22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4389 VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 19 juni 2026

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de minister van Justitie en Veiligheid over de Fiches: Simplificatie NIS2-richtlijn (Kamerstuk 22 112, nr. 4284) en Herziening Cybersecurity Act (Kamerstuk 22 112, nr. 4286)

De vragen en opmerkingen zijn op 3 april 2026 aan de minister van Justitie en Veiligheid voorgelegd. Bij brief van 19 juni 2026 zijn de vragen beantwoord.

De voorzitter van de commissie,
Dekker

Adjunct-griffier van de commissie,
Muller

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon

Vragen en opmerkingen van de leden van de D66-fractie

1. De leden van de D66-fractie hebben met interesse kennisgenomen van de fiches. Hierover hebben deze leden nog enkele vragen. Zij onderschrijven het belang van versterkte Europese samenwerking op het gebied van cyberveiligheid, mede gelet op de toename van cyberdreigingen en de groeiende digitale afhankelijkheden. De leden van de D66-fractie vragen het kabinet hoe zij de balans beoordeelt tussen versterkte EU-coördinatie en het behoud van nationale bevoegdheden, in het bijzonder waar het gaat om de uitbreiding van het mandaat van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA). Hoe wordt voorkomen dat overlap ontstaat met nationale structuren zoals Computer Security Incident Response Teams (CSIRT's), en welke inzet kiest het kabinet ten aanzien van de voorgestelde operationele taken van ENISA?

   Antwoord
   Het kabinet onderschrijft het belang van versterkte Europese samenwerking op het gebied van cyberveiligheid, mede gezien het grensoverschrijdende karakter van digitale dreigingen en de toenemende verwevenheid van digitale infrastructuren binnen de Europese Unie. In dat licht beoordeelt het kabinet een versterking van de rol van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) in beginsel positief, met name waar het gaat om kennisontwikkeling, capaciteitsopbouw en het bevorderen van samenwerking tussen lidstaten. Tegelijkertijd acht het kabinet het van wezenlijk belang

dat nationale bevoegdheden behouden blijven. De inzet van het kabinet is er dan ook op gericht dat ENISA een ondersteunende en faciliterende rol vervult, en niet treedt in verantwoordelijkheden die primair bij lidstaten liggen. In dit kader benadrukt het kabinet 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 zal dit actief inbrengen tijdens de onderhandelingen.

2. Voorts onderschrijven deze leden het belang van het beperken van risico's van hoog-risicoleveranciers. Daarnaast vragen zij hoe het kabinet aankijkt tegen de voorgestelde bevoegdheden van de Europese Commissie met betrekking tot ICT-toeleveringsketens en het aanwijzen van hoog-risico leveranciers. Welke waarborgen gelden hierbij, hoe wordt de proportionaliteit van maatregelen zoals verplichte uitfasering geborgd en welke gevolgen verwacht het kabinet voor Nederlandse bedrijven en vitale infrastructuur? Tevens vragen de leden van de D66-fractie hoe wordt voorkomen dat certificering feitelijk toezicht vervangt en leidt tot onevenredige lasten.

   Antwoord
   Het kabinet kijkt positief naar het doel van het voorstel om op Europees niveau cyberrisico's te mitigeren binnen de ICT-toeleveringsketens van essentiële en belangrijke entiteiten in kritieke sectoren. 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 EU. Hierbij benadrukt het kabinet het belang van een raamwerk dat casus-gericht en risico-gebaseerd is, omdat de mate van risico sterk afhankelijk is van het geleverde ICT-onderdeel, de geleverde (kritieke) dienst

en reeds genomen technisch-operationele en organisatorische maatregelen.
Het kabinet zal zich inzetten voor een evenwichtige rolverdeling tussen de Europese Commissie en de lidstaten binnen het ICT-toeleveringsketen certificeringsraamwerk. Hierbij heeft het kabinet zorgen bij de voorgestelde bevoegdheid van de Europese Commissie om landen en leveranciers als geheel aan te wijzen als hoog-risico, vanwege de mogelijke verstrekkende economische, juridische en geopolitieke gevolgen van dergelijke besluiten. Daarnaast acht het kabinet het problematisch dat de onderliggende criteria en procedures nog onvoldoende duidelijk en uitgewerkt zijn. Het kabinet acht het daarom van belang dat deze bevoegdheden gepaard gaan met duidelijke criteria, transparante procedures en een stevige betrokkenheid van de lidstaten. Op dit moment zijn deze criteria nog onduidelijk en breder dan noodzakelijk om het doel van het voorstel te bereiken. Het kabinet acht het daarnaast van belang dat certificering niet leidt tot automatische vrijstellingen van wettelijke verplichtingen, en dat nationale toezichthouders ruimte behouden voor risico-gebaseerd toezicht. Tevens dient te worden voorkomen dat certificering leidt tot onevenredige administratieve lasten, met name voor kleinere entiteiten. Het kabinet zet zich daarom in voor een proportionele en doelmatige inrichting van het certificeringsstelsel.

3. Deze leden steunen het streven naar vereenvoudiging en harmonisatie van het Europese cyberbeveiligingskader. Zij vragen het kabinet hoe de voorgestelde wijzigingen bijdragen aan lastenverlichting voor bedrijven en toezichthouders. Daarnaast zijn de leden van de D66-fractie benieuwd hoe wordt geborgd dat vereenvoudiging niet ten koste gaat van het cyberbeveiligingsniveau. In het bijzonder

vragen deze leden hoe de introductie van nieuwe categorieën entiteiten en aanpassingen in het toepassingsbereik van de NIS2-richtlijn in de praktijk uitwerken?

Antwoord
Het kabinet onderschrijft het grensoverschrijdende karakter van cyberdreigingen én de verwevenheid van digitale processen binnen de EU. Het kabinet onderkent de noodzaak van Europese samenwerking op het gebied van cybersecurity én gelet daarop verdere harmonisering en vereenvoudiging van de NIS2-richtlijn. Verschillende voorgestelde wijzigingen van de NIS2-richtlijn beogen bij te dragen aan lastenverlichting van de bedrijven en toezichthouders, zoals de introductie van een nieuwe categorie *small mid-cap* bedrijven, in lijn met de aanbeveling van de Europese Commissie 2025/1099.[1] Hierdoor zullen naar verwachting verschillende entiteiten, die nu nog als essentiële entiteit worden aangemerkt, voortaan als belangrijke entiteit worden aangemerkt. Zij zullen daarmee onder een 'lichter' toezichtregime vallen. Het kabinet kan nog onvoldoende beoordelen in hoeverre dit bijdraagt aan lastenverlichting.
Ook het gebruik van certificering als hulpmiddel bij het aantonen van naleving van de zorgplicht in de NIS2-richtlijn kan leiden tot lastenverlichting. Daarbij acht het kabinet onder meer van belang dat nationale toezichthouders ruimte behouden voor risico-gebaseerd toezicht. Certificering mag daarnaast niet leiden tot onnodige beperkingen van de auditbevoegdheden. De wijziging in het toezichtregime laat onverlet dat de betrokken entiteiten moeten voldoen aan de zorgplicht en de meldplicht, én het

[1] Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

beveiligingsniveau in relatie tot die entiteiten daarmee voldoende gewaarborgd moet blijven. Door de voorgestelde uitbreiding van het toepassingsbereik van de NIS2-richtlijn zullen nieuwe groepen van entiteiten, zoals aanbieders van European Business Wallets, onder andere moeten voldoen aan de zorgplicht, meldplicht en registratieplicht. De verwachting is overigens dat deze entiteiten nu, met het oog op de continuïteit van hun bedrijfsvoering, zelf wel al beveiligingsmaatregelen treffen. Op dit moment is het voor het kabinet nog onduidelijk hoeveel nieuwe entiteiten vanwege die voorgestelde uitbreiding aanvullend onder de NIS2-richtlijn komen te vallen. Het kabinet streeft ernaar hier zo snel mogelijk inzicht in te krijgen.

4. Tot slot vragen zij hoe het kabinet de voorgestelde harmonisatie beoordeelt, waarbij lidstaten minder ruimte krijgen om strengere eisen te stellen. In hoeverre acht het kabinet dit wenselijk, mede gelet op nationale veiligheidsbelangen en bestaande instrumenten? Ook vragen de leden van de D66-fractie hoe de opeenvolging van regelgeving, terwijl de implementatie van de NIS2-richtlijn nog niet is afgerond, zich verhoudt tot rechtszekerheid en uitvoerbaarheid voor betrokken partijen.

   Antwoord
   Het kabinet is op hoofdlijnen positief als het gaat om de voorgestelde harmonisatie. Dat geldt bijvoorbeeld ook, voor het door middel van uitvoeringshandelingen, stellen van nadere eisen aan de door essentiële entiteiten en belangrijke entiteiten te nemen zorgplichtmaatregelen. Bij de daaraan in het voorstel gekoppelde maximumharmonisatie heeft het kabinet wel kanttekeningen, in het bijzonder omdat het onduidelijk is of het hierdoor voor lidstaten mogelijk

blijft om, in geval van specifieke dreigingen in een lidstaat, aanvullende eisen te stellen aan zorgplichtmaatregelen. Daarbij is ook het risico aanwezig dat lidstaten worden belet om dergelijke eisen te stellen in situaties waarin de nationale veiligheid, naar het oordeel van een lidstaat, daartoe noopt. In dat kader zal het kabinet in de Europese onderhandelingen aandacht vragen voor het behoud van voldoende nationale beleidsruimte, zodat lidstaten waar nodig aanvullende eisen kunnen stellen ter bescherming van de nationale veiligheid. De bepalingen in de huidige NIS2-richtlijn, zullen na de inwerkingtreding van de Cyberbeveiligingswet voor de betrokken entiteiten duidelijk kenbaar gelden. De nu voorgestelde wijzigingen van de NIS2-richtlijn zullen, na de onderhandelingen hierover, tijdig kenbaar worden gemaakt aan betrokken entiteiten zodat zij zich tijdig kunnen voorbereiden op deze wijzigingen. De verwachting is dan ook dat er geen nadelige gevolgen voor de rechtszekerheid zullen zijn.

Vragen en opmerkingen van de leden van de VVD-fractie

5. De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Fiches Simplificatie NIS2-richtlijn (Kamerstuk 22112, nr. 4284) en Herziening Cybersecurity Act (Kamerstuk 22112, nr. 4286) (hierna: fiches). Deze leden onderschrijven het belang van een hoog niveau van cyberweerbaarheid in Europa, juist in een tijd waarin statelijke dreigingen, sabotage en afhankelijkheden in digitale ketens toenemen. Tegelijkertijd achten deze leden het essentieel dat nieuwe Europese regelgeving uitvoerbaar blijft voor ondernemers en dat onnodige regeldruk wordt voorkomen. Zij stellen nog enkele vragen. De leden van de VVD-fractie steunen het uitgangspunt dat de

implementatie van de NIS2-richtlijn eenvoudiger en beter uitvoerbaar moet worden gemaakt. Tijdens het wetgevingsoverleg over de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten op 23 maart 2026 heeft de VVD-fractie reeds benadrukt dat cyberweerbaarheid pas effectief is wanneer bedrijven en instellingen niet verdwalen in overlappende meldplichten, verschillende toezichtregimes en onduidelijke verantwoordelijkheidsverdelingen. Deze leden vragen het kabinet daarom hoe wordt voorkomen dat de voorgestelde Europese vereenvoudiging in de praktijk juist leidt tot nieuwe complexiteit, bijvoorbeeld doordat certificering naast bestaande nationale toezichtsystemen komt te staan in plaats van deze te vereenvoudigen?

Antwoord
Het kabinet deelt de zorg dat vereenvoudiging op Europees niveau in de praktijk niet mag leiden tot nieuwe complexiteit voor bedrijven, overheden en toezichthouders. Het kabinet zet zich er daarom voor in dat certificering en andere instrumenten daadwerkelijk bijdragen aan vereenvoudiging en niet naast bestaande nationale toezichtsystemen komen te staan als extra laag. Concreet betekent dit dat het kabinet inzet op een duidelijke samenhang tussen certificering en toezicht, het voorkomen van dubbele verplichtingen (zoals parallelle audits en certificering) en een praktische uitvoerbaarheid voor bedrijven, met name voor bedrijven die in meerdere lidstaten actief zijn. Indien certificering wordt ingezet, moet deze aantoonbaar bijdragen aan vermindering van toezichtlasten en niet leiden tot een cumulatie van verplichtingen. Het kabinet zal dit punt actief inbrengen in de onderhandelingen.

6. Zij constateren dat de Europese Commissie certificering nadrukkelijker wil inzetten als bewijs van naleving van zorgverplichtingen. De leden van de VVD-fractie begrijpen het streven naar uniformiteit, maar vragen het kabinet nadrukkelijk te bevestigen dat certificering nooit een papieren tijger mag worden als het gaat om feitelijke cyberweerbaarheid. Hoe voorkomt het kabinet dat nationale toezichthouders in audit- en inspectiebevoegdheden worden beperkt zodra certificering aanwezig is? En hoe wordt voorkomen dat bedrijven worden geconfronteerd met certificeringsverplichtingen terwijl certificeringsschema's nog niet volledig beschikbaar of operationeel zijn? Deze leden wijzen daarnaast op het advies van de Raad van State over de Cyberbeveiligingswet, waarin is gewezen op het belang van heldere taakafbakening tussen verschillende toezichthouders en bevoegde autoriteiten. In welke mate wordt dit advies volgens het kabinet opgevolgd met dit nieuwe voorstel?

Antwoord
Het kabinet is van mening dat certificering inderdaad nooit een doel op zich mag worden en geen papieren exercitie mag zijn. Certificering dient daadwerkelijk bij te dragen aan feitelijke cyberweerbaarheid en moet gebaseerd zijn op inhoudelijke eisen, technische eisen en actuele risico's. Het kabinet benadrukt daarom dat certificering moet aansluiten bij reële dreigingen en risico's. Certificering is geen substituut voor het daadwerkelijk treffen van beveiligingsmaatregelen, en het certificeringsraamwerk moet adaptief en flexibel worden ingericht. Deze inzet is mede ingegeven door de ervaring dat cyberdreigingen zich snel ontwikkelen en dat formele naleving zonder feitelijke weerbaarheid onvoldoende bescherming biedt. Het kabinet acht het van belang dat nationale toezichthouders hun audit- en

inspectiebevoegdheden behouden, ook wanneer een entiteit beschikt over een certificaat. Het kabinet heeft daarom bedenkingen bij het voorstel om auditbevoegdheden te beperken wanneer certificering aanwezig is. Certificering kan waardevol zijn, maar dekt niet altijd alle ICT-onderdelen, is vaak een momentopname en biedt niet altijd inzicht in actuele risico's en kwetsbaarheden. Toezichthouders moeten daarom de ruimte houden om risico-gebaseerd controles uit te kunnen voeren. Het kabinet zal zich inzetten om te voorkomen dat certificering leidt tot een beperking van effectief toezicht. Voorts acht het kabinet het onwenselijk dat bedrijven worden geconfronteerd met certificeringsverplichtingen voordat certificeringsschema's volledig zijn ontwikkeld en beschikbaar en operationeel zijn.
Daarnaast zal het kabinet aandacht vragen voor de uitvoerbaarheid van certificeringsverplichtingen en de beschikbaarheid van certificeringscapaciteit, zodat bedrijven niet in een situatie komen waarin zij niet aan verplichtingen kunnen voldoen. Het kabinet onderschrijft het belang van heldere taakafbakening tussen toezichthouders (bijv. sectorale toezichthouders, RDI, etc.), zoals ook door de Afdeling advisering van de Raad van State is benadrukt. In het licht van dit voorstel zet het kabinet zich in voor duidelijke rolverdelingen tussen Europese en nationale instanties, het voorkomen van overlappende bevoegdheden en het behouden van nationale aanspreekpunten voor bedrijven. Specifiek betekent dit dat nationale toezichthouders leidend blijven bij toezicht en handhaving, terwijl Europese toezichtstructuren een ondersteunende en coördinerende rol vervullen. Hiermee wordt beoogd duidelijkheid te verschaffen aan bedrijven en de effectiviteit van toezicht te vergroten.

7. Zij onderschrijven dat Europa strategischer moet omgaan met risicovolle afhankelijkheden in vitale digitale infrastructuur. Tegelijkertijd vragen zij of het kabinet van mening is dat de Europese Commissie voldoende transparante criteria hanteert bij het aanwijzen van derde landen of leveranciers als hoog-risico leveranciers? Op basis van welke objectieve criteria worden landen en leveranciers als hoog-risico aangemerkt? Welke formele rol behouden lidstaten bij deze aanwijzingen? In hoeverre kan Nederland zelfstandig aanvullende nationale veiligheidsafwegingen blijven maken wanneer nationale dreigingsbeelden daartoe aanleiding geven?

Antwoord
Het kabinet is van oordeel dat de huidige criteria om derde landen en leveranciers als hoog risico aan te wijzen nog onvoldoende duidelijk zijn. Zo vindt het kabinet het bijvoorbeeld onduidelijk of alle leveranciers, afkomstig uit het aangewezen derde land of onder zeggenschap van het aangewezen derde land én aanwezig in de ICT-toeleveringsketen van essentiële of belangrijke entiteiten, direct en voor al hun diensten gelden als een hoog-risicoleverancier. Het kabinet wijst in dat geval op de mogelijk zeer omvangrijke economische en politieke gevolgen van deze aanwijzingen. Tegelijkertijd plaatst het kabinet een fundamentele kanttekening bij de bevoegdheid om een derde land als geheel aan te wijzen, omdat de mate van risico sterk afhankelijk is van het specifieke geleverde ICT-onderdeel, de te beschermen belangen, de geleverde (kritieke) dienst en reeds genomen technisch-organisatorische maatregelen. Daarom spant het kabinet zich in voor een risico-gebaseerd raamwerk en acht het kabinet het van groot belang dat de criteria in het voorstel transparant, objectief, en juridisch toetsbaar zijn. Het kabinet zal daarom inzetten op

verdere verduidelijking en aanscherping van deze criteria.
Voor de landenaanwijzing (artikel 100) hanteert de Europese Commissie een aantal criteria die zullen worden betrokken bij de beoordeling of een derde land een hoog risico vormt, zoals het bestaan van wetten of bestaande praktijken in het derde land die inhouden of erop wijzen dat entiteiten verplicht zijn om informatie over kwetsbaarheden te delen met de autoriteiten.
Voor wat betreft de aanwijzing van leveranciers (artikel 104) hanteert de Commissie een aantal criteria om leveranciers als hoog risico aan te wijzen, waarbij de Commissie met name beziet of leveranciers in de ICT-toeleveringsketen zijn gevestigd in een aangewezen derde land of onder zeggenschap staan van dat derde land, van een in dat derde land gevestigde entiteit of van een onderdaan van dat derde land.
De lidstaten behouden zowel een rol bij de landen- als de leveranciersaanwijzing, omdat deze aanwijzingen via een uitvoeringshandeling worden geïmplementeerd. Deze uitvoeringshandelingen worden namelijk aangenomen via de onderzoeksprocedure, waarbij lidstaten met gekwalificeerde meerderheid stemmen over het voorgenomen uitvoeringsbesluit. Tegelijkertijd is het kabinet van mening dat deze aanwijzingen, naast een technisch-juridische weging, ook een politieke weging vergt, vanwege de mogelijk verstrekkende gevolgen. Bij beslissingen met grote geopolitieke gevolgen is voor het kabinet het niveau van besluitvorming, en de betrokkenheid van lidstaten, om deze reden van essentieel belang. Lidstaten behouden, op grond van artikel 98, derde lid, de bevoegdheid om zelfstandig aanvullende maatregelen te nemen om hun cyberbeveiligingsniveau te waarborgen. Daarnaast geldt uiteraard ook dat de bescherming van de nationale veiligheid een uitsluitende verantwoordelijkheid van lidstaten is. Het kabinet vindt

beide cruciaal en zal tegelijkertijd het belang van een goede samenhang tussen nationale en Europese instrumenten blijven benadrukken.

8. De leden van de VVD-fractie zien dat de Commissie bedrijven verplicht kan laten overgaan tot uitfasering van technologie van hoog-risicoleveranciers. Deze leden erkennen dat nationale veiligheid soms ingrijpende keuzes vereist, maar wijzen erop dat verplicht vervangen van bestaande infrastructuur grote gevolgen kan hebben voor investeringen, leveringszekerheid en continuïteit van vitale diensten. Zij vragen daarom hoe wordt voorkomen dat verplichte uitfasering leidt tot verstoringen van vitale dienstverlening en welke overgangstermijnen het kabinet noodzakelijk acht om de uitvoerbaarheid te waarborgen?

Antwoord
Het kabinet onderkent dat verplichte uitfasering van technologie van hoog-risicoleveranciers ingrijpende gevolgen kan hebben voor de dienstverlening van betrokken essentiële of belangrijke entiteiten. Om verstoringen te voorkomen acht het kabinet het onder meer van belang dat dergelijke maatregelen gebaseerd zijn op gedegen risicobeoordelingen, dat er voldoende betrouwbare alternatieven beschikbaar zijn, en dat bijvoorbeeld rekening wordt gehouden met de technische en operationele complexiteit, en de onderlinge verscheidenheid tussen de ICT-toeleveringsketens binnen de verschillende sectoren en lidstaten. Verder acht het kabinet differentiatie naar het risicoprofiel van onderdelen van netwerk- en informatiesystemen noodzakelijk, omdat niet alle onderdelen van een netwerk- en informatiesysteem even kritiek zijn. Daarbij zijn realistische en (sector)specifieke overgangstermijnen van groot

belang. Te korte termijnen kunnen namelijk leiden tot verstoringen van de continuïteit van de dienstverlening van essentiële entiteiten en belangrijke entiteiten. Het kabinet zet zich er daarom voor in dat bedrijven voldoende tijd krijgen om vervanging zorgvuldig uit te voeren, zodat de continuïteit van hun dienstverlening niet onnodig in gevaar komt.

Vragen en opmerkingen van de leden van de GL-PvdA-fractie

9. De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van zowel de voorgestelde simplificatie van de NIS2-richtlijn (en de kabinetspositie) als de herziening van de Cybersecurity Act. Deze leden hebben vragen en opmerkingen, ook gezien recent de Cyberbeveiligingswet is behandeld die de NIS2-richtlijn implementeert. De leden van de GroenLinks-PvdA-fractie zijn benieuwd naar de gevolgen van de simplificatie voor deze wetgeving. Deze leden zijn ervan op de hoogte dat de deadline voor de implementatie van de NIS2-richtlijn (17 oktober 2024) door Nederland niet is gehaald. Het valt op dat het Nederland vaker niet lukt om de implementatiedeadlines van Europese richtlijnen te halen. Dit baart deze leden zorgen, vooral als dit richtlijnen betreft die de cyberveiligheid van Nederland raken. Snelle implementatie is nodig om tijdig te reageren op nieuwe ontwikkelingen in het cyberdomein. Kan het kabinet aangeven wat de redenen zijn voor het vertraagd implementeren van verschillende richtlijnen in het verleden en wat het kabinet wil gaan doen om ervoor te zorgen dat de richtlijnen die in deze fiches worden besproken, en toekomstige richtlijnen, wél tijdig geïmplementeerd worden?

Antwoord
Het kabinet ziet in hoofdlijnen twee aspecten die een rol kunnen spelen bij het door Nederland niet tijdig implementeren van richtlijnen. Allereerst kent het Nederlands wetgevingsproces een aantal belangrijke verplichte stappen, waaronder de advisering door de Afdeling advisering van de Raad van State en de behandeling van wetsvoorstellen door de Tweede Kamer én Eerste Kamer. Er zijn EU-lidstaten die bijvoorbeeld beschikken over een eenkamerstelsel en/of de verplichte voorafgaande advisering door een onafhankelijk adviesorgaan niet kennen, dan wel in een andere vorm met een relatief kortere doorlooptijd in vergelijking met Nederland te maken hebben. Het kabinet wijst er ten eerste op dat deze verplichte en in de Grondwet verankerde wetgevingsstappen belangrijk zijn vanwege de impact van die wetgeving op burgers, bedrijven en instanties. Hoewel het wenselijk is om snel tot (implementatie)wetgeving te komen, hecht het kabinet tegelijkertijd ook grote waarde aan een zorgvuldig wetgevingsproces, ook als dat meer tijd kost. Zo is er bijvoorbeeld bewust voor gekozen het ontwerp van de Cyberbeveiligingswet in (internet)consultatie te brengen vanwege de grote impact van deze wet op bedrijven en organisaties in tal van sectoren in zowel de private als de publieke sector. Ten tweede kan ten aanzien van sommige richtlijnen worden gewezen op een relatief korte implementatietermijn, hetgeen botst met de tijd die in Nederland nodig is om op een zorgvuldige wijze, rekening houdend met de impact van wet- en regelgeving op burgers, bedrijven en instanties, te komen tot implementatiewet- en regelgeving. Specifiek ten aanzien van de NIS2-richtlijn wordt erop gewezen dat het merendeel van de EU-lidstaten, waaronder landen als Frankrijk, Duitsland en Spanje, er niet in

zijn geslaagd om binnen de implementatietermijn te komen met de benodigde nationale implementatiewetgeving.

Om ervoor te zorgen dat de richtlijnen die in deze fiches worden besproken en toekomstige richtlijnen wel tijdig geïmplementeerd kunnen worden, zal in elk geval ruim voor de vaststelling van die richtlijnen – zoals dat ook is gebeurd bij de NIS2-richtlijn – tijdig worden gestart met de voorbereidingen voor de implementatiewet- en regelgeving. Bij het implementatieproces hoort ook dat het kabinet vasthoudt aan het principe van zuivere implementatie, wat inhoudt dat in de implementatieregeling geen andere regels worden opgenomen dan voor implementatie noodzakelijk zijn, om ervoor te zorgen dat implementatie zo spoedig mogelijk kan plaatsvinden. Bij het implementatieproces zal het kabinet telkens bezien wanneer en in hoeverre een versnelling van dat proces mogelijk is, bijvoorbeeld, door gebruik te maken van de mogelijkheid om niet in internetconsultatie te gaan, het onder de aandacht brengen van het belang van spoedige advisering door de Afdeling advisering van de Raad van State en het in de Tweede Kamer en Eerste Kamer onder de aandacht brengen van het belang van een spoedige parlementaire behandeling. Hierbij tekent het kabinet wel aan dat versnelling niet altijd wenselijk is vanwege de noodzaak om tot zorgvuldige implementatiewet- en regelgeving te komen in verband met de impact daarvan op burgers, bedrijven en instanties. Daarnaast ligt het primaat van de parlementaire behandeling bij de Tweede Kamer en Eerste Kamer zelf.

10. Zij lezen dat voortaan elektriciteitsproducenten alleen onder de NIS2-richtlijn vallen als zij een totale opwekkingscapaciteit van meer dan 1 megawatt

hebben. De leden van de GroenLinks-PvdA-fractie zijn benieuwd naar de praktische gevolgen hiervan voor Nederland. Hoeveel elektriciteitsproducenten die minder dan 1 megawatt produceren kent Nederland? Wat is het totale aandeel van deze producenten van de elektriciteitsproductie in Nederland? Betekent het feit dat deze ‘kleine’ elektriciteitsproducenten worden uitgesloten van de NIS2-richtlijn dat er geen controlemechanisme meer is om ervoor te zorgen dat ook deze elektriciteitsproducenten cyberveilig zijn? En zo ja, wat zouden dan bijvoorbeeld de gevolgen zijn voor het Nederlandse elektranetwerk indien al deze ‘kleine’ elektriciteitsproducenten te maken krijgen met bijvoorbeeld sabotage?

11. Deze leden lezen dat het kabinet positief staat tegenover het beperken van het toepassingsbereik van elektriciteitsproducenten zodat alleen producenten die daadwerkelijk impact kunnen hebben op de stabiliteit van het elektriciteitsnetwerk onder het toepassingsbereik van de NIS2-richtlijn vallen. Zij zijn hier toch enigszins verbaasd over. Kan het kabinet aangeven wat het gevolg voor de stabiliteit van het elektriciteitsnetwerk in Nederland zou zijn als alle producenten die minder dan 1 megawatt produceren gelijktijdig verstoord raken? Is ons netwerk in staat om een dergelijke klap te ondervangen? Deelt het kabinet de leden van de GroenLinks-PvdA-fractie eens dat een dergelijke sabotageactie van een statelijke actor, ook naar aanleiding van sabotageacties die reeds zijn waargenomen in bijvoorbeeld Oekraïne in de afgelopen jaren, niet ondenkbaar is? Kan het kabinet aangeven waarom het, indien een dergelijke sabotageactie denkbaar is en ons netwerk een dergelijke klap niet op kan vangen, toch voorstander is van het uitsluiten van dergelijke elektriciteitsproducenten van de NIS2-richtlijn?

Antwoord 10 en 11
Bij het bepalen van het toepassingsbereik van de NIS2-richtlijn voor elektriciteitsproducenten heeft het kabinet oog voor zowel het waarborgen van de stabiliteit van het elektriciteitsnet als het opleggen van proportionele en uitvoerbare uitvoeringslasten voor bedrijven en toezichthouders. In het wetsvoorstel Cyberbeveiligingswet is gekozen om, binnen de mogelijkheden van de huidige NIS2-richtlijn, het toepassingsbereik zo vorm te geven dat mogelijk ook kleinere producenten met minder opwekkingscapaciteit onder de NIS2-richtlijn vallen, zolang zij aan de gestelde omvangcriteria uit de NIS2-richtlijn voldoen en opwekking van elektriciteit hun primaire dienst is.[2] Elektriciteitsproducenten die onder de NIS2-richtlijn/Cyberbeveiligingswet vallen, dienen zich te registreren (registratieplicht) in het centrale meld- en registratieportaal dat bij het Nationaal Cyber Security Centrum is belegd. De drempelwaarde van 1 megawatt is een Europees voorstel dat momenteel nog niet binnen de huidige NIS2-richtlijn bestaat. Daarom beschikt het kabinet niet over dit overzicht. Daarnaast geldt de registratieplicht, waarmee inzichtelijk wordt welke partijen precies onder het toepassingsbereik van de Cyberbeveiligingswet vallen, momenteel niet omdat de Cyberbeveiligingswet nog moet worden behandeld in de Eerste kamer.
Het Nederlandse energiesysteem wordt beschermd door een robuust ontwerp, redundantie, voldoende herstelcapaciteit en interconnectie met de ons omringende landen. Kleine producenten hebben per installatie doorgaans een beperktere systeemimpact en daarmee vormen ze een kleiner risico voor het systeem. Omdat kleine producenten vaak verschillende

[2] Kamerstuk 36764

digitale systemen en digitale producten gebruiken, ligt sabotage van al deze kleine producenten tegelijk niet voor de hand.
Het inregelen van de NIS2-richtlijn als controlemechanisme voor kleinere producenten beoordeelt het kabinet als niet-proportioneel omdat de verplichtingen en lasten die dit met zich meebrengt niet evenredig zijn met de individuele risico's. Het kabinet zal de Europese Commissie vragen om de keuze voor 1 megawatt aan totale opwekkingscapaciteit als drempelwaarde te verduidelijken. Hierbij zal het kabinet aandacht vragen voor proportionaliteit en evenredigheid.
Dit neemt niet weg dat de digitalisering van het energiesysteem met steeds meer kleine elektriciteitsproducenten andere risico's met zich meebrengt dan bij grote elektriciteitsproducenten. Het kabinet onderkent deze risico's als prioriteit. Om deze risico's te mitigeren, geldt Europese wetgeving die ziet op apparaatveiligheid (Radio Equipment Directive, RED) en wordt gewerkt aan de implementatie en uitvoering van de Cyber Resilience Act (CRA) voor het verbeteren van productveiligheid van producten met digitale elementen. Conform de Kamerbrief "Versterking van decentrale ontwikkelingen van het energiesysteem" (29023-643) verkent de Minister van Klimaat en Groene Groei momenteel of aanvullende acties en/of maatregelen nodig zijn om de weerbaarheid te vergroten.[3] De resultaten hiervan neemt het kabinet mee in zijn reactie op het recent gepubliceerde rapport van Topsector Energie over een autonoom en veilig energiesysteem.

[3] Kamerstuk 29023, nr. 643, Voorzienings- en leveringszekerheid energie | Tweede Kamer der Staten-Generaal

12. De leden van de GroenLinks-PvdA-fractie hebben een vergelijkbare vraag ten aanzien van DNS (Domain Name System) -dienstverleners. Hoeveel van deze dienstverleners die binnen de Nederlandse jurisdictie vallen worden als micro of klein beschouwd? Wat zijn de definities van een micro of kleine DNS-dienstverlener en hoe groot is hun aandeel in de markt? Heeft de minister zicht op hoeveel kritieke entiteiten, vitale organisaties of organisaties die onder de NIS2-richtlijn vallen gebruik maken van een micro of kleine DNS-dienstverlener die hiermee minder veilig zouden kunnen zijn? Of betekent dit een effectief verbod voor dergelijke entiteiten en organisaties om gebruik te maken van een micro of kleine DNS-dienstverlener?

Antwoord
Het kabinet heeft momenteel geen kwantitatief beeld van het aantal micro- en kleine DNS-dienstverleners in Nederland en hun marktaandeel. De definitie van micro- en kleine bedrijven is op Europees niveau bepaald. Artikel 6 lid 20 van de NIS2-richtlijn bepaalt dat een DNS-dienstverlener een entiteit is die openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers verleent, of die gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden verleent, met uitzondering van root-naamservers. Deze dienstverleners vallen momenteel nog ongeacht hun omvang onder de toepasselijkheid van de NIS2-richtlijn. De definitie van micro- en kleine ondernemingen is als volgt: micro-ondernemingen zijn ondernemingen met minder dan 10 personeelsleden en een jaaromzet of jaarlijks balanstotaal van niet meer dan 2 miljoen EUR. Kleine ondernemingen zijn ondernemingen met minder dan 50 personeelsleden en een jaaromzet of jaarlijks balanstotaal van niet meer dan 10 miljoen EUR.

Het voorstel om kleine of micro-DNS-dienstverleners niet langer onder de toepasselijkheid van de NIS2-richtlijn te laten vallen, betekent geenszins dat andere entiteiten die nog wel als essentiële entiteit of belangrijke entiteit onder de NIS2-richtlijn blijven vallen geen gebruik meer zullen kunnen maken van micro- en kleine DNS-dienstverleners. Essentiële en belangrijke entiteiten als bedoeld in de NIS2-richtlijn dienen in het kader van hun zorgplicht hun toeleveringsketen te beveiligen. In het ontwerp van het Concept-cyberbeveiligingsbesluit worden die maatregelen nader uitgewerkt. Zo dient de essentiële of belangrijke entiteit bijvoorbeeld periodiek te toetsen of haar rechtstreekse leveranciers en dienstverleners voldoen aan de beveiligingseisen van de essentiële entiteit of belangrijke entiteit zelf. Indien DNS-dienstverleners - net zoals andere micro- en kleine leveranciers – voldoen, kunnen zij in beginsel hun leverancier blijven of worden.

13. Deze leden snappen de behoefte voor een certificeringsraamwerk, maar zijn ook verbaasd dat toezichthouders entiteiten niet (meer) mogen onderwerpen aan beveiligingsaudits voor zover de betreffende onderdelen door de certificering worden gedekt. Zij begrijpen dat dit iets doet aan de regeldruk, maar maken zich ook zorgen over hoe zij in de praktijk regelmatig een ‘papieren’ certificering zien waarbij wordt voldaan aan de eisen die de certificering oplegt maar niet wordt gecontroleerd of die eisen ook daadwerkelijk worden nageleefd. De leden van de GroenLinks-PvdA-fractie roepen de minister op om zich in te zetten voor het behoud van de controlemogelijkheden van toezichthouders. Wat is de inzet van het kabinet in Brussel op dit gebied? Wat is de positie van andere lidstaten hierop?

Antwoord
Met betrekking tot certificering en toezicht deelt het kabinet de zorg dat certificering niet mag leiden tot een papieren werkelijkheid waarin formele naleving de plaats inneemt van feitelijk toezicht. Het kabinet zet zich daarom in voor behoud van de controlemogelijkheden van nationale toezichthouders. Certificering kan ondersteunend zijn, maar mag geen automatisme worden waardoor toezichthouders niet meer kunnen toetsen of door entiteiten, in het kader van de zorgplicht genomen maatregelen, in de praktijk daadwerkelijk toereikend zijn. De inzet van het kabinet is er in Brussel op gericht dat audit- en inspectiebevoegdheden van toezichthouders behouden blijven, juist omdat certificering niet altijd een volledig en actueel beeld geeft van feitelijke cyberweerbaarheid. Nederland heeft in het fiche expliciet bedenkingen geuit bij de beperking van de auditbevoegdheid, in het bijzonder voor belangrijke entiteiten. Over de precieze posities van andere lidstaten kan op dit moment nog geen definitief beeld worden gegeven, omdat de onderhandelingen onlangs zijn gestart. Wel is duidelijk dat meerdere lidstaten kritisch kijken naar de verhouding tussen certificering en toezicht, juist vanwege uitvoerbaarheid en de noodzaak van effectief toezicht.

14. Deze leden lezen tevens dat de Europese Commissie een maximumharmonisatie voorstelt in relatie tot de uitvoeringshandelingen met betrekking tot de zorgplichtmaatregelen. Hiermee wordt lidstaten de bevoegdheid ontzegd om, zoals nu nog wel mogelijk is, bepalingen vast te stellen of te handhaven die een hoger cyberbeveiligingsniveau waarborgen. Zij zijn hier hoogst verbaasd over. Hoewel de leden van de GroenLinks-PvdA-fractie snappen dat dit leidt tot

minder complexiteit, merken zij op dat dit in de praktijk ook regelmatig leidt tot lagere eisen en dus minder veiligheid. Zij roepen het kabinet dan ook op om zich in te zetten om deze maximumharmonisatie uit het voorstel te halen. Acht het kabinet de voorgestelde maximumharmonisatie proportioneel en verstandig? Behouden lidstaten ruimte om hogere beveiligingsniveaus te hanteren voor kritieke infrastructuur? Welke mogelijkheden behouden nationale toezichthouders om in te grijpen bij acute cyberdreigingen? Welke lidstaten zijn voor- en tegenstander van deze maximumharmonisatie? Heeft Nederland medestanders in het verzet tegen deze maximumharmonisatie?

Antwoord
Het kabinet is op hoofdlijnen positief als het gaat om de voorgestelde harmonisatie van de te nemen maatregelen door entiteiten in het kader van de zorgplicht, met name voor entiteiten die in meer dan één lidstaat hun diensten verlenen. Ten aanzien van de in het voorstel daaraan gekoppelde maximumharmonisatie plaatst het kabinet echter verschillende kanttekeningen. Nog niet duidelijk is hoe verstrekkend het aan lidstaten ontzeggen van de mogelijkheid om aanvullend eisen aan maatregelen in het kader van de zorgplicht te stellen zal zijn én of het ontzeggen van deze mogelijkheid wel noodzakelijk is. Zo is bijvoorbeeld onduidelijk of lidstaten al dan niet nog eisen kunnen stellen met betrekking tot andere dan de in artikel 21, tweede lid, onder a tot en met j, NIS2-richtlijn genoemde maatregelen. Ook is onduidelijk of en waarom het voor lidstaten hierdoor eventueel niet meer mogelijk zou zijn om, in geval van specifieke dreigingen in een lidstaat, eisen te stellen aan zorgplichtmaatregelen. Indien de voorgestelde maximumharmonisatie lidstaten zonder onderscheid

belet om in dergelijke situaties nadere eisen aan zorgplichtmaatregelen te stellen, gaat dit voorstel naar het oordeel van het kabinet dan ook verder dan noodzakelijk. Het kabinet zal hiervoor dan ook nadrukkelijk aandacht vragen in de komende onderhandelingen. Voorts zal het kabinet er ook in dit verband bij de onderhandelingen steeds op toe blijven zien dat de inhoud van het voorstel niet op gespannen voet komt te staan met in het bijzonder, de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van de nationale veiligheid (artikel 4, tweede lid, VEU). Het kabinet weet op dit moment nog niet welke andere lidstaten mogelijk ook kritisch zijn als het gaat om de voorgestelde maximumharmonisatie.

15. Deze leden hebben ook kennisgenomen van de voorgestelde herziening van de Cybersecurity Act (CSA2). Deze bevat een herschikking van taken en verantwoordelijkheden, waarin deze meer op Europees niveau worden belegd. Net als het kabinet zien deze leden voor- en nadelen waar zij nog vragen en opmerkingen over hebben. Zij roepen in herinnering dat de Kamer recent de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) heeft behandeld. De leden van de GroenLinks-PvdA-fractie vragen het kabinet om duidelijk toe te lichten welke gevolgen de herziening van de CSA heeft voor de twee wetten. Op welke wijze is er rekening gehouden met de CSA2 in hoe de wetten zijn vormgegeven, en voorziet het kabinet dat er wetswijzigingen nodig zijn om de Cbw en de Wwke in lijn te brengen met de CSA2? Zo ja, op welke termijn verwacht het kabinet dat deze aanpassingen nodig zullen zijn? Ook vragen deze leden de informatievoorziening van de overheid, bijvoorbeeld via handreikingen en bewustwordingscampagnes, nog actueel is als de CSA wordt herzien. Specifiek vragen zij om meer uitleg te geven over de zelfscantool die

TNO verzocht is te ontwikkelen. Hoe verhoudt deze zich tot de vitaalbeoordeling die moet plaatsvinden onder de Cbw en de Wwke? Wat is het doel van die tool, wordt hierin al rekening gehouden met de herziening van de CSA, en wat moeten vitale aanbieders doen met de uitkomsten? Per wanneer is de tool gereed?

Antwoord
De eerste gesprekken omtrent het voorstel aangaande de herziening van de CSA-verordening en de herziening van de NIS2-richtlijn zijn inmiddels gestart binnen de Horizontale Groep voor cybervraagstukken. Over de gevolgen van de herziening van de CSA voor de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, waarvan de voorstellen recentelijk door uw Kamer zijn behandeld, kan gelet daarop nog geen uitspraak worden gedaan. Daarbij geldt dat voor de inhoud van beide wetsvoorstellen nauw wordt aangesloten bij de inhoud van de richtlijnen waarvan het de implementatie betreft. Het kabinet investeert doorlopend in bewustwording, kennisopbouw en handelingsperspectief ter versterking van digitale en fysieke weerbaarheid. Het in kaart brengen en beheersen van risico's in de toeleverancierssketen is namelijk van groot belang voor het digitaal veilig functioneren van publieke en private organisaties. Daarom hebben de AIVD, CIO Rijk, het NCSC en de NCTV gezamenlijk de handreiking ´Cybercheck: ook jij hebt supply chain risico´s!´ gepubliceerd.[4] Deze handreiking biedt organisaties en bedrijven 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

[4] NCSC, Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum, 18 april 2024.

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.

16. De leden van de GroenLinks-PvdA-fractie constateren dat er een verschuiving plaatsvindt van de CSA als middel om cyberveiligheid te vergroten, naar een CSA die ook ingezet wordt voor Europese economische veiligheid en diplomatieke doeleinden. Het is onmogelijk om de herziening los te zien van de wens om met name Chinese leveranciers van de Europese markt te weren. Deze leden hebben begrip voor de voorgestelde maatregelen om leveranciers te weren, maar er bestaan zorgen over de diplomatieke gevolgen, de beperkte zeggenschap van lidstaten, en de uitvoerbaarheid van interventies voor entiteiten. Deze leden vragen het kabinet hoe zij kijkt naar de geopolitieke en de economische dimensie van de CSA. Vindt het kabinet het wenselijk dat via leveranciersverboden en certificeringsschema's de Europese strategische autonomie wordt versterkt? Ziet het kabinet het afbouwen van strategische afhankelijkheden en het stimuleren van Europese alternatieven als terecht doelen van de CSA? Zo niet, hoe kunnen deze doelen dan beter worden bereikt?

Antwoord
Het kabinet kijkt positief naar het doel van het voorstel om op Europees niveau cyberrisico’s te mitigeren binnen de ICT-toeleveringsketens van essentiële en

belangrijke entiteiten in kritieke sectoren. Het kabinet erkent verder dat de herziening van de Cybersecurity Act niet uitsluitend een technisch-cyberveiligheidsinstrument is, maar ook een duidelijke geopolitieke en economische dimensie heeft. Dat is op zichzelf niet verrassend, gezien de toegenomen verwevenheid tussen digitale infrastructuur, economische veiligheid en strategische afhankelijkheden. Het kabinet acht het legitiem dat de Unie bij cyberveiligheid mede oog heeft voor die bredere context, maar vindt wel dat het voorstel risico-gebaseerd, casus-gericht, proportioneel en juridisch houdbaar moet blijven. Het kabinet acht het in algemene zin wenselijk dat de Europese Unie haar strategische autonomie versterkt waar het gaat om kritieke digitale infrastructuur en risicovolle strategische afhankelijkheden. Tegelijkertijd moeten verboden betreffende leveranciers en certificeringsschema's niet worden ingezet als algemene economische beschermingsinstrumenten zonder noodzaak voor de beveiliging van netwerk- en informatiesystemen. De inzet van het kabinet is erop gericht dat dit gebeurt op basis van een risico-gebaseerde aanpak, met oog voor proportionaliteit en uitvoerbaarheid. Het kabinet merkt daarnaast op dat de CSA niet het vanzelfsprekende instrument is om deze bredere economische en industriële doelen te realiseren. Voor het stimuleren van Europese alternatieven zijn andere beleidsterreinen van belang, zoals industriebeleid, innovatiebeleid, marktontwikkeling en publieke inkoop.

17. Zij lezen het kabinetsstandpunt over het Europese Agentschap voor Cyberveiligheid (ENISA) met interesse. De leden van de GroenLinks-PvdA-fractie zijn van mening dat ENISA een ondersteunende en faciliterende rol moet spelen richting lidstaten en

toezichthouders. Tegelijk zijn deze leden waakzaam dat de rol van lidstaten en toezichthouders niet wordt beperkt. Kan het kabinet toelichten wat, naar haar mening, de ideale inrichting en het takenpakket zou zijn van ENISA, zodat lidstaten maximaal ondersteund worden? Welke concrete suggesties doet het kabinet om naar dit ideaalbeeld toe te werken? Als de voorstellen over ENISA niet wijzigen t.o.v. het huidige Commissievoorstel, gaat Nederland daar dan mee akkoord?

Antwoord
Het kabinet is positief over de rol van ENISA binnen het cyberlandschap, en werkt nauw samen met de lidstaten en instanties van de EU, aan de versterking van de cyberweerbaarheid binnen de Unie. Zo is het kabinet van mening dat ENISA een belangrijke rol speelt als expertisecentrum op het gebied van cybersecurity, en als coördinerend en ondersteunend orgaan fungeert binnen diverse EU-samenwerkingsverbanden (zoals het CSIRT-netwerk, EU-Cyclone, en de NIS Cooperation Group). Ook speelt ENISA een belangrijke rol als het gaat om de implementatie van effectieve EU-cybersecurity wetgeving, en een faciliterende en ondersteunende rol voor de operationele samenwerking tussen lidstaten. Het kabinet acht de ontwikkeling van cybersecurity-tools, -technieken, -en infrastructuur als essentiële taak voor de ondersteuning van nationale CSIRT’s. Deze voorziene rollen en taken zijn gepubliceerd in een non-paper ondertekend door 21 lidstaten waaronder Nederland. Het kabinet pleit in de Europese onderhandelingen voor dit takenpakket voor ENISA, en zal zich hier actief voor inzetten tijdens de onderhandelingen.

18. Zij zijn positief over het voorstel voor een certificeringsraamwerk. Dit zorgt volgens hen voor een eerlijkere markt, waarin Europese aanbieders vooraf kunnen aantonen dat zij voldoen aan alle relevante wet- en regelgeving. De leden van de GroenLinks-PvdA-fractie hopen ook dat autonomie expliciet onderdeel wordt van het Europese raamwerk, zodat aanbieders die bewezen autonome diensten leveren bij aanbestedingen een eerlijke kans krijgen. Is dit het geval, en deelt het kabinet deze opvatting? Deze leden lezen voorts dat het kabinet zich inzet “om te zorgen dat certificering technisch van aard blijft”: zij vragen om dit standpunt uit te leggen. Hoe heeft Nederland dit bepleit? Ook vragen deze leden welke termijn voor het opstellen van certificatieschema's wél reëel is.

Antwoord
Ten aanzien van het certificeringsraamwerk benadrukt het kabinet dat certificering technisch van aard moet blijven. Daarmee wordt bedoeld dat certificering zich moet richten op toetsbare, objectieve en technisch-inhoudelijke beveiligingseisen en niet moet verschuiven naar een breed politiek of geopolitiek instrument zonder duidelijke normatieve begrenzing. Het kabinet ziet de gedachte achter meer autonomie en een eerlijkere markt, maar is terughoudend met het expliciet opnemen van autonomie als zelfstandig certificeringscriterium als dat onvoldoende scherp en objectief af te bakenen is. Certificering moet helder en voorspelbaar blijven voor marktpartijen en gebaseerd zijn op concrete veiligheidsvereisten, zodat zij juridisch houdbaar en praktisch uitvoerbaar blijft. Nederland heeft in het fiche benadrukt dat certificering technisch van aard moet blijven en niet mag leiden tot onevenredige lasten, verplichtstelling zonder voldoende basis of feitelijke vervanging van toezicht. Ten aanzien van de termijnen voor certificatieschema’s

acht het kabinet de door de Commissie beoogde snelheid ambitieus. Een reële termijn hangt af van de complexiteit van het betreffende certificeringsschema, de betrokken sector en de beschikbaarheid van technische standaarden. Het kabinet vindt dat certificeringsschema's pas moeten worden vastgesteld wanneer kwaliteit, uitvoerbaarheid en draagvlak voldoende zijn geborgd.

19. Zij onderschrijven de zorg dat het toezicht op orde moet blijven en niet feitelijk verzwakt mag worden. De leden van de GroenLinks-PvdA-fractie vragen het kabinet welke voorstellen zij doet om de toezichthouders in positie te houden. Het pleidooi van het kabinet voor risico-gebaseerd en niet-discriminatoir uitsluiten van leveranciers staat op gespannen voet met wat de Commissie voorstelt en de rol van ENISA die groeit. Ook krijgt de Commissie de bevoegdheid om hele landen aan te wijzen als riskant en om leveranciers als "hoog risico" aan te merken. Hoe kijkt het kabinet naar deze bevoegdheid van de Commissie in relatie tot de interventiebevoegdheid die is opgenomen in het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten?[5] Is het weren van producten en diensten bij entiteiten onder de CSA2 nog een nationale bevoegdheid? Hoe ziet het kabinet dit voor zich?

Antwoord
Het kabinet pleit voor een goede samenhang tussen Europese instrumenten en nationale instrumenten, ook waar dit de interventiebevoegdheid betreft. Daarom zal het kabinet de proportionaliteit en de uitvoerbaarheid van de nieuw voorgestelde maatregelen doorlopend als

[5] Er zijn twee amendementen ingediend door het lid Kathmann die deze bevoegdheid naar de wet overhevelen [Kamerstukken 36764, nr. 25 en Kamerstuk 36765, nr. 13].

aandachtspunt inbrengen. In dat licht benadrukt het kabinet het belang van artikel 98, derde lid, waardoor lidstaten de bevoegdheid behouden om zelfstandig aanvullende maatregelen te nemen om hun cyberbeveiligingsniveau te waarborgen. Het kabinet onderstreept ook dat de bescherming van de nationale veiligheid een uitsluitende verantwoordelijkheid van de lidstaten is. Voor de inmiddels in de voorstellen voor de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten opgenomen bevoegdheid om entiteiten te verbieden gebruik te maken van producten of diensten van specifieke leveranciers geldt dat gebruikmaking daarvan nadrukkelijk is gekoppeld aan de noodzaak om risico's voor de nationale veiligheid te beheersen. Het kabinet acht het van belang dat het de lidstaten vrijstaat om op nationaal niveau entiteiten een verbod op te leggen om producten of diensten die van leveranciers te gebruiken, op basis van een eigenstandige afweging ten aanzien van bijvoorbeeld specifiek voor entiteiten binnen die lidstaat geldende dreigingen betreffende leveranciers uit derde landen.

20. Deze leden benadrukken de noodzaak om strategische digitale afhankelijkheden af te bouwen. Het grootste cyberveiligheidsrisico in hun ogen is de totale dominantie van enkele niet-Europese bedrijven in de digitale markt. Dit maakt de EU als geheel gevoelig voor politieke druk. De CSA2 mag dan ook niet uitsluitend zien op het weren van Chinese leveranciers, terwijl keer op keer wordt erkend dat ook de Verenigde Staten de machtspositie van haar techgiganten misbruikt om druk uit te oefenen op Europese besluitvorming. Ook moeten deze bedrijven voldoen aan Amerikaanse spionagewetgeving, zoals de CLOUD Act, de Foreign Intelligence Surveillance Act, en Executive Order 12333. Welke rol ziet het kabinet voor de CSA2 weggelegd om marktmonopolies te

doorbreken? Voldoen Amerikaanse leveranciers, die moeten voldoen aan de zojuist genoemde wetgeving, aan de criteria om aangemerkt te worden als “hoog risico” en afkomstig uit “een land dat cyberzorgen met zich meebrengt”? Zo nee, waarom zij niet, en Chinese leveranciers in de telecomsector bijvoorbeeld wel?

Antwoord
Het kabinet erkent zorgen over strategische afhankelijkheden, ook richting niet-Europese aanbieders. De Cybersecurity Act dient echter primair als middel om de cyberbeveiliging in de EU te bevorderen en risico’s daaromtrent te mitigeren. Zo is het doorbreken van marktmonopolies geen doel op zich, maar kan een te grote afhankelijkheid van één leverancier veiligheidsrisico’s met zich meebrengen. In dit verband kan worden gewezen op artikel 103, tweede lid, onderdeel g van de CSA2 waarin wordt bepaald dat via een uitvoeringshandeling aan essentiële en belangrijke entiteiten ook mitigerende maatregelen kunnen worden opgelegd met betrekking tot diversificatie van de toeleveringsketen. Daarnaast benadrukt het kabinet het belang van een risico-gebaseerd en casus-gericht raamwerk, waarbij op basis van objectieve criteria en een gedegen risicobeoordeling de maatregelen geformuleerd worden die zich verhouden tot het vastgestelde risico. In dat licht plaatst het kabinet dan ook kanttekeningen bij de generieke landen- en leveranciersaanwijzing.

21. Tot slot vragen de leden van de GroenLinks-PvdA-fractie of ook overwogen is om het uitsluiten van producten en diensten minder afhankelijk te maken van het land van afkomst. Een product uit een bevriend land kan evengoed een kwetsbaarheid bevatten die cyberrisico's met zich meedraagt. Wat vindt het kabinet van een nationale, of zelfs een Europese,

bevoegdheid om productverboden of leveranciersverboden op te leggen, los van de banden met een land? Zijn deze mogelijkheden onderzocht in het kader van de Cbw en de Wwke, die nu enkel een interventiebevoegdheid bevatten die ziet op het weren van producten en diensten bij specifieke entiteiten in plaats van een algemene interventie op het mogen leveren van die producten en diensten?

Antwoord
Het kabinet onderschrijft het belang van een casus-gerichte en risico-gebaseerde benadering, waarbij mitigerende maatregelen dus voornamelijk afhankelijk zijn van het vastgestelde risico voor de beveiliging van netwerk- en informatiesystemen. Hierdoor zijn mitigerende maatregelen gericht en staan zij in redelijke verhouding tot het beoogde doel om risico's te mitigeren. Voor de in de wetsvoorstellen voor de Cbw en de Wwke opgenomen interventiebevoegdheid geldt dat het verbod op gebruik van producten of diensten van specifieke leveranciers aan een essentiële entiteit of belangrijke entiteit zal worden opgelegd, indien dat gelet op hun specifiek betreffende omstandigheden ter beheersing van beveiligingsrisico's die de nationale veiligheid raken noodzakelijk is. De inzet van deze bevoegdheid richt zich dus bewust op maatwerk per entiteit, om in het bijzonder ook proportionaliteit te waarborgen. Een algemene bevoegdheid om producten of diensten in algemene zin van de markt te weren is in dat kader niet als uitgangspunt gekozen. Het kabinet blijft wel bezien of het bestaande instrumentarium voldoende toereikend is in het licht van veranderende risico's en Europese ontwikkelingen. Het kabinet mist deze risico-gebaseerde en casus-gerichte aanpak binnen het raamwerk, en is om deze reden kritisch op de bevoegdheid om een derde land als geheel aan te

wijzen als een land dat aanleiding geeft tot bezorgdheid over cyberbeveiliging. Het kabinet vindt daarnaast dat het voorstel op dit moment onduidelijk is over de vraag of alle leveranciers, afkomstig uit of onder invloed staand van het aangewezen derde land én aanwezig in de ICT-toeleveringsketen van essentiële of belangrijke entiteiten, direct gelden als een hoog-risicoleverancier. Het kabinet wijst op de mogelijk omvangrijke gevolgen van deze aanwijzingen. Het kabinet zal zich daarom gedurende de onderhandelingen inspannen voor een risico-gestuurd raamwerk.

Vragen en opmerkingen van de leden van de CDA-fractie

22. De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de fiches over de herziening van de Cybersecurity Act en de vereenvoudiging van de NIS2-richtlijn. Deze leden onderschrijven het belang van een sterker Europees cyberbeveiligingskader en van het verminderen van risicovolle strategische afhankelijkheden in vitale digitale infrastructuur. Tegelijk achten zij het van belang dat nieuwe Europese bevoegdheden voldoende risico-gebaseerd, proportioneel en uitvoerbaar blijven, en dat nationale veiligheidsafwegingen en effectief toezicht niet onnodig worden uitgehold. De leden van de CDA-fractie lezen dat de Commissie de bevoegdheid krijgt om derde landen en leveranciers als hoog risico aan te wijzen en daaraan bindende gevolgen te verbinden. Deze leden vragen op basis van welke criteria deze aanwijzingen plaatsvinden, welke rol lidstaten in deze besluitvorming behouden en hoe wordt geborgd dat nationale dreigingsbeelden en

bestaande nationale instrumenten voldoende gewicht houden.

Antwoord
De Europese Commissie hanteert in artikel 100 een aantal criteria die worden betrokken bij de beoordeling of een derde land als een hoog risico wordt aangewezen, zoals het bestaan van wetten in het derde land die entiteiten verplichten informatie over kwetsbaarheden te delen met de autoriteiten of ontbrekende juridische en rechtsstatelijke waarborgen. In artikel 104 schetst de Commissie de criteria om leveranciers als hoog-risico aan te wijzen, waarbij de Commissie met name kijkt naar welke leveranciers in de ICT-toeleveringsketen mogelijk zijn gevestigd in een aangewezen derde land of onder zeggenschap staan van dat derde land, van een in dat derde land gevestigde entiteit of van een onderdaan van dat derde land.
Het kabinet is van oordeel dat de aanwijzing van derde landen en leveranciers geheel als ‘hoog risico’ onwenselijk is, omdat de mate van risico sterk afhankelijk is van het geleverde ICT-onderdeel, de geleverde (kritieke) dienst en reeds genomen technisch-organisatorische maatregelen. Daarnaast dienen eventuele mitigerende maatregelen uitsluitend te worden vastgesteld op basis van transparante, objectieve en toetsbare criteria. Het kabinet benadrukt dat dergelijke besluiten niet louter technisch zijn, maar ook aanzienlijke veiligheids- en economische implicaties hebben. Lidstaten behouden een rol bij zowel de landen- als de leveranciersaanwijzing, omdat in het huidige voorstel deze aanwijzingen via een uitvoeringshandeling zullen worden geïmplementeerd. Tegelijkertijd is het kabinet van mening dat deze aanwijzingen, naast een technisch-juridische weging, ook een politieke afweging vergt vanwege de mogelijk

verstrekkende gevolgen. Bij beslissingen met grote geopolitieke gevolgen is voor het kabinet het niveau van besluitvorming daarom ook relevant. Het kabinet zal zich om deze reden ook inzetten voor een evenwichtigere rolverdeling tussen de Europese Commissie en de lidstaten binnen het raamwerk. Daarnaast pleit het kabinet voor een goede samenhang tussen nationale en Europese instrumenten, en onderstreept in dat licht in elk geval dat de bescherming van de nationale veiligheid een uitsluitende verantwoordelijkheid van de lidstaten is. Het kabinet acht het van belang dat het lidstaten vrij blijft staan om op basis van een eigenstandige afweging, bijvoorbeeld ter bescherming van de nationale veiligheid, mitigerende maatregelen te nemen.

23. Voorts vragen zij hoe het kabinet aankijkt tegen de proportionaliteit en uitvoerbaarheid van de verplichte uitfasering van technologie van hoog-risicoleveranciers, in het bijzonder in telecom- en andere vitale netwerken. Welke voorwaarden acht het kabinet daarbij noodzakelijk ten aanzien van de continuïteit van dienstverlening, de beschikbaarheid van alternatieve technologie, differentiatie naar het risicoprofiel van netwerkonderdelen en realistische overgangstermijnen?

Antwoord
Het kabinet acht een aantal randvoorwaarden cruciaal bij eventuele verplichte uitfasering. Allereerst moet de continuïteit van essentiële dienstverlening gewaarborgd blijven. Daarnaast is het van belang dat er voldoende beschikbare en betrouwbare alternatieve leveranciers zijn, zodat entiteiten daadwerkelijk kunnen overstappen. Verder acht het kabinet differentiatie naar het risicoprofiel van onderdelen van

netwerk- en informatiesystemen noodzakelijk. Niet alle onderdelen van een netwerk- en informatiesysteem zijn even kritiek; een generieke verplichting zonder onderscheid kan leiden tot onnodige lasten. Tot slot zijn realistische overgangstermijnen essentieel, zodat entiteiten de tijd hebben om aanpassingen zorgvuldig door te voeren zonder verstoring van hun dienstverlening.

24. De leden van de CDA-fractie lezen daarnaast dat certificering een veel centralere rol krijgt binnen het Europese cyberkader. Deze leden vragen hoe het kabinet voorkomt dat certificering in de praktijk een indirect instrument voor uitsluiting of markttoegang wordt, terwijl de onderliggende Europese certificeringskaders nog niet volledig zijn uitgewerkt. Ook vragen zij hoe wordt voorkomen dat het verminderen van afhankelijkheden uiteindelijk leidt tot nieuwe afhankelijkheden van een zeer beperkt aantal leveranciers.

Antwoord
Met betrekking tot certificering onderkent het kabinet dat een grotere rol van certificering voordelen kan bieden, maar ook risico’s met zich meebrengt. Het kabinet acht het van belang dat certificering primair een technisch instrument blijft dat gericht is op het aantonen van cyberbeveiligingsniveau, en niet de facto een instrument wordt voor markttoegang -of uitsluiting zonder dat de onderliggende kaders voldoende zijn uitgewerkt. Certificering mag niet vooruitlopen op certificeringsschema’s die nog niet volledig operationeel of uitgekristalliseerd zijn. Daarom zet het kabinet zich ervoor in dat certificeringsschema’s pas verplicht worden gesteld wanneer zij voldoende duidelijk, uitvoerbaar en beschikbaar zijn en dat bedrijven niet worden geconfronteerd met

verplichtingen waaraan zij feitelijk nog niet kunnen voldoen.
Daarnaast deelt het kabinet de zorg dat het verminderen van afhankelijkheden van bepaalde leveranciers niet mag leiden tot nieuwe afhankelijkheden van een beperkte groep alternatieve leveranciers. Het kabinet acht het daarom van belang dat beleid gericht is op diversificatie, het voorkomen van *lock-ins* en het stimuleren van een bredere en meer concurrerende leveranciersbasis, inclusief versterking van het Europese technologische ecosysteem. Het kabinet benadrukt dat strategische autonomie niet betekent dat afhankelijkheden worden verschoven, maar dat deze worden verminderd en beter beheersbaar worden gemaakt.

25. Ten aanzien van de vereenvoudiging van NIS2 vragen de leden van de CDA-fractie hoe het kabinet zich inzet om audit- en inspectiebevoegdheden van nationale toezichthouders te behouden, juist omdat certificering niet steeds een volledig beeld geeft van actuele risico’s of sectorspecifieke kwetsbaarheden. Ook vragen deze leden hoe ruimte behouden blijft voor andere bestaande normenkaders, zodat dubbel werk en onnodige lasten worden voorkomen**.**

Antwoord
Om de audit- en inspectiebevoegdheden van nationale toezichthouders te behouden, evenals ruimte te laten voor andere bestaande normenkaders, zet het kabinet in Brussel in op meerdere sporen. In de eerste plaats zal Nederland het belang van het behouden van zowel de bevoegdheden als de ruimte voor bestaande normenkaders, om zo onder meer de uitvoeringslasten voor entiteiten te beperken, actief inbrengen bij de onderhandelingen. Daarnaast zoekt het kabinet actief

naar lidstaten die dezelfde zorgen hebben zodat dit standpunt gezamenlijk ingebracht kan worden.

26. Tot slot vragen zij hoe het kabinet de versterkte rol van het ENISA en de voorgestelde maximumharmonisatie beoordeelt. Waar ligt voor het kabinet de grens tussen nuttige Europese coördinatie en een onwenselijke beperking van nationale beleidsruimte, zeker wanneer nationale veiligheid of een specifieke dreiging aanleiding geeft tot aanvullende maatregelen?

Antwoord
Voor het kabinet is het van belang dat ENISA geen operationele taken toebedeeld krijgt die raken aan nationale competenties of overlappen met bestaande nationale structuren. Daarbij geldt in het bijzonder dat de bescherming van de nationale veiligheid een uitsluitende verantwoordelijkheid van lidstaten betreft. Europese samenwerking is noodzakelijk en wenselijk, maar mag bijvoorbeeld niet verhinderen dat lidstaten zelfstandig aanvullende maatregelen nemen wanneer hun nationale dreigingsbeeld daartoe aanleiding geeft. Het kabinet zet zich daarom in voor een evenwichtige benadering, waarbij Europese maatregelen ondersteunend zijn aan nationale inspanningen en niet beperkend. In het bijzonder moet ruimte blijven bestaan voor sectorspecifieke maatregelen en snelle interventies bij acute dreigingen. In dit kader beoordeelt het kabinet de versterkte rol van ENISA in beginsel positief, maar benadrukt dat ENISA geen taken dient uit te voeren die raken aan nationale competenties of overlappen met al bestaande nationale structuren en dienstverlening.

Vragen en opmerkingen van de leden van de JA21-fractie

27. De leden van de JA21-fractie hebben kennisgenomen van de onderhavige stukken inzake de fiches over de herziening van de Cybersecurity Act en de vereenvoudiging van de NIS2-richtlijn. Deze leden besteden graag aandacht aan de versterkte rol van ENISA binnen het kader van het voorstel voor de herziening van de Cyber Security Act. ENISA fungeert als expertisecentrum voor cyberbeveiliging binnen de EU en krijgt met het voorstel een aanzienlijk uitgebreid mandaat, waarbij de organisatie zowel coördinerend als operationeel optreedt op het gebied van beleid, regelgeving en capaciteitsopbouw. ENISA zal een belangrijke rol vervullen bij de operationele samenwerking tussen lidstaten, onder meer door het faciliteren van informatie-uitwisseling. Zo wordt ENISA ook verantwoordelijk voor een early alerts-dienst voor CSIRT's en entiteiten, en voor het monitoren van trends en ransomware-aanvallen. Bovendien zal ENISA ondersteuning bieden bij concrete incidenten via een helpdesk. Deze leden zien deze versterking van ENISA als een kans voor betere samenwerking, maar wijzen ook op een aantal aandachtspunten en potentiële risico's op het gebied van coördinatie en verantwoordelijkheidsafbakening. Deze leden hebben de volgende vragen: hoe voorkomen we overlap of dubbel werk tussen ENISA en de nationale CSIRT's, en wie grijpt in als er overlap ontstaat? Kan het kabinet toelichten wat er gebeurt bij grensoverschrijdende incidenten die meerdere lidstaten raken: wie heeft de leiding en regie? Kan het kabinet verduidelijken, hoe bij grootschalige grensoverschrijdende incidenten de coördinatie wordt georganiseerd, en hoe versnippering wordt voorkomen als operationele taken bij nationale CSIRT's blijven?

Antwoord

Het kabinet zal zich tijdens de onderhandeling actief inzetten om duplicatie van (operationele) taken tussen ENISA en nationale CSIRT's te voorkomen. Het kabinet benadrukt dat ENISA geen operationele taken toebedeeld dient te krijgen en 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 een *early alerts helpdesk* van ENISA en heeft vragen over de voorgestelde rol om steun te verlenen rondom ransomware incidenten. Het kabinet ziet hier overlap met bestaande structuren en (nationale) competenties, waaronder de dienstverlening van nationale CSIRT's en het mandaat van Europol. Voor wat betreft de rol van ENISA in relatie tot grensoverschrijdende incidenten, ENISA vervult een ondersteunde rol bij de informatiedeling tussen de lidstatelijke CSIRT's en crisisbeheersingsautoriteiten. ENISA fungeert daarnaast als het secretariaat van het EU-CyCLONe netwerk en het CSIRT-netwerk die worden geactiveerd bij grensoverschrijdende cyberincidenten in de EU.

28. Zij besteden verder graag aandacht aan het voorstel van de Cyber Security Act rond de aanwijzing van hoog-risicoleveranciers binnen Europese en nationale infrastructuren. Het voorstel geeft de Europese Commissie de bevoegdheid om leveranciers uit derde landen, zoals China, Rusland en Noord-Korea, aan te merken als hoog-risico. Leveranciers die als hoog-risico worden aangemerkt, mogen vervolgens niet deelnemen aan overheidsaanbestedingen of aanspraak maken op EU-financiering. Dit kan bijdragen aan het versterken van de cyberbeveiliging. Tegelijkertijd kunnen lidstaten zelf hoog-risico leveranciers aanwijzen, waardoor sprake is van een combinatie van nationale en EU-brede maatregelen. Dit beleid is gericht op het versterken van de cyberveiligheid en

strategische autonomie van Europa, blijven er belangrijke vragen bestaan op het gebied van proportionaliteit, nationale zeggenschap en de betrouwbaarheid van de risicobeoordelingen. Het instrument dat de Europese Commissie zal introduceren voor risicobeoordelingen is namelijk nog niet volledig operationeel, enkel deels, waardoor extra aandacht voor waarborgen en uitvoering nodig is. De leden van de JA21-fractie zijn tevreden over deze strategische autonomie, maar hebben de volgende vragen: in hoeverre wordt het proportionaliteitsbeginsel gehanteerd, zodat economische schade beperkt blijft wanneer leveranciers als hoog-risico worden aangemerkt? Kan het kabinet verduidelijken welke mogelijkheden en criteria er bestaan om een leverancier in de toekomst weer van de hoog-risicolijst te verwijderen? Is er voorzien in periodieke herbeoordeling? Kan het kabinet verder toelichten in hoeverre lidstaten zelf de controle over de aanwijzing van hoog-risico leveranciers (preventieve uitsluiting) behouden? Kan het kabinet bovendien toelichten hoe wordt voorkomen dat de Europese Commissie te veel macht krijgt in nationale veiligheidskwesties? Kan het kabinet tot slot toelichten hoe betrouwbaar de risicobeoordelingen zijn, en of er hierbij voldoende handvatten voor de uitvoering zijn, aangezien het instrument dat de Commissie zal introduceren nog niet (geheel) aanwezig is?

Antwoord
Het kabinet acht het proportionaliteitsbeginsel essentieel bij het aanwijzen van hoog-risicoleveranciers. Dit betekent dat daaraan gekoppelde maatregelen in verhouding moeten staan tot het vastgestelde risico. Het kabinet zal de proportionaliteit en praktische uitvoerbaarheid van de voorgenomen maatregelen uit het raamwerk

doorlopend als aandachtspunt inbrengen in de verdere onderhandelingen.
Het kabinet acht het van belang dat er duidelijke en transparante criteria bestaan om leveranciers van de hoog-risicolijst te verwijderen. Het kabinet vindt het voorstel hierover onvoldoende duidelijk. Het voorstel specificeert weliswaar in artikel 104, zevende lid, dat de Europese Commissie de lijst regelmatig zal bijwerken ‘met het oog op de schrapping of toevoeging van leveranciers met een hoog risico’, maar de criteria voor verwijdering en periodieke herbeoordeling zijn alsnog onduidelijk. Zo’n mechanisme vereist tevens dat leveranciers aantoonbaar risico’s hebben gemitigeerd of dat omstandigheden zijn gewijzigd. Het kabinet zet zich in voor een dynamisch systeem waarin herbeoordeling mogelijk is.
Hoewel het kabinet een Europese aanpak onderschrijft, zal het kabinet doorlopend pleiten voor een stevigere rol van de lidstaten in alle onderdelen van het raamwerk. Hierbij merkt het kabinet op dat met name ook de aanwijzingscriteria van hoog-risicoleveranciers en de criteria om op Europees niveau mitigerende maatregelen te treffen onduidelijk en breder dan noodzakelijk zijn. Het kabinet zal dit, gedurende de onderhandelingen, onder de aandacht brengen. Ook is het kabinet van mening dat een dergelijke aanwijzing een politieke afweging vergt, vanwege de mogelijk verstrekkende gevolgen. Bij beslissingen met grote geopolitieke gevolgen is voor het kabinet het niveau van besluitvorming daarom ook relevant. In dat licht pleit het kabinet voor een goede samenhang tussen nationale en Europese instrumenten en benadrukt het kabinet in dat geval de bescherming van de nationale veiligheid een uitsluitende verantwoordelijkheid van de lidstaten blijft. Het kabinet zal zich daarnaast inzetten voor een evenwichtigere rolverdeling tussen de

Europese Commissie en de lidstaten binnen het Europees kader voor ICT-toeleveringsketens.
Het kabinet is positief over het principe om op basis van een risicobeoordeling maatregelen te formuleren, gericht op specifieke producten of diensten van specifieke leveranciers, die uiteindelijk een bindend karakter kunnen krijgen binnen de EU. Tegelijkertijd acht het kabinet de kwaliteit van de huidige beveiligingsrisicobeoordelingen onvoldoende robuust om op basis daarvan dergelijke bindende maatregelen te formuleren. Zo is de benodigde informatie voor een kwalitatief robuuste beoordeling, mede vanwege het gevoelige en gerubriceerde karakter, vaak enkel op nationaal niveau beschikbaar. Het kabinet zal daarom pleiten voor voldoende robuuste risicobeoordelingen.

29. Deze leden willen daarnaast nog aandacht vragen voor de evaluatiebepaling van het voorstel. Volgens het voorstel vindt een eerste evaluatie plaats na vijf jaar, gevolgd door periodieke evaluaties elke vijf jaar. Tegelijkertijd wordt voorzien dat de implementatie van het voorstel circa anderhalf jaar in beslag zal nemen, waardoor de regeling pas na verloop van tijd volledig operationeel zal zijn.
Zij merken op dat dit betekent dat eventuele knelpunten of onvoorziene effecten pas relatief laat in beeld komen. Juist bij complexe en ingrijpende regelgeving op het gebied van cybersecurity, waarin technologische ontwikkelingen en dreigingen zich snel opvolgen, is het van belang dat wetgeving tijdig kan worden bijgesteld indien deze in de praktijk niet effectief of proportioneel blijkt te zijn. Een te lange evaluatietermijn kan ertoe leiden dat inefficiënties of uitvoeringsproblemen onnodig lang blijven bestaan. Een evaluatietermijn van drie jaar zou daarom passend zijn. Kan het kabinet toelichten of de evaluatietermijn kan worden verkort en of een eerste evaluatie na drie

jaar niet passender zou zijn, zodat eventuele tekortkomingen eerder kunnen worden gesignaleerd en aangepakt?

Antwoord
Het kabinet begrijpt de zorg dat een evaluatietermijn van vijf jaar relatief lang is gezien de dynamiek van het cyberdomein. Het Kabinet staat om deze reden open voor een kortere eerste evaluatietermijn, bijvoorbeeld na drie jaar, mits dit uitvoerbaar is en voldoende gegevens beschikbaar zijn om een zinvolle evaluatie te doen.

30. De leden JA21-fractie willen tevens aandacht vragen voor de samenloop van verschillende wettelijke kaders op het gebied van cyberbeveiliging. Organisaties kunnen in de praktijk onder meerdere wetten vallen, zoals de Wet weerbaarheid kritieke entiteiten (Wwke), de Cyberbeveiligingswet (Cbw) en de Cybersecurity Act, die elk eigen verplichtingen kennen, bijvoorbeeld ten aanzien van zorgplicht, meldplicht en certificering. Dit kan ertoe leiden dat bij niet-naleving meerdere sancties worden opgelegd voor verschillende overtredingen. Deze leden begrijpen dat niet twee bestuurlijke boetes naast elkaar kunnen worden opgelegd indien het gaat om dezelfde overtreding. Het kan echter voorkomen dat de overtredingen verschillend zijn. Kan het kabinet daarom toelichten hoe in de praktijk wordt geborgd dat toezichthouders gescheiden sancties opleggen voor verschillende wettelijke verplichtingen, en hoe wordt voorkomen dat dit leidt tot onevenredige (financiële) lasten voor organisaties, terwijl tegelijkertijd de cyberweerbaarheid en naleving van alle relevante regels wordt gewaarborgd?

Antwoord

Het kabinet erkent dat samenloop van verschillende wettelijke kaders kan leiden tot complexiteit. Daarom wordt geborgd dat toezichthouders hun optreden afstemmen en dat er geen dubbele bestraffing plaatsvindt voor dezelfde overtreding. Wanneer sprake is van verschillende verplichtingen, kunnen afzonderlijke sancties worden opgelegd. Toezichthouders houden daarbij in de praktijk rekening met de totale lasten voor organisaties en stemmen hun handhaving hierop af, zodat onevenredige (financiële) lasten worden voorkomen.

31. Zij willen tot slot ingaan op de voorgestelde verplichting tot uitfasering van apparatuur van hoog-risicoleveranciers binnen kritieke infrastructuren. Deze verplichting kan grote financiële en operationele gevolgen hebben voor telecombedrijven en andere aanbieders van vitale diensten. Daarbij speelt dat niet alle netwerkonderdelen per definitie een hoog risicoprofiel hebben, waardoor het niet noodzakelijk hoeft te zijn om alle apparatuur te vervangen. Dit roept vragen op over de proportionaliteit en uitvoerbaarheid. De leden van de JA21-fractie maken zich zorgen over het feit dat lidstaten verschillen in hun afhankelijkheid van specifieke buitenlandse leveranciers, wat de onderhandelingen complex maakt en kan leiden tot politieke spanningen. Ook is het van belang dat maatregelen rondom uitfasering in lijn zijn met bestaande handelsafspraken en internationale verplichtingen, en dat zij niet leiden tot nadelige effecten voor de concurrentiepositie van Europese bedrijven. Tegelijkertijd moet worden voorkomen dat het beperken van het aantal toegestane leveranciers juist leidt tot nieuwe afhankelijkheden. Deze leden stellen daarom de volgende vragen: kan het kabinet toelichten of de uitfasering van Chinese of andere buitenlandse technologieën wordt afgestemd op

bestaande handelsafspraken of internationale verplichtingen? Kan het kabinet verduidelijken hoe het beleid bij kan dragen aan strategische autonomie zonder Europese bedrijven te benadelen in internationale concurrentie, mede gezien het feit dat niet elk netwerkonderdeel een hoog risicoprofiel heeft? Kan het kabinet ook toelichten hoe de verwachte kosten eruit zien voor kleinere bedrijven of leveranciers van kritieke infrastructuur, en kan het kabinet toelichten hoe deze kleinere bedrijven financiële lasten redelijkerwijs kunnen dragen, wordt er rekening gehouden met de financiële draagkracht? Hoe waarborgt het kabinet bovendien dat Cyber Security Act niet leidt tot een te beperkte groep leveranciers en zo de strategische afhankelijkheid vergroot? Kan het kabinet eveneens benadrukken hoe lock-ins (vastzitten aan één leverancier) en operationele kwetsbaarheid worden voorkomen, wanneer bepaalde leveranciers beperkt beschikbaar zijn?

Antwoord
Het kabinet acht het van belang dat de voorgestelde maatregelen in overeenstemming met de internationale verplichtingen van de EU worden vormgegeven, waaronder de akkoorden van de Wereldhandelsorganisatie en bilaterale handelsakkoorden. Het kabinet zal dit gedurende de onderhandelingen onder de aandacht brengen.
Het kabinet ziet de Cybersecurity Act primair als een instrument om de cyberbeveiliging van de EU te bevorderen, cyberbeveiligingsrisico’s te mitigeren en een geharmoniseerde toepassing van deze maatregelen in de Unie te bevorderen. Dit draagt op termijn bij aan de concurrentiekracht van de Europese economie, omdat een uniform kader uiteenlopende nationale maatregelen tegengaat en rechtszekerheid biedt. Het

kabinet ziet in dat licht meerwaarde om in bepaalde gevallen op Europees niveau mitigerende maatregelen te nemen, omdat dit bijdraagt aan een uniforme toepassing in de digitale interne markt en ongewenste overloopeffecten tegengaat. Tegelijkertijd benadrukt het kabinet een risico-gebaseerde en casus-gerichte aanpak, waarbij maatregelen proportioneel zijn en zich verhouden tot het vastgestelde risico. Hierbij onderschrijft het kabinet dat de mate van risico onder meer sterk afhankelijk is van het geleverde netwerk- en informatiesysteemonderdeel.
In de impact assessment van het voorstel stelt de Europese Commissie dat het mkb profiteert van betrouwbare technologie in ICT-toeleveringsketens, maar onderkent tegelijkertijd dat de impact groot is voor bedrijven of leveranciers op wie de restrictieve maatregelen van toepassing zijn.
Het kabinet pleit voor een ICT-toeleveringsketenraamwerk dat recht doet aan de onderlinge verscheidenheid van ICT-toeleveringsketens in de Unie, en daarmee voldoende maatwerk kan bieden. In artikel 103, vierde lid, houdt de Europese Commissie rekening met de potentiële risico’s op afhankelijkheden, met name ook waar dit gaat om aanwezigheid van alternatieve leveranciers. Het kabinet zal gedurende de onderhandelingen dan ook benadrukken dat de criteria om op Europees niveau mitigerende maatregelen te treffen duidelijk omschreven dienen te zijn, dat deze zich goed verhouden tot reeds getroffen maatregelen en rekening houden met de onderlinge verscheidenheid van ICT-toeleveringsketens.
Het kabinet benadrukt dat ICT-toeleveringsketens in kritieke sectoren binnen de Unie van elkaar kunnen verschillen. Wat het kabinet betreft dient het raamwerk recht te doen aan deze onderlinge verscheidenheid en zich goed te verhouden tot eventuele operationele

kwetsbaarheden in verschillende toeleveringsketens. In dat licht pleit het kabinet voor duidelijkere criteria waarmee op Europees niveau mitigerende maatregelen genomen kunnen worden, zodat deze maatregelen zich goed verhouden tot specifieke nationale omstandigheden en reeds getroffen maatregelen.

32. Zij hebben gezien dat het voorstel een nieuwe categorie kleinere bedrijven (‘small mid-cap’), introduceert, zodat zij onder lichter toezicht vallen. Ook European Business Wallets vallen nu ook onder de Richtlijn. Bedrijven kunnen aantonen dat ze voldoen aan de zorgplicht via een certificaat, waardoor extra audits door toezichthouders niet nodig zijn. Dit verlaagt de regeldruk, vooral voor bedrijven die in meerdere EU-landen actief zijn. De leden van de fractie JA21-fractie hebben de volgende vragen: Kan het kabinet aangeven welke Nederlandse entiteiten door deze wijzigingen nieuw in scope komen, waaronder ook European Business Wallets, en hoeveel entiteiten naar verwachting geraakt worden door de nieuwe categorie small mid-cap? Wat betekent dit concreet voor toezicht, regeldruk en cyberweerbaarheid? Kan het kabinet bovendien toelichten hoeveel Nederlandse entiteiten hierdoor naar verwachting van essentieel naar belangrijk zullen verschuiven met de introductie van de nieuwe categorie small mid-cap?

Antwoord
Voor de uitbreiding van het toepassingsbereik van de NIS2-richtlijn met enkele nieuwe soorten entiteiten, zoals aanbieders van European Business Wallets, geldt dat het kabinet verwacht dat een bredere groep van soorten entiteiten onder deze richtlijn zal vallen. Het kabinet beschikt op dit moment nog niet over exacte aantallen voor Nederland. Datzelfde geldt voor de hoeveelheid entiteiten die vanwege de voorgestelde

introductie van de categorie small mid-cap, in plaats van als essentiële entiteit, als belangrijke entiteit zullen worden aangemerkt. In algemene zin kan worden opgemerkt dat de introductie van deze categorie zal leiden tot een lichter toezichtregime voor bepaalde entiteiten en daarmee tot een vermindering van de regeldruk. Tegelijkertijd blijft het van belang dat deze differentiatie niet leidt tot een afname van het daadwerkelijke cyberbeveiligingsniveau. Daarvan zal naar het oordeel van het kabinet naar verwachting geen sprake zijn, met name ook omdat voor zowel essentiële entiteiten als belangrijke entiteiten verplichtingen als de zorgplicht en de meldplicht onverminderd van toepassing zijn.

33. Deze leden lezen verder dat het kabinet een bredere definitie van ransomware voorstaat en wil dat essentiële informatie in de richtlijn zelf wordt opgenomen. Welke definitie van ransomware wil het kabinet concreet bepleiten, mede gelet op nieuwe vormen van afpersing waarbij niet uitsluitend sprake is van versleuteling, maar wel van een losgeldeis? Acht het kabinet het verder wenselijk dat informatie over aanvalsvectoren, ransom-verzoeken, betalingen en betaalde bedragen rechtstreeks in de richtlijn wordt opgenomen in plaats van deels afhankelijk te maken van toekomstige uitvoeringshandelingen?

Antwoord
Het kabinet heeft een voorkeur voor een definitie die aansluit bij de definitie die momenteel nationaal wordt gehanteerd, waarbij er niet per definitie sprake hoeft te zijn van versleuteling van de gegevens. Nederland wil inzetten op een definitie van ransomware waar alle gevallen waarin losgeld gevraagd wordt onder de definitie komen te vallen.

Vragen en opmerkingen van de leden van de BBB-fractie

34. De leden van de BBB-fractie hebben met belangstelling kennisgenomen van de twee belangrijke voorstellen om de digitale weerbaarheid van de Europese Unie te versterken en hebben nog enkele vragen. Allereerst vragen deze leden hoe de minister de waarschuwing van het Adviescollege toetsing regeldruk (ATR) beoordeelt dat de regeldrukeffecten van het uitgebreide toepassingsbereik en de nieuwe richtlijnen van ENISA nog onvoldoende in kaart zijn gebracht.

Antwoord
Een aantal elementen van de voorstellen zijn op dit moment nog onvoldoende uitgewerkt, zoals de precieze invulling van uitvoeringshandelingen, certificeringsschema's en de rol van ENISA in de praktijk. Het kabinet acht het van belang dat besluitvorming over dergelijke voorstellen plaatsvindt op basis van een zo volledig mogelijk beeld van de gevolgen voor bedrijven, overheden en toezichthouders. Daarom zet het kabinet zich ervoor in dat de Europese Commissie de regeldrukeffecten nader onderbouwt en dat deze conform de gebruikelijke methodieken inzichtelijk worden gemaakt.

35. Verder lezen zij dat het kabinet aangeeft dat de voorgestelde implementatietermijn van 12 maanden voor de NIS2-wijzigingen niet haalbaar is. Welke concrete stappen onderneemt de minister in Brussel om een realistische termijn van minimaal 18 maanden te bepleiten, zodat ondernemers niet opnieuw in de knel komen door te krappe deadlines?

Antwoord

Om een realistische termijn te bepleiten, zet het kabinet in op meerdere sporen. In de eerste plaats wordt dit standpunt actief ingebracht in de onderhandelingen in de Raad, waarbij Nederland onder meer het belang van uitvoerbaarheid voor bedrijven, overheden en toezichthouders expliciet onder de aandacht brengt. Daarbij wordt onderbouwd dat een te korte implementatietermijn bijvoorbeeld kan leiden tot onduidelijkheid, verhoogde regeldruk en risico's voor de naleving. Het kabinet benadrukt in de onderhandelingen dat een zorgvuldige implementatie bijdraagt aan een effectievere cyberweerbaarheid, en dat snelheid niet ten koste mag gaan van kwaliteit en uitvoerbaarheid. Tot slot zoekt het kabinet actief samenwerking met andere lidstaten die vergelijkbare zorgen hebben, om gezamenlijk te pleiten voor een langere en realistischere termijn.

36. Tot slot vragen de leden van de BBB-fractie: waarom ondersteunt de minister de uitbreiding van het register bij ENISA naar alle essentiële en belangrijke entiteiten, terwijl het kabinet zelf toegeeft dat de noodzaak hiervan ongeclausuleerd en onvoldoende onderbouwd is?

Antwoord

Het kabinet zet kritische kanttekeningen bij de voorgestelde uitbreiding van het register bij ENISA met gegevens over alle essentiële entiteiten en belangrijke entiteiten, onder meer omdat in het desbetreffende voorgestelde artikel niet expliciet wordt gemaakt voor welke taken die uitbreiding van de registratie nodig is. Deze uitbreiding lijkt vooralsnog verder te gaan dan noodzakelijk is voor het bereiken van het doel van het voorstel, met name ook omdat het voorstel niet duidelijk is gekoppeld aan specifieke taken van het agentschap, de uitbreiding daarmee

ongeclausuleerd is, en het gelet hierop niet duidelijk is waarom deze uitbreiding noodzakelijk is. Het kabinet zal daarom tijdens de onderhandelingen eerst vragen om een nadere onderbouwing van het voorstel, in het bijzonder ook op bovengenoemde punten, om te kunnen beoordelen of de voorgestelde uitbreiding van het register geacht moet worden al dan niet noodzakelijk te zijn.