22112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4286 Brief van de minister van Buitenlandse Zaken

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 maart 2026

Overeenkomstig de bestaande afspraken ontvangt u hierbij vier fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Verordening versterking *Carbon Border Adjustment Mechanism* en verordening Tijdelijk Fonds voor Koolstofvrijmaking (Kamerstuk 22 112, nr. 4283)
Fiche: Simplificatie NIS2-richtlijn (Kamerstuk 22 112, nr. 4284)
Fiche: Mededeling EU *Anti-Racism Strategy* 2026-2030 (Kamerstuk 22 112, nr. 4285)
Fiche: Herziening *Cybersecurity Act*

De minister van Buitenlandse Zaken,
T.B.W. Berendsen

Fiche: Herziening Cybersecurity Act

1. Algemene gegevens

a) Titel voorstel

Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

b) Datum ontvangst Commissiedocument

20 januari 2026

c) Nr. Commissiedocument

COM (2026) 11

d) EUR-Lex

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0011

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

SWD (2026)11

f) Behandelingstraject Raad

Raad voor Vervoer, Telecommunicatie en Energie (Telecomraad)

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid, in nauwe samenwerking met het ministerie van Economische Zaken en Klimaat

h) Rechtsbasis

Artikel 114 Verdrag betreffende de Werking van de Europese Unie (VWEU)

i) Besluitvormingsprocedure Raad
Gekwalificeerde meerderheid

j) Rol Europees Parlement
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 20 januari 2026 heeft de Europese Commissie (hierna: «de Commissie») de herziene versie van de Cybersecurity Act (hierna CSA) gepubliceerd. Deze herziening markeert een belangrijke verschuiving in het Europese cyberbeveiligingsbeleid.
Met de CSA beoogt de Europese Unie haar vermogen te versterken om digitale risico's te beheersen, de interne markt te beschermen en risicovolle strategische afhankelijkheden te verminderen. Deze hervorming moet worden gezien tegen de achtergrond van een steeds onvoorspelbaarder dreigingslandschap, toenemende geopolitieke spanningen en de groeiende verwevenheid tussen digitale infrastructuur, economische veiligheid en nationale weerbaarheid.

Het voorstel omvat drie onderdelen: het EU Agentschap voor Cyberbeveiliging (hierna: « ENISA»), een Europees kader voor cyberbeveiligingscertificering, en de beveiliging van ICT-toeleveringsketens.

Allereerst wordt het mandaat van ENISA uiteengezet. ENISA is een expertisecentrum op het gebied van cyberbeveiliging, en acteert als coördinerend en ondersteunend orgaan binnen diverse EU-samenwerkingsverbanden. Het mandaat van ENISA wordt via dit voorstel aanzienlijk versterkt voor de komende jaren. Zo wordt het huidige takenpakket van deze organisatie flink uitgebreid. ENISA zal een grotere rol gaan spelen op het gebied van de implementatie van beleid en regelgeving, operationele samenwerking, capaciteitsopbouw en (de ontwikkeling van) cyberbeveiligingscertificeringen. ENISA krijgt in het voorstel daarnaast de expliciete taak om de operationele samenwerking tussen de lidstaten te bevorderen, door een gezamenlijk situationeel bewustzijn, van informatie-

uitwisseling en betere tooling te faciliteren. ENISA zal ook een aanzienlijke rol vervullen op het gebied van incidentmanagement, en zal – zoals eerder aangekondigd via de Digitale Omnibus – een rol spelen rondom het beheer van een Europees toegangspunt voor incidentmeldingen.[1] Verder zal ENISA ook nieuwe taken vervullen op het gebied van kwetsbaarhedenmanagement, door middel van de inrichting van een (kwetsbaarheden)platform en early alerts dienst voor CSIRT's en entiteiten. Op het gebied van ransomware krijgt ENISA de taak om trends te signaleren en aanvallen te monitoren, alsook de opdracht om entiteiten te helpen bij ransomware aanvallen, door de inrichting van een helpdesk. Verder wordt ENISA verantwoordelijk gesteld voor de ontwikkeling van de Cybersecurity Skills Academy, en krijgt zij in dit kader ook een belangrijke rol als het gaat om de ontwikkeling van het EU-raamwerk voor cyberbeveiligingsvaardigheden (ECSF). Ook dient ENISA een attestatie schema voor cybervaardigheden te ontwikkelen op basis waarvan individuen vrijwillig kunnen aantonen dat zij over de benodigde cyberbeveiliging kennis beschikken. Een dergelijk bewijs zou uitgegeven moeten kunnen worden via Europese Digitale Identiteit (EUDI)-wallets. De uitbreiding van het takenpakket van ENISA gaat gepaard met een groei van 81,5% van het budget voor ENISA, wat zich vertaalt in 118 fte's extra. Ook stelt de Commissie een vergoedingsmechanisme voor waarbij organisaties bijdragen aan het ENISA-budget middels vergoedingen voor diensten die ENISA levert op het gebied van bijvoorbeeld certificeringen en de ontwikkeling van tooling. Ook zijn er wijzigingen gemaakt als het gaat om de governancestructuur van het agentschap: de Commissie krijgt een vetorecht binnen de Management Board, en lidstaten worden gevraagd om tenminste twee verbindingsfunctionarissen aan te wijzen voor ENISA om operationele samenwerking te ondersteunen.

De reikwijdte van het al bestaande Europese (cyber)certificeringsraamwerk wordt met dit voorstel aanzienlijk versterkt, waarbij veel van de bestaande CSA nog steeds van toepassing is. Certificering zal gebaseerd blijven op technische risicofactoren en vereisten. Daarnaast beperkt dit raamwerk zich niet langer tot producten, diensten en processen, maar kan het ook betrekking hebben op de algehele cyberweerbaarheid van organisaties, met name van essentiële entiteiten en belangrijke entiteiten in kritieke sectoren. Hiermee sluit het

[1] Zoals reeds voorgesteld in de Digitale Omnibus, zie: Fiche Omnibus AI en Omnibus Digitaal (Kamerstuk 22 112, nr. 4223).

certificeringsraamwerk zich nauwer aan bij de risicobenadering van de NIS2-richtlijn. Een tweede kernpunt van het voorstel is de expliciete inzet van certificering ter ondersteuning van naleving van EU-wetgeving. Door certificering te koppelen aan een vermoeden van conformiteit met andere cyberbeveiligingsverplichtingen, beoogt de Commissie fragmentatie te verminderen en administratieve lasten te verlagen. Dit zal volgens de Commissie bijdragen aan de versterking van de interne markt en het vergroten van de uitvoerbaarheid van EU-regelgeving. Deze wetswijziging versterkt ook de rol van ENISA als centrale uitvoerende en coördinerende autoriteit op het gebied van cyberbeveiligingscertificering. Door snellere besluitvorming, vaste termijnen en structureel onderhoud van certificeringsschema's wordt beoogd de effectiviteit en voorspelbaarheid van cyberbeveiligingscertificeringen te vergroten. Dit ondersteunt de ambitie om de Europese Unie als geloofwaardige en slagvaardige actor op het gebied van cyberbeveiliging te positioneren. Daarnaast wordt het juridische karakter van certificering versterkt. Waarmee het een instrument wordt met afdwingbare rechtsgevolgen. Dit versterkt de handhaafbaarheid van EU-cyberbeveiligingsbeleid en de rol van nationale autoriteiten binnen een gemeenschappelijk kader. Een wezenlijk nieuw element is de expliciete koppeling tussen certificering en cyberrisico's in ICT-toeleveringsketens. Leveranciers die als hoog risico worden aangemerkt, bijvoorbeeld vanwege eigendoms- of controlevraagstukken in derde landen, kunnen feitelijk worden uitgesloten van Europese cyberbeveiligingscertificering. Ook geeft het (cyber)certificeringskader de Commissie meer mogelijkheden om met internationale partners in gesprek te gaan over wederzijdse erkenning van certificeringen en gemeenschappelijke veiligheidsnormen en deze middels uitvoeringswetgeving te implementeren. De Commissie gaat haar prioritering voor de ontwikkeling van cyberbeveiligingsschema's met belanghebbenden bespreken in minimaal jaarlijks georganiseerde European Cybersecurity Certification Assembly en publiceert deze op een speciale website.

Het voorstel beoogt daarnaast de beveiliging van de ICT-toeleveringsketens van essentiële entiteiten en belangrijke entiteiten in kritieke sectoren, zoals bedoeld in de NIS2-richtlijn, te versterken tegen (cyber)dreigingen. De Commissie richt hiertoe een raamwerk in voor vertrouwde ICT-toeleveringsketens (hierna: het raamwerk) dat niet-technische risico's adresseert, zoals bijvoorbeeld aanvallen van kwaadwillende actoren in de vorm van digitale spionage of sabotage. De Commissie stelt voor om dit raamwerk ook direct na inwerkingtreding van de

verordening toe te passen op elektronische communicatienetwerken. Hiermee kunnen kritieke ICT-componenten voor ICT-toeleveringsketens, afkomstig van leveranciers uit derde landen met een hoog risico (hierna: de hoog-risico leveranciers) uiteindelijk verplicht worden uitgefaseerd.
Dit raamwerk gaat over het door de Commissie bepalen van de kritieke ICT-onderdelen van essentiële en belangrijke entiteiten in relatie tot risico's vanuit de ICT-toeleveringsketen, het aanmerken van – kort gezegd – derde landen die een risico kunnen vormen voor de cyberveiligheid van de Europese Unie en hoog-risico leveranciers uit die derde landen. De Commissie kan in dit kader risico mitigerende maatregelen aan entiteiten. Daarbij wordt deze beoordeling door de Commissie gebaseerd op de bestaande 'EU gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens' (hierna: beveiligingsrisicobeoordelingen), voortvloeiend uit de NIS 2-richtlijn. Een werkgroep binnen de NIS Cooperation Group voert deze beveiligingsrisicobeoordelingen uit. Met dit nieuwe voorstel kan de Commissie, of een groep van ten minste drie lidstaten, deze gecoördineerde beveiligingsrisicobeoordelingen aanvragen via de NIS Cooperation Group.
Wanneer de Commissie voldoende redenen ziet om, op basis van voornoemde beveiligingsbeoordelingen, aan te nemen dat sprake is van een significante cyberdreiging, dan heeft de Commissie de mogelijkheid om zelfstandig beveiligingsrisicoanalyses uit te voeren. In het kader van deze beoordelingen wordt onder meer meegenomen welke kritieke ICT-onderdelen in relatie tot de ICT-toeleveringsketen er zijn, welke risico's en kwetsbaarheden daarvoor gelden én welke actoren mogelijk een dreiging vormen. De Commissie krijgt naast deze zelfstandige beveiligingsanalyses de mogelijkheid om lidstaten te raadplegen over de noodzaak tot het nemen van EU brede mitigerende maatregelen.
Indien er uit genoemde beveiligingsbeoordelingen of andere bronnen blijkt dat een derde land een risico vormt, kan de Commissie aan de hand van een aantal criteria eigenstandig verifiëren of dit daadwerkelijk zo is. Als dit risico wordt vastgesteld kan de Commissie vervolgens via een uitvoeringshandeling een derde land aanwijzen als een land dat 'cyberveiligheidszorgen' met zich meebrengt. In vervolg hierop zal de Commissie door middel van uitvoeringshandelingen lijsten opstellen van hoog-risico-leveranciers, op basis van een beoordeling waaruit blijkt welke leveranciers gevestigd zijn of onder invloed staan van derde landen die volgens de Commissie 'cyberveiligheidszorgen' met zich meebrengen. Deze hoog-risico leveranciers

mogen niet meer deelnemen aan bepaalde activiteiten binnen de interne markt, zoals bijvoorbeeld aanbestedingen en financieringsprogramma's.
De Commissie krijgt tevens de mogelijkheid om kritieke ICT-onderdelen van essentiële en belangrijke entiteiten te identificeren op basis van een aantal criteria. Vervolgens kan de Commissie via uitvoeringshandelingen - op basis van eerdergenoemde aanwijzingen van hoog-risico-leveranciers en kritieke ICT-onderdelen- mitigerende maatregelen nemen ten aanzien van essentiële en belangrijke entiteiten. Deze maatregelen betreffen met name, en via uitvoeringsonderhandelingen, de oplegging van een verbod aan specifieke groepen essentiële en belangrijke entiteiten om ICT-componenten van hoog-risico leveranciers in kritieke ICT-onderdelen te gebruiken, installeren of integreren. De Commissie kan aan de entiteiten tevens vragen om (verplichte) audits uit te voeren voor bepaalde essentiële ICT-onderdelen, of verplichtingen opnemen met betrekking tot operationele maatregelen zoals segmentatie van netwerksystemen.

Het voorstel past dit raamwerk direct toe op elektronische communicatienetwerken, omdat de reeds vastgestelde toolbox inzake 5G-beveiliging hiervoor voldoende aanleiding biedt volgens de Commissie. ICT-componenten die aangeboden worden door leveranciers die al bestempeld zijn als hoog-risico leveranciers, dienen binnen 36 maanden na inwerkingtreding van deze wet, daarmee te worden uitgefaseerd uit de belangrijkste ICT-onderdelen binnen mobiele elektronische communicatienetwerken.
Daarnaast doet de Commissie het voorstel om het raamwerk toe te passen op vaste communicatie en satellietnetwerken, in samenhang met de Digital Networks Act. De uitfaseringsperiode voor vaste en satellietnetwerken worden nader vastgesteld in uitvoeringshandelingen.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De Nederlandse Cybersecuritystrategie (NLCS) zet de vier pijlers uiteen van de kabinetsinzet voor het realiseren van een digitaal veilige en weerbare samenleving. Naast acties en samenwerking op nationaal niveau, benadrukt de NLCS dat internationale samenwerking, zowel in EU en NAVO-verband als daarbuiten, essentieel is gezien het grensoverschrijdende karakter van cyberdreigingen. Het kabinet zet zich daarom actief in bij de verschillende

Europese gremia en samenwerkingsverbanden met als doel de digitale weerbaarheid van de EU te vergroten.

In pijler II van de NLCS wordt het belang van veilige en innovatieve digitale producten en diensten benadrukt, waarin het kabinet zich tot doel stelt in samenwerking met private partijen bij te dragen aan de ontwikkeling en aanname van Europese cyberbeveiligingscertificeringschema's voor ICT-producten, diensten en processen. Dit is onder meer tot uiting gekomen in de constructieve Nederlandse inzet bij de ontwikkeling van cyberbeveiligingsschema’s zoals het EUCC en het aangekondigde EUCS.

Het kabinet onderschrijft daarnaast de verbondenheid van Europese economieën op de interne markt en de ambitie om deze te versterken. Om deze reden streeft kabinet ernaar om maatregelen op het gebied van economische veiligheid in samenhang met de EU te ontwikkelen, en de effectiviteit van deze maatregelen te vergroten en alsmede gelijk Europees speelveld te waarborgen. Dit draagt bij aan het beperken van de lastendruk voor internationaal opererende bedrijven en kennisinstellingen en het creëren van kansen voor Nederlandse bedrijven in Europa.

Daarnaast implementeert het kabinet de Critical Entities Resilience Directive (CER) en de Network and Information Security Directive (NIS2) richtlijnen ter versterking van de bescherming van vitale infrastructuur en de (digitale) weerbaarheid van essentiële en belangrijke entiteiten. Het kabinet zet zich actief in op bilaterale en multilaterale samenwerking om oneerlijke handelspraktijken tegen te gaan, de markttoegang voor Nederlandse bedrijven te vergroten en vanuit Europa gezamenlijk op te treden tegen statelijke actoren.

Het kabinet investeert tevens doorlopend in bewustwording op nationaal niveau, kennisopbouw, en handelingsperspectief ter versterking van digitale en fysieke weerbaarheid. Omdat het beheersen van risico’s in de toeleverancierskеten van groot belang is voor het digitaal veilig functioneren van publieke en private organisaties, heeft het kabinet de handreiking ´Cybercheck: ook jij hebt supply chain risico’s!´ gepubliceerd. Deze handreiking biedt entiteiten handvatten om te inventariseren of de inzet van een bepaald product of dienst afkomstig uit een land met een offensief cyberprogramma mogelijk tot een verhoogd

beveiligingsrisico leidt. Daarnaast is TNO verzocht om een zelfscantool te ontwikkelen waarmee vitale aanbieders een risicoafweging kunnen maken van hardware en software ten aanzien van operationele technologie van leveranciers uit risicolanden.

De inzichten uit bovengenoemde handreiking en de zelfscantool zijn verspreid en worden geïncorporeerd in de risicobeoordelingen die op grond van de Cbw en Wwke moeten worden uitgevoerd door kritieke entiteiten.

In juni 2023 is de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) in werking getreden. Deze wet geldt voor vitale aanbieders, bedrijven actief op het gebied van sensitieve technologie en beheerders van bedrijfscampussen. Op basis van deze wet moeten wijzigingen in zeggenschap of significante invloed bij vitale aanbieders, ondernemingen die actief zijn in sensitieve technologie en beheerders van bedrijfscampussen worden gemeld.

Op 6 december 2019 is het Besluit veiligheid en integriteit telecommunicatie (Bvit) van kracht geworden. Daarin is geregeld dat bij ministeriële regeling nadere regels kunnen worden gesteld met betrekking tot de in artikel 11a.1 van de Telecommunicatiewet bedoelde zorgplicht. Eveneens kunnen op grond van Bvit aanbieders van openbare elektronische communicatienetwerken en -diensten worden verplicht om in daarbij aangewezen onderdelen van hun netwerk niet langer gebruik te maken van door de minister van EZ aangewezen leveranciers als dat een gevaar voor de nationale veiligheid oplevert.

Ten slotte constateert het kabinet dat er in belangrijke mate rekening is gehouden met aandachtspunten die Nederland, mede op basis van de non-paper inzake de herziening van de Cybersecurity Act, heeft ingebracht.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt de doelstelling van de Commissie om de weerbaarheid van de EU te bevorderen door de versterking van de rol van ENISA binnen het cyberstelstel, de consolidatie van het certificeringsstelsel en de aansluiting daarvan op andere EU-regelgeving, alsook de bekrachtiging van een EU-instrumentarium om EU brede risico’s te mitigeren en risicovolle leveranciers te weren. Het kabinet ziet de herziening van de CSA tevens als een mogelijkheid

om aandacht te besteden aan de scope en reikwijdte van de wet, met name als het gaat om (de eenduidigheid van) definities.

Het kabinet kijkt positief naar de verduidelijking en aanscherping van het mandaat aangaande ENISA in het voorstel. De rol van ENISA om als expertisecentrum best practices te ontwikkelen op het gebied van NIS2-verplichtingen, zoals risicomanagement en volwassenheidsmetingen, wordt in het bijzonder positief beoordeeld. Ook ondersteunt het kabinet het voorstel om de samenwerking tussen nationale CSIRT's te verbeteren met de ontwikkeling van tooling door ENISA, en de bevordering van een beter gezamenlijk situationeel bewustzijn, om de cyberweerbaarheid te verhogen. Daarnaast is het kabinet tevreden over de expliciete rol die aan ENISA is toebedeeld op het gebied van capaciteitsopbouw en het voorbereiden op de impact van nieuwe technologieën op cyberbeveiliging. ENISA zal als ondersteunend orgaan fungeren voor nationale CSIRT's, om hiermee de capaciteit te vergroten op het gebied van o.a. detectie, preventie en incidentmanagement. ENISA draagt op deze wijze effectief bij aan de versterking van bestaande nationale en EU-structuren binnen het cyberlandschap.

Nationale CSIRT's spelen namelijk een centrale rol binnen het cyberlandschap. Het investeren in deze structuren draagt bij aan de versterking van de weerbaarheid van de Unie.

Het kabinet benadrukt in dit kader dat ENISA geen (operationele) taken toebedeeld dient te krijgen en dient uit te voeren die raken aan nationale competenties of overlappen met al bestaande nationale structuren en dienstverlening. Het kabinet kijkt om deze reden kritisch naar het opzetten van een '*early alert'* helpdesk door ENISA, en heeft vragen over voorgestelde rol om steun te verlenen rondom ransomware incidenten en de link naar rechtshandhaving en opsporing. Het kabinet ziet overlap met bestaande structuren en (nationale) competenties, waaronder de dienstverlening van nationale CSIRT's en het mandaat van Europol. Ook kijkt het kabinet terughoudend naar de verantwoordelijkheid die aan ENISA is toebedeeld om rechtstreeks met Nederlandse organisaties te schakelen. Deze taak dient te worden behouden door nationale CSIRT's, om daarmee ook verwarring te voorkomen richting entiteiten. Het kabinet zet tevens grote vraagtekens bij de toebedeling van twee liaisons officers, aangezien hun rol lijkt te overlappen met

de reeds bestaande leden binnen het CSIRT-netwerk. Ook zijn er grote vraagtekens over de wenselijkheid om ENISA als volwaardig lid aan te merken voor het CSIRT-netwerk.

Ten aanzien van skills en de ontwikkeling en het beheer van gezamenlijke cyberveiligheidsoplossingen voor CSIRT's acht het kabinet het van belang dat nieuwe taken van ENISA niet overlappen met taken die al zijn toebedeeld aan bijvoorbeeld het ECCC, en benadrukt zij het belang van samenhang en effectieve samenwerking. Verder ziet het kabinet minder meerwaarde in de rol van ENISA op het gebied van cyberrisico bewustwording, alsook de uitvoering van analyses van de markt op het gebied van technologische ontwikkelingen. Het kabinet heeft echter geen bezwaren tegen de mogelijkheid om een attestatie voor cyberbeveiligingsvaardigheden uit te geven via EUDI-wallets, maar wijst wel op het vrijwillig gebruik van EUDI-wallets en het belang om ook zonder EUDI-wallet een bewijs van cyberbeveiligingsvaardigheden te kunnen delen. Ten aanzien van normalisatie stelt het kabinet dat de rol die hiervoor reeds is belegd bij CEN-CENELEC en ETSI, en dat nationale normalisatieorganisaties behouden dienen te blijven. De versterkte rol die ENISA krijgt toebedeeld dient complementair hieraan te blijven.

Ook stelt het kabinet vraagtekens bij de rol van ENISA ten aanzien van een Europees centraal platform voor rapportageverplichtingen, daar waar de zorgen die het kabinet reeds in het BNC- fiche heeft geuit aangaande de Digitale Omnibus, op het moment van dit schrijven, nog niet zijn weggenomen.

Het kabinet kijkt overwegend positief naar het voorgestelde certificeringsraamwerk, maar hecht groot belang aan een zorgvuldige en proportionele uitwerking van het voorstel waarbij een belangrijke rol van de lidstaten in het certificeringsraamwerk behouden blijft. Het kabinet heeft zich de afgelopen jaren hard gemaakt om te zorgen dat certificering technisch van aard blijft, de Commissie heeft dit omarmt in dit voorstel.

Het kabinet onderschrijft de noodzaak om Europese cyberbeveiligingscertificering effectiever te maken en het proces efficiënter in te richten, mits dit niet leidt tot onnodige lastenverzwaring, handelsproblemen, centralisatie zonder voldoende lidstaatinvloed of een verplichtstelling van certificering. Het kabinet heeft echter

twijfels of de genoemde termijnen voor het opstellen van certificatieschema’s reëel zijn en leiden tot kwalitatief goede resultaten.

Het kabinet staat positief tegenover de verbreding van certificering naar de cyberweerbaarheid van entiteiten, maar benadrukt dat deze uitbreiding duidelijk afgebakend moet blijven. Certificering van entiteiten mag toezicht niet vervangen en mag niet leiden tot automatische vrijstellingen van wettelijke verplichtingen onder NIS2-richtlijn, CRA en DORA. Ook benadrukt het kabinet dat Europese cyberbeveiligingscertificering onder de Cybersecurity Act niet kan worden gelijkgesteld aan, noch in de plaats kan treden van, de specifieke assurance-, toezicht- en notificatievereisten die gelden onder eIDAS voor elektronische identificatiemiddelen, vertrouwensdiensten en EUDI-wallets.

Het kabinet ondersteunt het principe van certificering als hulpmiddel bij het aantonen van naleving van wettelijke voorschriften, mits dit leidt tot aantoonbare lastenverlichting en geen extra administratieve verplichtingen creëert. Daarbij acht het kabinet het van belang dat nationale toezichthouders ruimte behouden voor risico gebaseerd toezicht.

Het kabinet ziet meerwaarde in een versterkte rol van ENISA in relatie tot dit raamwerk, maar acht het essentieel dat lidstaten substantieel betrokken blijven bij strategische keuzes, waaronder de prioritering van certificeringsschema’s, alsmede de beoordeling en goedkeuring van individuele certificeringsschema’s en de internationale erkenning van certificaten. De bevoegdheid van ENISA tot het ontwikkelen van technische specificaties dient transparant te worden toegepast en niet te leiden tot feitelijke normstelling zonder de waarborgen die zijn opgenomen in de richtlijnen rond standaardisatie. Het kabinet erkent het belang van het adresseren van toeleveringsketen-risico’s via het certificeringskader, maar benadrukt dat uitsluiting van leveranciers uitsluitend risico gebaseerd, juridisch houdbaar en niet-discriminatoir dient plaats te vinden. Daarnaast hecht het kabinet eraan dat de voorgestelde maatregelen in overeenstemming met de internationale verplichtingen van de EU worden vormgegeven, waaronder de akkoorden van de Wereldhandelsorganisatie (WTO) en bilaterale handelsakkoorden.

Het kabinet vraagt ook aandacht voor de uitvoerbaarheid voor nationale autoriteiten en de administratieve gevolgen voor bedrijven, met name het MKB. Nieuwe verplichtingen dienen te worden voorzien van duidelijke overgangstermijnen en samenloop met bestaande nationale toezichtstructuren moet worden voorkomen.

Het kabinet kijkt positief naar het doel van het voorstel om op Europees niveau cyberrisico’s voor essentiële onderdelen in kritieke ICT-toeleveringsketens te mitigeren. De toenemende geopolitieke en geo-economische spanningen, in combinatie met de groeiende complexiteit van (cyber)beveiligingsuitdagingen in een onderling verbonden digitale interne markt, benadrukken het belang van een Europese aanpak. Dit draagt bij aan een gelijk speelveld binnen de interne markt, voorkomt ongewenste overloopeffecten en realiseert een hoger en consistenter niveau van cyberbeveiliging in de Unie. Tegelijkertijd blijft het kabinet zich inzetten voor de totstandbrenging van internationaal weerbare en betrouwbare waardeketens met partnerlanden, wat cruciaal is om kwetsbaarheden te verminderen en de (economische) veiligheid te waarborgen. Dit vereist een op risico's gebaseerde aanpak om marktverstoring zoveel mogelijk te voorkomen.

Het kabinet is positief over het principe om op basis van een beveiligingsrisicobeoordeling maatregelen te formuleren, gericht op specifieke producten of diensten van specifieke leveranciers, die uiteindelijk een bindend karakter kunnen krijgen binnen de EU. Hoewel lidstaten volgens het kabinet op zich het beste in staat zijn om de noodzaak van maatregelen vanwege risico’s voor de beveiliging van ICT-systemen op het niveau van specifieke entiteiten te beoordelen, draagt een gezamenlijk beeld van de lidstaten bij aan het (waar passend) zo uniform mogelijk treffen van maatregelen binnen de Unie.

Wel betwijfelt het kabinet of de bestaande beveiligingsrisicobeoordelingen hiervoor op dit moment het geijkte middel zijn. Allereerst vindt het kabinet dat de huidige beveiligingsrisicobeoordelingen kwalitatief onvoldoende robuust zijn om als basis te dienen voor de voorgestelde, bindende en daarmee impactvolle maatregelen. Tevens is bepaalde benodigde informatie, vanwege het gevoelige karakter ervan, alleen op nationaal niveau beschikbaar.

Ook heeft het kabinet zorgen over de verstrekkende bevoegdheden voor de Commissie om derde landen als geheel aan te wijzen als ‘een land dat cyberzorgen met zich meebrengt’, en leveranciers aan te wijzen als zijnde ‘hoog risico’. Deze aanwijzingen, en de daarmee verband houdende voorgestelde maatregelen, vergen niet alleen een technisch-juridische, maar ook een politieke afweging vanwege mogelijk verstrekkende diplomatieke en economische gevolgen. Het kabinet acht het daarom van belang dat geopolitieke afwegingen voldoende zijn gewaarborgd bij een eventuele aanwijzing van een land of leverancier. Het voorstel roept ook de fundamentele vraag op hoe de Commissie een derde land of leverancier als geheel kan kwalificeren als risico, omdat de mate van risico sterk afhankelijk is van een geleverde dienst of product en op welke dienstlevering of activiteit een dienst of product wordt toegepast. Dat is ook de reden dat het kabinet op nationaal niveau bewust een landen-neutrale, risico-gerichte, casus-specifieke aanpak hanteert. Het kabinet zal zich inzetten een evenwichtige rolverdeling tussen de Europese Commissie en de lidstaten binnen dit raamwerk, met een stevigere rol van de lidstaten in alle onderdelen van het proces om de kwaliteit van de beveiligingsrisicobeoordelingen en de proportionaliteit en uitvoerbaarheid van maatregelen te waarborgen.

Het kabinet ziet de meerwaarde van een aanpak op Europees niveau, maar benadrukt wel dat ICT-toeleveringsketens, en ook de geldende nationale wetgeving in dat verband, sterk kunnen verschillen tussen lidstaten onderling. De mitigerende maatregelen binnen het raamwerk dienen recht te doen aan deze onderlinge verscheidenheid. Het kabinet wijst hierbij op de complexiteit van de voorgestelde maatregelen voor entiteiten en zal daarom de praktische uitvoerbaarheid en proportionaliteit ervan doorlopend inbrengen als aandachtspunt in de verdere onderhandelingen. Het kabinet zet daarmee in op een raamwerk dat voldoende maatwerk kan bieden, en waarbinnen de samenhang tussen nationale en Europese instrumenten wordt geborgd.

Tot slot gaat het voorstel onvoldoende in op belangrijke praktische en juridische randvoorwaarden voor alle stappen in de voorgestelde procedures, waaronder de

rechtsbescherming in alle fases van het proces ,voor entiteiten en hoog-risico-leveranciers.

Het kabinet hecht waarde aan het opnemen van de nodige waarborgen in het proces om tot een gedegen oordeel over mitigerende maatregelen te komen.

Wat betreft de toepassing op elektronische communicatienetwerken, ondersteunt het kabinet de doelstelling om de weerbaarheid van kritieke elektronische communicatienetwerken te vergroten. Tegelijkertijd, benadrukt het kabinet dat de maatregelen sterk ingrijpen in markttoegang, en investeringsvrijheid. De maatregelen voor de ICT-toeleveringsketen in de elektronische telecommunicatienetwerken hebben in potentie ingrijpende gevolgen voor zowel entiteiten als de leveranciers. Het kabinet steunt deze maatregelen dan ook voorwaardelijk, en is van mening dat de stappen uit het voorgestelde generieke raamwerk in eerste instantie moeten worden doorlopen, voordat besloten kan worden welke maatregelen uiteindelijk noodzakelijk zijn.

Voor mobiele netwerken vraagt dit een nadere robuuste beveiligingsrisicobeoordeling met actualisatie van de gecoördineerde 5G risicobeoordeling uit 2019. Voor vaste- en satellietcommunicatienetwerken vraagt dit om een specifieke beveiligingsrisicobeoordeling op Europees niveau. Ten aanzien van de verplichte uitfasering benadrukt Nederland dat proportionaliteit en uitvoerbaarheid randvoorwaardelijk zijn. Onvoldoende flexibele of te korte transitieperiodes kunnen leiden tot aanzienlijke economische schade, verstoring van essentiële diensten en verminderde investeringszekerheid. Het kabinet signaleert daarnaast dat in het voorstel een koppeling wordt gelegd tussen naleving van de verplichtingen en mogelijke gevolgen voor frequentievergunningen, onder meer via andere Europese wetgevingsinitiatieven. Aangezien spectrumtoegang essentieel is voor mobiele aanbieders, betwijfelt het kabinet of het intrekken van een frequentievergunning in dit kader als een proportionele sanctiemogelijkheid moet worden gezien.

c) Eerste inschatting van krachtenveld

De verwachting is dat een brede meerderheid van lidstaten het voorstel positief zal benaderen, mede gezien het verslechterde cyberdreigingslandschap. De positie van het Europees Parlement is onbekend.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet of de EU handelt binnen de grenzen van de bevoegdheden die haar door de lidstaten in de EU-verdragen zijn toegedeeld om de daarin bepaalde doelstellingen te verwezenlijken. Het oordeel van het kabinet ten aanzien hiervan is voor dit voorstel positief. Het voorstel is gebaseerd op artikel 114 VWEU. Artikel 114 VWEU geeft de EU de bevoegdheid tot het vaststellen van harmoniserende maatregelen betreffende de interne markt. Hoewel dit voorstel ook zaken regelt die eerder zien op openbare orde en veiligheid, is het kabinet van mening dat deze rechtsgrondslag desondanks passend is. Op het terrein van de interne markt is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, tweede lid, sub a, VWEU).

Wel zal het kabinet om nadere toelichting vragen over hoe het gebruik van artikel 114 VWEU als rechtsgrondslag zich verhoudt tot het onderdeel van het voorstel dat ziet op de ICT-toeleveringsketen, waarbij harmonisatie wordt beoogd met betrekking tot een cyberveilige toeleveringsketen en het weren van leveranciers door rechtstreeks werkende maatregelen die door de Commissie worden opgelegd, in plaats van aanpassing van reeds bestaande nationale wettelijke en bestuursrechtelijke bepalingen zoals benoemd in artikel 114 VWEU.

Tenslotte benadrukt het kabinet dat nationale veiligheid op grond van het Verdrag betreffende de Europese Unie een uitsluitende verantwoordelijkheid van de lidstaten is en dat het de lidstaten vrijstaat om op nationaal niveau op basis van een eigenstandige afweging ten aanzien van dreigingen vanuit leveranciers uit derde landen zelf met name ook te beslissen dat producten van leveranciers worden geweerd indien dit ter bescherming van de nationale veiligheid noodzakelijk is.

b) Subsidiariteit

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet de subsidiariteit van het optreden van de Commissie. Dit houdt in dat het kabinet op de gebieden die niet onder de exclusieve bevoegdheid van de Unie vallen of wanneer sprake is van een voorstel dat gezien zijn aard enkel door de EU kan worden uitgeoefend, toetst of het overwogen optreden niet voldoende door de lidstaten op centraal, regionaal of lokaal niveau kan worden verwezenlijkt, maar vanwege de omvang of de gevolgen van het overwogen optreden beter door de Unie kan worden bereikt (het subsidiariteitsbeginsel).

Het oordeel van het kabinet ten aanzien van de subsidiariteit is positief, met een kanttekening. De verordening heeft tot doel het versterken en harmoniseren van het EU-kader voor cyberbeveiliging door het herzien van de rol en taken van ENISA, het verder ontwikkelen van een Europees cybersecurity-certificeringskader en het versterken van de beveiliging van ICT-leveringsketens binnen de interne markt. Gezien grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt, daarom is een EU-aanpak wel nodig. Door het vaststellen van geharmoniseerde regels en gemeenschappelijke normen wordt het gelijk speelveld op het terrein van interne markt verbeterd. Om die redenen is optreden op het niveau van de EU gerechtvaardigd.

Wel plaatst het kabinet een kanttekening bij het uitbreiden van de rol van ENISA met operationele takenomdat deze taken beter op nationaal niveau kunnen worden uitgevoerd. Deze taken zouden overlappen met de bestaande nationale structuren ten aanzien van onderling samenwerken en het rechtstreeks uitwisselen van operationele informatie. Deze taken worden nu al voldoende uitgevoerd door de CSIRT’s van lidstaten, zonder duidelijke indicaties dat dit beter op Unieniveau zou kan kunnen worden opgepakt. In de uitvoering van deze taken is er dan ook ogenschijnlijk geen gerechtvaardigde reden voor optreden specifiek op het Unieniveau.

c) Proportionaliteit

Als onderdeel van de toets of de EU mag optreden conform de EU-verdragen toetst het kabinet of de inhoud en vorm van het optreden van de Unie niet verder gaan dan wat nodig is om de doelstellingen van de EU-verdragen te verwezenlijken (het proportionaliteitsbeginsel). Het oordeel van het kabinet ten aanzien van de proportionaliteit is positief, met een kanttekening en een aandachtspunt.

De verordening heeft tot doel het versterken en harmoniseren van het EU-kader voor cyberbeveiliging door het herzien van de rol en taken van ENISA, het verder ontwikkelen van een Europees cybersecurity-certificeringskader en het versterken van de beveiliging van ICT-leveringsketens binnen de interne markt. Het voorstel is geschikt om deze doelstelling te bereiken, omdat de voorgestelde acties, zoals bijvoorbeeld het versterken van het certificeringsraamwerk en de veiligheid van de toeleveringsketen, wezenlijk bijdragen aan Europese cyberbeveiliging en effectief worden geacht in het helpen realiseren van versterkte en geharmoniseerde cyberveiligheid binnen de EU. Bovendien gaat het voorgestelde optreden in het algemeen niet verder dan noodzakelijk, nu in het voorstel grotendeels voldoende rekening houdt met de expertise van de lidstaten en nationale structuren en daarmee voldoende ruimte overlaat aan de lidstaten.

Het kabinet plaatst echter een kanttekening bij met name de criteria voor het aanwijzen van hoog-risico leveranciers ten aanzien van de ICT-toeleveringsketen én het opleggen van het verbod aan entiteiten om in kritieke ICT-onderdelen ICT-componenten van die leveranciers te gebruiken, des te meer nu de gevolgen hiervan groot zijn. Ook de procedure voor het identificeren van essentiële ICT-onderdelen in relatie tot de veiligheidsrisicobeoordeling van de Commissie en de NIS2-groep is onvoldoende duidelijk, maar is tegelijkertijd een wezenlijk element voor de mitigerende maatregelen die op een dergelijke identificatie kunnen volgen. Het kabinet is van mening dat de criteria zoals die nu zijn opgeschreven onduidelijk en breder dan noodzakelijk zijn om het doel van het voorstel te bereiken, evenals dat de procedure voor het identificeren van essentiële ICT-onderdelen nader dient te worden toegelicht. Het kabinet stelt als minder vergaand alternatief voor dat deze criteria nader worden afgebakend en

ingeperkt, en zal aandringen op nadere toelichting omtrent de identificatie van essentiële ICT-onderdelen.

Ook plaatst het kabinet een aandachtspunt bij de maatregelen omtrent certificering. Voor het kabinet is belangrijk dat verdubbelingen en overlap met bestaande certificeringsstructuren worden voorkomen, om zo een effectief en adequaat raamwerk te ontwikkelen. Het kabinet zal op nadere toelichting aandringen over hoe dit zal worden voorkomen.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

De Commissie raamt voor de versterking van het mandaat van het Europees Agentschap voor Cybersecurity (ENISA) een totaalbudget van € 341 miljoen voor de periode 2028–2034.

Daarnaast voorziet het voorstel in 118 extra FTE bij ENISA en 50 extra FTE bij de Europese Commissie. Het kabinet is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Voor zover uitgaven betrekking hebben op de periode na 2027 geldt dat het kabinet niet vooruit wil lopen op de integrale afweging van middelen na 2027.

Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de ER-conclusies van juli 2020 over het MFK-akkoord. Het kabinet is kritisch over de stijging van het aantal werknemers.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of medeoverheden

De Commissie raamt in de toelichting toezichtskosten voor publieke autoriteiten in de gehele Unie van maximaal € 80 miljoen over een periode van vijf jaar (rekening houdend met relevante kostenbesparingen). (Eventuele) budgettaire gevolgen voor de Nederlandse rijksoverheid worden ingepast op de begroting

van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

Nederland zet zich in voor het verminderen van regeldruk en het bevorderen van betere regelgeving, zoals vastgelegd in het Actieprogramma Minder Druk Met Regels (MDMR).[2] In lijn met deze inzet is een van de uitgangspunten van het kabinet in de non-paper over regeldruk en digitale wetgeving in november 2025 met uw Kamer gedeeld.[3] De simplificatievoorstellen uit het voorstel passen binnen de bredere doelstelling van het kabinet om de regeldruk terug te dringen. Daarbij zal het voorstel volgens het kabinet in brede zin bijdragen aan het vergroten van de cyberveiligheid en weerbaarheid in de gehele Unie.

ATR advies

Het eerste concept van het BNC-fiche is voor advies voorgelegd aan het Adviescollege toetsing regeldruk (ATR). Het ATR adviseert over de regeldrukeffecten van het voorstel van de Europese Commissie. Het ATR adviseert als volgt:

“Adviespunten over Certificeringssystematiek:

1. ATR adviseert om in de beoordeling van het Commissievoorstel meer inzicht te bieden in de actiepunten die het kabinet koppelt aan de door ons genoemde risico’s op een toename van de regeldruk.

2. ATR adviseert om specifiek rekening te houden met de positie van kleinere bedrijven en bedrijven die voornamelijk nationaal opereren.

Adviespunten over veiligheid van ICT-toeleveringsketens:

3. ATR adviseert om voorafgaand aan de definitieve standpuntbepaling de regeldrukkosten van uitfasering van hoog-risico leveranciers in de Nederlandse 5G-

---

[2] Kamerbrief over actieprogramma Minder Druk Met Regels | Kamerstuk | Rijksoverheid.nl.

[3] https://www.tweedekamer.nl/kamerstukken/detail?id=2025D46264&did=2025D46264.

sector in beeld te brengen. Hierbij kan gebruik worden gemaakt van scenario's of bandbreedtes.

4. ATR adviseert om voorafgaand aan de definitieve standpuntbepaling specifiek de werkbaarheid en haalbaarheid te toetsen van de voorgestelde termijn van 36 maanden voor de uitfasering van hoog-risico leveranciers in de Nederlandse 5G-sector.

5. ATR adviseert om bij de Commissie aan te dringen om niet zonder nadere regel-drukanalyse het toepassingsbereik naar andere sectoren via implementing acts uit te breiden.

- ATR adviseert dit keer uitsluitend op basis van de regeldrukparagraaf. ATR heeft op basis van de verstrekte informatie niet kunnen adviseren over de volle breedte van de taakopdracht met betrekking tot de BNC-fiches.

Reactie kabinet

Hieronder volgt een reactie van het kabinet op de adviespunten:

Gezien de korte doorlooptijd van het BNC-fiche is het niet mogelijk om solide berekeningen te doen en deze te verifiëren. Het kabinet licht ten aanzien van de specifieke punten het volgende toe:

De risico’s die door de ATR zijn benoemd gaan over het risico van een certificaat. Het kabinet wijst er op dat het op dit moment gaat om de mogelijkheid van het vaststellen van een certificeringssystematiek en niet een certificaat. Het kabinet wijst erop dat bij het vaststellen van een certificaat en het bepalen van de verplichting om hier aan te voldoen onderwerp is van onderhandeling zodra er een certificeringssystematiek is vastgesteld.

Het kabinet vindt de risico-analyse onder de 5G *toolbox* op dit moment onvoldoende om deze als bindende maatregelen op te leggen. Daarmee wil het kabinet eerst verrijking en verduidelijking van deze *toolbox*. Na verrijking van de *toolbox* zal het kabinet bezien op welke manier gevolg kan worden gegeven aan de adviespunten van het ATR. Het kabinet heeft als onderhandelingsinzet dat de uitfaseringstermijn proportioneel en uitvoerbaar moet zijn. Het kabinet zal bij de

onderhandelingen over nieuwe *implementing acts* bezien op welke manier gevolg kan worden gegeven aan de adviespunten van het ATR.

Wanneer duidelijk is of en in welke vorm de voorstellen van de Europese Commissie daadwerkelijk tot wet worden verheven en er daarmee meer informatie is over de regeldrukeffecten, zal het kabinet weer bezien op welke manier gevolg kan worden gegeven aan de adviespunten van het ATR.

Wat betreft het punt van het ATR over de advisering op basis van de regeldrukparagraaf hecht het kabinet te benoemen dat het ATR vroegtijdig is betrokken en een conceptversie van het fiche heeft ontvangen. Het kabinet hecht waarde aan deze adviestaak van het ATR en gaat met ATR in gesprek over de informatievoorziening aan het ATR bij toekomstige Commissievoorstellen voor deze nieuwe adviestaak.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten
Het voorstel beoogt de digitale weerbaarheid van de Unie te versterken door verdere harmonisatie van het Europese cybersecuritykader, waaronder het certificeringsstelsel en maatregelen ter versterking van de veiligheid van ICT-toeleveringsketens. Door het bevorderen van een uniform kader op EU-niveau kan het uiteenlopen van nationale maatregelen worden verminderd, wat bijdraagt aan rechtszekerheid voor ondernemingen en het functioneren van de interne markt. Dit kan op langere termijn positief uitwerken op de concurrentiekracht van de Europese digitale economie.

Het voorstel heeft mogelijk verstrekkende diplomatieke en economische gevolgen, aangezien het de Commissie bevoegdheden geeft om derde landen als geheel aan te wijzen als ‘een land dat cyberzorgen met zich meebrengt’. Het kabinet acht het daarom van belang dat geopolitieke afwegingen voldoende zijn gewaarborgd bij een eventuele aanwijzing van een land of leverancier. In den brede past het voorstel geopolitiek bezien binnen de inzet van de Unie op versterking van economische veiligheid en vermindering van strategische afhankelijkheden.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

N.v.t.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het voorstel bevat verschillende bevoegdheden voor uitvoeringshandelingen en gedelegeerde handelingen.

Allereerst bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 47, lid 5 van het voorstel, samen met artikel 109, lid 4 van het voorstel. Dit betreft de bevoegdheid om regels vast te leggen over de vergoedingskosten die door ENISA en de Commissie kunnen worden geïnd. Het toekennen van deze bevoegdheden is mogelijk, omdat het niet essentiële onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, gelet op het feit dat het niet noodzakelijk wordt geacht om deze details via de wetgevingsprocedure te regelen en dit zo snel en flexibel kan worden opgesteld. De keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand omdat het hier gaat om uitvoering volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet wel op zijn plaats omdat het gaat om uitvoeringshandelingen van algemene strekking.

Ten tweede bevat het voorstel een bevoegdheid om uitvoeringshandelingen vast te stellen op grond van artikel 74, lid 9 van het voorstel. Dit betreft de bevoegdheid om uitvoeringshandelingen vast te stellen die voorzien in een Europees cybersecurity certificatiekader voor ICT-producten, diensten en processen. Het toekennen van deze bevoegdheden is mogelijk, omdat het niet essentiële onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, omdat het mogelijk maakt om op

snelle wijze de details omtrent het certificatiekader te regelen en indien nodig te wijzigen, zonder dat een wetgevingsprocedure moet worden ingelast, die voor dergelijke details door het kabinet niet wenselijk wordt geacht. De keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet wel op zijn plaats omdat het uitvoeringshandelingen van algemene strekking betreffen.

Ten derde bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 81, lid 5 van het voorstel. Dit betreft een bevoegdheid om uitvoeringshandelingen vast te stellen waarin gemeenschappelijke principes en modelbepalingen voor het certificatiekader worden vastgesteld. Het toekennen van deze bevoegdheden is wel mogelijk, omdat het niet essentiële onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, omdat dit naar het oordeel van het kabinet niet op wetgevingsniveau hoeft te worden geregeld en via uitvoeringshandelingen deze gemeenschappelijke principes en modelbepalingen snel kunnen worden opgesteld en indien nodig snel kunnen worden gewijzigd. De keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat het gaat om uitvoeringshandelingen van algemene strekking.

Ten vierde bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 87, lid 1 van het voorstel. Dit betreft een bevoegdheid om door middel van uitvoeringshandelingen certificaten van derde landen te erkennen als equivalent aan EU-certificaten. Het toekennen van deze bevoegdheden is wel mogelijk, omdat het niet essentiële onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, omdat de beoordeling van certificaten van derde landen doorlopend moet kunnen plaatsvinden en in dit

kader de beoordeling op snelle en flexibele wijze moet kunnen plaatsvinden in plaats van via de wetgevingsprocedure. Met betrekking tot de keuze voor uitvoering i.p.v. delegatie en de keuze voor vaststelling volgens de onderzoeksprocedure zijn dezelfde keuzes gemaakt als voor de vaststelling van certificatiekaders, dit is passend aangezien het gaat om uitvoering van de verordening volgens eenvormige voorwaarden en het gaat om uitvoeringhandelingen van algemene strekking.

Ten vijfde bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van 89, lid 6 van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandelingen om een plan voor intercollegiale toetsing van nationale cybersecurity certificatieautoriteiten vast te stellen. Het toekennen van deze bevoegdheden is mogelijk, omdat het niet een essentieel onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, omdat het niet nodig wordt geacht om de details van dergelijke intercollegiale toetsing via een wetgevingsprocedure te regelen en hiermee de Commissie snel een plan voor intercollegiale toetsing kan opstellen. De keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat het gaat om uitvoeringshandelingen van algemene strekking.

Ten zesde bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 92, lid 8 van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandelingen procedures voor de autorisatie van conformiteitsbeoordelingsinstanties vast te stellen, onder andere in het kader van grensoverschrijdende samenwerking. Het toekennen van deze bevoegdheden is wel mogelijk, omdat het niet essentiële onderdelen van de basishandeling betreft. Toekenning van deze bevoegdheden acht het kabinet wenselijk, omdat het niet nodig wordt geacht om dergelijke details via wetgevingsprocedure te regelen en hiermee dit snel kan worden geregeld via uitvoeringshandelingen, en indien nodig snel kan worden gewijzigd. De keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand omdat het gaat om

uitvoering volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet wel op zijn plaats het uitvoeringshandelingen van algemene strekking betreffen.

Ten zevende bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 93, lid 3 van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandelingen de formats, procedures en omstandigheden omtrent notificatie van de accreditaties van conformiteitsbeoordelingsinstanties vast te stellen. Als het een niet essentieel onderdeel van de basishandeling betreft, zou het kabinet het wenselijk achten om deze bevoegdheden toe te kennen, nu het mogelijk zou maken om details omtrent de notificatie snel vast te stellen en indien nodig snel te wijzigen. De keuze voor uitvoering i.p.v. delegatie zou daarnaast ook hierbij voor de hand liggen, omdat het zou gaan om uitvoering volgens eenvormige voorwaarden. Tevens zou de keuze van procedure, namelijk vaststelling volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011, van toepassing zijn, omdat het zou gaan om uitvoeringshandelingen van algemene strekking.

Het kabinet hecht er ook wat deze uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Tevens bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 100, lid 2. Dit betreft de bevoegdheid om derde landen als risicolanden aan te wijzen (al dan niet via een lijst) ten aanzien van ICT-toeleveringsketens. Het kabinet ziet mogelijke geopolitieke risico’s in dit voorstel. Deze risico’s zijn echter onvoldoende duidelijk, en daarom twijfelt het kabinet of het opstellen van een lijst als bedoeld in het tweede lid tezamen met een verificatie van risico’s als bedoeld in het eerste lid een essentieel onderdeel vormt van de basisbehandeling.. Het kabinet heeft daaromtwijfels over de wenselijkheid van deze bevoegdheid en kan op dit moment nog geen oordeel hierover vellen. Bij beslissingen met grote geopolitieke

gevolgen is voor het kabinet het niveau van besluitvorming daarnaast ook relevant, en belangrijk dat er op politiek niveau een besluit wordt genomen. Het kabinet gaat daarom nog nader onderzoeken welke specifieke procedure en bevoegdheid in het kader van dergelijke geopolitieke gevolgen en risico's passend zou zijn: een uitvoeringshandeling door de Raad, een uitvoeringhandeling door de Commissie, of een andere procedure. Het kabinet hecht er ook wat deze uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Ook bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 102, lid 1, van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandelingen, indien uit een risicobeoordeling overeenkomstig artikel 99, lid 1 of lid 3, van het voorstel blijkt dat sprake is van significante cybersecurityrisico's in relatie tot de ICT-toeleveringsketen, kritieke ICT-onderdelen, die essentiële entiteiten of belangrijke entiteiten als bedoeld in de NIS2-richtlijn gebruiken voor de vervaardiging van producten of de verlening van diensten, te identificeren. Het toekennen van deze bevoegdheid is mogelijk, nu het identificeren als zodanig niet een essentieel onderdeel van de basishandeling betreft. Toekenning van deze bevoegdheid acht het kabinet in principe wenselijk, gelet op dat het wenselijk is dat de identificatie snel en flexibel kan plaatsvinden, zonder een wetgevingsprocedure hiervoor door te lopen. Het kabinet is overigens wel van mening dat de procedure voor het identificeren van essentiële ICT-onderdelen nader dient te worden toegelicht. Het kabinet heeft om deze reden vragen over de regeling betreffende gebruikmaking van deze bevoegdheid. De keuze voor uitvoering i.p.v. delegatie zou voor de hand liggen omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure zou hier volgens het kabinet op zijn plaats omdat dit uitvoeringshandelingen van algemene strekking betreffen. Het kabinet hecht er ook wat deze uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Verder bevat het voorstel bevoegdheden voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 103, lid 1 en lid 7, van het voorstel.

Dit betreft in het geval van artikel 103, lid 1, de bevoegdheid om via uitvoeringshandeling vast te stellen dat het een specifieke groep essentiële entiteiten of belangrijke entiteiten als bedoeld in de NIS2-richtlijn verboden wordt om ICT-componenten van hoog-risico-leveranciers te gebruiken, installeren of integreren in bovenbedoelde kritieke ICT-onderdelen, indien dat noodzakelijk is om een hoog niveau van cybersecurity, cyberweerbaarheid en vertrouwen binnen de EU te waarborgen. In het geval van artikel 103, lid 7, betreft het de bevoegdheid voor de Commissie om in uitzonderlijke omstandigheden, waarin er sprake is van onder meer een significant cybersecurityrisico voor economische activiteiten in ten minste drie lidstaten, eenzelfde verbod op te leggen aan een specifieke groep essentiële entiteiten of belangrijke entiteiten, voor zover het gaat om ICT-componenten van entiteiten die gevestigd zijn, of onder controle staan van, een derde land. Toekenning van deze bevoegdheid acht het kabinet in principe wenselijk. Een dergelijk verbod dient snel en flexibel plaats te vinden, zonder dat een wetgevingsprocedure hiervoor dient te worden doorlopen. Het kabinet is overigens wel van mening dat de procedure voor het verbieden van essentiële ICT-onderdelen nader dient te worden toegelicht. Het kabinet heeft daarnaast nog vragen over de regeling betreffende gebruikmaking van deze bevoegdheid. De keuze voor uitvoering i.p.v. delegatie zou voor de hand liggen omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden in deze gevallen vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat dit uitvoeringshandelingen van algemene strekking betreffen. Het kabinet hecht er ook wat deze uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Daarnaast bevat het voorstel een bevoegdheid voor de Commissie om uitvoeringshandelingen vast te stellen op grond van artikel 103, lid 2 en 3, van het voorstel. Dit betreft de bevoegdheid om via uitvoeringshandeling vast te stellen dat een specifieke groep essentiële entiteiten of belangrijke entiteiten als bedoeld in de NIS2-richtlijn met betrekking tot hun ICT-toeleveringsketen, en in

het bijzonder bovenbedoelde kritieke ICT-onderdelen, onderworpen zal zijn aan een of meerdere maatregelen om cybersecurityrisico's te mitigeren, waaronder technische maatregelen die door een derde partij worden ge-audit en beperkingen inzake het aangaan van contractuele relaties met leveranciers. Toekenning van deze bevoegdheid acht het kabinet in principe wenselijk. Een dergelijk verbod dient snel en flexibel plaats te vinden, zonder dat een wetgevingsprocedure hiervoor dient te worden doorlopen. Het kabinet is overigens wel van mening dat de procedure voor het mitigeren van risico's aan de hand van maatregelen nader dient te worden toegelicht. Het kabinet heeft daarnaast vragen over de regeling betreffende gebruikmaking van deze bevoegdheid. De keuze voor uitvoering i.p.v. delegatie ligt voor de hand omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden in deze gevallen vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat dit uitvoeringshandelingen van algemene strekking betreffen. Het kabinet hecht er ook wat deze uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Het voorstel bevat voorts een bevoegdheid voor de Commissie om via uitvoeringshandelingen een lijst op te stellen van hoog-risico leveranciers op grond van artikel 104, eerste lid. Het kabinet ziet mogelijke geopolitieke risico's in dit voorstel. Deze risico's zijn echter onvoldoende duidelijk, en daarom twijfelt het kabinet of het opstellen van een lijst een essentieel onderdeel vormt van de basisbehandeling. Bij beslissingen met grote geopolitieke gevolgen is voor het kabinet het niveau van besluitvorming daarnaast ook relevant, en belangrijk dat er op politiek niveau een besluit wordt genomen. Het kabinet gaat daarom nog nader onderzoeken welke specifieke procedure en bevoegdheid in het kader van dergelijke geopolitieke gevolgen en risico's passend zou zijn: een uitvoeringshandeling door de Raad, een uitvoeringhandeling door de Commissie, of een andere procedure. Indien voor een uitvoeringshandeling wordt gekozen ligt de keuze voor uitvoering i.p.v. delegatie ligt hier voor de hand, omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat dit uitvoeringshandelingen van algemene strekking betreffen. Het kabinet hecht er ook wat deze

uitvoeringshandelingen betreft waarde aan dat de lidstaten met betrekking tot het vaststellen hiervan een belangrijke rol hebben.

Hiernaast bevat het voorstel een bevoegdheid om uitvoeringshandelingen vast te stellen op grond van artikel 105, lid 3 van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandeling regels vast te stellen over de omstandigheden en procedures inzake uitzonderingsverzoeken door entiteiten in hoog risico landen ten aanzien van de categorisatie als hoog risico derde land en de extra lasten die daaruit voor die entiteiten volgen. Het kabinet twijfelt of deze aanwijzing niet een essentieel onderdeel vormt van de basisbehandeling betreft, aangezien de hieraan verbonden gevolgen en risico’s nog onduidelijk zijn en volgens het kabinet van fundamentele aard kunnen zijn. Het kabinet heeft dan ook eveneens twijfels over de wenselijkheid van deze bevoegdheid, en kan op dit moment nog geen definitief oordeel hierover vellen. Indien voor een uitvoeringshandeling wordt gekozen, merkt het kabinet op dat de keuze voor uitvoering i.p.v. delegatie hier echter niet voor de hand zou liggen, omdat het hier gaat om een aanvulling of wijziging van bepaalde - in dat geval - niet-essentiële onderdelen van de wetgevingshandeling.

Tenslotte bevat het voorstel een bevoegdheid om uitvoeringshandelingen vast te stellen op grond van artikel 110, lid 4 van het voorstel. Dit betreft een bevoegdheid om via uitvoeringshandeling de tijdsperiode voor het uitfaseren van ICT-componenten die zijn geleverd door hoog-risico leveranciers met betrekking tot elektronische communicatienetwerken vast te stellen. Het kabinet twijfelt of deze aanwijzing een essentieel onderdeel vormt van de basisbehandeling betreft, aangezien de hieraan verbonden gevolgen en risico’s nog onduidelijk zijn. Het kabinet heeft daarnaast twijfels over de wenselijkheid van deze bevoegdheid, en kan hier nog geen definitief oordeel over vellen. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure zou hier volgens het kabinet op zijn plaats omdat in deze procedure de stem van de lidstaten sterker weegt dan in de raadplegingsprocedure.

Ook kent het voorstel de Commissie verscheidene bevoegdheden toe met betrekking tot gedelegeerde handelingen. Zo geeft artikel 80, lid 2 de Commissie de bevoegdheid om via gedelegeerde handeling de veiligheidsdoelen voor het Europese cybercertificatieschema te wijzigen of aan te vullen. Het kabinet meent dat deze bevoegdheid zodanig raakt aan het doel en reikwijdte van deze verordening, dat het zich afvraagt of het hier geen essentieel onderdeel betreft dat beter voorbehouden kan blijven aan de Uniewetgever, omdat het een essentieel onderdeel van de basishandeling betreft. Als gevolg daarvan acht het kabinet de toekenning van deze bevoegdheid verder ook niet wenselijk, en ligt de vorm van gedelegeerde handeling i.p.v. uitvoeringshandeling ook niet voor de hand.

Ook geeft artikel 110, lid 5 van het voorstel de Commissie de bevoegdheid om via gedelegeerde handelingen bijlage 2 van de verordening (essentiële ICT-middelen voor mobiele en vaste elektronische communicatienetwerken) te wijzigen naar aanleiding van technologische ontwikkelingen, rekening houdende met de elementen die benoemd zijn in artikel 103, lid 4 van het voorstel. Het kabinet is van mening dat de stappen uit het voorgestelde generieke raamwerk in eerste instantie moeten worden doorlopen, voordat kan worden besloten tot welke onderdelen in communicatienetwerken essentieel zijn. In het verlengde daarvan vindt het kabinet dat de procedure voor het identificeren van essentiële ICT-onderdelen nader dient te worden toegelicht en kan het kabinet nog geen oordeel vellen over of het een essentieel onderdeel van het voorstel betreft. Het kabinet heeft om deze reden ook nog twijfels over de wenselijkheid en afbakening van deze bevoegdheid in het kader van onduidelijkheden over het voorstel, en kan het kabinet nog geen definitief oordeel hierover vellen. In dat kader zal het kabinet nadere toelichting vragen van de Commissie. Indien het geen essentieel onderdeel zou betreffen en verder wenselijk zou zijn, zou delegatie i.p.v. uitvoering wel voor de hand liggen, aangezien het zou gaan om het wijzigen van niet-essentiële onderdelen van het voorstel.

c) *Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid*

De verordening treedt in werking op de twintigste dag na de dag van publicatie. Om de verordening in Nederland te kunnen uitvoeren is formele wetgeving vereist. Daarvoor is doorgaans minstens anderhalf jaar nodig. Vervolgens moet wellicht een nieuwe overheidsinstantie worden opgericht en bemenst (de toezichthouder). Het in het voorstel opgenomen tijdpad is dan ook niet realistisch.

d) Wenselijkheid evaluatie-/horizonbepaling

De verordening bepaalt dat de Commissie de verordening iedere vijf jaar evalueert (art. 56) en dat die evaluatie ertoe kan leiden dat de Commissie voorstelt om de taken van ENISA te wijzigen of om ENISA op te heffen.

e) Constitutionele toets

De toezichthouder moet bevoegd zijn «to impose penalties». Volgens de verklaring van de Raad van 27 april 2006, PbEU 2006, L 114, moet de term «penalties» in rechtsinstrumenten van de EU vertaald worden als «sancties». Zo gelezen vereist de verordening niet dat de toezichthouder bevoegd is om punitieve sancties op te leggen (zoals een bestuurlijke boete of bijvoorbeeld een punitief bedoelde intrekking van een erkenning) en staat zij ook bestuursrechtelijke herstelsancties toe. De verordening laat ook ruimte voor strafrechtelijke handhaving.

7. Implicaties voor uitvoering en/of handhaving

Uitvoeringsorganisaties hechten aan vereenvoudiging van wet- en regelgeving. De eerste inschatting is dat de voorgestelde wetgeving voor overheidsorganisaties een toenemende last met zich meebrengt op het gebied van verantwoording en/over certificeringen en dat dit extra capaciteit zal vragen. Een goede balans tussen gebruikmaking van beveiligingsrisicobeoordelingen van de EU en de inzet van eigen kennis en inzicht in gevolgen in de praktijk is belangrijk. Zodra de details van de verordening meer duidelijk zijn, moeten de implicaties in kaart worden gebracht met de uitvoeringstoets. Daarnaast is het wenselijk dat er meer duidelijkheid komt over de samenhang tussen de recente wetsvoorstellen van de Europese Commissie onderling en bestaande wet- en regelgeving. Ook is het wenselijk om de uitvoeringsconsequenties van het totaal van nieuwe wet- en regelgeving te onderzoeken.

8. Implicaties voor ontwikkelingslanden

N.v.t.