36 875 Uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid)

Nr. 6 NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 23 april 2026

Hoofdstuk I Algemeen

1. Inleiding

De leden van de D66-fractie hebben met interesse kennisgenomen van de Uitvoeringswet verordening cyberweerbaarheid. Deze leden steunen de inzet om cyberbeveiligingsvereisten aan te scherpen. Zij achten dit noodzakelijk voor de weerbaarheid van Nederland en Europa, mede gelet op de potentiële kostenbesparingen van €180 tot €290 miljard per jaar als gevolg van minder cyberincidenten. De leden van de D66-fractie hebben enkele vragen over de praktische werking van de wet en de samenhang met andere Europese wetgeving.
De leden van de GroenLinks-PvdA-fractie hebben met interesse kennisgenomen van de uitvoeringswet. Deze leden onderstrepen het belang van het wetsvoorstel: in een steeds verder digitaliserende wereld is het van belang dat de veiligheidseisen die worden gesteld aan digitale producten en diensten worden geharmoniseerd. Zij hebben wel een paar vragen over deze uitvoeringswet.
De leden van de VVD-fractie hebben met interesse kennisgenomen van het wetsvoorstel en hebben hierover enkele vragen.
De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en hebben geen verdere vragen.
De leden van de BBB-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en hebben hierover enkele vragen.

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van het onderhavige wetsvoorstel. Deze leden hebben een aantal vragen.

Met belangstelling heb ik kennisgenomen van de vragen van de leden van de vaste commissie voor Digitale Zaken over het wetsvoorstel Uitvoeringswet verordening cyberweerbaarheid (Kamerstukken 36 875, hierna: het wetsvoorstel). Hieronder ga ik graag in op de vragen en opmerkingen van de leden van de fracties van D66, GroenLinks-PvdA, de VVD, het CDA, de BBB en de ChristenUnie. Daarbij volg ik de inhoudsopgave van het verslag waarbij in een aantal gevallen naar antwoorden op samenhangende vragen wordt verwezen.

Zij zien allereerst dat deze wet gericht is op de veiligheid van producten en daarmee een plek inneemt in het bredere beleid over cyberveiligheid en -weerbaarheid, zoals beleid gericht op het afbouwen of voorkomen van ongewenste strategische afhankelijkheden. De leden van de ChristenUnie-fractie vragen of de regering een overzicht wil geven van (toekomende) EU-wetgeving op het gebied van cyberveiligheid en -weerbaarheid, welke eventuele lacunes de regering nog ziet, en wat de inzet van de regering is (zowel in EU-verband als eventueel op nationaal niveau).

Wat cybersecurity betreft bestrijkt het regelgevend kader verschillende niveaus van het Europese cybersecurityecosysteem, en zowel de interne cybersecurityhuishouding van kritieke en belangrijke entiteiten als de producten die op de interne markt worden aangeboden. De Cyber Resilience Act (CRA) completeert het Europese raamwerk voor cybersecuritywetgeving. De CRA vervangt en verbreedt de eisen in de Radioapparatuurrichtlijn. Door de veiligheid van producten te reguleren, vormt de CRA een aanvulling op de netwerk- en informatiebeveiligingsrichtlijn die cybersecurity van belangrijke en kritieke entiteiten reguleert. Daarnaast is er de Cybersecurity Act. Daarmee wordt onder meer certificering voor cybersecurity en veiligheid van ICT-toeleveringsketens geregeld. De Europese Commissie heeft recentelijk een voorstel uitgebracht ter herziening van deze verordening. Het kabinet onderschrijft nut en noodzaak van deze regels, maar ziet geen reden om nog aanvullende wetgeving te introduceren. In plaats daarvan zou de focus de komende jaren moeten liggen op de uitvoering en op het

bezien waar regelgeving efficiënter gemaakt kan worden om zo de administratieve druk voor bedrijven te verlichten.

2. De hoofdlijnen van de Verordening cyberweerbaarheid

De leden van de D66-fractie onderschrijven het uitgangspunt dat cyberveiligheid gedurende de gehele levenscyclus van een product moet worden geborgd. Deze leden vragen de regering hoe in de praktijk toezicht wordt gehouden op de naleving van ex-post verplichtingen, zoals het tijdig uitbrengen van beveiligingsupdates en het adequaat omgaan met kwetsbaarheden.

Fabrikanten stellen – alvorens een product met digitale elementen in de handel te brengen – technische documentatie op waarin zij aangeven hoe zij aan de essentiële cyberbeveiligingseisen die de CRA voorschrijft, voldoen. Daarnaast schrijft de CRA voor dat fabrikanten beleid invoeren en handhaven ten aanzien van openbaarmaking van kwetsbaarheden.
De Rijksinspectie Digitale Infrastructuur (RDI) is de toezichthouder in Nederland die erop toeziet dat digitale verbindingen, apparaten en informatiesystemen veilig en betrouwbaar zijn. De RDI houdt toezicht op de naleving van wet- en regelgeving op het gebied van telecommunicatie, cyberveiligheid en de veiligheid van apparatuur. De RDI wordt in het wetsvoorstel aangewezen als toezichthouder op de CRA. De ex-post verplichtingen onder de CRA zien met name op het adequaat omgaan met kwetsbaarheden en incidenten nadat een product in de handel is gebracht. Het toezicht hierop zal risicogestuurd en informatiegedreven worden ingericht. De RDI zal steekproefsgewijs en signaalgestuurd toezicht houden. Signaalgestuurd toezicht is toezicht naar aanleiding van meldingen van kwetsbaarheden (bijv. via CSIRT's), signalen uit de markt, berichtgeving in media, informatie van andere toezichthouders binnen de EU, klachten van gebruikers of zakelijke afnemers die onder andere binnenkomen via een (overheids)meldpunt.

De leden van de GroenLinks-PvdA-fractie lezen dat fabrikanten moeten zorgen dat gedurende de gehele levensduur van een product met digitale elementen het

product van veiligheidsupdates wordt voorzien om kwetsbaarheden in het product aan te pakken. Deze leden maken zich echter zorgen dat fabrikanten van dergelijke producten zullen proberen te claimen dat de levenscyclus van een product korter is dan de periode dat een dergelijk product daadwerkelijk functioneert. Zij denken hierbij bijvoorbeeld aan 'smart' koelkasten, waarbij deze leden zich kunnen voorstellen dat fabrikanten zullen stellen dat deze een verwachte levenscyclus van vijf jaar zullen hebben. Dit terwijl een reguliere koelkast, zonder smart functionaliteiten, vaak een levenscyclus van zeker 15 jaar heeft. Kan de regering aangeven hoe zij van plan is om dit probleem te voorkomen, dan wel aan te pakken? De leden van de GroenLinks-PvdA-fractie zijn van mening dat als een reguliere koelkast een levenscyclus van 15 jaar heeft, de smart-versie van een koelkast eveneens een levenscyclus van 15 jaar moet hebben. Deze leden pleiten bij de regering om alles op alles te zetten om zogenoemde 'planned digital obsolescence' (waarmee functionerende apparaten in 'e-waste' kunnen veranderen), nationaal dan wel in Europees verband tegen te gaan.

Fabrikanten zijn onder de CRA verplicht om de ondersteuningsperiode zo vast te stellen dat deze de verwachte gebruiksduur weerspiegelt. Daarbij moet rekening worden gehouden met: redelijke verwachtingen van de gebruikers, de aard van het product (inclusief het beoogde doel van het product) en EU-wetgeving die de minimale levensduur van producten met digitale elementen bepaalt, zoals de ecodesign-richtlijn. Deze schrijft vanuit duurzaamheidsoogpunt een minimale levensduur voor. Andere factoren waar fabrikanten rekening mee kunnen houden zijn: de ondersteuningsperiode van vergelijkbare producten die door andere fabrikanten op de markt worden gebracht, de beschikbaarheid van de operationele omgeving, de ondersteuningsperiode van geïntegreerde componenten en relevante richtsnoeren vanuit de Administratievesamenwerkingsgroep (ADCO, bestaande uit nationale toezichthouders) en de Europese Commissie. Al deze factoren dienen op evenredige manier mee te worden genomen bij het vaststellen van de ondersteuningsperiode.

Fabrikanten dienen de onderbouwing die gebruikt is om de ondersteuningsperiode van een product te bepalen op te nemen in de technische documentatie. RDI zal hier toezicht op houden.

De ADCO kan op grond van de CRA statistieken publiceren over de gemiddelde ondersteuningsperiode die fabrikanten hebben vastgesteld voor producten met digitale elementen. Ook kan zij richtsnoeren verstrekken voor de vaststelling van passende ondersteuningsperioden voor verschillende categorieën van digitale producten. De Commissie kan – wanneer uit de markttoezichtgegevens blijkt dat de ondersteuningsperiode ontoereikend is – met een gedelegeerde handeling de minimale ondersteuningsperiode voor specifieke productcategorieën vaststellen.
Om fabrikanten te bewegen een realistische ondersteuningstermijn te hanteren die de verwachte gebruiksduur weerspiegelt, zijn fabrikanten bovendien verplicht bij de verkoop van het product duidelijk de maand en het jaar te vermelden tot wanneer de ondersteuningstermijn op het product loopt. Dat maakt een product met een langere ondersteuningstermijn tot een aantrekkelijkere keuze voor consumenten.

De leden van de VVD-fractie constateren dat het Adviescollege toetsing regeldruk (ATR) heeft geadviseerd in de memorie van toelichting aandacht te besteden aan de wijze waarop bedrijven ondersteund zullen worden bij het naleven van de verplichtingen die voortvloeien uit voorliggende regelgeving. Hierop is paragraaf 2 in de memorie van toelichting aangevuld. Deze leden lezen daarin het volgende: "De CRA voorziet ook in manieren om bedrijven te ondersteunen bij het naleven van de verplichtingen. Zo zullen lidstaten waar nodig zorgen voor bewustwordingsactiviteiten en trainingen, een speciaal ingericht communicatiekanaal en ondersteuning van test- en conformiteitsbeoordelingsactiviteiten. Daarbij staan de behoeftes van kleine en microbedrijven centraal." Hoe wil de regering deze ondersteuning vormgeven, in het specifiek ook voor start-ups?

Het ministerie van Economische Zaken en Klimaat (EZK) zorgt in samenwerking met de RDI voor het informeren van bedrijven. Dat gebeurt door middel van webinars,

informatiesessies bij beurzen, conferenties en door presentaties te verzorgen bij koepelorganisaties van het bedrijfsleven. Ook is vorig jaar een handzame Gids CRA uitgebracht die de hoofdlijnen van de wet en de daaruit voortvloeiende verplichtingen op een duidelijke en toegankelijke manier uitlegt. Er komt inderdaad een nationaal communicatiekanaal. Over de precieze inrichting hiervan wordt nog nagedacht, maar bedrijven kunnen momenteel al bij EZK terecht met specifieke vragen. Daarnaast worden er door de Europese Commissie verschillende ondersteuningsprojecten speciaal gericht op het MKB opgezet onder het Digital Europe-programma. Zo is er een project waarbij subsidie beschikbaar wordt gesteld voor acties van bedrijven die bijdragen aan CRA-naleving. Andere projecten zien bijvoorbeeld in trainingen of in AI-gestuurde tools om gemakkelijker documentatie voor conformiteitsbeoordeling bijeen te kunnen krijgen.

Daarnaast lezen zij het volgende: "Lidstaten kunnen ook een testomgeving voor regelgeving opzetten ('regulatory sandbox'), waarin voorafgaand aan het op de markt brengen van een product gekeken kan worden naar ontwikkeling, ontwerp, validering en het testen, met het oog op een goede naleving van de regels." Is de regering voornemens gebruik te maken van de mogelijkheid van een 'regulatory sandbox'? Zo ja, hoe wordt dit concreet vormgegeven? Zo nee, waarom niet?

Het kabinet is voornemens om gebruik te maken van de mogelijkheid tot het opzetten van een testomgeving voor regelgeving ('regulatory sandbox'). De RDI gaat dit opzetten als beoogd toezichthouder. Daarbij is het doel dat bedrijven in gesprek kunnen met de toezichthouder over innovatieve producten en hoe die CRA-conform op de markt gezet kunnen worden. Op dit moment wordt nog nagedacht over de precieze invulling van de testomgeving voor regelgeving.

Tot slot lezen de leden van de VVD-fractie dat onder het Digital Europe-programma subsidie beschikbaar wordt gesteld voor ondersteuning bij naleving. Om welk bedrag gaat het en hoe wordt deze subsidie precies ingezet?

Onder het Digital Europe-programma wordt door de Europese Commissie subsidie beschikbaar gesteld via het project SECURE. Het totale voor bedrijven beschikbare subsidiegeld bedraagt € 16,5 miljoen, dat beschikbaar wordt gesteld in verschillende tranches. Onder dit project kunnen

bedrijven subsidie aanvragen voor acties die bijdragen aan het kunnen naleven van de vereisten van de CRA. Bedrijven kunnen per actie tot maximaal € 30.000,- cofinanciering ontvangen.

3. Hoofdlijnen van het wetsvoorstel

De leden van de BBB-fractie lezen dat het wetsvoorstel toezichthouders de bevoegdheid geeft om woningen te betreden zonder toestemming (met machtiging), omdat veel digitale handel vanuit huis plaatsvindt. Voor veel mensen is de grens tussen bedrijfsvoering en privéleven flinterdun, bijvoorbeeld bij zzp'ers zonder extern kantoor. Kan de regering concreet aangeven hoe de Rijksinspectie Digitale Infrastructuur (RDI) denkt effectief toezicht te houden op de digitale veiligheid van software door fysiek een woning binnen te stappen? Is de regering van mening dat het binnentreden van een woning voor een softwarecontrole een disproportionele inbreuk is op het huisrecht, terwijl de wet niet duidelijk maakt welk fysiek bewijs daar aangetroffen zou kunnen worden dat niet via digitale weg of op de markt zelf verkregen kan worden?

De wetgeving op dit punt is Europees geharmoniseerd. Het binnentreden van een woning is een bevoegdheid die een lidstaat op grond van de markttoezichtverordening (Verordening (EU) 2019/1020), verplicht moet toekennen aan een markttoezichtautoriteit om effectief toezicht te bewerkstelligen. Lidstaten mogen hiervan niet op nationaal niveau afwijken. Zodoende wordt deze bevoegdheid, waar dat van toepassing is, toegekend aan de relevante toezichthouder die binnen het domein van de markttoezichtverordening valt, onder meer door middel van de Wet uitvoering markttoezichtverordening.
De RDI mag onder strikte voorwaarden een woning binnentreden. Hier is met name relevant dat de RDI niet zelfstandig kan overgaan tot inzet van deze bevoegdheid: de RDI heeft daarvoor een voorafgaande machtiging van de rechter-commissaris nodig. Bij de beoordeling van het verzoek daartoe wordt de proportionaliteit en de subsidiariteit van het verzoek getoetst. Op deze wijze wordt gewaarborgd dat binnentreding enkel kan plaatsvinden in die gevallen waarin inzet van die bevoegdheid gerechtvaardigd is. De regels voor het binnentreden van een woning zijn verder vastgelegd in de Grondwet en de Algemene wet op het binnentreden (Awbi).

4. Verhouding tot overig EU-recht

De leden van de D66-fractie vragen hoe de regering de samenhang borgt tussen de cyberweerbaarheidsverordening en andere relevante Europese kaders, zoals de NIS2-richtlijn en de AI-verordening. Op welke wijze wordt in de uitvoering voorkomen dat bedrijven worden geconfronteerd met overlappende of tegenstrijdige verplichtingen? Daarnaast vragen deze leden hoe de afstemming tussen toezichthouders in de praktijk vorm krijgt bij samenloop van toezicht.

De verschillende wetgevende kaders op digitaal gebied zijn complementair aan elkaar. De NIS2 regelt de cybersecurity van netwerken en systemen van vitale entiteiten. De CRA regelt de cybersecurity van digitale producten die op de markt worden gebracht. De AI Act regelt de veiligheid en functionaliteit van AI-modellen. De onderlinge samenhang is voor een deel al geborgd in deze richtlijn en verordeningen. Zo geeft de CRA bijvoorbeeld specifieke regels voor het geval van overlap tussen producten die onder het bereik van de CRA vallen en die als AI-systemen met een hoog risico worden aangemerkt op basis van de AI-verordening. In een dergelijk geval moet een product aan de essentiële cybersecurity-eisen van de CRA voldoen, maar wordt het conformiteitsregime van de AI Act gevolgd. Bij de nationale uitvoering van de verschillende verplichtingen wordt getracht om die zo goed mogelijk op elkaar aan te laten sluiten om zo de werklast voor partijen die aan de wetgeving moeten voldoen zoveel mogelijk te verlichten. Zo wordt voor het inrichten van het meldloket waar mogelijk aangesloten bij het meldloket voor de NIS2-richtlijn (implementatie in de Cyberbeveiligingswet), zodat voor alle cybermeldplichten één loket wordt ingericht bij het als coördinator aangewezen CSIRT (in Nederland: het Nationaal Cyber Security Centrum (NCSC)). Met de keuze voor RDI als toezichthouder en aanmeldende autoriteit wordt aangesloten bij de bestaande taken, bevoegdheden en expertise op grond van de radioapparatenrichtlijn (RED), de Cyberbeveiligingsverordening, de NIS2-richtlijn en de AI-verordening. De RDI heeft ook de coördinerende taak

opgepakt om te zorgen voor afstemming tussen de verschillende toezichthouders om samenhang te borgen tussen de verschillende bestaande en toekomstige reguleringen.

5. Regeldruk

De leden van de fractie van de VVD lezen dat de kosten van deze regelgeving voor de EU als geheel kunnen oplopen tot €29 miljard per jaar. Daartegenover staat een verwachte kostenverlaging van €180 tot €290 miljard per jaar door minder incidenten. Waarop is deze schatting gebaseerd?

Dit betreft een schatting van de Europese Commissie op basis van een effectbeoordeling[1]. Daarbij wordt uitgegaan van een verlaging van de kosten als gevolg van een afname van het aantal (succesvolle) cyberaanvallen en de ernst ervan.

De leden van de BBB-fractie lezen dat circa 52.000 fabrikanten gemiddeld €42.700 extra ontwikkelingskosten per product kwijt zijn, bovenop conformiteitskosten. Gezien de brede reikwijdte vrezen deze leden dat kleine ontwikkelaars deze kosten niet kunnen dragen. Heeft de regering in kaart gebracht in hoeverre deze wetgeving leidt tot een verdere marktconcentratie bij enkele grote 'Big Tech'-spelers, omdat kleine, innovatieve familiebedrijven in de techniek de regeldruk simpelweg niet meer kunnen financieren? Dreigt hierdoor niet een situatie waarin innovatieve Nederlandse hardware onbetaalbaar wordt ten opzichte van producten uit derde landen die minder nauwgezet worden gecontroleerd?

De CRA is van toepassing op alle producten die op de Europese markt worden aangeboden, ongeacht of de fabrikant binnen of buiten de EU is gevestigd. De nalevingslasten uit de CRA kunnen in bepaalde gevallen voor kleine bedrijven moeilijker te dragen zijn dan voor grote bedrijven. De CRA probeert daar waar mogelijk rekening mee te houden. Om het midden- en klein bedrijf (MKB) te ondersteunen bevat de CRA diverse ondersteuningsmaatregelen die specifiek gericht zijn op het MKB. Om voor MKB-bedrijven de administratieve lasten te verlichten hebben zij de mogelijkheid om vereenvoudigde

[1] Cyber Resilience Act - Impact assessment | Shaping Europe’s digital future

technische documentatie op te stellen. Daarnaast bepaalt de CRA dat bij het vaststellen van de vergoeding voor de conformiteitsbeoordelingsprocedures rekening dient te worden gehouden met de belangen en behoeften van het MKB en de vergoeding dient te worden verlaagd in verhouding tot de belangen en behoeften. De Europese Commissie verstrekt daarnaast richtsnoeren voor MKB-ondernemingen waarmee naleving kan worden vergemakkelijkt. Daarnaast zal er een testomgeving worden opgezet (‘regulatory sandbox’) waar bedrijven in een gecontroleerde testomgeving in gesprek kunnen met de toezichthouder over hun product en hoe die CRA-conform op de markt gezet kan worden. Ook kan er onder een van de projecten onder het Digital Europe-programma subsidie aangevraagd worden om producten aan de eisen uit de CRA te laten voldoen. Voorts zijn er andere hulpmiddelen die vanuit Digital Europe ontwikkeld worden voor het MKB, zoals trainingen en AI-gestuurde tools voor het bijeenbrengen van documentatie.

6. Advies en consultatie

6.1. Uitvoering- en handhaafbaarheidstoets Rijksinspectie Digitale Infrastructuur en Nationaal Cyber Security Centrum

De leden van de D66-fractie hebben kennisgenomen van de conclusies uit de quick scan van het Nationaal Cyber Security Centrum (NCSC). Deze leden vragen of aan de randvoorwaarden geschetst door het NCSC voldaan gaat worden en of dit naar verwachting ook tijdig lukt, gezien de regering dit niet expliciet benoemd heeft in de memorie van toelichting.

Ik zet mij ervoor in om tijdig aan de voorwaarden – zoals door het NCSC geschetst in de quick scan – te voldoen. Ik ben hier samen met de minister van Justitie en Veiligheid over in gesprek met het NCSC. Op dit moment zijn nog niet alle technische details bekend ten aanzien van de aansluiting op het Europese centrale meldingsplatform. Over deze aansluiting en de technische architectuur komt naar verwachting spoedig meer duidelijkheid vanuit ENISA. In de tussentijd is het NCSC gevraagd om te starten met de voorbereidingen, zodat met de inwerkingtredingsdatum van de meldplicht (11 september 2026) een elektronisch meldloket in bedrijf is.

Voor een precieze inschatting van de kosten is het noodzakelijk om de technische details ten aanzien van de aansluiting op het Europese meldingsplatform te hebben. Daarom heeft het NCSC een schatting (bandbreedte) van de kosten gemaakt. In de opdrachtbrief aan het NCSC zijn de benodigde middelen toegezegd, met daarbij het verzoek om na een half jaar de uitvoeringskosten te evalueren.

Tot slot wijst het NCSC in de quick scan op de afweging wanneer bewustmaking van het publiek 'noodzakelijk' is om een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen te voorkomen of te beperken. Het NCSC is gevraagd om vanuit haar rol als CSIRT dit te beoordelen. Indien noodzakelijk zal de minister van Justitie en Veiligheid met het NCSC bezien of er aanvullend beleid nodig is en hoe dit eruit moet zien.

Daarnaast vragen zij wanneer inzichtelijk wordt wat de structurele personele en financiële gevolgen zijn voor het NCSC, aangezien deze in de memorie van toelichting nog niet expliciet zijn uitgewerkt.

In de 'quick-scan uitvoeringstoets' is door het NCSC aangegeven dat de inrichting van de meldfunctionaliteit incidentele en structurele kosten met zich meebrengt. De incidentele kosten hebben betrekking op het ontwerp en de bouw van de meldfunctionaliteit en zijn afhankelijk van de precieze inrichting en koppeling met het Europese portaal. De structurele kosten hebben betrekking op het beheer van de applicatie en de benodigde capaciteit voor het beoordelen van de meldingen en de opvolging ervan. Omdat op dit moment nog niet alle technische details ten aanzien van de koppeling met het Europese portaal bekend zijn, zijn de precieze (incidentele) kosten voor het bouwen van de meldfunctionaliteit nog niet bekend. Door het NCSC is een schatting gemaakt van de kosten - afhankelijk van de noodzakelijke inrichting en koppeling - tussen de € 220.000 en € 510.000,- incidenteel. Daarnaast zijn de geschatte structurele kosten € 361.000,- voor het beheer van de applicatie en de capaciteit voor het beoordelen van de meldingen en de opvolging daarvan. Ik blijf met het NCSC in gesprek over de meldfunctionaliteit en de uitvoeringskosten.

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting geen expliciete reactie van de regering op de quick scan van het NCSC, bijvoorbeeld over de noodzaak om beleid te formuleren over het moment waarop het publiek moet worden geïnformeerd bij ernstige incidenten. Deze leden vragen de regering hier alsnog een reactie op te geven en uiteen te zetten hoe de regering wil borgen dat de NCSC de toebedeelde taken straks goed kan uitvoeren.

Zie het antwoord op bovenstaande vragen.

6.2. *Advies van de Raad voor de rechtspraak*

De Raad voor de rechtspraak en de RDI constateren overlap met andere Europese regelgeving. De leden van de VVD-fractie behouden daarom zorgen over dubbele regelgeving en hoge regeldrukkosten. Deze leden verzoeken om een duidelijk, schematisch overzicht van bestaande en te verwachten regelgeving die overlap vertoont, inclusief de verantwoordelijke toezichthouder per kader. Aanvullend verzoeken zij om een toelichting hoe naleving zo eenvoudig mogelijk wordt gemaakt voor ondernemers.

De verschillende wetgevende kaders op digitaal gebied zijn complementair aan elkaar. De NIS2 regelt de cybersecurity van netwerken en systemen van vitale entiteiten. De CRA regelt de cybersecurity van digitale producten die op de markt worden gebracht. De Cybersecurity Act regelt certificering voor cybersecurity en veiligheid van ICT-toeleveringsketens. De AI Act regelt de veiligheid en functionaliteit van AI-modellen, en regelt het verantwoord ontwikkelen en gebruiken van AI-modellen door bedrijven, overheden en andere organisaties. De onderlinge samenhang is voor een deel al geborgd in deze richtlijn en verordeningen. Bij de nationale uitvoering van verschillende verplichtingen wordt getracht om die zo goed mogelijk op elkaar aan te laten sluiten om zo de werklast voor entiteiten zoveel mogelijk te beperken. Ook is er voor al deze wetten een en dezelfde toezichthouder, namelijk de RDI.

Om het midden- en klein bedrijf (MKB) te ondersteunen bevat de CRA diverse ondersteuningsmaatregelen die specifiek gericht zijn op het MKB. Om voor MKB-bedrijven de administratieve lasten te verlichten hebben zij de mogelijkheid om vereenvoudigde technische documentatie op te stellen. Daarnaast bepaalt de CRA dat bij het vaststellen van de vergoeding voor de

conformiteitsbeoordelingsprocedures rekening dient te worden gehouden met de belangen en behoeften van het MKB en de vergoeding dient te worden verlaagd in verhouding tot de belangen en behoeften. De Europese Commissie verstrekt daarnaast richtsnoeren voor MKB-ondernemingen waarmee naleving kan worden vergemakkelijkt. Daarnaast zal er een testomgeving worden opgezet (‘regulatory sandbox’) waar bedrijven in een gecontroleerde testomgeving in gesprek kunnen met de toezichthouder over hun product en hoe die CRA-conform op de markt gezet kan worden. Voorts kan er onder een van de projecten onder het Digital Europe-programma subsidie aangevraagd worden om producten aan de eisen uit de CRA te laten voldoen. Ook zijn er andere hulpmiddelen die vanuit Digital Europe ontwikkeld worden voor het MKB, zoals trainingen en AI-gestuurde tools voor het bijeenbrengen van documentatie.

De leden van de ChristenUnie-fractie merken op dat de regering geen expliciete reactie heeft gegeven op het advies van de Raad voor de rechtspraak, waarin aandacht wordt gevraagd voor een aantal praktische en procedurele punten. Kan de regering alsnog expliciet op deze punten ingaan, en daarbij uiteenzetten welke wel en welke niet zijn overgenomen, en waarom?

De Raad voor de rechtspraak geeft in zijn advies aan geen zwaarwegende bezwaren te hebben tegen het wetsvoorstel, maar geeft in overweging om de samenloop met andere Europese regelgeving te verduidelijken. Op basis van dit advies is paragraaf 4 (verhoudingen tot overig EU-recht) van de memorie van toelichting aangevuld.

Hoofdstuk II ARTIKELSGEWIJZE TOELICHTING

Artikel 3.7

De leden van de GroenLinks-PvdA-fractie lezen dat de minister van Economische Zaken de bevoegdheid krijgt tot oplegging van een bestuurlijke boete ter hoogte van het hoogste bedrag, genoemd in artikel 64, tweede tot en met vierde lid, van de Verordening cyberweerbaarheid, ter handhaving van het artikel. Ook wordt de minister bevoegd tot oplegging van een last onder bestuursdwang ter

handhaving. Deze leden kennen meerdere voorbeelden van zeer grote multinationals en tech-unicorns die opereren op basis van een 'move-fast and break stuff' principe, waarbij de kosten van boetes als onderdeel van de bedrijfslast wordt gezien. Zij zijn van mening dat de opgelegde boetebedragen daarom in principe van een zodanige hoogte moeten zijn dat "ingecalculeerde onveiligheid" en daarmee "ingecalculeerde boetebedragen" nooit winstgevend kunnen zijn voor fabrikanten. Deelt de regering deze mening? Is de regering ervan overtuigd dat het opgenomen sanctiekader voldoende afschrikwekkend is om te voorkomen dat bedrijven incalculeren dat ze veel winst maken en de boete op de koop toe nemen omdat deze niet hoog genoeg is? Zo nee, kan de regering zich voorstellen dat er bedrijven zullen zijn die zich niets van deze regelgeving zullen aantrekken? Welke mogelijkheden ziet de regering in dat geval nog meer om bedrijven te dwingen zich aan de wet te houden?

Niet-naleving van de CRA kan resulteren in boetes die kunnen oplopen tot 2,5 procent van de wereldwijde omzet van een fabrikant. Dat is ook voor zeer grote multinationals een sterke prikkel om de CRA na te leven. Bovendien kan niet-naleving resulteren in reputatieschade, zeker omdat de eisen die de CRA stelt aansluiten bij wat vanuit cybersecurity bezien een kwalitatief goed product is. In het geval van voortdurende non-conformiteit kan de nationale markttoezichthouder maatregelen nemen om het op de markt aanbieden van het product te beperken of te verbieden of om het product terug te roepen of uit de handel te nemen. Bovendien kan ook de Europese Commissie een corrigerende of beperkende maatregel op het niveau van de Unie opleggen, bijvoorbeeld het uit de handel nemen of terugroepen van de desbetreffende producten.

OVERIG

De leden van de GroenLinks-PvdA-fractie willen nog een opmerking maken over 'security-by-design'. Volgens de cyberweerbaarheidsverordening (Annex I) moeten producten 'secure by design' zijn en beveiliging bieden tegen ongeautoriseerde toegang. Fabrikanten gebruiken deze eis echter regelmatig als voorwendsel om onafhankelijke reparateurs buiten te sluiten (bijvoorbeeld door het versleutelen van 'bootloaders'). Hoe interpreteert de regering deze eis? Blijven audits en reparaties door derden onder de cyberweerbaarheidsverordening mogelijk? Zo nee, gaat de regering zich ervoor inzetten om dit wel mogelijk te

maken? Deze leden zijn van mening dat de eisen uit de cyberweerbaarheidsverordening de gebruiker beschermt tegen zaken als ransomware en staatsactoren. Volgens deze leden is het niet bedoeld om de fabrikant te beschermen tegen reparateurs. Deelt de regering deze mening?

De CRA erkent expliciet het belang van reparaties van producten, zo blijkt specifiek uit overweging 29. Om producten met digitale elementen doeltreffend te repareren is de CRA niet van toepassing op reserveonderdelen die op de markt worden aangeboden ter vervanging van identieke componenten en die zijn vervaardigd volgens dezelfde specificaties als de componenten die zij beogen te vervangen (artikel 2, lid 6). De eisen uit de CRA kunnen daarmee geen argument zijn om onafhankelijke reparateurs buiten te sluiten. De CRA staat daarbij niet op zichzelf. Fabrikanten worden, onder Ecodesign wetgeving, verplicht om bepaalde producten zo te ontwerpen dat reparatie mogelijk is en om onderdelen en informatie beschikbaar te stellen. De toegang hiertoe geldt niet alleen voor de fabrikant zelf, maar ook voor onafhankelijke reparateurs. Onder een nieuwe Europese richtlijn die per 31 juli 2026 in werking treedt[2] mogen fabrikanten reparaties door onafhankelijke reparateurs niet belemmeren op grond van contractuele, hardware-, software- of andere redenen, zoals eerdere reparaties door een andere partij. Dergelijke beperkingen mogen alleen worden toegepast als deze gerechtvaardigd zijn door legitieme en objectieve factoren, bijvoorbeeld ter bescherming van intellectuele eigendom of veiligheid.

[2] Richtlijn (EU) 2024/1799 betreffende gemeenschappelijke regels ter bevordering van de reparatie van goederen.