaalt in samenspraak met de uitvoerend directeur van het kenniscentrum en na goedkeuring door de raad van bestuur op welke datum het kenniscentrum de capaciteit heeft om zijn eigen begroting uit te voeren. Vanaf dat moment onthoudt de Commissie zich van het aangaan van verbintenissen en het uitvoeren van betalingen voor de activiteiten van het kenniscentrum.

Artikel 46

Duur

1. Het kenniscentrum wordt opgericht voor de periode van 1 januari 2021 tot en met 31 december 2029.

2. Aan het einde van deze periode wordt de ontbindingsprocedure ingeleid, tenzij door een herziening van deze verordening anders wordt besloten. De ontbindingsprocedure wordt automatisch ingeleid ingeval de Unie zich uit het kenniscentrum terugtrekt of ingeval alle deelnemende lidstaten dat doen.

3. Voor de uitvoering van de procedure tot ontbinding van het kenniscentrum benoemt de raad van bestuur een of meer vereffenaars die handelen volgens de besluiten van de raad van bestuur.

4. Wanneer het kenniscentrum wordt ontbonden, worden zijn activa gebruikt ter voldoening van zijn verplichtingen en voor de uitgaven in verband met zijn ontbinding. Een eventueel overschot wordt verdeeld over de Unie en de deelnemende lidstaten in verhouding tot hun financiële bijdragen aan het kenniscentrum. Een eventueel overschot dat de Unie toevalt, wordt teruggeboekt naar de begroting van de Unie.

Artikel 47

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur

1.3. Aard van het voorstel/initiatief

1.4. Doelstelling(en)

1.5. Motivering van het voorstel/initiatief

1.6. Duur en financiële gevolgen

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesysteem

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

3.2.2. Geraamde gevolgen voor de beleidskredieten

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidige meerjarig financieel kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur[35]

Onderzoek en innovatie

Europese strategische investeringen

1.3. Aard van het voorstel/initiatief

☒ Het voorstel/initiatief betreft **een nieuwe actie**

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[36]

☐ Het voorstel/initiatief betreft **de verlenging van een bestaande actie**

☐ Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

1. Een connectieve digitale eengemaakte markt

2. Een nieuwe impuls voor banen, groei en investeringen

1.4.2. Betrokken specifieke doelstelling(en)

Specifieke doelstellingen

1.3 De digitale economie kan haar volledige potentieel ontplooien dankzij initiatieven die een volledige groei van digitale en datatechnologieën mogelijk maken.

2.1 Europa behoudt zijn positie als wereldleider in de digitale economie, waarin Europese ondernemingen wereldwijd kunnen groeien dankzij sterk digitaal ondernemerschap en goed presterende start-ups, en waarin de industrie en de openbare diensten de digitale transformatie beheersen.

2.2. Het Europese onderzoek biedt mogelijkheden voor investeringen in potentiële technologische doorbraken en vlaggenschipinitiatieven, met name in het kader van het programma Horizon 2020 / Horizon Europa en dankzij publiek-private partnerschappen.

35 ABM: activity-based management; ABB: activity-based budgeting.

36 In de zin van artikel 54, lid 2, onder a) of b), van het Financieel Reglement.

1.4.3. Verwacht(e) resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben voor de begunstigden/doelgroepen.

Het kenniscentrum streeft samen met het netwerk en de kennisgemeenschap de volgende doelstellingen na:

1) bijdragen aan de uitvoering van het onderdeel cyberbeveiliging van het bij Verordening XXX vastgestelde programma Digitaal Europa, en met name aan acties met betrekking tot artikel 6 van Verordening (EU) XXX [programma Digitaal Europa], alsook van het bij Verordening XXX vastgestelde programma Horizon Europa, en met name punt 2.2.6 van bijlage I bij Besluit nr. XXX tot vaststelling van het specifieke programma tot uitvoering van Horizon Europa – het kaderprogramma voor onderzoek en innovatie , en van andere programma's van de Unie indien hierin wordt voorzien in rechtshandelingen van de Unie;

2) de capaciteiten, de kennis en de infrastructuur op het gebied van cyberbeveiliging verbeteren ten behoeve van de industrie, de publieke sector en de onderzoeksgemeenschappen;

3) ertoe bijdragen dat de nieuwste cyberbeveiligingsproducten en -oplossingen op ruim schaal worden aangewend in de hele economie;

4) zorgen voor een beter begrip van cyberbeveiliging en helpen om het gebrek aan cyberbeveiligingsvaardigheden in de Unie aan te pakken;

5) bijdragen aan de versterking van het onderzoek en de ontwikkeling op het gebied van cyberbeveiliging in de Unie;

6) de samenwerking tussen de civiele en de defensie-industrie verbeteren als het gaat om technologieën en toepassingen voor tweeërlei gebruik;

7) de synergieën tussen de civiele en de defensiedimensie van cyberbeveiliging versterken;

8) de werkzaamheden van het in artikel 10 bedoelde netwerk van nationale coördinatiecentra ("het netwerk") en de in artikel 12 bedoelde kennisgemeenschap voor cyberbeveiliging helpen coördineren en vergemakkelijken.

1.4.4. Resultaat- en effectindicatoren

Vermeld de indicatoren aan de hand waarvan kan worden nagegaan in hoeverre het voorstel/initiatief is uitgevoerd.

· Aantal gezamenlijk verworven infrastructuurvoorzieningen / instrumenten op het gebied van cyberbeveiliging

· Toegang tot test- en experimenteertijd voor Europese onderzoekers en ondernemingen in het netwerk en het kenniscentrum. Indien de faciliteiten reeds bestaan, moeten deze gemeenschappen een groter aantal uren toegewezen krijgen in vergelijking met de uren die momenteel beschikbaar zijn.

· Toename van het aantal bediende gebruikersgemeenschappen en onderzoekers dat toegang krijgt tot de Europese cyberbeveiligingsfaciliteiten in vergelijking met het aantal onderzoekers dat dergelijke middelen buiten Europa moet zoeken.

· Beginnende toename van het concurrentievermogen van Europese leveranciers, gemeten aan het wereldwijde marktaandeel (doelstelling van 25 % marktaandeel in 2027) en aan het aandeel van Europese O&O-resultaten dat door het bedrijfsleven wordt toegepast.

· Bijdrage aan nieuwe cyberbeveiligingstechnologieën, gemeten in termen van auteursrechten, octrooien, wetenschappelijke publicaties en commerciële producten.

· Aantal geëvalueerde en aangepaste leerplannen met betrekking tot cyberbeveiliging, aantal beoordeelde programma's voor professionele certificering op het gebied van cyberbeveiliging;

· Aantal opgeleide wetenschappers, studenten, gebruikers (uit het bedrijfsleven en de overheidssector).

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien

Een kritische massa van investeringen in technologie en industriële ontwikkeling op het gebied van cyberbeveiliging bereiken en de versnippering van de relevante capaciteit in de EU tegengaan.

1.5.2. Toegevoegde waarde van de deelname van de EU

Cyberbeveiliging is een zaak van gemeenschappelijk belang voor de Unie, zoals ook is bevestigd in de hierboven vermelde conclusies van de Raad. Goede voorbeelden zijn de omvang en het grensoverschrijdende karakter van incidenten zoals WannaCry en NonPetya. Gezien de aard en de omvang van de technologische uitdagingen op het gebied van cyberbeveiliging en het feit dat de inspanningen in het bedrijfsleven, de overheidssector en de onderzoeksgemeenschappen, alsook tussen deze sectoren onderling, onvoldoende worden gecoördineerd, moet de EU de coördinatie-inspanningen verder ondersteunen, zowel om een kritische massa aan middelen bijeen te brengen als om een beter beheer van kennis en activa te garanderen. Dit is noodzakelijk aangezien er middelen nodig zijn voor bepaalde capaciteiten voor het onderzoek naar en de ontwikkeling en invoering van cyberbeveiligingstechnologieën; aangezien er toegang moet worden verleend tot interdisciplinaire kennis op het gebied van cyberbeveiliging in verschillende disciplines (vaak slechts gedeeltelijk beschikbaar op nationaal niveau); aangezien de industriële waardeketens een mondiaal karakter hebben en de concurrenten overal ter wereld op allerlei markten actief zijn.

Hiervoor zijn middelen en expertise vereist van een niveau dat moeilijk kan worden bereikt met afzonderlijke maatregelen van een lidstaat. Zo zou een pan-Europees kwantumcommunicatienetwerk een investering in de grootorde van 900 miljoen EUR van de EU vergen, afhankelijk van de investeringen van de lidstaten (te koppelen / aan te vullen) en de mate waarin voor de technologie bestaande infrastructuren kunnen worden hergebruikt.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

De tussentijdse evaluatie van Horizon 2020 heeft onder meer het blijvende belang van EU-steun voor O&O en maatschappelijke uitdagingen aangetoond (waaronder "veilige samenlevingen", in het kader waarvan O&O op het gebied van cyberbeveiliging wordt ondersteund). Tegelijkertijd bevestigt de evaluatie dat het versterken van het industriële leiderschap een uitdaging blijft en dat er nog steeds een innovatiekloof is, waarbij de EU achterloopt op het gebied van baanbrekende, marktcreërende innovatie.

De tussentijdse evaluatie van de Connecting Europe Facility (CEF) lijkt de toegevoegde waarde van EU-interventie die verder gaat dan O&O, te bevestigen, al

had cyberbeveiliging in het kader van de CEF een iets andere focus (op operationele beveiliging) en interventielogica. Tegelijkertijd heeft de meerderheid van de ontvangers van CEF-subsidies voor cyberbeveiliging – de gemeenschap van nationale CSIRT's – kenbaar gemaakt dat zij in het kader van het volgende MFK een ondersteuningsprogramma op maat wensen.

Toen in 2016 het publiek-private partnerschap voor ("cPPP") in de EU werd opgezet, was dit een eerste grote stap om de onderzoeksgemeenschap, de industrie en de publieke sector samen te brengen om onderzoek en innovatie op het gebied van cyberbeveiliging te vergemakkelijken en dit zou binnen de grenzen van het meerjarig financieel kader voor de periode 2014-2020 goede, meer gerichte resultaten op het gebied van onderzoek en innovatie moeten opleveren. Dankzij het cPPP konden industriële partners toezeggingen doen over hun individuele uitgaven met betrekking tot gebieden die in de strategische agenda voor onderzoek en innovatie van het partnerschap zijn vastgesteld.

1.5.4. Verenigbaarheid en eventuele synergie met andere passende instrumenten

Het kennisnetwerk voor cyberbeveiliging en het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zullen een extra ondersteuning zijn voor de bestaande beleidsbepalingen en spelers op het gebied van cyberbeveiliging. Het mandaat van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal een aanvulling vormen op de inspanningen van het Enisa, maar legt een andere nadruk en vereist andere vaardigheden. Terwijl het Enisa een adviserende rol speelt inzake onderzoek en innovatie op het gebied van cyberbeveiliging in de EU, is het voorgestelde mandaat van het kenniscentrum vooral gericht op andere taken die cruciaal zijn voor de versterking van de weerbaarheid van de EU op het gebied van cyberbeveiliging. Het kenniscentrum moet de ontwikkeling en aanwending van cyberbeveiligingstechnologie bevorderen en een aanvulling vormen op de inspanningen inzake capaciteitsopbouw die op dit gebied zowel op EU-niveau als op nationaal niveau worden geleverd.

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal samen met het kenniscentrum voor cyberbeveiliging ook werken aan de ondersteuning van onderzoek om de standaardiserings- en certificeringsprocessen te vergemakkelijken en te versnellen, met name die met betrekking tot regelingen voor cyberbeveiligingscertificering in de zin van de cyberbeveiligingsverordening.

Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal optreden als één uitvoeringsmechanisme voor twee Europese programma's ter ondersteuning van cyberbeveiliging (de programma's "Digitaal Europa" en "Horizon Europa") en zal de samenhang en de synergieën tussen deze programma's verbeteren.

Dit initiatief maakt het mogelijk de inspanningen van de lidstaten aan te vullen door makers van onderwijsbeleid passende input te geven voor de verbetering van het onderwijs op het gebied van cyberbeveiliging (bv. door voor de civiele en militaire onderwijsstelsels leerplannen voor cyberbeveiliging te ontwikkelen, maar ook door input te geven voor basisopleidingen in cyberbeveiliging). Dankzij dit initiatief zouden ook de onderlinge afstemming en continue beoordeling van de certificeringsprogramma's inzake cyberbeveiliging kunnen worden ondersteund – alle noodzakelijke activiteiten om de kloof op het gebied van

cyberbeveiligingsvaardigheden te dichten en ervoor te zorgen dat industrieën en andere gemeenschappen gemakkelijker toegang krijgen tot cyberbeveiligingsspecialisten. Het op elkaar afstemmen van onderwijs en vaardigheden zal bijdragen tot de scholing van personeel in de EU dat gekwalificeerd is op het gebied van cyberbeveiliging, een essentieel instrument voor cyberbeveiligingsondernemingen en andere sectoren die een belang hebben in cyberbeveiliging.

1.6. Duur en financiële gevolgen

☒ Voorstel/initiatief met een **beperkte geldigheidsduur**

– ☒ Looptijd vanaf 1.1.2021 tot en met 31.12.2029

– ☒ Financiële gevolgen: van 2021 tot en met 2027 voor vastleggingskredieten en van 2021 tot en met 2031 voor betalingskredieten.

☐ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Uitvoering met een opstartperiode vanaf JJJJ tot en met JJJJ,

– gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)[37]

☐ **Direct beheer** door de Commissie

– ☐ door haar diensten, waaronder het personeel in de delegaties van de Unie

– ☐ door de uitvoerende agentschappen

☐ **Gedeeld beheer** met de lidstaten

☒

Indirect beheer door begrotingsuitvoeringstaken te delegeren aan:

– ☐ derde landen of de door hen aangewezen organen;

– ☐ internationale organisaties en hun agentschappen (geef aan welke);

– ☐ de EIB en het Europees Investeringsfonds;

– ☒ de in de artikelen 70 en 71 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbaredienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

– ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

– ☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

[37] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

Artikel 28 bevat gedetailleerde bepalingen inzake toezicht en verslaglegging.

2.2. Beheers- en controlesysteem

2.2.1. Mogelijke risico's

Om de risico's in verband met de werking van het kenniscentrum na de oprichting ervan, alsook risico's op vertraging te vermijden, zal de Commissie het kenniscentrum in deze fase ondersteunen met het oog op een snelle aanwerving van belangrijke personeelsleden en het opzetten van een efficiënt systeem voor interne controle en degelijke procedures.

2.2.2. Informatie over het ingestelde systeem voor interne controle

De uitvoerend directeur is verantwoordelijk voor de werkzaamheden en de dagelijkse leiding en is de wettelijke vertegenwoordiger van het kenniscentrum. Hij of zij legt verantwoording af aan de raad van bestuur en brengt de raad van bestuur permanent verslag uit over de ontwikkeling van de activiteiten van het kenniscentrum.

De raad van bestuur draagt de volledige verantwoordelijkheid voor de strategische koers en de werkzaamheden van het kenniscentrum en houdt toezicht op de uitvoering van zijn activiteiten.

Na raadpleging van de Commissie stelt de raad van bestuur de financiële voorschriften vast die van toepassing zijn op het kenniscentrum. Deze regeling wijkt niet af van Gedelegeerde Verordening (EU) nr. 1271/2013, tenzij dit in verband met de werking van het kenniscentrum specifiek vereist is en de Commissie vooraf toestemming heeft verleend.

De intern controleur van de Commissie oefent ten aanzien van het kenniscentrum dezelfde bevoegdheden uit als die welke hij met betrekking tot de Commissie uitoefent. De Rekenkamer is bevoegd om bij alle begunstigden van subsidies, contractanten en subcontractanten die van het kenniscentrum middelen van de Unie hebben ontvangen, controles op stukken of controles ter plaatse te verrichten.

2.2.3. Raming van de kosten en baten van de controles en evaluatie van het verwachte foutenrisico

Kosten en baten van controles

De controlekosten voor het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging bestaan uit de kosten van het toezicht op het niveau van de Commissie en de kosten van operationele controles op het niveau van de uitvoeringsorganen.

De kosten van de controles op het niveau van het kenniscentrum bedragen naar schatting 1,19 % van de operationele betalingskredieten die ten uitvoer worden gelegd op het niveau van het kenniscentrum.

De kosten van het toezicht op het niveau van de Commissie bedragen naar schatting 1,20 % van de operationele betalingskredieten die ten uitvoer worden gelegd op het niveau van het kenniscentrum.

Indien de activiteiten volledig door de Commissie zouden worden beheerd zonder de steun van het uitvoeringsorgaan, zouden de controlekosten veel hoger liggen en zouden zij ongeveer 7,7 % van de betalingskredieten kunnen bedragen.

Het doel van de beoogde controles is het waarborgen van soepel en doeltreffend toezicht door de Commissie op de uitvoeringentiteiten en het waarborgen van de nodige mate van zekerheid op het niveau van de Commissie.

De controles leveren de volgende voordelen op:

- er wordt vermeden dat zwakkere en ongeschikte voorstellen worden geselecteerd;
- de planning en het gebruik van EU-middelen worden geoptimaliseerd teneinde de EU-meerwaarde in stand te houden;
- de kwaliteit van de subsidieovereenkomsten wordt gewaarborgd, fouten bij het aanwijzen van juridische entiteiten worden voorkomen, de correcte berekening van de EU-bijdragen wordt gewaarborgd en de nodige garanties voor een correcte uitvoering van de subsidies worden vastgesteld;
- in de betalingsfase worden niet-subsidiabele kosten opgespoord;
- in de auditfase worden fouten opgespoord die afbreuk doen aan de wettigheid en de rechtmatigheid van de acties.

Geschat foutenpercentage

Het doel is ervoor te zorgen dat het resterende foutenpercentage voor het hele programma onder de drempel van 2 % blijft en tegelijkertijd de controlelasten voor de begunstigden wat betreft het bereiken van het juiste evenwicht tussen de doelstelling inzake wettigheid en de rechtmatigheid en andere doelstellingen, zoals de aantrekkingskracht van het programma voor met name kleine en middelgrote ondernemingen en de kosten van controles, beperkt blijven.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen.

OLAF kan overeenkomstig de bepalingen en procedures van Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad en Verordening (Euratom, EG) nr. 2185/9640 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Unie tegen fraudes en andere onregelmatigheden controles en verificaties ter plaatse verrichten om vast te stellen of er in verband met een door het kenniscentrum gefinancierde subsidie of overeenkomst sprake is van fraude, corruptie of andere illegale handelingen waardoor de financiële belangen van de Unie worden geschaad.

Overeenkomsten, besluiten en contracten die voortvloeien uit de uitvoering van deze verordening, bevatten bepalingen die de Commissie, het kenniscentrum, de Rekenkamer en OLAF uitdrukkelijk de bevoegdheid verlenen om audits en onderzoeken te verrichten overeenkomstig hun respectieve bevoegdheden.

Het kenniscentrum zorgt er, door het uitvoeren of laten uitvoeren van de nodige interne en externe controles, voor dat de financiële belangen van zijn leden op adequate wijze worden beschermd.

Het kenniscentrum treedt toe tot het Interinstitutioneel Akkoord van 25 mei 1999 tussen het Europees Parlement, de Raad van de Europese Unie en de Commissie van de Europese Gemeenschappen betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF). Het kenniscentrum stelt de nodige maatregelen vast om interne onderzoeken door OLAF te vergemakkelijken.

Het kenniscentrum stelt een fraudebestrijdingsstrategie vast op basis van een frauderisicoanalyse en kosten-batenoverwegingen. Het beschermt de financiële belangen van de Unie door maatregelen ter voorkoming van fraude, corruptie en andere onwettige activiteiten toe te passen, controles te verrichten en, wanneer er onregelmatigheden worden ontdekt, ten onrechte betaalde bedragen terug te vorderen en, waar nodig, effectieve, evenredige en afschrikkende administratieve en geldelijke sancties op te leggen.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek van het meerjarig financieel kader en voorgesteld(e) nieuw(e) begrotingsonderde(e)l(en) voor uitgaven

- Te creëren nieuwe begrotingsonderdelen

  In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort krediet	Bijdrage			
	Nummer	GK/NGK[38]	van EVA-landen[39]	van kandidaat-lidstaten[40]	van derde landen	in de zin van artikel 21, lid 2, onder b), van het Financieel Reglement
Rubriek 1: Eengemaakte markt, innovatie en digitaal beleid	01 02 XX XX Horizon Europa Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging – ondersteunende uitgaven 01 02 XX XX Horizon Europa Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging 02 06 01 XX Programma Digitaal Europa Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging – ondersteunende uitgaven 02 06 01 XX Programma Digitaal Europa Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging	GK	JA	JA (indien vermeld in het jaarlijkse werkprogramma)	JA (beperkt tot bepaalde delen van het programma)	NEE

[38] GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

[39] EVA: Europese Vrijhandelsassociatie.

[40] Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaten van de Westelijke Balkan.

- De bijdragen voor deze begrotingsonderdelen zullen naar verwachting komen uit:

in miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel	Jaar 2021	Jaar 2022	Jaar 2023	Jaar 2024	Jaar 2025	Jaar 2026	Jaar 2027	**Totaal**
01 01 01 01 Uitgaven in verband met onderzoeksambtenaren en tijdelijke functionarissen – Horizon Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Extern personeel dat belast is met de uitvoering van onderzoeksprogramma's – Horizon Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Overige beheersuitgaven voor onderzoek – Horizon Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Wereldwijde uitdagingen en industrieel concurrentievermogen	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Administratieve ondersteuning – Programma Digitaal Europa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cyberbeveiliging – Programma Digitaal Europa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Totaal uitgaven	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

De bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21, lid 1, onder b), zal door de Commissie worden voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt. Het voorstel zal worden gebaseerd op de resultaten van het in artikel 6, lid 6, van Verordening XXX [kaderprogramma Horizon Europa] omschreven strategische planningsproces.

Bovenstaande bedragen omvatten niet de bijdrage van de lidstaten aan de operationele en administratieve kosten van het kenniscentrum, die in verhouding moeten staan tot de financiële bijdrage van de Unie.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

in miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	**1**	Eengemaakte markt, innovatie en digitaal beleid

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Na 2027***	**TOTAAL**
Titel 1 (Personeelsuitgaven)	Vastleggingen = betalingen	1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titel 2 (Infrastructuur- en operationele uitgaven)	Vastleggingen = betalingen	2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Titel 3 (Operationele uitgaven)	Vastleggingen	3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Betalingen	4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTAAL kredieten voor het budget van het programma[42]	Vastleggingen	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	Betalingen	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 De personeelskredieten voor 2021 zijn slechts berekend op een half jaar

42 De totale kredieten hebben alleen betrekking op de financiële middelen van de EU voor cyberbeveiliging in het kader van Digitaal Europa. De bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 5, lid 1, onder b), zal door de Commissie worden voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt. Het voorstel zal worden gebaseerd op de resultaten van het in artikel 6, lid 6, van Verordening XXX [kaderprogramma Horizon Europa] omschreven strategische planningsproces.

Rubriek van het meerjarig financieel kader	7	"Administratieve uitgaven"

in miljoen EUR (tot op drie decimalen)

		2021	2022	2023	2024	2025	2026	2027	*Na 2027*	TOTAAL
Personele middelen		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Andere administratieve uitgaven		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAAL kredieten onder RUBRIEK 7 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

in miljoen EUR (tot op drie decimalen)

		2021	2022	2023	2024	2025	2026	2027	*Na 2027*	TOTAAL
TOTAAL kredieten voor alle RUBRIEKEN van het meerjarig financieel kader	Vastleggingen	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Betalingen	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 061,715**	**2 005,637**

3.2.2. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoen EUR (tot op drie decimalen)

Jaren	2021	2022	2023	2024	2025	2026	2027	TOTAAL
RUBRIEK 7 van het meerjarig financieel kader								
Personele middelen	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Andere administratieve uitgaven	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotaal RUBRIEK 7 van het meerjarig financieel kader	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Buiten RUBRIEK 7[43] van het meerjarig financieel kader								
Personele middelen								
Andere administratieve uitgaven	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotaal buiten RUBRIEK 7 van het meerjarig financieel kader	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
TOTAAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

De benodigde kredieten voor personeel en andere administratieve uitgaven zullen worden gefinancierd uit de kredieten van het DG die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

De bovenstaande kredieten die nodig zijn voor personele middelen en andere administratieve uitgaven buiten rubriek 7, komen overeen met de bedragen die worden gedekt door de financiële bijdrage van de Unie uit het programma Digitaal Europa.

De kredieten die nodig zijn voor personele middelen en andere administratieve uitgaven buiten rubriek 7, zullen worden verhoogd met de bedragen die worden gedekt door de financiële bijdrage van de Unie uit het programma Horizon Europa, zodra de bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21,

[43] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

lid 1, onder b), door de Commissie wordt voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt.

De bovenvermelde kredieten die nodig zijn voor personele middelen en andere administratieve uitgaven buiten rubriek 7, omvatten niet de bijdrage van de lidstaten aan de administratieve kosten van het kenniscentrum, die in verhouding staan tot de financiële bijdrage van de Unie.

3.2.2.1. Geraamde behoefte aan personele middelen voor de Commissie

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

– ■ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

Jaren		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)								
zetel en vertegenwoordigingen van de Commissie		20	21	21	21	21	21	22
Delegaties								
Onderzoek								
• Extern personeel (in voltijdequivalenten: VTE) – AC, AL, END, INT en JPD [44] Rubriek 7								
Gefinancierd uit RUBRIEK 7 van het meerjarig financieel kader	- zetel	3	3	3	3	3	3	3
	- delegaties							
Gefinancierd uit het budget van het programma [45]	- zetel							
	- delegaties							
Onderzoek								
Andere (geef aan welke)								
TOTAAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	Coördinatie, toezicht en sturing van de taken die aan het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zijn toevertrouwd, met inbegrip van ondersteunings- en coördinatiekosten. Ontwikkeling en coördinatie van het beleid op het gebied van cyberbeveiliging met betrekking tot de taken waarmee het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging wordt belast, bv. in verband met de vaststelling van prioriteiten voor onderzoeksbeleid en industrieel beleid, de algemene samenwerking tussen lidstaten en marktdeelnemers, de samenhang met het toekomstige EU-kader voor cyberbeveiligingscertificering, de werkzaamheden inzake aansprakelijkheid en zorgplicht, of coördinatie met beleid op het gebied van HPC, KI en digitale vaardigheden. .

44 AC = Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JPD = Jeune Professionnel en Délégation (jonge professional in delegaties).

45 Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

Extern personeel	Coördinatie, toezicht en sturing van de taken die aan het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zijn toevertrouwd, met inbegrip van ondersteunings- en coördinatiekosten. Ontwikkeling en coördinatie van het beleid op het gebied van cyberbeveiliging met betrekking tot de taken waarmee het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging wordt belast, bv. in verband met de vaststelling van prioriteiten voor onderzoeksbeleid en industrieel beleid, de algemene samenwerking tussen lidstaten en marktdeelnemers, de samenhang met het toekomstige EU-kader voor cyberbeveiligingscertificering, de werkzaamheden inzake aansprakelijkheid en zorgplicht, of coördinatie met beleid op het gebied van HPC, KI en digitale vaardigheden. .

3.2.2.2. Geraamde behoeften aan personele middelen voor het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging

	2021	2022	2023	2024	2025	2026	2027
Functionarissen van de Commissie							
Waarvan AD							
waarvan AST							
Waarvan AST-SC							
Tijdelijke functionarissen							
Waarvan AD	10	11	13	13	13	13	13
waarvan AST							
Waarvan AST-SC							
Arbeidscontractanten	26	32	39	39	39	39	39
Gedetacheerde nationale deskundigen	1	1	1	1	1	1	1
Totaal	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	Operationele uitvoering van de taken die overeenkomstig artikel 4 van deze verordening aan het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zijn toevertrouwd, met inbegrip van ondersteunings- en coördinatiekosten.
Extern personeel	Operationele uitvoering van de taken die overeenkomstig artikel 4 van deze verordening aan het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zijn toevertrouwd, met inbegrip van ondersteunings- en coördinatiekosten.

De bovenvermelde geraamde personeelsbehoeften van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging komen overeen met de geraamde behoeften voor de uitvoering van de financiële bijdrage van de Unie in het kader van Digitaal Europa.

De bovenvermelde geraamde personeelsbehoeften van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zullen worden verhoogd met de geraamde behoeften voor de uitvoering van de financiële bijdrage van de Unie in het kader van Horizon Europa, zodra de bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21, lid 1, onder b), door de Commissie wordt voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt.

3.2.2.3. Lijst van het aantal ambten van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging

Functiegroep en rang	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Totaal AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
Totaal AST							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Totaal AST/SC							
EINDTOTAAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Geraamde gevolgen voor het personeel (extra) – extern personeel van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging

Arbeidscontractanten	2021	2022	2023	2024	2025	2026	2027
Functiegroep IV	20	22	29	29	29	29	29
Functiegroep III	2	4	4	4	4	4	4
Functiegroep II	4	6	6	6	6	6	6
Functiegroep I							
Totaal	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Teneinde de neutraliteit in de personeelsbezetting te waarborgen zal het bijkomende personeel in het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging gedeeltelijk worden gecompenseerd door de verlaging van het aantal ambtenaren en externe personeelsleden in de betrokken diensten van de Commissie (dat wil zeggen de personeelsformatie en het extern personeel van dit moment).
Het aantal personeelsleden van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging in de punten 3.2.2.2 tot en met 3.2.2.4 wordt als volgt gecompenseerd[46]:

TOTAAL	2021	2022	2023	2024	2025	2026	2027
Functionarissen van de Commissie	5	5	6	6	6	6	6

[46] Afhankelijk van het definitieve bedrag van de begrotingsmiddelen die aan het kenniscentrum zullen worden toegewezen.

Tijdelijke functionarissen							
Arbeidscontractanten	14	17	20	20	20	20	20
Gedetacheerde nationale deskundigen							
Totaal aantal VTE's	19	22	26	26	26	26	26
Aantal personeelsleden	19	22	26	26	26	26	26

De compensatie van de personele middelen voor het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging zal in verhouding staan tot het aandeel van de financiële bijdrage van de Unie, d.w.z. 50 %.

De bovenvermelde compensatie heeft betrekking op de geraamde personeelsbehoeften van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging voor de uitvoering van de financiële bijdrage van de Unie in het kader van Digitaal Europa.

De bovenvermelde compensatie zal worden verhoogd met de geraamde behoeften voor de uitvoering van de financiële bijdrage van de Unie in het kader van Horizon Europa, zodra de bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21, lid 1, onder b), door de Commissie wordt voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt.

3.2.3. Bijdragen van derden

Het voorstel/initiatief:

– ☐ voorziet niet in medefinanciering door derden

– ☒ voorziet in de hieronder geraamde medefinanciering door derden[47]:

Kredieten in miljoenen euro's (tot op drie decimalen)

Jaren	2021	2022	2023	2024	2025	2026	2027	TOTAAL
Lidstaten – bijdrage aan de personeelsuitgaven	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Lidstaten – bijdrage aan infrastructuur en administratieve uitgaven	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Lidstaten – bijdrage aan operationele uitgaven	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTAAL medegefinancierde kredieten	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

De bovenvermelde bijdrage van derden heeft alleen betrekking op de medefinanciering die in verhouding staat tot de financiële middelen van de EU voor cyberbeveiliging in het kader van Digitaal Europa. De bovenvermelde bijdrage van derden wordt verhoogd zodra de financiële bijdrage uit het budget van de cluster "Inclusieve en veilige samenleving" van pijler II "Wereldwijde uitdagingen en industrieel concurrentievermogen" van Horizon Europa (totaal budget van 2 800 000 000 EUR), zoals vermeld in artikel 21, lid 1, onder b), door de Commissie wordt voorgesteld tijdens het wetgevingsproces en in elk geval voordat een politiek akkoord wordt bereikt. Het voorstel zal worden gebaseerd op de resultaten van het in artikel 6, lid 6, van Verordening XXX [kaderprogramma Horizon Europa] omschreven strategische planningsproces.

3.3. Geraamde gevolgen voor de ontvangsten

– ☒ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

☐ voor de eigen middelen

☐ voor de overige ontvangsten

Geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven ☐

in miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Gevolgen van het voorstel/initiatief[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**

47 Geraamde bijdrage in natura van de lidstaten

48 Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.

Artikel …….							

Vermeld voor de toegewezen ontvangsten het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

Andere opmerkingen (bijv. over de methode/formule voor de berekening van de gevolgen voor de ontvangsten of andere informatie).