2026D15953

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de Minister van Justitie en Veiligheid inzake «Fiches Simplificatie NIS2-richtlijn (Kamerstuk 22 112, nr. 4284) en Herziening Cybersecurity Act (Kamerstuk 22 112, nr. 4286)».

De voorzitter van de commissie,
Dekker

Adjunct-griffier van de commissie,
Muller

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de D66-fractie

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 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?

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.

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 in de praktijk uitwerken.

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.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Fiches Simplificatie NIS2-richtlijn (Kamerstuk 22 112-4284) en Herziening Cybersecurity Act (Kamerstuk 22 112-4286) (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?

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?

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?

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?

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

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. 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?

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?

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?

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?

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?

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?

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?

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?

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?

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.

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?[1] Is het weren van producten en diensten bij entiteiten onder de CSA2 nog een nationale bevoegdheid? Hoe ziet het kabinet dit voor zich?

[1] Er zijn twee amendementen ingediend door het lid Kathmann die deze bevoegdheid naar de wet overhevelen [Kamerstukken 36 764-25 en 36 765-13].

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?

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?

Vragen en opmerkingen van de leden van de CDA-fractie

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 risicogebaseerd, 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.

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?

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 onderlig-

gende 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.

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.

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?

Vragen en opmerkingen van de leden van de JA21-fractie

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?

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?

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?

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?

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?

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?

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?

Vragen en opmerkingen van de leden van de BBB-fractie

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.

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?

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?

II Antwoord/reactie van de bewindspersoon